

ISPProtect Web Security for Contao

ISPProtect Web Security für Contao: Handbuch

Version 1.0.0

2026-11-23

Inhalt

1. **Einleitung**
   - Was das Bundle leistet
   - Was das Bundle nicht leistet
   - Kostenlose und kostenpflichtige Teile
   - Voraussetzungen
   - Wer es nutzen kann
   - Aufbau dieses Handbuchs
2. **Installation und erste Schritte**
   - Bundle installieren
   - Datenbanktabellen anlegen
   - Assets installieren
   - Die Seiten öffnen
   - Erste Schritte
   - Hinter einem Reverse-Proxy oder CDN
   - Zeitplanung mit Cron
3. **Übersicht**
   - Menüeintrag und Tabs
   - Die Übersichtsseite
   - Wenn die Tabellen fehlen
4. **Firewall**
   - Wie die Firewall entscheidet
   - Firewall-Modi
   - Was ein abgewiesener Besucher sieht
   - Sperren
   - Die eigene Adresse des Administrators
   - Adresslisten
   - Eigene Regeln
   - Fallenpfade und Pfade ohne Anfragegrenze
   - Schutz vor dem Aussperren
   - Wenn die Firewall selbst ausfällt
   - Grenzen der Firewall
   - OWASP-CRS-Regeln
5. **Dateiscanner**
   - Was ein Scan prüft
   - Welche Dateien geprüft werden
   - Einen Scan starten und stoppen
   - Geplante Scans
   - Die Liste der Funde
   - Was Sie mit einem Fund tun können
   - Details eines Funds
   - Bekannte Fehlalarme
   - Sicherheitslücken installierter Pakete
   - Grenzen des Scanners
6. **Remote-Scan und Lizenz**
   - Modi
   - Was den Server verlässt
   - Den lokalen Scan-Dienst verwenden
   - Den eigenen Scan-Dienst verwenden

- Den gehosteten Scan-Dienst mit einer Lizenz verwenden
- Verbindung testen
- Ergebnis des letzten Scans
- Wenn der Dienst ablehnt oder nicht erreichbar ist
- So werden Zugangsdaten gespeichert
- Grenzen des Remote-Scans

7. Anmeldeschutz

- Was gezählt wird
- Einzelheiten
- Was nicht abgedeckt ist
- Der Tab Anmeldeschutz
- Sperre eines Benutzernamens aufheben
- Sperre einer Adresse aufheben
- Gekürzte Adressen im Protokoll

8. Zwei-Faktor-Authentifizierung

- Den zweiten Schritt für Administratoren verlangen
- Was die Einstellung nicht leistet
- Nach dem Verlust eines Geräts

9. Sicherheits-Checkup

- Punktzahl und Status
- Die Prüfungen
- Aufgeführte Dateien und die Korrektur der Rechte
- Sicherheits-Header

10. Ereignisprotokoll und Benachrichtigungen

- Das Ereignisprotokoll
- Benachrichtigungen

11. Einstellungsreferenz

- Einstellungen im Backend ändern
- Einstellungen auf der Konsole ändern
- Werttypen
- Gruppe Firewall
- Gruppe Anfragelimit
- Gruppe Fehlende Seiten
- Gruppe Fallenpfade
- Gruppe Eigene Regeln
- Gruppe Sperren
- Gruppe Anmeldeschutz
- Gruppe Zwei-Faktor-Authentifizierung
- Gruppe Ereignisprotokoll
- Gruppe Benachrichtigungen
- Gruppe Scanner
- Gruppe Remote-Scan
- Gruppe Sicherheits-Header
- Gruppe OWASP-CRS-Regeln

12. Kommandozeile

- Liste der Befehle
- Status und Checkup
- Scan und Funde
- Ereignisprotokoll
- Adressen
- Anmeldesperren

- Einstellungen
- Wartung
- Befehle für den Remote-Scan
- Entfernen

I.3. Zurück ins System und Fehlerbehebung

- Sie sind von der Firewall gesperrt oder blockiert
- Sie sind vom Anmeldeschutz gesperrt
- Ein Fallenpfad oder eine Regel blockiert die falschen Anfragen
- Die Zwei-Faktor-Authentifizierung ist vorgeschrieben und ein Administrator kann sie nicht nutzen
- Die Seiten melden fehlende Tabellen
- Die Seiten des Bundles haben kein Layout
- Alle Besucher haben dieselbe Adresse
- Scans oder E-Mails finden nicht statt
- Der Remote-Scan oder die Lizenz funktioniert nicht
- Etwas anderes
- Die OWASP-CRS-Regeln weisen eine normale Anfrage ab

I.4. Datenschutz und externe Dienste

- Kontakt zu externen Diensten
- Daten in Ihrer Datenbank

I.5. Das Bundle entfernen

- Die Daten löschen
- Den Code entfernen

Einleitung

ISPProtect Web Security ist ein Sicherheits-Bundle für Contao. Sie verwalten es auf Seiten im Contao-Backend und mit Konsolenbefehlen. Die Seiten gibt es auf Englisch und auf Deutsch.

Was das Bundle leistet

- **Anfrage-Firewall.** Sie prüft jede Anfrage, bevor Contao sie weiterleitet. Sie arbeitet mit Adresslisten, Anfragehäufigkeiten, Fallenpfaden und Regeln, die Sie selbst schreiben. Siehe Firewall.
- **Anmeldeschutz.** Er zählt fehlgeschlagene Anmeldungen im Backend und im Frontend, sperrt Adressen und Benutzernamen. Siehe Anmeldeschutz.
- **Zwei-Faktor-Authentifizierung.** Sie kann von Administratoren verlangen, die Zwei-Faktor-Authentifizierung einzurichten, die Contao bereits mitbringt. Siehe Zwei-Faktor-Authentifizierung.
- **Dateiscanner.** Er führt einfache Prüfungen der Dateien Ihrer Installation durch: Änderungen, PHP in Upload-Ordnern, Überreste und wenige allgemeine Prüfungen auf verdächtigen Code. Gründlich ist der Remote-Scan. Er liest Dateien nur. Er löscht, verschiebt, repariert oder isoliert nie eine Datei. Siehe Dateiscanner.
- **Remote-Scan.** Optional prüft ein Scan-Dienst die Code-Dateien anhand ihrer Prüfsummen. Siehe Remote-Scan und Lizenz.
- **Sicherheits-Checkup.** 20 Prüfungen ergeben eine Punktzahl von 0 bis 100. Siehe Sicherheits-Checkup.
- **Ereignisprotokoll und Benachrichtigungen.** Sicherheitsrelevante Ereignisse werden aufgezeichnet, und schwerwiegende Ereignisse erhalten Sie per E-Mail. Siehe Ereignisprotokoll und Benachrichtigungen.
- **Sicherheits-Header.** Drei Antwort-Header können gesetzt oder entfernt werden. Siehe Sicherheits-Header.

Was das Bundle nicht leistet

- Die Firewall hat keine Liste von Angriffsmustern. Sie sucht in Anfragen weder nach SQL-Injection noch nach Cross-Site-Scripting und ist keine Web Application Firewall. Sie entscheidet nach Adresse, Anfragehäufigkeit, Pfad und Ihren eigenen Regeln.
- Der lokale Scanner führt einfache Prüfungen durch und findet Änderungen. Er ist keine Garantie dafür, dass eine Website sauber ist.
- Das Bundle repariert oder entfernt keine infizierten Dateien. Das erledigen Sie selbst.

Kostenlose und kostenpflichtige Teile

Alles im Bundle funktioniert ohne Lizenzschlüssel, mit einer Ausnahme: Der Remote-Scan im Modus **Gehosteter Scan-Dienst (Lizenz)** braucht einen Lizenzschlüssel. Die Modi des Remote-Scans, die einen Scan-Dienst auf Ihrem eigenen Server oder einen Scan-Dienst nutzen, den Sie selbst betreiben, brauchen von diesem Bundle keinen Lizenzschlüssel. Siehe Remote-Scan und Lizenz.

Voraussetzungen

- PHP 8.3 oder neuer
- Contao 5.7 (`contao/core-bundle` ^5.7)
- Die Datenbank, die Contao verwendet

Der Paketname ist `ispprotect/contao-web-security-bundle`. Das Bundle wird unter der Lizenz LGPL-3.0-or-later veröffentlicht.

Wer es nutzen kann

Nur Backend-Benutzer mit der Administratorrolle können die Seiten des Bundles öffnen. Anderen Benutzern wird der Menüeintrag nicht angezeigt, und jede Seite weist sie ab. Jede Änderung auf den Seiten braucht ein gültiges Contao-Anfrage-Token. Fehlt das Token oder ist es abgelaufen, wird nichts geändert, und die Seite fordert Sie auf, sie neu zu laden und es erneut zu versuchen.

Aufbau dieses Handbuchs

- Installation und erste Schritte richtet das Bundle ein.
- Die Kapitel von Übersicht bis Ereignisprotokoll und Benachrichtigungen beschreiben jeweils eine Funktion.
- Einstellungsreferenz listet jede Einstellung auf, Kommandozeile jeden Konsolenbefehl.
- Zurück ins System und Fehlerbehebung hilft, wenn Sie ausgesperrt sind.
- Datenschutz und externe Dienste nennt jeden externen Dienst, den das Bundle kontaktieren kann.
- Das Bundle entfernen beschreibt die Entfernung.

In diesem Handbuch beginnen Konsolenbefehle mit `vendor/bin/contao-console`. Führen Sie sie im Projektverzeichnis Ihrer Contao-Installation aus, mit der PHP-Programmdatei der Website.

Installation und erste Schritte

Bundle installieren

Installieren Sie das Bundle mit Composer:

```
composer require ispprotect/contao-web-security-bundle
```

Sie können es auch mit dem Contao Manager installieren: Suchen Sie nach `ispprotect/contao-web-security-bundle`. Das Bundle registriert sich selbst im Contao Manager, Sie brauchen also keine weitere Konfiguration.

Wenn Sie das Bundle als ZIP-Datei erhalten haben, laden Sie die Datei im Contao Manager auf der Seite „Pakete“ mit „Pakete hochladen“ hoch, bestätigen Sie den Upload mit „Uploads bestätigen“ und installieren Sie es dort. Nur mit Composer legen Sie die Datei in einen Ordner, den `composer.json` als Repository vom Typ `artifact` nennt, und führen dann den Befehl `composer require` von oben aus.

Datenbanktabellen anlegen

Legen Sie die Tabellen des Bundles mit der Contao-Migration an:

```
vendor/bin/contao-console contao:migrate
```

Führen Sie im Contao Manager stattdessen das Datenbank-Update aus. Das Bundle speichert seine Einstellungen, Adresslisten, das Ereignisprotokoll, Scan-Ergebnisse und Zähler in Tabellen, deren Namen mit `ispprotect_` beginnen.

Solange Sie die Migration nicht ausgeführt haben, zeigen die Seiten des Bundles diesen Hinweis: „Die Datenbanktabellen von ISPProtect existieren noch nicht. Führen Sie “contao:migrate” auf der Kommandozeile oder im Contao Manager aus.“ Die Firewall, der Anmeldeschutz und das Ereignisprotokoll tun in dieser Zeit nichts. Sie stören Contao nicht.

Assets installieren

Die Seiten laden ein Stylesheet und ein Skript aus den öffentlichen Assets des Bundles. Die Installationsskripte von Contao führen `assets:install` nach `composer require` aus. Wenn die Seiten ohne Layout erscheinen, führen Sie den Befehl selbst aus:

```
vendor/bin/contao-console assets:install
```

Die Seiten öffnen

Melden Sie sich als Administrator im Backend an. Die Seiten finden Sie unter **System > ISPProtect Web Security**. Andere Benutzer sehen diesen Eintrag nicht. Die Tabs finden Sie in Übersicht.

Erste Schritte

Gehen Sie bei einer neuen Installation diese Schritte in dieser Reihenfolge durch.

1. Öffnen Sie den Tab **Checkup** und arbeiten Sie die Warnungen ab. Die Punktzahl zeigt, wie viele Prüfungen bestehen. Siehe Sicherheits-Checkup.
2. Öffnen Sie den Tab **Scanner** und klicken Sie auf **Scan starten**. Ein Scan liest jede Datei einmal. Der erste vollständige Scan wird zur Basis, dem aufgezeichneten Zustand Ihrer Dateien, mit dem spätere Scans vergleichen. Er meldet keine geänderten oder neuen Dateien, weil es noch nichts zu vergleichen gibt. Sehen Sie sich die Funde zum Dateiinhalt in

diesem ersten Scan an, denn sie hängen nicht von der Basis ab. Siehe Dateiscanner.

3. Prüfen Sie den Firewall-Modus. Der Standard ist **An**: Die Firewall weist Anfragen ab, die gegen eine Regel verstoßen. Wenn Sie zuerst sehen möchten, was sie tun würde, stellen Sie **Firewall-Modus** auf dem Tab **Firewall** auf **Nur protokollieren**. Dann zeichnet sie die Anfragen auf, die sie abweisen würde, und weist keine ab. Sehen Sie sich nach einigen Tagen den Tab **Ereignisse** an. Wenn nur Anfragen erscheinen, die Sie stoppen wollen, stellen Sie den Modus auf **An**. Siehe Firewall.
4. Tragen Sie auf dem Tab **Einstellungen** eine E-Mail-Adresse bei **Adresse für Benachrichtigungen** ein oder prüfen Sie, ob die Administratoradresse von Contao gesetzt ist. Ohne Empfänger wird weder eine Warnung noch eine Zusammenfassung gesendet. Siehe Ereignisprotokoll und Benachrichtigungen.
5. Wenn die Website hinter einem Reverse-Proxy oder einem CDN liegt, setzen Sie `TRUSTED_PROXIES`. Siehe Hinter einem Reverse-Proxy oder CDN.
6. Richten Sie den System-Cron ein. Siehe Zeitplanung mit Cron.

Hinter einem Reverse-Proxy oder CDN

Das Bundle verwendet die Client-Adresse, die Contao sieht. Contao entnimmt sie Headern wie `X-Forwarded-For` nur, wenn die Anfrage von einem vertrauenswürdigen Proxy kommt. Wenn Ihre Website hinter einem Reverse-Proxy, einem Load Balancer oder einem CDN läuft, tragen Sie die Adressen dieser Proxys, und nur diese, in die Umgebungsvariable `TRUSTED_PROXIES` ein. Schreiben Sie sie als kommagetrennte Liste, zum Beispiel in `.env.local`.

Was sonst schiefgeht:

- Fehlt ein Proxy in der Liste, hat jeder Besucher die Adresse des Proxys. Das Anfragelimit, die Sperren und die Anmeldesperren treffen dann alle Besucher gemeinsam: Ein Besucher, der eine Sperre auslöst, sperrt alle.
- Wenn die Liste jedem vertraut (ein Eintrag, der auf `/0` endet, oder `REMOTE_ADDR` auf einer Website mit öffentlichen Besuchern), kann jeder Besucher die Adresse wählen, die die Firewall, der Anmeldeschutz und das Ereignisprotokoll sehen. Dieser Besucher kann Sperren umgehen oder die Adresse eines anderen sperren lassen.

Der Checkup hat dafür eine Prüfung: Sie schlägt fehl, wenn die Liste jeder Adresse vertraut, und warnt, wenn eine Anfrage einen Weiterleitungs-Header trug, obwohl sie nicht von einem vertrauenswürdigen Proxy kam. Auf der Kommandozeile kann er nur die konfigurierte Liste beurteilen.

Zeitplanung mit Cron

Der Scan und die Wartungsarbeiten (Warn-Mails, Entfernen abgelaufener Daten, die Zusammenfassung per E-Mail) laufen nur weiter, wenn der Cron von Contao läuft. Das Bundle registriert einen Job, der jede Minute läuft.

Richten Sie den System-Cron so ein, dass der Befehl von Contao jede Minute läuft:

```
* * * * * /usr/bin/php /path/to/project/vendor/bin/contao-console contao:cron
```

Verwenden Sie die PHP-Programmdatei und den Pfad Ihres Servers. Mit dem System-Cron darf jeder Lauf bis zu 20 Sekunden lang scannen. Eine Datenbanksperre verhindert, dass sich zwei Läufe überschneiden. Ein fehlgeschlagener Schritt wird protokolliert und in der nächsten Minute erneut versucht.

Ohne System-Cron führt Contao seinen Zeitplaner nach Seitenaufrufen aus (Web-Cron). Das funktioniert, aber ein Lauf darf nur 5 Sekunden lang scannen, und es läuft nichts, solange niemand die Website besucht. Ein Scan kommt dann nur in kurzen Abschnitten voran und dauert viel länger. Verwenden Sie den System-Cron.

Dieselbe Arbeit können Sie von Hand mit `ispprotect:maintenance` ausführen, oder einen Scan auf der Konsole mit `ispprotect:scan`. Siehe Kommandozeile.

Übersicht

Menüeintrag und Tabs

Das Bundle fügt den Eintrag **ISPProtect Web Security** zum Menü **System** des Contao-Backends hinzu. Nur Administratoren sehen ihn. Die Seiten liegen unter `/contao/ispprotect`, mit Ihrem konfigurierten Backend-Präfix. Sie haben neun Tabs:

Tab	Was er zeigt
Übersicht	Den Zustand auf einen Blick.
Firewall	Adresslisten, Sperren und die Firewall-Einstellungen. Siehe Firewall.
OWASP-CRS-Regeln	Die OWASP-CRS-Regeln installieren, aktualisieren und entfernen, eine Regel abschalten und die CRS-Einstellungen. Siehe OWASP-CRS-Regeln.
Anmeldeschutz	Sperren, Anmeldeereignisse und die Anmeldeeinstellungen. Siehe Anmeldeschutz.
Scanner	Einen Scan starten und stoppen, die Funde, den Bereich Remote-Scan. Siehe Dateiscanner.
Ereignisse	Das Ereignisprotokoll mit Filtern. Siehe Ereignisprotokoll und Benachrichtigungen.
Checkup	Alle Ergebnisse der Prüfungen. Siehe Sicherheits-Checkup.
Einstellungen	Allgemeine Einstellungen: Sicherheits-Header, Ereignisprotokoll, Benachrichtigungen, Scanner und Remote-Scan.
Handbuch	Dieses Handbuch, mit einem Link zum Herunterladen als PDF.

Jede Einstellungsgruppe hat ihren eigenen Platz:

Tab	Einstellungsgruppen
Firewall	Firewall, Anfragelimit, Fehlende Seiten, Fallenpfade, Eigene Regeln, Sperren
OWASP-CRS-Regeln	OWASP-CRS-Regeln
Anmeldeschutz	Anmeldeschutz, Zwei-Faktor-Authentifizierung
Einstellungen	Sicherheits-Header, Ereignisprotokoll, Benachrichtigungen, Scanner, Remote-Scan

Die Gruppen sind mit allen ihren Einstellungen in der Einstellungsreferenz aufgeführt. Jede Gruppe hat unter dem Formular eine Schaltfläche **Gruppe „%group%“ zurücksetzen** (statt %group% steht der Name der Gruppe), die die Gruppe nach Ihrer Bestätigung auf ihre Standardwerte zurücksetzt. Die Werte, die Sie im Formular darüber eingegeben haben, werden dadurch nicht gespeichert.

Die Übersichtsseite

Die Übersicht zeigt:

- **Sicherheits-Checkup**: die Punktzahl und die wichtigsten Ergebnisse. Der Link **Alle Ergebnisse** führt zum Tab **Checkup**. Wenn nichts Aufmerksamkeit braucht, steht dort „Keine offenen Probleme.“
- **Firewall**: den Firewall-Modus und einen Hinweis, wenn der Modus **Aus** ist („Die Firewall ist ausgeschaltet. Anfragen werden weder geprüft noch abgewiesen.“) oder **Nur protokollieren** („Die Firewall protokolliert nur. Anfragen, die eine Regel verletzen, werden noch nicht abgewiesen.“).
- **Aktive Sperren**: wie viele Sperren aktiv sind.
- **Offene Scan-Funde**: die offenen Funde nach Stufe.
- **Letzter Scan**: wann der letzte Scan beendet wurde, oder „Es wurde noch kein Scan abgeschlossen.“ Eine Schaltfläche **Scan starten** startet einen.
- **Ereignisse**: die Anzahl der Ereignisse in den letzten 24 Stunden und den letzten 7 Tagen sowie die neuesten Ereignisse.

Wenn die Tabellen fehlen

Bevor Sie `contao:migrate` ausführen, zeigen die Seiten einen Hinweis auf die fehlenden Tabellen. Siehe Installation und erste Schritte.

Firewall

Die Firewall prüft jede Anfrage, bevor Contao sie weiterleitet, eine Sitzung startet oder eine Seite lädt. Die Einstellungen finden Sie auf dem Tab **Firewall**, aufgelistet sind sie in der Einstellungsreferenz.

Wie die Firewall entscheidet

Die Firewall entscheidet in dieser Reihenfolge:

1. Modus **Aus**: Die Anfrage kommt durch.
2. Eine Adresse auf der Liste der erlaubten Adressen: Die Anfrage kommt durch.
3. Eine Adresse auf der Liste der gesperrten Adressen oder auf der Liste der Sperren: Die Anfrage wird mit dem Status 403 abgewiesen.
4. Eine Anfrage an einen Fallenpfad: Die Adresse wird gesperrt, und die Anfrage wird mit dem Status 403 abgewiesen.
5. Ihre eigenen Regeln, in der angegebenen Reihenfolge. Die erste passende Regel mit der Aktion `block` weist die Anfrage mit dem Status 403 ab. Eine Regel mit der Aktion `log` zeichnet die Anfrage nur auf.
6. Das Anfragelimit: Eine Adresse, die im Zeitfenster mehr Anfragen sendet als erlaubt, erhält den Status 429. Die Anmeldepfade des Backends (`/contao/login` und `/contao/login-link`, mit Ihrem konfigurierten Backend-Präfix) haben ein eigenes, strengeres Limit. Nach der Zahl von Abweisungen, die bei **Sperren nach Abweisungen** innerhalb von 10 Minuten eingestellt ist, wird die Adresse gesperrt.

Nach der Antwort zählt die Firewall die Antworten „nicht gefunden“ (Status 404) pro Adresse. Eine Adresse, die im Zeitfenster zu viele davon auslöst, wird gesperrt.

Die Firewall selbst arbeitet mit Adressen, Anfragehäufigkeiten, Pfaden und den Regeln, die Sie selbst schreiben. Die Suche nach Angriffsmustern wie SQL-Injection oder Cross-Site-Scripting ist ein eigener Teil, die OWASP-CRS-Regeln. Siehe OWASP-CRS-Regeln.

Firewall-Modi

Die Einstellung **Firewall-Modus** hat drei Werte:

Wert	Bedeutung
An	Anfragen, die gegen eine Regel verstoßen, werden abgewiesen. Das ist der Standard.
Nur protokollieren	Die Firewall entscheidet und zeichnet auf, weist aber nie ab. Verwenden Sie diesen Modus, um zu sehen, was die Firewall tun würde.
Aus	Die Firewall tut nichts.

Was ein abgewiesener Besucher sieht

Eine abgewiesene Anfrage erhält eine kleine Seite ohne externe Ressourcen, auf Englisch oder Deutsch. Die Antwort ist mit `no-store` markiert und trägt einen Header `Retry-After`.

Sperren

Eine Sperre ist ein Block einer Adresse, der nach einiger Zeit endet. Die erste Sperre einer Adresse dauert so viele Minuten, wie **Sperrdauer (Minuten)** angibt. Jede wiederholte Sperre derselben Adresse innerhalb von 30 Tagen dauert viermal so lang, höchstens so lange wie **Längste Sperre (Minuten)**.

- IPv6-Adressen werden pro /64-Bereich gezählt und gesperrt.
- Loopback-Adressen (zum Beispiel 127.0.0.1) können nicht blockiert oder gesperrt werden.
- Die Anfragezähler liegen im Cache-Pool des Bundles. Sie sind ungenau, wenn viele Anfragen gleichzeitig eintreffen.

- Anfragen an `/_fragment`, `/_wdt` und `/_profiler` werden vom Anfragelimit nicht gezählt. Weitere Pfade können Sie bei **Pfade ohne Anfragegrenze** hinzufügen.

Die eigene Adresse des Administrators

Wenn sich ein Administrator anmeldet, ist diese Adresse (bei IPv6: ihr /64-Bereich) 24 Stunden lang geschützt, solange **Adressen von Administratoren schützen** eingeschaltet ist. Eine geschützte Adresse überspringt nur die automatischen Maßnahmen:

- Sperren gelten für sie nicht, auch nicht solche, die vor Beginn des Schutzes entstanden sind.
- Sie wird nicht gegen die Fallenpfade, das Anfragelimit und die Zählung der Antworten „nicht gefunden“ geprüft.

Die Liste der gesperrten Adressen und Ihre eigenen Regeln gelten für sie wie für jede andere Adresse. Nur die Liste der erlaubten Adressen lässt eine Adresse jeden Schritt überspringen. Zu viele fehlgeschlagene Anmeldungen von einer geschützten Adresse sperren die Anmeldung von dort trotzdem für eine Weile. Siehe Anmeldeschutz.

Wenn Sie **Adressen von Administratoren schützen** ausschalten, warnt Sie die Seite, dass Ihre Adresse wie jede andere gesperrt werden kann und dass Sie sich dadurch aus dem Backend aussperren können.

Adresslisten

Die Seite zeigt „Ihre Adresse aus Sicht dieses Servers“. Prüfen Sie diese Adresse zuerst, wenn die Website hinter einem Proxy liegt: Wenn es nicht Ihre eigene Adresse ist, siehe Hinter einem Reverse-Proxy oder CDN.

Die **Adressliste** zeigt jeden Eintrag mit seiner Art (**Erlaubt**, **Gesperrt** oder **Automatisch gesperrt**), der Adresse oder dem Bereich, der Quelle, dem Grund, der Erstellungszeit und der Endzeit. Die Quelle sagt, woher der Eintrag stammt: **Manuell**, **Anmeldeschutz**, **Anfragelimit**, **Fehlende Seiten**, **Fallenpfad** oder **Regel**. Ein Eintrag Ihrer eigenen Adresse ist mit „(Ihre Adresse)“ markiert.

Unter **Eintrag hinzufügen** fügen Sie eine Adresse oder einen Bereich hinzu, zum Beispiel `203.0.113.7` oder `203.0.113.0/24`:

1. Wählen Sie die Art: **Erlaubt** oder **Gesperrt**. Sperren legt die Firewall selbst an. Eine Sperre können Sie auf der Konsole mit `ispprotect:ip:add` hinzufügen.
2. Geben Sie die Adresse oder den Bereich ein.
3. Geben Sie optional eine Lebensdauer in Minuten ein. Ohne Lebensdauer hat der Eintrag kein Ende. Die längste Lebensdauer ist 5256000 Minuten.
4. Geben Sie optional einen Grund ein, bis zu 190 Zeichen.
5. Klicken Sie auf **Hinzufügen**.

Wenn der Eintrag Ihre eigene Adresse sperren würde, weist die Seite ihn ab, bis Sie das Häkchen setzen bei „Mir ist bewusst, dass dieser Bereich meine eigene Adresse enthalten und mich aussperren kann.“ Ein gesperrter Bereich darf die lokale Loopback-Adresse nicht enthalten.

Die Schaltfläche **Entfernen** löscht einen Eintrag der Art Erlaubt oder Gesperrt. Die Schaltfläche **Sperre aufheben** beendet eine Sperre. Änderungen an den Listen werden im Ereignisprotokoll aufgezeichnet.

Eigene Regeln

Eine eigene Regel prüft einen Teil der Anfrage mit einem Vergleich und weist dann ab oder protokolliert.

Teil	Bedeutung
`path`	Der Pfad der Anfrage
`query`	Die Query-Zeichenfolge
`user_agent`	Die Browserkennung

Teil	Bedeutung
`referer`	Die Herkunftsseite
`method`	Die HTTP-Methode
`host`	Der Hostname

Die Vergleiche sind `equals`, `prefix`, `suffix`, `contains` und `regex`. Ein regulärer Ausdruck wird ohne Begrenzer geschrieben und ohne Beachtung der Groß- und Kleinschreibung verglichen. Ein Regelwert darf nicht leer sein und höchstens 500 Bytes lang sein. Sie können bis zu 100 Regeln festlegen.

Auf der Seite enthält das Feld **Eigene Regeln** die Regeln als JSON-Liste. Auf der Konsole enthält `rules.custom` dieselbe Liste. Jede Regel hat diese Schlüssel:

Schlüssel	Bedeutung
`id`	Optional. Buchstaben, Ziffern, `-` und `_`, bis zu 32 Zeichen. Ohne ID legt das Bundle eine an
`field`	Einer der Teile in der Tabelle oben
`op`	Einer der Vergleiche oben
`value`	Der Text, mit dem verglichen wird
`action`	`block` oder `log`
`enabled`	Optional. `true`, um die Regel zu verwenden (der Standard), `false`, um sie auszuschalten

Beispiel:

```
vendor/bin/contao-console ispprotect:settings:set rules.custom '[{"id":"no-env","field":"path","op":"suffix","v
alue":".env","action":"block","enabled":true}]'
```

Fallenpfade und Pfade ohne Anfragegrenze

Fallenpfade und **Pfade ohne Anfragegrenze** sind Listen von Pfaden, einer pro Zeile. Die Einträge werden in Kleinschreibung verglichen. Ein Eintrag trifft den ganzen Pfad oder den Anfang des Pfades, wenn er auf `*` endet: `/backup/*` trifft `/backup` und `/backup/x`, aber nicht `/backups`. Ein Eintrag, der die ganze Website umfassen würde, wird abgewiesen.

Schutz vor dem Aussperren

Damit sich niemand aus dem Backend aussperrt:

- Ein Fallenpfad, der das Backend (`/contao`, mit Ihrem Backend-Präfix) oder seine Anmeldepfade trifft, wird beim Speichern abgewiesen. Das gilt auf den Seiten und für `ispprotect:settings:set`.
- Eine eingeschaltete eigene Regel mit der Aktion `block`, die eine Anmeldeanfrage trifft, wird auf dieselbe Weise abgewiesen. Eine Anmeldeanfrage ist hier einer der beiden Anmeldepfade, mit `GET` oder `POST`, ohne Query-Zeichenfolge, auf dem Host der Website (die Domain der ersten veröffentlichten Website-Startseite, sonst der konfigurierte Router-Host). Geprüft werden also Regeln für `path`, `query`, `method` und `host`. Eine Regel für `host` wird nicht geprüft, solange der Host der Website unbekannt ist, und bei mehreren Website-Startseiten wird nur diese eine Domain geprüft. Regeln für `user_agent` und `referer` hängen vom Besucher ab und werden nicht abgewiesen.
- Nach dem Speichern auf dem Tab **Firewall** warnt die Seite, wenn eine eingeschaltete Regel mit Abweisung Ihre eigene Anmeldeanfrage trifft (Ihre Adresse und Ihr Browser, der Host, den Sie verwenden, und der Host der Website).

Die Prüfung läuft, wenn eine Einstellung gespeichert wird. Wenn Sie das Backend-Präfix (`contao.backend.route_prefix`) später ändern, werden gespeicherte Einträge erst beim nächsten Speichern erneut geprüft. Wenn Sie trotzdem ausgesperrt sind, siehe Zurück ins System und Fehlerbehebung.

Wenn die Firewall selbst ausfällt

Wenn die Datenbank oder der Cache ausfällt, lässt die Firewall die Anfrage durch und protokolliert das Problem, höchstens einmal in fünf Minuten. Sie sperrt wegen eines eigenen Fehlers nicht alle aus.

Grenzen der Firewall

- Eine Seite, die der HTTP-Cache von Contao beantwortet, erreicht den Kernel nicht und damit auch nicht die Firewall. Anfragelimits und Sperren gelten nicht für Cache-Treffer. Um eine Adresse daran zu hindern, zwischengespeicherte Seiten abzurufen, brauchen Sie eine Regel in Ihrem Proxy oder Webserver.
- Der Contao Manager (`contao-manager.phar.php`) ist eine eigene Anwendung. Die Firewall, der Anmeldeschutz und das Ereignisprotokoll decken ihn nicht ab.

OWASP-CRS-Regeln

Das OWASP Core Rule Set (CRS) ist ein weit verbreiteter, offen gepflegter Satz von Regeln, der typische Angriffe auf Webanwendungen erkennt, zum Beispiel SQL-Injection, Cross-Site-Scripting, Versuche, Dateien zu lesen oder Befehle auszuführen, und Anfragen von Scannern und Angriffswerkzeugen. Im Backend haben sie einen eigenen Tab, **OWASP-CRS-Regeln**, zwischen **Firewall** und **Anmeldeschutz**. Die CRS-Regeln sind der Teil der Firewall, der nach Angriffsmustern sucht; das Bundle fügt nur vier eigene Regeln hinzu, für Anfragen, die die CRS-Regeln nicht erkennen (siehe ISPProtect-Regeln). Die Regeln laufen mit einer in PHP geschriebenen Engine des Plugins, ein zusätzliches Programm oder Servermodul ist nicht nötig. Sie sind aus, bis Sie sie installieren.

Der Tab **OWASP-CRS-Regeln** zeigt den Zustand, den Modus, die Version, die SHA-256-Prüfsumme des Downloads, den Zeitpunkt der Installation, die Zahl der Regeln und die ausgelassenen Regeln. Er hat die Schaltflächen **Regeln installieren**, **Regeln aktualisieren**, **Regeln entfernen** und **Lizenztext**, das Formular **Eine Regel abschalten** und die Einstellungen der CRS-Regeln (siehe Einstellungsreferenz).

Die Regeln installieren

1. Öffnen Sie den Tab **OWASP-CRS-Regeln** und klicken Sie auf **Regeln installieren**.
2. Das Plugin lädt eine feste Version der Regeln von GitHub (vom CRS-Projekt, in dieser Version des Plugins 4.25.2) über `https` herunter. Ihr Server braucht ausgehenden `https`-Zugriff auf `github.com` und auf den Download-Host, auf den GitHub weiterleitet, und PHP braucht `allow_url_fopen` und OpenSSL. Das Plugin vergleicht den Download mit einer Prüfsumme (SHA-256), die im Plugin eingebaut ist, und weist alles andere ab. Eine neuere Version der Regeln kommt nur mit einer neueren Version des Plugins; sonst wird nie etwas heruntergeladen oder ausgeführt.
3. Bei der ersten Installation setzt das Plugin den Modus (`waf.mode`) auf **Nur protokollieren**.

Die Seite zeigt danach die Version, die Prüfsumme, den Zeitpunkt der Installation, die Zahl der verwendeten Regeln und die Nummern der nicht unterstützten Regeln (siehe Was die CRS-Regeln nicht abdecken). Nach einem Update des Bundles kann sich die feste Version der Regeln ändern. Nach einem Update des Bundles bringt **Regeln aktualisieren** die Regeln auf die Version, die zum neuen Bundle gehört. **Regeln entfernen** löscht sie wieder. Die Regeln liegen in `var/ispprotect/waf`, außerhalb des öffentlichen Ordners.

Mit dem Protokollieren beginnen

Lassen Sie den Modus zuerst auf **Nur protokollieren**. In diesem Modus wird eine passende Anfrage nur ins Ereignisprotokoll geschrieben und nie abgewiesen. Sehen Sie die Einträge einige Tage an, in denen alle Arten von Seiten und Formularen und die Backend-Seiten benutzt werden, schalten Sie Regeln ab, die normale Anfragen Ihrer Website melden (siehe unten), und stellen Sie den Modus erst dann auf **Blockieren**.

Wert	Wirkung
Aus (`off`)	Anfragen werden nicht mit den CRS-Regeln geprüft. Das ist der Zustand, bis Sie die Regeln installieren.
Nur protokollieren (`log`)	Eine Anfrage, die die Schwelle erreicht, wird als **Anfrage von der Firewall protokolliert** aufgezeichnet und geht durch.

Wert	Wirkung
Blockieren (`block`)	Eine Anfrage, die die Schwelle erreicht, wird mit Status 403 abgewiesen und als **Anfrage von der Firewall abgewiesen** aufgezeichnet.

Die CRS-Prüfung hat einen eigenen Modus (`waf.mode`) und hängt nicht vom Firewall-Modus ab. Sie läuft nach den Adresslisten, Sperren und Limits der Firewall: Eine Anfrage von einer Adresse auf der Erlaubnisliste wird nie mit den CRS-Regeln geprüft. Alle anderen werden geprüft, auch angemeldete Administratoren.

Einen Eintrag lesen

Eine Anfrage, die die Schwelle erreicht hat, steht im Ereignisprotokoll mit dem Ereignis **Anfrage von der Firewall protokolliert** oder **Anfrage von der Firewall abgewiesen**. Die Details enthalten:

- die Nummern und die Meldungen der Regeln, die gepasst haben, zum Beispiel `942190` und den Namen des vermuteten Angriffs,
- zu jeder Regel den Namen des Teils der Anfrage, der gepasst hat (zum Beispiel `ARGS:comment` , `REQUEST_COOKIES:name` oder `REQUEST_URI`), und einen kurzen Auszug des Werts, dessen empfindlicher Teil maskiert ist,
- die Gesamtpunktzahl, die Schwelle, die Paranoia-Stufe, die Methode, den Pfad und die Antwort (nie die Query-Zeichenfolge, die Header oder den Inhalt als solchen).

Eine Anfrage gilt als Angriff, wenn sich die Punktzahlen aller passenden Regeln zur **Anomalie-Schwelle** addieren. Jede Regel gibt je nach Schweregrad Punkte: ein kritischer Treffer 5, ein Fehler 4, eine Warnung 3 und ein Hinweis 2. Bei der Standardschwelle 5 genügt ein kritischer Treffer; bei einem höheren Wert müssen mehrere Regeln passen.

Hat die CRS-Prüfung selbst ein Problem (zum Beispiel sind die kompilierten Regeln nicht lesbar), geht die Anfrage durch und das Ereignis **Problem mit den CRS-Regeln** wird aufgezeichnet, höchstens einmal pro Stunde und Art des Problems.

Eine Regel meldet eine normale Anfrage

Meldet eine Regel Anfragen, die für Ihre Website normal sind (ein Fehlalarm), schalten Sie diese Regel ab:

1. Öffnen Sie den Eintrag im Ereignisprotokoll und notieren Sie Nummer und Meldung der Regel.
2. Tragen Sie auf dem Tab **OWASP-CRS-Regeln** die Nummer im Feld **Regel-ID** des Formulars **Eine Regel abschalten** ein und klicken Sie auf **Regel abschalten**.

Sie können Regelnummern auch von Hand unter **Abgeschaltete Regeln** (`waf.disabled_rules`) eintragen, eine pro Zeile. Eine abgeschaltete Regel läuft für keine Anfrage mehr, auch nicht für die, bei denen sie recht hatte; schalten Sie nur die falsche Regel ab, nicht eine ganze Gruppe. Haben Sie eine Regel versehentlich abgeschaltet, entfernen Sie ihre Nummer aus der Liste.

Paranoia-Stufe und Schwelle

Die **Paranoia-Stufe** (`waf.paranoia` , 1 bis 4, Standard 1) bestimmt, wie viele Regeln laufen. Stufe 1 enthält die Regeln mit sehr wenigen Fehlalarmen und wird für die meisten Websites empfohlen. Jede höhere Stufe fügt strengere Regeln hinzu, die mehr Angriffe finden und auch mehr normale Anfragen melden, vor allem in Formularen mit freiem Text, in Editoren und in Seiteninhalten. Erhöhen Sie die Stufe erst, wenn die Einträge der Stufe davor sauber sind, jeweils um eine Stufe, und beginnen Sie wieder mit dem Protokollieren.

Die **Anomalie-Schwelle** (`waf.threshold` , 1 bis 100, Standard 5) ist die Punktzahl, ab der eine Anfrage als Angriff gilt. Erhöhen Sie sie nur, wenn Sie in Kauf nehmen, dass einzelne Regeltreffer nicht mehr zählen.

Anfragen, die nicht vollständig geprüft werden können

Manche Anfragen lassen sich nicht vollständig prüfen: Der Inhalt ist größer, als die Engine liest, die Anfrage hat mehr Felder, als sie ansieht, der Inhalt ist nicht lesbar oder die Prüfung dauert zu lange. Ein Angreifer könnte so eine Anfrage nutzen, um die Regeln zu umgehen, daher behandelt das Plugin sie standardmäßig wie einen Angriff: Im Modus **Blockieren** wird sie abgewiesen, im Modus **Nur protokollieren** aufgezeichnet. Der Eintrag zeigt eine dieser Nummern:

Nummer	Bedeutung	Antwort bei Abweisung
`200002`	Der Inhalt war nicht lesbar (zum Beispiel ungültiges JSON oder XML).	400
`200004`	Der Inhalt ist ein Formular-Upload ohne abschließende Begrenzung.	400
`200005`	Das Muster einer Regel stieß an die Grenzen von PHP für reguläre Ausdrücke.	403
`200007`	Mehr Felder, Header, Cookies oder Teile, als die Engine prüft (1000).	403
`200100`	Das Zeitlimit der Anfrage war aufgebraucht, bevor alle Regeln liefen.	403
`200101`	Der Inhalt ist größer als die **Geprüfte Größe des Inhalts**.	413
`200102`	Ein Wert ist länger, als die Engine prüft (65536 Bytes).	403

Sie können diese Nummern wie jede andere Regel abschalten. Zwei Einstellungen sind für die beiden häufigen Fälle da:

- **Geprüfte Größe des Inhalts** (`waf.body_limit`, 1024 bis 1048576 Bytes, Standard 131072 = 128 KiB). Eine größere Anfrage kann nicht vollständig geprüft werden. Ein Speichervorgang mit sehr viel Inhalt kann größer sein und wird dann mit Status 413 und der Nummer `200101` beantwortet. Scheitern große Speichervorgänge im Modus **Blockieren**, erhöhen Sie den Wert, zum Beispiel auf 524288, oder lassen Sie solche Anfragen durch (siehe unten).
- **Zeitlimit pro Anfrage** (`waf.time_budget_ms`, 5 bis 10000 Millisekunden, Standard 200). Die Zeit, die die Regeln für eine Anfrage höchstens brauchen dürfen. Eine normale Seite oder ein Speichervorgang braucht 2 bis 10 Millisekunden, das Speichern von 42 KB Inhalt etwa 100 Millisekunden auf dem Server, auf dem gemessen wurde. Eine Anfrage nahe der Inhaltsgrenze kann bei Paranoia-Stufe 2 den Standard erreichen. Brechen Anfragen mit `200100` ab, erhöhen Sie den Wert. Halten Sie ihn so niedrig, wie Ihre Website es erlaubt: Das Limit ist auch das, was ein Angreifer Ihren Server für eine Anfrage aufwenden lassen kann.
- **Programmcode in einem Formularfeld.** Programmcode, der in ein Formularfeld eingefügt wird (eingerückter PHP- oder Python-Code, etwa 20 bis 40 KB), kann das voreingestellte Zeitlimit von 200 Millisekunden aufbrauchen; die Anfrage wird dann im Modus Blockieren mit `200100` abgelehnt. Erhöhen Sie bei einer Website, auf der Programmcode in Formulare eingefügt wird, das Zeitlimit, schalten Sie `200100` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können. Normaler Text, HTML und die Speichervorgänge der Editoren, die die Ausnahmen abdecken, sind nicht betroffen.
- **Grenzen der Muster.** Selten bringt ein langes Feld mit Programmcode das Muster einer CRS-Regel über die Grenzen von PHP für reguläre Ausdrücke, und die Anfrage wird mit `200005` abgelehnt. Die Antworten sind dieselben: Schalten Sie `200005` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können.

Anfragen durchlassen, die nicht vollständig geprüft werden können (`waf.pass_uninspected`, Standard aus) lässt solche Anfragen durch (sie werden trotzdem aufgezeichnet). Große Speichervorgänge funktionieren dann weiter, aber eine präparierte Anfrage, die zu groß oder zu langsam ist, wird nicht mehr vollständig geprüft. Nutzen Sie dies nur, wenn Sie die Limits nicht erhöhen können, oder schalten Sie die einzelne Nummer ab, die das Problem verursacht, zum Beispiel `200100`.

Ein XML-Anfrageinhalt mit einer Entitätsdeklaration oder einem Verweis auf eine externe DTD wird im Modus **Blockieren** auch bei eingeschaltetem **Anfragen durchlassen, die nicht vollständig geprüft werden können** mit `200002` (HTTP 400) abgewiesen. Heruntergeladene CRS-Ausnahmen können weder `200002` noch die Regel `200004` für eine fehlende Multipart-Begrenzung entfernen; beide Nummern lassen sich in den Einstellungen ausdrücklich abschalten.

Ausnahmen für Contao

Das Bundle bringt eigene Ausnahmeregeln in `rules/contao-exclusions.conf` mit. Sie werden vor den CRS-Regeln geladen und haben die Nummern 10000 bis 10999. Jede ist auf einen Pfad oder ein Formular und auf benannte Felder begrenzt, und keine schaltet eine ganze Art von Angriffen ab. Sie beseitigen Fehlalarme, die normale Arbeit in Contao bei den Paranoia-Stufen 1 und 2 ausgelöst hat:

- das Cookie `sf_redirect` des Symfony Web Profilers (nur die Umgebung `dev` liest es),
- das Feld `_target_path` der Anmeldeformulare, solange es reines Base64 enthält,
- die Felder für Rich Text, HTML und Code der Inhaltselemente und die Teasertexte von Artikeln, Nachrichten und Veranstaltungen,
- die Meta-Beschreibung und der Seitentitel in den Seiteneinstellungen,

- die Listen der erlaubten HTML-Tags und Attribute in den Systemeinstellungen,
- das Feld `source` des Quelltext-Editors und des Template-Editors,
- die Textfelder der Seiten von ISPProtect Web Security (Fallenpfade, eigene Regeln, Header-Werte), nur auf ihren Speicherwegen.

Die CRS-Regeln laufen, bevor Contao die Sitzung prüft, daher kann auch eine nicht angemeldete Anfrage diese Formulare nennen. Contao weist so eine Anfrage selbst ab, die übersprungenen Felder werden also nur für angemeldete Backend-Benutzer verarbeitet. Alle anderen Felder, Header und Cookies werden weiter geprüft.

> Der Pfad des Backends ist Ihr Backend-Präfix (`contao.backend.route_prefix`, Standard `/contao`). Das Bundle setzt das Präfix beim Laden in die Datei ein, eine Änderung des Präfixes wird also übernommen. Eine Website in einem Unterverzeichnis (Pfade wie `/sub/contao`) oder ein Präfix, das kein einfacher Pfad ist, erhält keine der Backend-Ausnahmen. Sie sehen dann mehr Einträge, der Schutz ist aber nicht schwächer.

ISPProtect-Regeln

Das Bundle bringt vier eigene Regeln in `rules/ispprotect-contao.conf` mit, mit den Nummern 12000 bis 12999. Sie melden Anfragen, die die CRS-Regeln auf Paranoia-Stufe 1 nicht erkennen. Sie laufen mit den CRS-Regeln, also nur, solange die CRS-Regeln installiert sind und der Modus **Nur protokollieren** oder **Blockieren** ist: nach den CRS-Regeln, vor den Regeln Ihrer eigenen Datei und vor der Entscheidung über die Schwelle. Jeder Treffer zählt als kritisch (5), mit der voreingestellten Schwelle reicht also ein Treffer. Der Tab **OWASP-CRS-Regeln** zeigt in der Zeile **ISPProtect-Regeln in Gebrauch**, wie viele davon laufen.

Regel	Meldet
`12001`	Die Versionsverwaltungsordner von Bazaar (`.bzr/`) und Darcs (`_darcs/`) und die Dateien `CVS/Entries`, `CVS/Root` und `CVS/Repository`. `.git/`, `.svn/`, `.hg/` und `.env` melden die CRS-Regeln selbst.
`12002`	Kopien von PHP- und YAML-Dateien (auch `.phtml`, `.phar`, `.inc`) mit der Endung `.orig` oder `.rej`, einer Zahl (`config.yml.1`) oder einem nummerierten `.bak`, `.old` oder `.save` (`index.php.bak1`) sowie die Emacs-Dateien `#name#` und `.#name`. `.bak`, `.old`, `.save`, `.swp` und `~` melden die CRS-Regeln selbst.
`12200`	Ein PHP-Skript im Upload-Ordner (`contao.upload_path`, voreingestellt `files`), auch `name.php.jpg` und `name.php/mehr`. Das Bundle setzt den Ordner beim Laden in die Regel ein, ein geänderter Upload-Ordner wird also übernommen. Eine Website in einem Unterverzeichnis oder ein Upload-Ordner, der kein einfacher Pfad ist, bekommt keinen Treffer.
`12201`	Die Konfigurationsdatei `localconfig.php` älterer Contao-Versionen und Kopien davon. Contao 5 legt sie außerhalb des öffentlichen Ordners ab, eine Anfrage danach ist also immer eine Suche nach ihren Passwörtern.

Wann die Regeln helfen:

- Die Regeln sehen nur Anfragen, die den Front-Controller von Contao (`public/index.php`) erreichen. Mit der `.htaccess`-Datei von Contao geht eine Anfrage nach einer Datei, die es im öffentlichen Ordner nicht gibt, an Contao, das mit „nicht gefunden“ antwortet. Die Regeln weisen eine solche Anfrage ab und zeichnen sie mit ihrer Nummer auf, so erscheint eine Suche nach liegen gebliebenen Dateien im Protokoll als das, was sie ist. Manche Server beantworten eine fehlende `.php`-Datei selbst (nginx mit `try_files $uri =404`, Apache mit `ProxyPassMatch`); eine solche Anfrage erreicht Contao nie.
- Eine Datei, die es im öffentlichen Ordner gibt, liefert der Webserver ohne Contao aus, und ein vorhandenes PHP-Skript führt PHP ohne Contao aus. Diese Anfragen sehen die Regeln nie und können sie nicht aufhalten, auch keine echte Kopie `index.php.orig` und kein Skript im Upload-Ordner.

Die eigentliche Abhilfe ist die Konfiguration des Webservers und ein aufgeräumter öffentlicher Ordner: Der Server weist Versionsverwaltungsordner und Kopien von Dateien ab und führt im Upload-Ordner kein PHP aus. Die Prüfung **Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner** des Sicherheits-Checkups führt Sicherungen und Debug-Dateien auf, die sie im öffentlichen Ordner findet.

Die Regeln werden wie CRS-Regeln abgeschaltet: eine Regel über ihre Nummer (das Formular **Eine Regel abschalten** oder **Abgeschaltete Regeln** in den Einstellungen), alle vier mit der Zeile `SecRuleRemoveByTag ispprotect` in Ihrer eigenen Regeldatei (siehe unten). Die Tags `ispprotect/source-disclosure` (`12001`, `12002`, `12201`) und `ispprotect/upload-script`

(`12200`) schalten eine Gruppe ab. Ein Update des Bundles kann geänderte Regeln bringen; das Bundle kompiliert die Regeln dann bei der nächsten Anfrage neu.

Eigene CRS-Regeln

Sie können eigene Regeln in SecLang, der Sprache des CRS, in die Datei `var/ispprotect/rules/own.conf` Ihrer Installation schreiben. Das Plugin legt die Datei nie an. Die Seite zeigt, ob sie in Gebrauch ist. Regeln darin:

- brauchen eine Nummer von 11000 bis 11999; eine Regel mit anderer Nummer wird übersprungen,
- laufen nach den CRS-Regeln und vor der Entscheidung über die Schwelle, eine Regel kann also zur Punktzahl beitragen,
- nutzen die Teilmenge von SecLang, die die Engine unterstützt: `SecRule`, `SecAction`, `SecMarker`, `SecRuleRemoveById`, `SecRuleRemoveByTag`, `SecRuleUpdateTargetById` und `SecRuleUpdateTargetByTag` sowie Ketten. Regeln, die etwas anderes brauchen, werden übersprungen und als nicht unterstützt gezählt.

Ein Beispiel, das für ein PHP-Tag in einem Parameter eine kritische Punktzahl addiert:

```
SecRule ARGS "@rx (?i)<\?php" \
    "id:11001,phase:2,block,t:none,t:urlDecodeUni,\
    msg:'PHP open tag in a parameter',severity:'CRITICAL',\
    setvar:'tx.inbound_anomaly_score_pl1=+%{tx.critical_anomaly_score}'"
```

Das Plugin bemerkt eine geänderte Datei bei der nächsten Anfrage und kompiliert die Regeln neu. Lassen sie sich nicht kompilieren, läuft die CRS-Prüfung nicht, Anfragen gehen durch und das Problem wird als **Problem mit den CRS-Regeln** aufgezeichnet.

Was die CRS-Regeln nicht abdecken

- Das Plugin prüft nur Anfragen. Regeln für Antworten (die „Response“-Phasen des CRS) laufen nicht.
- Regeln, die die Bibliothek libinjection brauchen, laufen nicht, weil PHP sie nicht hat: `941100` und `941101` (XSS) sowie `942100` und `942101` (SQL-Injection). Die übrigen CRS-Regeln für diese Angriffe laufen. Die Seite listet die nicht unterstützten Regeln.
- Die Teil-Header eines Formular-Uploads (`MULTIPART_PART_HEADERS`) sind nicht verfügbar, weil PHP den Upload liest, bevor das Plugin ihn sieht. Dateinamen und Größen werden geprüft.
- Die CRS-Prüfung sieht nur die Anfrage an. Sie scannt keine Dateien und ersetzt keine Updates.

Kosten der Prüfung

Bei einer normalen Anfrage kostet die Prüfung 2 bis 10 Millisekunden. Das Speichern von 42 KB Inhalt dauerte etwa 100 Millisekunden. Ab Paranoia-Stufe 2 und bei großem Inhalt dauert die Prüfung länger; das Zeitlimit stoppt sie beim eingestellten Wert. Programmcode in einem Formularfeld (etwa 20 bis 40 KB eingerückter PHP- oder Python-Code) kann das voreingestellte Zeitlimit von 200 Millisekunden aufbrauchen; normaler Text, HTML und die Speichervorgänge der Editoren, die die Ausnahmen abdecken, nicht.

Wenn die CRS-Regeln Sie aussperren

Schalten Sie die CRS-Prüfung auf der Konsole ab:

```
vendor/bin/contao-console ispprotect:settings:set waf.mode off
```

Melden Sie sich danach wieder an, suchen Sie im Ereignisprotokoll die Regel, die das Problem verursacht hat, schalten Sie sie ab und stellen Sie den Modus wieder auf **Nur protokollieren**. Siehe auch Zurück ins System und Fehlerbehebung.

Lizenz und Hinweis

Verwendet das OWASP® Core Rule Set (CRS) 4.25.2, © Trustwave Holdings, Inc. und die Mitwirkenden des OWASP-CRS-Projekts, lizenziert unter der Apache License 2.0. Die Regeln werden direkt vom CRS-Projekt auf GitHub heruntergeladen. OWASP® ist eine eingetragene Marke der OWASP Foundation; ISPProtect ist nicht mit OWASP verbunden und wird nicht von OWASP unterstützt.

Die Seite zeigt denselben Text. Der Lizenztext des CRS ist Teil des Downloads; die Schaltfläche **Lizenztext** zeigt ihn.

Dateiscanner

Der Scanner führt einfache Prüfungen der Dateien Ihrer Installation durch: Änderungen, PHP in Upload-Ordnern, Überreste und wenige allgemeine Prüfungen auf verdächtigen Code. Gründlich ist der Remote-Scan. Er liest Dateien nur. Er löscht, verschiebt, repariert oder isoliert nie eine Datei. Sie arbeiten mit ihm auf dem Tab **Scanner**. Seine Einstellungen stehen in den Gruppen Scanner und Remote-Scan, siehe Einstellungsreferenz.

Was ein Scan prüft

Ein Scan liefert Funde dieser Arten. Die Namen sind die, die in der Spalte **Art** angezeigt werden.

Art	Stufe	Was sie bedeutet
Eine Datei wurde seit dem letzten Scan verändert	Mittel	Eine Code-Datei weicht von der Basis ab.
Eine neue Datei ist aufgetaucht	Mittel	Eine Code-Datei ist nicht in der Basis.
Eine Datei fehlt	Niedrig	Eine Datei der Basis existiert nicht mehr.
Verdächtiger Inhalt in einer Datei	Mittel oder Hoch	Die einfachen Inhaltsprüfungen haben ein verdächtiges Konstrukt gefunden. Sie sind allgemein gehalten und erkennen keine bekannte Schadsoftware (dafür gibt es den Remote-Scan). Sie durchsuchen PHP-Code (auch `.html5` und Twig-Templates sowie einige andere Template-Dateitypen), `.htaccess`-Dateien und Skriptcode.
Eine PHP-Datei in einem Upload-Ordner	Hoch	Eine PHP-Datei im Upload-Verzeichnis oder PHP-Code, der in einer Mediendatei versteckt ist.
Eine Datei, die nicht im öffentlichen Verzeichnis liegen sollte	Mittel	Zum Beispiel Sicherungs- und Debug-Dateien.
Ein installiertes Paket hat eine bekannte Sicherheitslücke	Niedrig, Mittel oder Hoch, je nach Schweregrad des Sicherheitshinweises	Nur wenn **Auf bekannte Sicherheitslücken prüfen** eingeschaltet ist.
Der Scan-Dienst hat Schadcode in einer Datei erkannt	Hoch	Nur mit dem Remote-Scan, siehe Remote-Scan und Lizenz.

Die Basis ist der aufgezeichnete Zustand Ihrer Code-Dateien: Der Scanner speichert einen Hash jeder Datei und vergleicht spätere Scans damit. Dateien von Paketen, die Composer seit dem letzten Scan geändert hat, werden nicht als geändert gemeldet. Der erste vollständige Scan wird zur Basis und meldet keine geänderten, neuen oder entfernten Dateien.

Die Stufen sind **Niedrig**, **Mittel** und **Hoch**.

Welche Dateien geprüft werden

- Das Projektverzeichnis wird gegen die Basis und auf Inhalt geprüft.
- Diese erzeugten Verzeichnisse und das Upload-Verzeichnis werden nur auf Inhalt geprüft: `assets`, `public/assets`, `public/bundles`, `public/share`, `system/cache`, `system/tmp` und `var`. Contao und Composer schreiben sie von selbst neu, ein Vergleich mit der Basis würde also eine Flut von Funden „geändert“ erzeugen.

- Der Scanner überspringt `var/cache`, `var/log`, `var/logs`, `.git`, `node_modules`, symbolische Links und die Pfade unter **Ausgenommene Pfade**.
- Dateien, die größer sind als **Größte geprüfte Datei (KB)**, werden nicht vollständig gelesen.

Einen Scan starten und stoppen

Klicken Sie auf dem Tab **Scanner** auf **Scan starten**. Ein Scan läuft in Abschnitten von höchstens 200 Dateien und speichert nach jedem Abschnitt seine Position, sodass ein unterbrochener Scan dort weitermacht, wo er aufgehört hat. Solange Sie die Seite offen halten, bringt sie den Scan in kurzen Schritten voran und zeigt den Zustand, die Phase, die Zahl der Dateien und Skripte und die Zahl der neuen Funde. Klicken Sie auf **Scan abbrechen**, um ihn zu stoppen.

Ohne JavaScript wird der Fortschritt nicht live angezeigt. Der Scan kommt dann mit dem Contao-Cron-Job voran. Siehe Zeitplanung mit Cron.

Auf der Konsole tut `ispprotect:scan` dasselbe, siehe Kommandozeile.

Geplante Scans

Zeitplan der Dateiprüfung kann **Aus**, **Täglich** oder **Wöchentlich** sein. Ein geplanter Scan startet, wenn die Stunde bei **Uhrzeit der Dateiprüfung** (in UTC) erreicht ist und seit Beginn des aktuellen Tages (täglich) oder in den letzten 7 Tagen (wöchentlich) kein Scan gestartet wurde. Der Cron von Contao treibt den Scan an. Ohne funktionierenden Cron startet kein geplanter Scan.

Die Liste der Funde

Die Liste unter dem Bereich Remote-Scan zeigt die Funde. Sie können sie nach **Status** (**Offen**, **Ignoriert**, **Behoben**), **Mindeststufe**, **Art** und einem Suchtext filtern, mit der Schaltfläche **Filtern**. **Filter zurücksetzen** löscht den Filter. Die Spalten sind **Stufe**, **Art**, **Pfad**, **Signatur**, **Zuerst gesehen** und **Aktion**. Ein Fund, den ein späterer Scan nicht mehr meldet, wird **Behoben**.

Was Sie mit einem Fund tun können

- **Ignorieren** blendet einen Fund aus, bis sich die Datei wieder ändert. **Nicht mehr ignorieren** holt ihn zurück.
- **Akzeptieren** wird für geänderte, neue und entfernte Dateien angeboten. Es macht den aktuellen Zustand der Datei zur neuen Basis. Verwenden Sie es, nachdem Sie die Änderung geprüft haben. Wenn die Datei nach dem Scan geändert wurde oder nicht gelesen werden kann, lehnt das Bundle ab und bittet Sie, erneut zu scannen.
- **Alle akzeptieren** tut das für jede geänderte, neue und entfernte Datei. Der Link über der Liste zeigt, wie viele Funde er umfasst. Eine Bestätigungsseite sagt Ihnen, wie viele offene und ignorierte Funde eingeschlossen sind. Sie müssen das Bestätigungsfeld ankreuzen und auf **Alle akzeptieren** klicken. Wenn sich die Funde in der Zwischenzeit geändert haben, wird nichts akzeptiert, und Sie bestätigen erneut. Dateien, die sich nach dem Scan geändert haben oder nicht lesbar sind, bleiben offen. Dateien werden nie geändert oder gelöscht.

Funde der anderen Arten können nicht akzeptiert werden. Beheben Sie die Ursache und scannen Sie dann erneut, oder ignorieren Sie den Fund.

Schadcode, den der Scan-Dienst meldet, kann nicht als neue Basis akzeptiert werden, daher umfasst **Alle akzeptieren** ihn nicht.

Details eines Funds

Details in der Spalte **Aktion** öffnet die Details eines Funds: Stufe, Art, Pfad, Signatur, Zeile, Status und wann er zuerst und zuletzt gesehen wurde. Unter **Zeilen der Datei** sehen Sie die Datei, wie sie jetzt ist, höchstens 4 Zeilen vor und nach der Zeile des Funds. Die Zeile des Funds ist markiert. Nennt der Fund keine Zeile, werden die ersten Zeilen der Datei gezeigt. Die Seite liest die Datei nur und ändert nichts. Nur Administratoren können sie öffnen.

Statt der Zeilen zeigt die Seite einen Hinweis, wenn:

- die Datei nach dem Scan entfernt oder verschoben wurde,
- die Datei Passwörter oder Schlüssel enthalten kann, zum Beispiel `.env`-Dateien, `.htaccess`, `system/config/localconfig.php`, Schlüsseldateien, Datenbank-Dumps und der Ordner `var`. Das sind die Dateien, die der Remote-Scan nie oder nur geschwärzt sendet, siehe Remote-Scan und Lizenz. Das gilt auch für Sicherungen und Kopien von Editoren solcher Dateien, zum Beispiel `.env.bak` oder `.env.swp`,
- die Datei ein Archiv oder ein Datenbank-Dump ist (zum Beispiel `.sql`, `.sql.gz`, `.zip`, `.tar.gz`) oder der Fund eine Datei ist, die nicht in das öffentliche Verzeichnis gehört (eine Sicherung oder Kopie): ihr Inhalt wird nie angezeigt,
- der Pfad ein symbolischer Link ist, keine reguläre Datei ist, mehr als eine harte Verknüpfung hat oder aus dem Projektverzeichnis hinausführt,
- die Datei größer als 5 MB ist.

Ein Hinweis sagt auch, wenn die Datei nach dem letzten Sehen des Funds geändert wurde, die Zeilen also von dem abweichen können, was der Scan gesehen hat, und wenn eine Zeile nach 500 Zeichen abgeschnitten wurde. Zeichen, die nicht sicher angezeigt werden können (Steuerzeichen, unsichtbare Zeichen und Zeichen, die die Schreibrichtung ändern), erscheinen als `�`.

Bekannte Fehlalarme

Der Scanner kann Dateien bekannter Pakete melden, obwohl sie harmlos sind, zum Beispiel `vendor/league/uri/Uri.php`, `vendor/doctrine/inflector/src/Inflector.php` und `vendor/contao/core-bundle/src/Translation/Translator.php`. Sie können sie ignorieren. Pfade, die Sie nie scannen lassen wollen, tragen Sie bei **Ausgenommene Pfade** ein.

Sicherheitslücken installierter Pakete

Wenn **Auf bekannte Sicherheitslücken prüfen** eingeschaltet ist, fragt der Scanner packagist.org nach bekannten Sicherheitshinweisen zu den installierten Paketen. Nur Paketnamen verlassen den Server; die Versionen werden auf Ihrem Server verglichen. Siehe Datenschutz und externe Dienste.

Grenzen des Scanners

- Der lokale Scanner führt einfache Prüfungen durch und findet Änderungen. Er ist keine Garantie dafür, dass eine Website sauber ist.
- Er repariert oder entfernt nichts.

Remote-Scan und Lizenz

Der Remote-Scan ist optional und standardmäßig aus. Mit ihm fragt der Scanner zusätzlich einen Scan-Dienst nach den Code-Dateien der Website. Der Dienst kennt Prüfsummen von Dateien, die bekanntermaßen harmlos oder schädlich sind, und kann so Schadcode finden, den die lokalen Regeln nicht finden. Alles andere am Scanner funktioniert auch ohne ihn, und ein Scan hängt nie von ihm ab: Wenn der Dienst nicht erreichbar ist, wird der lokale Scan trotzdem abgeschlossen, und der Scan vermerkt, dass der Remote-Teil fehlgeschlagen ist.

Modi

Den Modus wählen Sie mit der Einstellung **Remote-Scan** auf dem Tab **Einstellungen**. Die Verbindung betreuen Sie im Bereich **Remote-Scan** auf dem Tab **Scanner**. Der Modus wird gelesen, wenn ein Scan startet.

Modus	Wo die Dateien geprüft werden	Was Sie brauchen
Aus	Nirgends. Es wird nichts gesendet. Das ist der Standard.	Nichts.
Lokaler Scan-Dienst (Socket)	Ein Scan-Dienst auf demselben Server, erreicht über einen Unix-Socket. Nichts verlässt den Server.	Den Socket-Pfad bei **Socket des lokalen Scan-Dienstes**. Keinen Zugangstoken und keinen Lizenzschlüssel.
Eigener Scan-Dienst	Ein Scan-Dienst, den Sie selbst betreiben, erreicht über HTTPS.	Seine Adresse bei **Adresse des Scan-Dienstes** und seinen Zugangstoken.
Gehosteter Scan-Dienst (Lizenz)	Der gehostete ISPProtect-Scan-Dienst, erreicht über HTTPS. Das ist der einzige kostenpflichtige Teil des Bundles.	Einen Lizenzschlüssel.

Der Standard-Socket ist `/run/ispprotect/scand.sock`. Das Bundle braucht für den lokalen Scan-Dienst einer ISPProtect-Serverlizenz keinen Website-Schlüssel. Nur der gehostete Dienst braucht einen Lizenzschlüssel.

Was den Server verlässt

Für jede nicht leere Code-Datei mit einem UTF-8-Dateinamen sendet das Bundle die SHA-256-Prüfsumme und einen Namenshinweis (den Dateinamen oder nur `file.<extension>`). Es sendet nie einen Dateinamen mit Pfad. Nur Dateien, die der Dienst nicht kennt, werden hochgeladen, und nur innerhalb der Grenze **Upload-Grenze je Scan (MB)** eines Scans und der Grenzen des Dienstes. Mit dem Wert `0` werden nur Prüfsummen gesendet. Dateien, die größer sind als **Größte geprüfte Datei (KB)**, werden ebenfalls nicht gesendet. Im Modus **Lokaler Scan-Dienst (Socket)** bleibt das alles auf dem Server.

Nie gesendet werden diese Dateien, obwohl der lokale Scanner sie trotzdem prüft:

- `.htaccess`-, `.user.ini`- und `.env*`-Dateien;
- Dateien, deren Name der einer Konfigurations- oder Zugangsdatei entspricht, wie `parameters.yml`, `auth.json`, `.htpasswd`, `.npmrc`, `.netrc` und Dateien mit privaten Schlüsseln (`id_rsa` und ähnliche), sowie Kopien davon (Namen, die mit `wp-config`, `localconfig`, `parameters.y` oder `config.local` beginnen), außer den unten genannten PHP-Dateien;
- Dateien mit der Endung `pem`, `key`, `crt`, `p12`, `pfx`, `jks`, `kdbx`, `sql`, `sqlite`, `db` oder `ini`;
- Dateien, deren Name mit einem Leerzeichen oder einem anderen Leerraum beginnt oder endet, etwa `localconfig.php`;
- Dateien, deren Name einer Konfigurationsdatei nur ähnelt und die keine PHP-Dateien sind, etwa `local_config.yml`, `wp_config.php.bak` oder `wpconfig.txt`, auch mit einem unsichtbaren oder nicht lateinischen Zeichen im Namen;
- alles in `config/jwt`, `config/secrets`, `contao-manager`, `config`, `system/config`, `var`, `.git` und `.ssh`;
- Dateien in `config/packages` mit „secret“ im Namen;
- die Pfade unter **Nicht an den Scan-Dienst gesendete Pfade**.

Nur in geschwärzter Form gesendet werden PHP-Konfigurationsdateien mit dem Namen `localconfig.php`, `config.local.php` oder `wp-config.php`, Kopien, deren Name mit `wp-config` beginnt und auf `.php` endet, sowie PHP-Dateien, deren Name einer Konfigurationsdatei nur ähnelt (etwa `local_config.php`, `localconfig-sample.php`, `wp_config.php` oder `my-wp-config.php`, auch mit einem unsichtbaren oder nicht lateinischen Zeichen, mit einer Endung, die PHP ausführt, wie `.php`, `.phtml` oder `.inc`), wenn sie nicht in einem der oben genannten Ordner liegen. Die `localconfig.php` von Contao selbst liegt in `system/config` und wird daher nie gesendet. Bevor die Prüfsumme gebildet und die Datei hochgeladen wird, werden in einer solchen Datei alle Zeichenketten, Zahlen und Kommentare ersetzt: jede Zeichenkette durch `ISPP_REDACTED` (auch Schlüssel wie `dbPass` in `$GLOBALS['TL_CONFIG']['dbPass']`), jede Zahl durch `0`, der Text jedes Kommentars durch `ISPP_REDACTED`, ein Variablenname in einer Zeichenkette (etwa `"pa$word"`) durch `$ISPP_REDACTED`, jeder Name innerhalb von `{$...}` oder `${...}` in einer Zeichenkette durch `ISPP_REDACTED`. Erhalten bleiben nur die Struktur des Codes, die Namen (Funktionen, Variablen, Konstanten) und die Konstantennamen in `define()` (in einer Datei mit einer `namespace`-Deklaration, einem `use`-Import oder PHP-8-Attributen werden auch diese ersetzt), sodass Passwörter und andere Werte den Server nie verlassen. Von Angreifern eingefügter Code wird weiterhin an seiner Struktur gefunden: Der Dienst sieht Aufrufe wie `eval()`, `base64_decode()` oder `include`, aber nicht ihren wörtlichen Inhalt. Nachgefragt wird die Prüfsumme der geschwärzten Form; die der Originaldatei wird nie gesendet. Der Dienst kann eine leere Zeichenkette und die führenden Leerzeichen einer Zeile in einer Zeichenkette erkennen, aber keinen Wert lesen. Eine Datei, die sich nicht sicher schwärzen lässt (sie lässt sich nicht einlesen, ist größer als 1 MB, enthält `__halt_compiler` oder verwendet ein kurzes Öffnungs-Tag `<?` oder beginnt mit `<?xml`, deren Bedeutung von der PHP-Einstellung `short_open_tag` abhängt), wird gar nicht gesendet. In der geschwärzten Form gefundene Schadsoftware wird für die echte Datei gemeldet, mit dem Hinweis, dass sie in geschwärzter Form geprüft wurde.

Der gehostete Dienst führt eine Tabelle von Prüfsummen mit dem Urteil und der Zeit. Hochgeladene Dateien behält er nicht: Sie werden direkt nach dem Scan gelöscht, auch wenn sie Schadcode sind.

Geben Sie nur die Adresse eines Scan-Dienstes ein, dem Sie vertrauen: Die Zugangsdaten und der Inhalt unbekannter Dateien gehen an die Adresse, die eingestellt ist.

Den lokalen Scan-Dienst verwenden

1. Stellen Sie **Remote-Scan** auf **Lokaler Scan-Dienst (Socket)**.
2. Wenn der Socket nicht unter dem Standardpfad liegt, setzen Sie **Socket des lokalen Scan-Dienstes**.
3. Öffnen Sie den Tab **Scanner** und klicken Sie auf **Verbindung testen**.

Den eigenen Scan-Dienst verwenden

1. Stellen Sie **Remote-Scan** auf **Eigener Scan-Dienst**.
2. Geben Sie die HTTPS-Adresse bei **Adresse des Scan-Dienstes** ein und speichern Sie.
3. Öffnen Sie den Tab **Scanner**. Geben Sie im Bereich **Remote-Scan** den Zugangstoken bei **Neuer Zugangstoken** ein und klicken Sie auf **Token speichern**. **Token entfernen** löscht ihn wieder.
4. Klicken Sie auf **Verbindung testen**.

Auf der Konsole verwenden Sie `ispprotect:remote token:set` und `ispprotect:remote token:clear`, siehe Kommandozeile. Der Token muss aus 1 bis 4096 druckbaren Zeichen ohne Leerzeichen bestehen.

Den gehosteten Scan-Dienst mit einer Lizenz verwenden

1. Stellen Sie **Remote-Scan** auf **Gehosteter Scan-Dienst (Lizenz)** und speichern Sie.
2. Der gehostete Scan-Dienst unter `https://scan.ispprotect.com` und die Lizenz-API unter `https://license.ispprotect.com` sind eingebaut; Sie tragen keine Adresse ein. Die Einstellung **Adresse des gehosteten Scan-Dienstes** (`remote.hosted_url`) ist eine optionale Überschreibung zum Testen und bleibt normalerweise leer. Die Einstellung `remote.portal_url` überschreibt diese Adresse nur für eine andere Portal-Installation (Konsolenbefehl `ispprotect:settings:set`); sie ist nicht die Konto-Konsole unter `https://console.ispprotect.com`.

3. Öffnen Sie den Tab **Scanner**. Geben Sie im Bereich **Remote-Scan** den Schlüssel bei **Lizenzschlüssel** ein und klicken Sie auf **Verbinden**. Auf der Konsole verwenden Sie `ispprotect:remote connect`.
4. Klicken Sie auf **Verbindung testen**.

Der Bereich zeigt dann:

Feld	Bedeutung
Lizenz	**Verbunden** oder **Nicht verbunden**
Tarif	Der Tarif der Lizenz
Lizenz gültig bis	Das Ende der Lizenz
Websites	Wie viele Websites die Lizenz nutzen und wie viele sie erlaubt
Host, der dem Lizenzportal gemeldet wurde	Der Hostname dieser Website
Zugang gültig bis	Das Ende des aktuellen Zugangs dieser Website zum Dienst
Automatische Erneuerung	**Etwa einmal täglich**, der Zeitpunkt des nächsten Versuchs oder **Angehalten**
Letzte Erneuerung	Wann der Zugang zuletzt erneuert wurde
Lizenzproblem	Der letzte Grund, den das Portal genannt hat, falls vorhanden

Eine verbundene Website wird beim Lizenzportal gezählt. Das Bundle erneuert seinen Zugang zum Dienst selbst, etwa einmal täglich und noch einmal, wenn der Zugang innerhalb von zwei Tagen abläuft. Das tut es auch im Modus **Aus**, solange eine Lizenz verbunden ist. Nach einer eindeutigen Ablehnung durch das Portal oder wenn die Uhr des Servers falsch geht, wird die Erneuerung angehalten. Beheben Sie die Ursache und klicken Sie dann auf **Jetzt prüfen** (Konsole: `ispprotect:remote refresh`), oder trennen Sie die Verbindung und verbinden Sie erneut mit einem Schlüssel.

Trennen fragt nach einer Bestätigung („Ja, trennen“). Es gibt die Website beim Lizenzportal frei und entfernt die Lizenzdaten auf dem Server. Die Daten werden in jedem Fall entfernt, auch wenn das Portal nicht erreicht werden konnte. Dann zählt die Website möglicherweise noch zur Lizenz, bis Sie sie in Ihrem Konto im Lizenzportal freigeben. Auch das Entfernen des Bundles gibt die Website frei, siehe Das Bundle entfernen.

Verbindung testen

Verbindung testen fragt den Dienst nach seinem Status und zeigt die Engine, die Signaturen, die Zahl der geladenen Signaturen, die größte Datei, den Upload pro Tag und die Anfragen pro Minute, die der Dienst meldet. Es ändert nichts.

Ergebnis des letzten Scans

Der Bereich zeigt den Remote-Teil des letzten Scans: seinen Zustand und diese Zahlen.

Zahl	Bedeutung
Abgefragt	Dateien, nach deren Prüfsumme gefragt wurde
Unauffällig	Dateien, die der Dienst als harmlos kennt
Hochgeladen	Dateien, die hochgeladen wurden
Schadcode	Dateien, die der Dienst als Schadcode gemeldet hat
Übersprungen	Dateien, die nicht gelesen werden konnten oder sich beim Senden geändert haben
Nicht geprüft	Dateien, die der Dienst nicht geprüft hat
Gesendet	Die Menge der hochgeladenen Daten

Schadcode, den der Dienst meldet, ist ein Fund der Art „Vom Scan-Dienst gefundener Schadcode“, mit dem Namen der Erkennung. Siehe Dateiscanner.

Wenn der Dienst ablehnt oder nicht erreichbar ist

Der lokale Scan wird immer abgeschlossen. Der Scan vermerkt den Grund, und der Bereich zeigt ihn mit dem Zustand des letzten Scans. Die Gründe sind:

Grund	Bedeutung
Der Scan-Dienst war nicht erreichbar.	Ein Netzwerk- oder Socket-Problem.
Der Scan-Dienst hat die Zugangsdaten nicht akzeptiert.	Falscher oder abgelaufener Token oder falsche oder abgelaufene Lizenz.
Der Scan-Dienst ist noch nicht bereit.	Zum Beispiel lädt er noch seine Signaturen.
Der Scan-Dienst ist ausgelastet oder hat um eine Pause gebeten.	Der Scan versucht es später erneut.
Das Kontingent des Scan-Dienstes ist aufgebraucht.	Die Grenze des Dienstes ist erreicht.
Eine Datei war für den Scan-Dienst zu groß.	Der Dienst hat eine eigene Grenze für die Dateigröße.
Der Scan-Dienst hat den Zugriff verweigert.	Der Dienst lässt diesen Server-Benutzer nicht zu, oder die Zugangsdaten umfassen den Remote-Scan nicht.
Der Scan-Dienst konnte mehrere Dateien nacheinander nicht prüfen.	Der Scan versucht es später erneut.
Die Upload-Grenze dieses Scans ist erreicht.	Die übrigen Dateien folgen im nächsten Scan.
Für den Scan-Dienst ist keine gültige Adresse und kein gültiger Socket eingestellt.	Prüfen Sie die Einstellungen.
Es fehlt ein Zugangstoken oder eine verbundene Lizenz.	Verbinden Sie zuerst.
Die Einstellung des Remote-Scans wurde während des Scans geändert.	Der nächste Scan verwendet die neue Einstellung.

Grenzen des gehosteten Dienstes: Die Lizenz begrenzt die Zahl der Websites, und der Dienst hat eigene Grenzen für die Größe einer Datei, Uploads pro Tag und Anfragen pro Minute, die **Verbindung testen** anzeigt.

So werden Zugangsdaten gespeichert

Der Zugangstoken und der Lizenzschlüssel werden verschlüsselt in der Datenbank gespeichert, mit einem Schlüssel, der aus dem Application Secret von Contao abgeleitet wird. Sie werden nie wieder angezeigt, nie in das Protokoll geschrieben und nie an den Browser zurückgesendet. Die Seite zeigt nur, ob sie gesetzt sind, und bei einem Zugangstoken von mindestens 12 Zeichen seine letzten vier Zeichen. Beim Lizenzschlüssel zeigt die Seite nur, dass einer gesetzt ist. Der Befehl `ispprotect:remote` läuft auf dem Server und zeigt von beiden die letzten vier Zeichen, wenn der Wert mindestens 12 Zeichen hat.

Wenn das Application Secret kürzer als 16 Bytes ist oder keine Verschlüsselung installiert ist, können Geheimnisse nicht gespeichert werden, und die Seite sagt es. Wenn sich das Application Secret ändert, können der gespeicherte Token und die Lizenzdaten nicht mehr gelesen werden. Die Seite sagt es dann, und Sie geben sie erneut ein. Änderungen am Token und an der Lizenz werden im Ereignisprotokoll aufgezeichnet.

Grenzen des Remote-Scans

- Der Remote-Scan prüft Code-Dateien anhand ihrer Prüfsumme und lädt nur Dateien hoch, die der Dienst nicht kennt. Er findet, was der Dienst kennt. Er ist keine Garantie dafür, dass eine Website sauber ist.

Anmeldeschutz

Der Anmeldeschutz überwacht die Anmeldung im Backend und die Anmeldung im Frontend (Mitglieder). Seine Einstellungen stehen in den Gruppen Anmeldeschutz und Zwei-Faktor-Authentifizierung, siehe Einstellungsreferenz.

Was gezählt wird

Falsche Passwörter, unbekannte Benutzernamen und falsche oder wiederverwendete Codes des zweiten Schritts zählen als Fehlversuche, je Adresse und je Benutzername. Ein Versuch mit leerem Benutzernamen oder leerem Passwort wird nicht gezählt. Veraltete Formular-Token werden ebenfalls nicht gezählt.

Wenn innerhalb des Zeitfensters eine Grenze erreicht wird:

- Die Adresse wird gesperrt (**Fehlgeschlagene Anmeldungen pro Adresse**). Eine geschützte Administrator-Adresse wird nicht gesperrt, siehe Die eigene Adresse des Administrators. Stattdessen wird nur die Anmeldung von dort gesperrt, und der Rest der Website bleibt erreichbar. Die erste solche Sperre dauert so viele Minuten, wie **Sperrdauer für Benutzernamen (Minuten)** angibt. Hat die vorherige Sperre der Adresse in den letzten 30 Tagen begonnen, dauert die neue viermal so lange wie jene, höchstens aber **Längste Sperre (Minuten)**.
- Der Benutzername wird gesperrt (**Fehlgeschlagene Anmeldungen pro Benutzername**), für **Sperrdauer für Benutzernamen (Minuten)**.

Beide Prüfungen laufen, bevor das Passwort oder der Code geprüft wird. Ein abgewiesener Versuch zeigt die allgemeine Contao-Meldung „Zu viele Anmeldeversuche“. Sie sagt dem Besucher nicht, ob die Adresse oder der Name die Ursache war. Der Grund steht im Ereignisprotokoll, beim Ereignis „Anmeldung abgewiesen“.

Einzelheiten

- Auch der zweite Schritt wird gezählt, sodass ein gestohlenes Passwort allein keine unbegrenzten Versuche beim Code erlaubt.
- Eine Anmeldung gilt nur dann als erfolgreich, wenn sie vollständig ist, einschließlich des zweiten Schritts. Eine Anmeldung über ein „Angemeldet bleiben“-Cookie wird ignoriert.
- Benutzernamen werden über einen Schlüssel verglichen. Groß- und Kleinschreibung, umgebende Leerzeichen und unsichtbare Zeichen spielen keine Rolle, sodass alle Schreibweisen eines Namens gegen dasselbe Konto zählen.
- Contao speichert Benutzernamen genau so, wie sie geschrieben sind. „john“ und „JOHN“ (oder das vollbreite „ｊｏｈｎ“) können deshalb zwei Konten im selben Bereich mit demselben Schlüssel sein. Kann der Name eines anderen Kontos denselben Schlüssel haben (verglichen ohne Rücksicht auf Groß- und Kleinschreibung, Zeichenbreite und Akzente), setzt eine Anmeldung des Kontos den Fehlerzähler des Namens nicht zurück und macht ihre Adresse nicht zu einer bekannten Adresse für eine Namenssperre. Sie wird nicht als „Erfolgreiche Anmeldung“ oder „Anmeldung von einer neuen Adresse“ aufgezeichnet und schützt die Adresse eines Administrators nicht. Sonst könnte eines dieser Konten verhindern, dass der Name des anderen gesperrt wird.
- Erlaubte Adressen werden nie gezählt, gesperrt oder ausgesperrt.
- Adressen, die durch eine Administrator-Anmeldung geschützt sind, werden wie jede andere Adresse gezählt, sodass eine gestohlene Sitzung an einer solchen Adresse nicht für unbegrenztes Passwort-Raten genutzt werden kann. Ihre Sperren gelten nicht für die Anmeldung, Einträge der Liste der gesperrten Adressen aber schon.
- IPv6-Adressen werden je /64-Bereich gezählt, gesperrt, ausgesperrt und geschützt. Geräte wechseln ihre temporären IPv6-Adressen innerhalb dieses Bereichs.
- Ein gesperrter Benutzername hält eine Adresse nicht zurück, von der aus dieses Konto in den letzten 90 Tagen eine Anmeldung abgeschlossen hat (IPv6: derselbe /64-Bereich). Sonst könnte jeder den Inhaber aus dem Konto fernhalten, indem er falsche Passwörter für den Namen eingibt. Der Preis dafür: Jemand anderes an einer solchen Adresse, zum Beispiel im selben Büronetz, kann weiter probieren, während der Name gesperrt ist. Die Adressgrenze gilt für ihn trotzdem.

- Meldet sich ein Administrator von einer Adresse an, die für diesen Benutzer in den letzten 90 Tagen nicht gesehen wurde, zeichnet das Bundle das Ereignis „Anmeldung von einer neuen Adresse“ auf und sendet, wenn **Bei Anmeldung von neuen Adressen warnen** eingeschaltet ist, eine E-Mail.
- Abmeldungen und Benutzerwechsel werden im Ereignisprotokoll aufgezeichnet.
- Fehlen die Tabellen des Bundles oder fällt die Datenbank aus, läuft die Anmeldung weiter, als wäre das Bundle nicht installiert.

Was nicht abgedeckt ist

Anmeldungen mit einem Anmeldelink oder einem „Angemeldet bleiben“-Cookie und andere Anmeldungen ohne Benutzernamen und Passwort werden vom Anmeldeschutz nicht vorab geprüft, ebenso wenig Passkeys. Die Firewall weist gesperrte Adressen trotzdem bei jeder Anfrage ab.

Der Tab Anmeldeschutz

Der Tab zeigt diese Teile:

- **Gesperrte Konten**: gesperrte Benutzernamen mit **Bereich** (Backend oder Frontend), **Benutzername**, **Erstellt** und **Läuft ab**. Die Schaltfläche **Entsperren** hebt eine Sperre auf.
- **Für die Anmeldung gesperrte Adressen**: Sperren geschützter Administrator-Adressen, mit **Bereich**, **Erstellt**, **Läuft ab** und **Minuten**. Es wird nur ein Hash der Adresse gespeichert, daher kann die Seite die Adresse nicht auflisten. Jede Zeile hat ein Feld **Adresse** und eine Schaltfläche **Entsperren**.
- **Nach fehlgeschlagenen Anmeldungen gesperrte Adressen**: die Sperren, die der Anmeldeschutz verhängt hat, mit einer Schaltfläche **Sperre aufheben**.
- **Letzte Anmeldeereignisse**.
- Die Einstellungen der Gruppen Anmeldeschutz und Zwei-Faktor-Authentifizierung.

Sperre eines Benutzernamens aufheben

1. Öffnen Sie den Tab **Anmeldeschutz**.
2. Suchen Sie das Konto unter **Gesperrte Konten**.
3. Klicken Sie auf **Entsperren**.

Auf der Konsole:

```
vendor/bin/contao-console ispprotect:unlock <username>
```

Ersetzen Sie `<username>` durch den Benutzernamen. Der Befehl hebt die Sperre in jedem Bereich auf, in dem es eine gibt. Mit `--realm=backend` oder `--realm=frontend` hebt er nur die Sperre in diesem Bereich auf.

Sperre einer Adresse aufheben

Eine Adresse, die die Fehlergrenze erreicht hat, während sie als Adresse eines angemeldeten Administrators geschützt war, wird nicht gesperrt. Stattdessen kann sie sich eine Zeit lang nicht anmelden. Um diese Sperre aufzuheben, müssen Sie die Adresse eingeben.

1. Suchen Sie die Adresse. Sie steht beim Ereignis „Anmeldung für eine Adresse gesperrt“ auf dem Tab **Ereignisse**: in der Spalte **Adresse** und in den Details unter `rule`. Bei IPv6 genügt eine beliebige Adresse des /64-Bereichs.
2. Suchen Sie auf dem Tab **Anmeldeschutz** die Zeile unter **Für die Anmeldung gesperrte Adressen**, geben Sie die Adresse in ihr Feld ein und klicken Sie auf **Entsperren**.

Auf der Konsole:

```
vendor/bin/contao-console ispprotect:unlock --address=203.0.113.7
```

Geben Sie entweder einen Benutzernamen oder `--address` an, nicht beides und nicht keines von beiden. Die Option `--realm=backend` oder `--realm=frontend` beschränkt den Befehl auf einen Bereich.

Das Aufheben der Sperre setzt auch den Fehlerzähler der Adresse in diesem Bereich zurück und entfernt die Vorgeschichte, die die nächste Sperre verlängert. Eine Firewall-Sperre der Adresse hebt es nicht auf. Heben Sie diese auf dem Tab **Firewall** oder mit `ispprotect:ip:remove` auf. Ein Eintrag in der Liste der erlaubten Adressen lässt die Adresse die Anmeldeprüfung passieren, solange der Eintrag besteht, entfernt die Sperre aber nicht. Wird der Eintrag entfernt, bevor die Sperre endet, gilt die Sperre wieder.

Wird eine Sperre tatsächlich aufgehoben, zeichnet das Bundle das Ereignis „Benutzername entsperrt“ oder „Anmeldung für eine Adresse entsperrt“ auf. Das Ereignis nennt den Benutzernamen oder die Adresse, nicht, wer die Sperre aufgehoben hat. Gab es keine Sperre, wird nichts aufgezeichnet. Diese Ereignisse werden nicht als Warnungen per E-Mail gesendet.

Gekürzte Adressen im Protokoll

Ist **Adressen im Protokoll kürzen** eingeschaltet, enthält das Ereignis nur die gekürzte Adresse und kein `rule`. Die vollständige Adresse lässt sich dann nicht aus dem Ereignis lesen. Sie steht nur im Zugriffsprotokoll des Webservers, oder Sie warten, bis die Sperre endet. Bei dieser Einstellung werden auch die gekürzten Adressen verglichen, wenn das Bundle prüft, ob eine Adresse für ein Konto bekannt ist. Der ganze /24-Bereich (IPv4) oder /48-Bereich (IPv6) einer bekannten Adresse gilt dann als bekannt.

Wenn Sie selbst aus dem Backend ausgesperrt sind, siehe Zurück ins System und Fehlerbehebung.

Zwei-Faktor-Authentifizierung

Das Bundle bringt keine eigene Zwei-Faktor-Authentifizierung mit. Es nutzt die, die Contao bereits hat. Das Bundle ergänzt drei Dinge:

- Der Checkup meldet aktive Administratoren, die keine Zwei-Faktor-Authentifizierung eingerichtet haben. Er zählt Konten, die nicht deaktiviert sind und innerhalb ihres Start- und Stoppdatums liegen. Siehe Sicherheits-Checkup.
- Falsche Codes des zweiten Schritts werden vom Anmeldeschutz gezählt und als Ereignis „Falscher Code beim zweiten Anmeldeschritt“ aufgezeichnet. Siehe Anmeldeschutz.
- Die Einstellung **Zweiten Anmeldeschritt verlangen** kann die Zwei-Faktor-Authentifizierung für Administratoren erzwingen.

Den zweiten Schritt für Administratoren verlangen

Zweiten Anmeldeschritt verlangen steht auf dem Tab **Anmeldeschutz**. Standardmäßig ist die Einstellung aus. Wenn Sie sie einschalten, müssen Administratoren mit einer Authenticator-App einen zweiten Anmeldeschritt einrichten.

Ein Administrator, der die Zwei-Faktor-Authentifizierung nicht eingeschaltet hat, wird dann auf die Seite „Sicherheit“ des Backends umgeleitet, bis er sie eingerichtet hat. Was ein Benutzer sieht:

- Jede Seite des Backends führt zur Seite „Sicherheit“, auf der der Benutzer den zweiten Schritt einrichtet.
- Die Anmeldung selbst, der zweite Anmeldeschritt, der Anmeldelink, die Abmeldung und die Passwortänderung bleiben offen. Die Seite „Sicherheit“ mit ihrem Einrichtungsformular ebenfalls.
- Hintergrundanfragen (XHR, Turbo-Frames und -Streams) können keiner Umleitung folgen. Sie werden mit Status 403 und einem kurzen Text abgewiesen, oder mit JSON, wenn die Anfrage es verlangt.

Die Prüfung gilt für jede Route des Backends, nicht nur für die Hauptseiten: Popups, Hinweise, Auswahl, Bestätigung, Hilfe, Favoriten, Vorschau, Jobs, Suche, das Template Studio und die Seiten dieses Bundles. GET- und POST-Anfragen werden umgeleitet (Status 303), bevor der Controller läuft, sodass nichts geändert werden kann.

Die Einstellung gilt nur für Administratoren. Andere Backend-Benutzer und Frontend-Mitglieder sind nicht betroffen. Benutzer, die zuerst ihr Passwort ändern müssen, und Sitzungen, in denen ein Administrator zu einem anderen Benutzer gewechselt hat, werden nicht umgeleitet, wie bei Contaos eigener Option. Schlägt die Prüfung selbst fehl, zum Beispiel weil die Datenbank nicht gelesen werden kann, wird die Anfrage durchgelassen und der Fehler ins Protokoll geschrieben, damit eine Störung nicht alle Administratoren aussperrt.

Was die Einstellung nicht leistet

- Sie lässt Administratoren den zweiten Schritt einrichten. Sie ist kein zweiter Schritt für Konten, die noch keinen haben. Wer das Passwort eines solchen Administrators hat, kann sich weiterhin anmelden und dann die Zwei-Faktor-Authentifizierung mit einem eigenen Gerät einrichten.
- Sie deckt weder die Konsole noch andere Backend-Benutzer oder Frontend-Mitglieder ab.

Contao hat eine eigene Option, `contao.security.two_factor.enforce_backend`, die alle Backend-Benutzer umfasst. Sie wird in der Contao-Konfiguration gesetzt. Der Hinweis des Checkups für Administratoren ohne Zwei-Faktor-Authentifizierung nennt beide Optionen.

Nach dem Verlust eines Geräts

Ein Benutzer, der das Gerät mit der Authenticator-App verloren hat, kann den richtigen Code nicht angeben. Falsche Codes zählen als Fehlversuche, sodass die Anmeldung dieses Benutzernamens oder dieser Adresse eine Zeit lang gesperrt sein kann. Siehe Zurück ins System und Fehlerbehebung.

Ein anderer Administrator kann die Zwei-Faktor-Authentifizierung des Benutzers im Benutzerformular des Contao-Backends ausschalten. Das Bundle zeichnet dies als Warnung auf, Ereignis „Zweiter Anmeldeschritt ausgeschaltet“. Der Benutzer meldet sich dann mit dem Passwort an und richtet den zweiten Schritt neu ein. Bei eingeschalteter Einstellung **Zweiten Anmeldeschritt verlangen** öffnet sich die Seite „Sicherheit“ sofort.

Schaltet ein Benutzer die Zwei-Faktor-Authentifizierung in seinen eigenen Kontoeinstellungen ein oder aus, zeichnet das Bundle dies nicht auf.

Sicherheits-Checkup

Der Checkup führt 20 Prüfungen aus und gibt eine Punktzahl von 0 bis 100. Sie finden ihn auf dem Tab **Checkup**, die Punktzahl und die wichtigsten Ergebnisse auf der **Übersicht**. Auf der Konsole gibt `ispprotect:checkup` dasselbe aus.

Punktzahl und Status

Jede Prüfung hat ein Gewicht und einen Status. Die Punktzahl ist der gewichtete Anteil der bestandenen Prüfungen. Eine Warnung zählt halb, ein Problem zählt nichts, und Hinweise werden nicht bewertet.

Angezeigter Status	Bedeutung
In Ordnung	Die Prüfung wurde bestanden.
Beachten	Eine Warnung.
Problem	Die Prüfung ist fehlgeschlagen.
Unbekannt	Der Wert konnte nicht gelesen werden. Die Prüfung wird nicht bewertet.

Zu jedem Ergebnis gehört eine kurze Erklärung, was zu ändern ist. Eine Prüfung, die mit einem Fehler abbricht, wird als „Eine Prüfung konnte nicht abgeschlossen werden“ angezeigt. Die anderen Prüfungen sind davon nicht betroffen.

Die Prüfungen

Prüfungen zum Server und zur Installation:

Prüfung	Was sie ansieht
PHP erhält Sicherheitsupdates	PHP bekommt noch Sicherheitskorrekturen.
Das Anwendungsgeheimnis ist lang und kein Beispielwert	Das Anwendungsgeheimnis (Application Secret) ist lang und kein Beispielwert.
PHP zeigt Besuchern keine Fehlermeldungen an	`display_errors`: PHP zeigt Besuchern keine Fehlermeldungen an.
PHP verrät seine Version nicht	`expose_php`: PHP gibt seine Version nicht bekannt.
PHP lädt keinen Code von fremden Servern	`allow_url_include`: PHP bindet keinen Code von anderen Servern ein.
Produktivmodus ohne Debugging	Contao läuft im Produktivmodus ohne Debugging.
Die Adresse der Seite nutzt HTTPS	Die Adresse der Website beginnt mit `https://`.
Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar	Andere Benutzer können sie nicht lesen.
Keine Datei und kein Ordner im Code ist für alle beschreibbar	Keine Datei und kein Ordner im Code kann von jedem geändert werden.
Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner	Im öffentlichen Ordner liegen keine Sicherungen und keine Debug-Dateien.
Genug freier Speicherplatz	Genug freier Platz. Unter 5 Prozent ist es eine Warnung, unter 1 Prozent ein Problem.

Die Werte von `display_errors`, `expose_php` und `allow_url_include` lassen sich von der Kommandozeile aus nicht zuverlässig lesen, weil der Webserver eine andere PHP-Konfiguration verwenden kann. Öffnen Sie dafür den Tab **Checkup** im Backend.

Ohne konfigurierten Host bewertet der Checkup die HTTPS-Prüfung der Website-Adresse nicht.

Prüfungen zum Bundle:

Prüfung	Was sie ansieht
Die Firewall ist eingeschaltet	**Firewall-Modus** ist **An**. **Nur protokollieren** ist eine Warnung, **Aus** ein Problem.
Der Anmeldeschutz ist eingeschaltet	**Anmeldeschutz** ist eingeschaltet. Ausgeschaltet ist ein Problem.
Warnungen haben einen Empfänger	Eine Benachrichtigungsadresse ist vorhanden.
Der Dateiscan lief in den letzten 8 Tagen	Ein Scan wurde in den letzten 8 Tagen abgeschlossen.
Keine offenen Funde mit hoher Stufe	Ein offener Fund der Stufe Hoch ist ein Problem, ein offener der Stufe Mittel eine Warnung.

Prüfungen speziell für Contao:

Prüfung	Was sie ansieht
Administratoren nutzen die Zwei-Faktor-Authentifizierung	Warnt, solange aktive Administratoren keine haben.
Wenige Administrator-Konten, alle in Gebrauch	Mehr als 5 aktive Administratoren oder ein Administrator, der sich seit 180 Tagen nicht angemeldet hat, ist eine Warnung.
Contao Manager liegt nicht auf dem Server	Die Prüfung sucht im öffentlichen Verzeichnis nach `contao-manager.phar.php` und meldet es als Hinweis, wenn es dort liegt.
Vertrauenswürdige Proxys passen zum tatsächlichen Aufbau	Siehe Hinter einem Reverse-Proxy oder CDN.

Aufgeführte Dateien und die Korrektur der Rechte

Drei Prüfungen führen unter ihrem Hinweis auf, was sie gefunden haben: **Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar**, **Keine Datei und kein Ordner im Code ist für alle beschreibbar** und **Keine Sicherungen oder Debug-Dateien im öffentlichen Ordner**. Die Namen sind relativ zum Projektordner, bei den Dateien im öffentlichen Ordner relativ zu diesem. Die Listen stehen auf dem Tab **Checkup**, auf der **Übersicht** und in der Ausgabe von `ispprotect:checkup`. Die Liste der für alle beschreibbaren Pfade hat höchstens 20 Einträge, die der Dateien im öffentlichen Ordner höchstens 50. Eine längere Liste endet mit „Die Liste zeigt nur die ersten {count} Einträge.“

Hat die Prüfung **Dateien mit Passwörtern und Schlüsseln sind für andere Benutzer nicht lesbar** das Ergebnis **Beachten**, entzieht die Schaltfläche **Rechte korrigieren** den aufgeführten Dateien alle Rechte für „andere“, wie `chmod o-rwx`. Besitzer und Gruppe behalten ihre Rechte. Die Schaltfläche nimmt die Dateinamen aus der Prüfung selbst, nie aus dem Browser, und ändert nur eine Datei, die

- eine normale Datei direkt im Projektordner ist, kein Link und kein Ordner, keinen zweiten Namen (Hardlink) hat und
- dem Benutzer gehört, unter dem PHP läuft.

Die Schaltfläche erscheint, wenn sich mindestens eine aufgeführte Datei ändern lässt. Für jede andere Datei nennt die Meldung den Befehl, den Sie im Projektordner ausführen, zum Beispiel `chmod o-rwx .env`. Danach läuft die Prüfung erneut und zeigt das neue Ergebnis. Die Änderung steht im Audit-Log als „Dateirechte durch den Checkup geändert“, mit den Namen der geänderten und der nicht geänderten Dateien.

Ein Programm, das diese Dateien unter einem anderen Benutzerkonto liest, zum Beispiel ein Cronjob, muss nach der Änderung zur Gruppe der Datei gehören.

Die beiden anderen Prüfungen haben keine Schaltfläche. Entziehen Sie den aufgeführten Pfaden das Schreibrecht für „andere“, zum Beispiel mit `chmod o-w`, und löschen Sie die aufgeführten Dateien im öffentlichen Ordner oder verschieben Sie sie von dort.

Sicherheits-Header

Das Bundle kann drei Header von Antworten ändern. Die Einstellungen stehen in der Gruppe Sicherheits-Header, siehe Einstellungsreferenz.

- **PHP-Version verbergen** entfernt den Header `X-Powered-By`. Die Einstellung ist standardmäßig eingeschaltet.
- **HTTPS erzwingen (HSTS)** fügt `Strict-Transport-Security` hinzu, mit der Dauer aus **HSTS-Dauer (Sekunden)**. Er wird nur bei HTTPS-Anfragen gesendet und ist standardmäßig aus. Schalten Sie ihn nur ein, wenn HTTPS auf der ganzen Website funktioniert, denn Browser merken sich ihn für die gesamte Dauer.
- **Header Permissions-Policy** setzt den Header `Permissions-Policy` auf den Text, den Sie eingeben. Lassen Sie das Feld leer, um keinen zu senden.

Ereignisprotokoll und Benachrichtigungen

Das Ereignisprotokoll

Das Ereignisprotokoll ist der Tab **Ereignisse**. Es zeichnet sicherheitsrelevante Ereignisse mit Zeit, Stufe, Adresse, Benutzername und Details auf. Die Stufen sind Info, Hinweis, Warnung und Alarm. Der Tab listet die Ereignisse, die neuesten zuerst, und Sie können sie filtern:

Filter	Bedeutung
Ereignis	Eine Art von Ereignis
Mindeststufe	Nur Ereignisse dieser Stufe oder höher
Adresse	Eine Adresse
Benutzername	Ein Benutzername
Bereich	Der Bereich, `backend` oder `frontend`
Von (Datum) und **Bis (Datum)**	Ein Datumsbereich
Suche	Text im Ereignis

Klicken Sie auf **Filtern**, um den Filter anzuwenden, und auf **Filter zurücksetzen**, um ihn zu löschen. Die Spalten sind **Zeit**, **Stufe**, **Ereignis**, **Adresse**, **Benutzername**, **Bereich** und **Details**.

Was aufgezeichnet wird

- Anmeldungen: erfolgreiche, fehlgeschlagene, abgewiesene, Abmeldung, Benutzerwechsel, Anmeldung von einer neuen Adresse, gesperrte Benutzernamen und Adressen, aufgehobene Sperren, falsche Codes des zweiten Schritts.
- Firewall: abgewiesene und protokollierte Anfragen, Sperren, aufgehobene Sperren, Änderungen der Adresslisten.
- Scanner: gestartete und abgeschlossene Scans, Funde, geänderte Pakete, bekannte Sicherheitslücken und Systemhinweise wie eine E-Mail, die nicht gesendet werden konnte.
- Konten: Anlegen, Ändern und Löschen von Backend-Benutzern, Backend-Benutzergruppen und Mitgliedern sowie Rollenänderungen, wenn sie im Backend erfolgen.
- Einstellungen: Änderungen an den Einstellungen dieses Bundles, vorgenommen auf den Seiten oder mit `ispprotect:settings:set` (Ereignis „Einstellungen geändert“).
- Remote-Scan: Speichern und Entfernen des Zugangstokens, Verbinden, Erneuern und Trennen der Lizenz sowie Ablehnungen durch das Lizenzportal.

Bei Konten zeichnet das Protokoll die Namen der geänderten Felder auf, nie die alten oder neuen Werte, mit einer Ausnahme: Bei Backend-Benutzern zeichnet es die alte und die neue E-Mail-Adresse auf. Ob sich ein Passwort geändert hat, ist daran bekannt, dass das Feld übermittelt wurde. Das Passwort und sein Hash werden nie gelesen oder gespeichert. Das Anlegen eines Administrators, das Befördern eines Benutzers zum Administrator und das Ausschalten der Zwei-Faktor-Authentifizierung eines Benutzers im Benutzerformular sind Warnungen. Auch das Kopieren eines Datensatzes, das Wiederherstellen aus „Rückgängig“ und das Wiederherstellen einer älteren Version werden aufgezeichnet. Ebenso werden Frontend-Mitglieder aufgezeichnet, die sich registrieren, ihr Konto aktivieren oder schließen oder ein neues Passwort setzen.

Eine Änderung an den Einstellungen dieses Bundles wird mit den Namen der geänderten Einstellungen aufgezeichnet, nie mit ihren Werten.

E-Mail-Adressen werden im Ereignisprotokoll nur für Backend-Benutzer gespeichert, nie für Mitglieder.

Aufbewahrung und gekürzte Adressen

Protokolleinträge aufbewahren (Tage) legt fest, wie lange Einträge bleiben. Abgelaufene Einträge werden einmal pro Stunde entfernt. Bei eingeschalteter Einstellung **Adressen im Protokoll kürzen** IPv4-Adressen werden ohne die letzte ihrer vier Zahlen gespeichert (sie wird auf 0 gesetzt, aus 192.0.2.17 wird 192.0.2.0); von IPv6-Adressen werden nur die

ersten 48 Bit behalten.

Lücken im Ereignisprotokoll

- Konten, die auf der Kommandozeile oder direkt in der Datenbank angelegt oder geändert werden, werden nicht aufgezeichnet.
- Ein Benutzer, der die Zwei-Faktor-Authentifizierung in seinen eigenen Kontoeinstellungen ein- oder ausschaltet, wird nicht aufgezeichnet. Eine Änderung durch einen Administrator im Benutzerformular wird aufgezeichnet.
- Frontend-Mitglieder, die andere persönliche Daten als das Passwort ändern, werden nicht aufgezeichnet.
- Beim Wiederherstellen einer Version wird nur aufgezeichnet, dass eine Version wiederhergestellt wurde, und ihre Nummer, nicht was sich geändert hat.
- Einstellungen, die direkt in der Datenbank geändert werden, werden nicht aufgezeichnet.
- Schlägt das Speichern eines Eintrags fehl, wird der Fehler protokolliert, und Contao speichert den Datensatz trotzdem.

Auf der Konsole zeigt `ispprotect:events` die neuesten Ereignisse, siehe Kommandozeile.

Benachrichtigungen

Das Bundle sendet E-Mails über den Mailer von Contao, als reinen Text. Absender ist die Adresse des Systemadministrators von Contao, falls eine gesetzt ist. Es gibt drei Arten:

- **Sofortige Warnungen**: E-Mails zu Ereignissen der Stufe Alarm, wenn diese Einstellung eingeschaltet ist. Es gibt höchstens eine E-Mail je Ereignisart und Stunde. Nach einer fehlgeschlagenen E-Mail wartet das Bundle 15 Minuten, bevor es es erneut versucht.
- **Zusammenfassung per E-Mail**: eine tägliche oder wöchentliche Liste der Sicherheitsereignisse, je nach Einstellung. Der Wert **Aus** sendet keine.
- Eine E-Mail über eine Anmeldung von einer neuen Adresse, wenn **Bei Anmeldung von neuen Adressen warnen** eingeschaltet ist.

Empfänger ist **Adresse für Benachrichtigungen**. Ist sie leer, verwendet das Bundle die Administrator-Adresse in den Contao-Einstellungen, und ohne eine solche die Adresse des ersten aktiven Administrators. Ohne Empfänger wird keine Warnung und keine Zusammenfassung gesendet. Der Checkup meldet das.

Die Website-Adresse in den E-Mails stammt von der ersten Wurzelseite mit einer Domain, sonst vom konfigurierten Request-Kontext von Contao (`router.request_context.host` und `router.request_context.scheme` oder `framework.router.default_uri`). Sie wird nie der aktuellen Anfrage entnommen, weil die E-Mails oft über die Cron-Route `/_contao/cron` gesendet werden, die jeder mit einem beliebigen Host-Header aufrufen kann. Ohne konfigurierten Host lassen die E-Mails die Adresse weg.

E-Mails werden vom Wartungslauf gesendet, daher brauchen sie den Cron, siehe Zeitplanung mit Cron.

Einstellungsreferenz

Dieses Kapitel listet jede Einstellung des Bundles, gruppiert so, wie die Seiten sie zeigen. Zu jeder Einstellung sehen Sie die Bezeichnung, wie die Seite sie zeigt, den Schlüssel, den die Konsole verwendet, den Standardwert und was sie bewirkt.

Einstellungen im Backend ändern

Die Einstellungen stehen auf vier Tabs:

Tab	Gruppen
Firewall	Firewall, Anfragelimit, Fehlende Seiten, Fallenpfade, Eigene Regeln, Sperren
OWASP-CRS-Regeln	OWASP-CRS-Regeln
Anmeldeschutz	Anmeldeschutz, Zwei-Faktor-Authentifizierung
Einstellungen	Sicherheits-Header, Ereignisprotokoll, Benachrichtigungen, Scanner, Remote-Scan

Ändern Sie die Werte und klicken Sie auf **Speichern**. Die Seite prüft jeden Wert. Ein nicht erlaubter Wert wird nicht gespeichert, und die Seite zeigt den Grund neben dem Feld. Unter dem Formular setzt eine Schaltfläche **Gruppe „%group%“ zurücksetzen** (mit dem Namen der Gruppe anstelle von %group%) eine Gruppe nach Ihrer Bestätigung auf ihre Standardwerte zurück. Die Einstellung `remote.portal_url` steht auf keiner Seite.

Einstellungen auf der Konsole ändern

Eine Einstellung oder alle anzeigen:

```
vendor/bin/contao-console ispprotect:settings:get firewall.mode
vendor/bin/contao-console ispprotect:settings:get
```

Eine Einstellung ändern:

```
vendor/bin/contao-console ispprotect:settings:set firewall.mode log
vendor/bin/contao-console ispprotect:settings:set trap.paths '["/wp-login.php","/xmlrpc.php"]'
```

Der Wert wird als JSON gelesen, wenn das möglich ist, zum Beispiel `true`, `5` oder `["a","b"]`, sonst als Text. Ein nicht erlaubter Wert wird mit Exit-Code 2 und dem Grund abgelehnt. Eine Änderung wird im Ereignisprotokoll mit dem Schlüssel und ohne den Wert aufgezeichnet. Siehe Kommandozeile.

Werttypen

- Schalter werden als Kontrollkästchen angezeigt. Auf der Konsole akzeptieren sie `1`, `0`, `true`, `false`, `on`, `off`, `yes` und `no`. Die Tabellen zeigen sie als `true` und `false`.
- Zahlen haben einen kleinsten und einen größten Wert. Die Tabellen nennen sie.
- Listen nehmen bis zu 500 eindeutige Einträge von je höchstens 255 Bytes auf. In den Formularen und bei `ispprotect:settings:get` steht ein Eintrag pro Zeile. Auf der Konsole nimmt `ispprotect:settings:set` eine JSON-Liste.
- Listen von Pfaden (**Fallenpfade**, **Pfade ohne Anfragegrenze**) lehnen einen Eintrag ab, der die ganze Website umfassen würde.

Gruppe Firewall

Bezeichnung	Schlüssel	Standard	Wirkung
Firewall-Modus	`firewall.mode`	`on`	`on` weist Anfragen ab, die eine Regel verletzen, `log` protokolliert sie nur, `off` schaltet die Firewall aus.
Adressen von Administratoren schützen	`firewall.allow_admin_ip`	`true`	Nachdem sich ein Administrator angemeldet hat, kann diese Adresse 24 Stunden lang nicht gesperrt werden.

Gruppe Anfragelimit

Bezeichnung	Schlüssel	Standard	Wirkung
Anfragen pro Adresse begrenzen	`rate.enabled`	`true`	Weist Adressen ab, die innerhalb des Zeitfensters mehr Anfragen senden als erlaubt.
Anfragen pro Zeitfenster	`rate.limit`	`600`	Wie viele Anfragen eine Adresse innerhalb des Zeitfensters senden darf, 30 bis 100000.
Zeitfenster (Sekunden)	`rate.window`	`60`	Länge des Zeitfensters für die Anfragegrenzen, 10 bis 3600.
Anmeldeanfragen pro Zeitfenster	`rate.signin_limit`	`30`	Wie viele Anfragen an die Anmeldepfade eine Adresse innerhalb des Zeitfensters senden darf, 5 bis 1000.
Pfade ohne Anfragegrenze	`rate.exempt_prefixes`	leer	Anfragepfade, die nicht gezählt werden, zusätzlich zur eigenen Liste des Bundles.
Sperren nach Abweisungen	`rate.ban_after`	`3`	Sperrt eine Adresse nach so vielen Abweisungen innerhalb von 10 Minuten, 0 bis 100. `0` sperrt nie.

Gruppe Fehlende Seiten

Bezeichnung	Schlüssel	Standard	Wirkung
Antworten „nicht gefunden“ überwachen	`notfound.enabled`	`true`	Sperrt Adressen, die viele Antworten „nicht gefunden“ verursachen, was für Scanner typisch ist.
Antworten „nicht gefunden“ pro Zeitfenster	`notfound.limit`	`40`	Wie viele solche Antworten eine Adresse innerhalb des Zeitfensters verursachen darf, bevor sie gesperrt wird, 5 bis 10000.
Zeitfenster für „nicht gefunden“ (Sekunden)	`notfound.window`	`300`	Länge des Zeitfensters, 60 bis 3600.

Gruppe Fallenpfade

Bezeichnung	Schlüssel	Standard	Wirkung
Fallenpfade	`trap.paths`	leer	Eine Anfrage an einen dieser Pfade sperrt die Adresse sofort.

Gruppe Eigene Regeln

Bezeichnung	Schlüssel	Standard	Wirkung
Eigene Regeln	`rules.custom`	leer	Ihre eigenen Regeln, die Anfragen nach Pfad, Query, Browserkennung, Referrer, Methode oder Host blockieren oder protokollieren. Bis zu 100 Regeln, siehe Eigene Regeln.

Gruppe Sperren

Bezeichnung	Schlüssel	Standard	Wirkung
Sperrdauer (Minuten)	`ban.base_minutes`	`15`	Dauer der ersten Sperre einer Adresse, 1 bis 10080.
Längste Sperre (Minuten)	`ban.max_minutes`	`10080`	Die längste Sperre oder Anmeldesperre, 1 bis 525600. Jede wiederholte Sperre innerhalb von 30 Tagen dauert viermal so lange, bis zu dieser Länge.

Gruppe Anmeldeschutz

Bezeichnung	Schlüssel	Standard	Wirkung
Anmeldeschutz	`login.enabled`	`true`	Zählt fehlgeschlagene Anmeldungen, sperrt Adressen und Benutzernamen, wenn die Grenzen erreicht sind.
Fehlgeschlagene Anmeldungen pro Adresse	`login.ip_limit`	`5`	Sperrt eine Adresse nach so vielen fehlgeschlagenen Anmeldungen innerhalb des Zeitfensters, 2 bis 1000.
Fehlgeschlagene Anmeldungen pro Benutzername	`login.user_limit`	`10`	Sperrt einen Benutzernamen nach so vielen fehlgeschlagenen Anmeldungen innerhalb des Zeitfensters, 2 bis 1000.
Zeitfenster für Anmeldungen (Minuten)	`login.window_minutes`	`15`	Länge des Zeitfensters, in dem fehlgeschlagene Anmeldungen gezählt werden, 1 bis 1440.
Sperrdauer für Benutzernamen (Minuten)	`login.lock_minutes`	`15`	Wie lange ein gesperrter Benutzername gesperrt bleibt, 1 bis 1440. Es ist auch die Dauer der ersten Anmeldesperre einer geschützten Administrator-Adresse.
Bei Anmeldung von neuen Adressen warnen	`login.alert_new_address`	`true`	Sendet eine E-Mail, wenn sich ein Administrator von einer Adresse anmeldet, die für diesen Benutzer seit 90 Tagen nicht gesehen wurde.

Gruppe Zwei-Faktor-Authentifizierung

Bezeichnung	Schlüssel	Standard	Wirkung
Zweiten Anmeldeschritt verlangen	`twofactor.required`	`false`	Administratoren müssen mit einer Authenticator-App einen zweiten Anmeldeschritt einrichten. Siehe Zwei-Faktor-Authentifizierung.

Gruppe Ereignisprotokoll

Bezeichnung	Schlüssel	Standard	Wirkung
Protokolleinträge aufbewahren (Tage)	`audit.retention_days`	`90`	Protokolleinträge, die älter sind, werden entfernt, 1 bis 3650.
Adressen im Protokoll kürzen	`audit.anonymize_ip`	`false`	Speichert IPv4-Adressen ohne die letzte ihrer vier Zahlen (auf 0 gesetzt) und behält von IPv6-Adressen nur die ersten 48 Bit.

Gruppe Benachrichtigungen

Bezeichnung	Schlüssel	Standard	Wirkung
Adresse für Benachrichtigungen	`notify.email`	leer	Empfängt Warnungen und Zusammenfassungen. Eine gültige E-Mail-Adresse mit bis zu 254 Zeichen, oder leer, um die Administrator-Adresse von Contao zu verwenden.

Bezeichnung	Schlüssel	Standard	Wirkung
Sofortige Warnungen	`notify.alerts`	`true`	Sendet eine E-Mail bei den schwersten Ereignissen, höchstens eine je Ereignisart und Stunde.
Zusammenfassung per E-Mail	`notify.digest`	`daily`	Sendet eine Zusammenfassung der Sicherheitsereignisse: `off`, `daily` oder `weekly`.

Gruppe Scanner

Bezeichnung	Schlüssel	Standard	Wirkung
Zeitplan der Dateiprüfung	`scanner.schedule`	`daily`	Wie oft die Dateien automatisch geprüft werden: `off`, `daily` oder `weekly`.
Uhrzeit der Dateiprüfung	`scanner.hour`	`3`	Stunde des Tages, in UTC, ab der der geplante Scan starten darf, 0 bis 23.
Geänderte Dateien erkennen	`scanner.baseline`	`true`	Vergleicht Code-Dateien mit dem letzten Scan und meldet geänderte, neue und entfernte Dateien.
Nach Schadcode suchen	`scanner.content`	`true`	Führt eine kleine Zahl allgemeiner Prüfungen auf verdächtigen Code in Dateiinhalten durch.
Auf bekannte Sicherheitslücken prüfen	`scanner.advisories`	`true`	Fragt packagist.org nach bekannten Sicherheitslücken der installierten Pakete. Nur Paketnamen verlassen den Server.
Ausgenommene Pfade	`scanner.exclude`	leer	Pfade relativ zum Projektverzeichnis, die der Scan überspringt.
Größte geprüfte Datei (KB)	`scanner.max_file_kb`	`5120`	Größte Datei, die vollständig gelesen wird, 64 bis 102400. Größere Dateien werden nicht vollständig gelesen.

Gruppe Remote-Scan

Bezeichnung	Schlüssel	Standard	Wirkung
Remote-Scan	`remote.mode`	`off`	Der Modus: `off`, `daemon` (**Lokaler Scan-Dienst (Socket)**), `service` (**Eigener Scan-Dienst**) oder `license` (**Gehosteter Scan-Dienst (Lizenz)**). Siehe Remote-Scan und Lizenz.
Socket des lokalen Scan-Dienstes	`remote.socket`	`/run/ispprotect/scand.sock`	Socket des lokalen Scan-Dienstes, verwendet im Modus `daemon`.
Adresse des Scan-Dienstes	`remote.service_url`	leer	HTTPS-Adresse Ihres eigenen Scan-Dienstes, verwendet im Modus `service`.
Adresse des gehosteten Scan-Dienstes	`remote.hosted_url`	leer	Optionale Überschreibung des eingebauten gehosteten Scan-Dienstes `https://scan.ispprotect.com` (Modus `license`). Normalerweise leer; eine HTTPS-Adresse nur eintragen, um eine andere Installation zu nutzen, etwa zum Testen.
Adresse des Lizenzportals	`remote.portal_url`	leer (nutzt `https://license.ispprotect.com`)	HTTPS-Adresse einer anderen Lizenz-API-Installation. Sie steht auf keiner Seite; überschreiben Sie sie nur bei Bedarf auf der Konsole.
Upload-Grenze je Scan (MB)	`remote.upload_mb`	`200`	Die größte Datenmenge, die ein Scan hochlädt, 0 bis 4096. `0` sendet nur Prüfsummen.
Nicht an den Scan-Dienst gesendete Pfade	`remote.exclude`	leer	Pfade relativ zum Projektverzeichnis, die nie an den Dienst gesendet werden.

Gruppe Sicherheits-Header

Bezeichnung	Schlüssel	Standard	Wirkung
PHP-Version verbergen	`headers.hide_php_version`	`true`	Entfernt den Header `X-Powered-By` aus Antworten.
HTTPS erzwingen (HSTS)	`headers.hsts`	`false`	Sendet `Strict-Transport-Security` bei HTTPS-Anfragen. Schalten Sie es nur ein, wenn HTTPS überall funktioniert.
HSTS-Dauer (Sekunden)	`headers.hsts_max_age`	`31536000`	Wie lange Browser sich merken, nur HTTPS zu verwenden, 300 bis 63072000.
Header Permissions-Policy	`headers.permissions_policy`	leer	Wert des Headers `Permissions-Policy`, bis zu 1024 Bytes ohne Steuerzeichen. Leer sendet keinen Header.

Gruppe OWASP-CRS-Regeln

Die Gruppe steht auf dem eigenen Tab **OWASP-CRS-Regeln**. Die Regeln müssen installiert sein, damit der Modus **Nur protokollieren** oder **Blockieren** wirkt. Siehe OWASP-CRS-Regeln.

Bezeichnung	Schlüssel	Standard	Wirkung
Modus der CRS-Regeln	`waf.mode`	`off`	`off`, `log` oder `block`. Die erste Installation der Regeln setzt `log`. Siehe Mit dem Protokollieren beginnen.
Paranoia-Stufe	`waf.paranoia`	`1`	1 bis 4. Höhere Stufen führen mehr Regeln aus und melden mehr normale Anfragen. Siehe Paranoia-Stufe und Schwelle.
Anomalie-Schwelle	`waf.threshold`	`5`	Punktzahl, ab der eine Anfrage als Angriff gilt (1 bis 100).
Abgeschaltete Regeln	`waf.disabled_rules`	leer	Regelnummern, die nicht ausgeführt werden, eine pro Zeile (bis zu 500). Eine Regelnummer ist eine ganze Zahl, zum Beispiel `942190`.
Geprüfte Größe des Inhalts	`waf.body_limit`	`131072`	Bytes eines Anfrageinhalts, die geprüft werden (1024 bis 1048576). Ein größerer Inhalt wird mit Status 413 abgewiesen, sofern nicht geprüfte Anfragen durchgelassen werden.
Zeitlimit pro Anfrage	`waf.time_budget_ms`	`200`	Höchstzahl an Millisekunden, die die Regeln für eine Anfrage brauchen dürfen (5 bis 10000).
Anfragen durchlassen, die nicht vollständig geprüft werden können	`waf.pass_uninspected`	false	Lässt Anfragen durch, die zu groß, zu langsam oder nicht lesbar sind. Sie werden trotzdem aufgezeichnet. Siehe Anfragen, die nicht vollständig geprüft werden können.

Kommandozeile

Alle Befehle beginnen mit `vendor/bin/contao-console` und laufen im Projektverzeichnis, als der Benutzer, dem die Dateien gehören. Die Beispiele lassen das Präfix weg, wenn sie nur den Namen des Befehls zeigen.

Der Exit-Code ist bei Erfolg 0. Exit-Code 1 bedeutet, dass der Befehl lief und ein Problem gefunden hat. Exit-Code 2 bedeutet, dass ein Argument oder eine Option nicht gültig war. Anfragen über die Konsole werden von der Firewall nicht geprüft.

Liste der Befehle

Befehl	Was er tut
`ispprotect:status`	Zeigt den Zustand des Schutzes
`ispprotect:checkup`	Führt den Sicherheits-Checkup aus
`ispprotect:scan`	Führt einen Dateiscan aus
`ispprotect:findings`	Listet Funde auf und akzeptiert sie
`ispprotect:events`	Zeigt das Ereignisprotokoll
`ispprotect:ip:list`	Listet die Adresslisten und Sperren auf
`ispprotect:ip:add`	Fügt einer Liste eine Adresse hinzu
`ispprotect:ip:remove`	Entfernt eine Adresse aus allen Listen
`ispprotect:unlock`	Hebt eine Anmeldesperre auf
`ispprotect:settings:get`	Zeigt Einstellungen
`ispprotect:settings:set`	Ändert eine Einstellung
`ispprotect:maintenance`	Führt die regelmäßigen Arbeiten aus
`ispprotect:remote`	Betreut den Remote-Scan und die Lizenz
`ispprotect:uninstall`	Entfernt die Daten des Bundles

Status und Checkup

`ispprotect:status` zeigt den Firewall-Modus, den Anmeldeschutz, die Zahl der aktiven Sperren, die offenen Funde, den letzten vollständigen Scan und die Zahl der Ereignisse der letzten 24 Stunden mit der Stufe Warnung oder höher. Er endet immer mit Exit-Code 0.

`ispprotect:checkup` gibt die Punktzahl und jede Prüfung mit ihrem Status aus. Er endet mit Exit-Code 1, wenn mindestens eine Prüfung den Status **Problem** hat, sodass Sie ihn für die Überwachung nutzen können.

Scan und Funde

```
ispprotect:scan [--budget=SECONDS] [--no-wait]
```

Startet einen Scan oder setzt einen laufenden fort und arbeitet in Schritten von 5 Sekunden, bis er fertig ist.

Option	Bedeutung
`--budget=SECONDS`	Hält nach so vielen Sekunden an, höchstens 86400. Der Scan wird beim nächsten Mal fortgesetzt. Ein Wert, der keine Zahl oder zu groß ist, ergibt Exit-Code 2.

Option	Bedeutung
`--no-wait`	Wartet nicht auf einen Scan, den ein anderer Prozess ausführt.

Exit-Code 1 bedeutet, dass der Scan fehlgeschlagen ist oder dass nach seinem Ende offene Funde der Stufe Mittel oder Hoch existieren.

```
ispprotect:findings [--all] [--accept=ID] [--accept-all]
```

Listet die offenen Funde auf, höchstens 500 Zeilen. `--all` schließt Funde ein, die nicht offen sind. `--accept=ID` akzeptiert die geänderte, neue oder entfernte Datei eines Fundes als neue Basis, `--accept-all` tut das für jeden solchen Fund. Ein Fund, der sich seit dem Auflisten geändert hat oder nicht existiert, ergibt Exit-Code 1. Eine ungültige ID ergibt Exit-Code 2. Ohne Akzeptieren-Option ist der Exit-Code 1, wenn offene Funde der Stufe Mittel oder Hoch existieren, bei einer sauberen Liste ist er 0.

Ereignisprotokoll

```
ispprotect:events [--type=NAME] [--since=MINUTES|DATE] [--limit=N]
```

Option	Bedeutung
`--type`	Nur diese Art von Ereignis
`--since`	Ereignisse der letzten angegebenen Minuten oder seit einem Datum mit Uhrzeit in UTC
`--limit`	Zahl der Ereignisse, 1 bis 500, Standard 50

Adressen

```
ispprotect:ip:list
ispprotect:ip:add KIND ADDRESS [--minutes=N] [--reason=TEXT]
ispprotect:ip:remove ADDRESS
```

`ispprotect:ip:list` zeigt die Liste der erlaubten Adressen, die Liste der gesperrten Adressen und die aktiven Sperren.

`ispprotect:ip:add` nimmt die Art `allow`, `block` oder `ban` und eine Adresse oder einen Bereich in CIDR-Schreibweise. `--minutes` (1 bis 5256000) legt die Dauer einer Sperre fest, `--reason` eine Notiz. Eine ungültige Art, Adresse oder Zahl ergibt Exit-Code 2. Eine Adresse, die nicht gespeichert werden kann, etwa eine Loopback-Adresse, ergibt Exit-Code 1.

`ispprotect:ip:remove` entfernt die Adresse aus jeder Liste, einschließlich der Sperren. Eine Adresse, die auf keiner Liste steht, ergibt Exit-Code 1, eine ungültige Adresse Exit-Code 2.

Anmeldesperren

```
ispprotect:unlock [USERNAME] [--address=IP] [--realm=backend|frontend]
```

Geben Sie genau eines von Benutzername und `--address` an, sonst ergibt sich Exit-Code 2. Eine ungültige Adresse ergibt Exit-Code 2. Wenn nichts gesperrt war, ist der Exit-Code 1. Siehe Anmeldeschutz. Der Befehl hebt keine Firewall-Sperre auf und setzt den Zähler falscher Codes des zweiten Schritts für einen Benutzernamen nicht zurück.

Einstellungen

```
ispprotect:settings:get [KEY]
ispprotect:settings:set KEY VALUE
```

Ein unbekannter Schlüssel ergibt Exit-Code 2. `settings:set` liest den Wert als JSON, wenn es möglich ist, sonst als Text. Ein abgelehnter Wert ergibt Exit-Code 2 und den Grund. Siehe Einstellungsreferenz.

Wartung

`ispprotect:maintenance` führt die regelmäßigen Arbeiten aus: geplante Scans, Entfernen alter Protokolleinträge, E-Mails, Erneuern der Lizenz. Er endet mit Exit-Code 1, wenn ein Schritt fehlgeschlagen ist. Normalerweise überlassen Sie ihn dem Cron, siehe Zeitplanung mit Cron.

Befehle für den Remote-Scan

```
ispprotect:remote [ACTION]
```

Ohne Aktion zeigt er den Status. Die Aktionen sind:

Aktion	Was sie tut
`status`	Zeigt Modus, Verbindung und den letzten Scan
`test`	Testet die Verbindung
`token:set`	Speichert den Zugangstoken
`token:clear`	Entfernt den Zugangstoken
`connect`	Verbindet einen Lizenzschlüssel
`refresh`	Erneuert den Zugang einer verbundenen Lizenz
`disconnect`	Gibt die Lizenz frei und entfernt ihre Daten

Der Zugangstoken und der Lizenzschlüssel werden nie als Argumente übernommen, sodass sie nicht in der Prozessliste oder im Verlauf der Shell erscheinen. Leiten Sie sie per Pipe ein oder geben Sie sie an der verdeckten Eingabeaufforderung ein:

```
printf '%s' "$TOKEN" | vendor/bin/contao-console ispprotect:remote token:set
```

Ein zusätzliches Argument oder eine unbekannte Aktion ergibt Exit-Code 2, ebenso ein leeres oder zu langes Geheimnis. Ist keine verdeckte Eingabe möglich, ist der Exit-Code 1. Ein fehlgeschlagener Test, eine fehlgeschlagene Verbindung, Erneuerung oder Speicherung ergibt Exit-Code 1, ebenso `connect`, wenn bereits eine Lizenz verbunden ist. `disconnect` endet mit Exit-Code 0, auch wenn das Portal nicht erreicht werden konnte; die lokalen Daten werden in jedem Fall entfernt. Siehe Remote-Scan und Lizenz.

Entfernen

`ispprotect:uninstall` ist in Das Bundle entfernen beschrieben.

Zurück ins System und Fehlerbehebung

Sie sind von der Firewall gesperrt oder blockiert

Die Firewall weist Anfragen einer gesperrten oder blockierten Adresse ab, auch fürs Backend. Anfragen auf der Konsole sind nicht betroffen, sodass Sie es dort beheben können:

```
vendor/bin/contao-console ispprotect:ip:list
vendor/bin/contao-console ispprotect:ip:remove 203.0.113.7
```

`ispprotect:ip:list` zeigt die Sperren und Listen, `ispprotect:ip:remove` entfernt die Adresse aus allen. Um die Firewall kurz auszuschalten, setzen Sie den Modus auf `off`:

```
vendor/bin/contao-console ispprotect:settings:set firewall.mode off
```

Schalten Sie sie danach mit `on` wieder ein. Siehe Firewall.

Wenn die ganze Website für alle Besucher unerreichbar ist, prüfen Sie zuerst, ob die Adresse, die das Bundle sieht, die des Besuchers ist, siehe Hinter einem Reverse-Proxy oder CDN.

Sie sind vom Anmeldeschutz gesperrt

Nach zu vielen fehlgeschlagenen Anmeldungen ist der Benutzername oder die Adresse gesperrt. Heben Sie die Sperre auf dem Tab **Anmeldeschutz** von einem anderen Browser oder einer anderen Adresse aus auf, oder auf der Konsole:

```
vendor/bin/contao-console ispprotect:unlock USERNAME
vendor/bin/contao-console ispprotect:unlock --address=203.0.113.7
```

Fügen Sie `--realm=backend` oder `--realm=frontend` hinzu, um den Befehl auf einen Bereich zu beschränken. Eine Sperre endet von selbst nach **Sperrdauer für Benutzernamen (Minuten)**. Siehe Anmeldeschutz.

Ein Fallenpfad oder eine Regel blockiert die falschen Anfragen

Ein zu weit gefasster Fallenpfad oder eine zu weite eigene Regel kann Besucher sperren oder blockieren, auch Sie. Entfernen Sie sie auf der Konsole:

```
vendor/bin/contao-console ispprotect:settings:set trap.paths '[]'
vendor/bin/contao-console ispprotect:settings:set rules.custom '[]'
```

Heben Sie dann Ihre eigene Sperre auf, wie oben beschrieben. Um eine Regel zuerst zu testen, schalten Sie **Firewall-Modus** auf **Nur protokollieren**, was nur aufzeichnet, was abgewiesen würde.

Die Zwei-Faktor-Authentifizierung ist vorgeschrieben und ein Administrator kann sie nicht nutzen

Schalten Sie **Zweiten Anmeldeschritt verlangen** auf dem Tab **Anmeldeschutz** aus, oder auf der Konsole:

```
vendor/bin/contao-console ispprotect:settings:set twofactor.required false
```

Contaos eigene Option `contao.security.two_factor.enforce_backend` wird dadurch nicht geändert. Siehe Zwei-Faktor-Authentifizierung.

Die Seiten melden fehlende Tabellen

Die Seite meldet, dass die Tabellen fehlen, wenn die Datenbank nach der Installation nicht aktualisiert wurde. Führen Sie `contao:migrate` aus oder nutzen Sie den Contao Manager, siehe Installation und erste Schritte und Wenn die Tabellen fehlen.

Die Seiten des Bundles haben kein Layout

Die Assets sind nicht installiert. Führen Sie aus:

```
vendor/bin/contao-console assets:install
```

Alle Besucher haben dieselbe Adresse

Das Bundle sieht nur die Adresse Ihres Proxys oder CDN. Tragen Sie dessen Adressen in der Contao-Konfiguration als vertrauenswürdige Proxys ein, siehe Hinter einem Reverse-Proxy oder CDN. Der Checkup meldet eine falsche Einstellung als „Vertrauenswürdige Proxys passen zum tatsächlichen Aufbau“.

Scans oder E-Mails finden nicht statt

Geplante Scans, die Zusammenfassungen per E-Mail und das Entfernen alter Protokolleinträge brauchen den Cron von Contao. Prüfen Sie, dass der System-Cron den Contao-Cron jede Minute aufruft, siehe Zeitplanung mit Cron. Sie können die regelmäßigen Arbeiten auch von Hand ausführen:

```
vendor/bin/contao-console ispprotect:maintenance
```

Ein Scan, der nicht voranzukommen scheint, wird bei jedem Lauf in Schritten fortgesetzt. `ispprotect:scan` beendet ihn auf der Konsole.

Wenn keine E-Mails ankommen, prüfen Sie **Adresse für Benachrichtigungen**, den Mail-Transport von Contao und die Ereignisse der Art „Systemhinweis“ auf dem Tab **Ereignisse**. Der Checkup sagt Ihnen, wenn kein Empfänger existiert. Siehe Ereignisprotokoll und Benachrichtigungen.

Der Remote-Scan oder die Lizenz funktioniert nicht

- Klicken Sie auf dem Tab **Scanner** auf **Verbindung testen**. Der Bereich **Remote-Scan** zeigt den Grund einer Ablehnung, siehe Remote-Scan und Lizenz.
- Zeigt der Lizenzbereich ein Problem, beheben Sie die Ursache und klicken Sie auf **Jetzt prüfen**, oder führen Sie `ispprotect:remote refresh` aus.
- Wurde das Application Secret von Contao geändert, können der gespeicherte Token und die Lizenzdaten nicht mehr gelesen werden. Geben Sie den Token oder den Lizenzschlüssel erneut ein.
- Keine Schaltfläche **Verbinden**: Prüfen Sie, ob die eingebaute Lizenz-API-Adresse durch einen ungültigen Wert von `remote.portal_url` überschrieben wurde; siehe Remote-Scan und Lizenz.

Etwas anderes

Der Tab **Ereignisse** zeigt, was das Bundle getan hat und warum. Filtern Sie nach der Adresse oder dem Benutzernamen, die das Problem haben. Fallen die Seiten selbst aus, lässt das Bundle Anfragen durch, statt sie zu blockieren: Eine ausfallende Firewall legt die Website nicht lahm. Der Fehler steht im Protokoll von Contao.

Die OWASP-CRS-Regeln weisen eine normale Anfrage ab

Die OWASP-CRS-Regeln können eine normale Anfrage abweisen (ein Fehlalarm). Die Anfrage wird mit Status 403 beantwortet, bei einer nicht vollständig prüfbaren Anfrage mit 413 oder 400. Den Hintergrund finden Sie unter OWASP-CRS-Regeln.

1. Öffnen Sie den Tab **Ereignisse** und suchen Sie den Eintrag **Anfrage von der Firewall abgewiesen** (oder **Anfrage von der Firewall protokolliert**, im Modus **Nur protokollieren**). Notieren Sie die Regelnummern in den Details.
2. Schalten Sie die falsche Regel ab: Tragen Sie ihre Nummer in dem Formular **Eine Regel abschalten** auf dem Tab **OWASP-CRS-Regeln** ein. Eine abgeschaltete Regel läuft für keine Anfrage mehr, schalten Sie daher nur die Regel ab, die das Problem verursacht hat.
3. Scheitert das Speichern von sehr viel Inhalt mit Status 413 und der Nummer `200101`, erhöhen Sie **Geprüfte Größe des Inhalts** (`waf.body_limit`), zum Beispiel auf 524288.
4. Brechen Anfragen mit der Nummer `200100` ab, erhöhen Sie **Zeitlimit pro Anfrage** (`waf.time_budget_ms`) oder schalten Sie die Nummer `200100` ab. Programmcode in einem Formularfeld (etwa 20 bis 40 KB) kann das voreingestellte Limit von 200 Millisekunden aufbrauchen. Anfragen, die mit der Nummer `200005` abgelehnt werden (selten überschreitet ein langes Feld mit Programmcode die Grenzen von PHP für reguläre Ausdrücke), behandeln Sie genauso: Schalten Sie `200005` ab oder lassen Sie Anfragen durch, die nicht vollständig geprüft werden können.

Um die Ursache zu finden, ohne Besucher auszusperren, stellen Sie **Modus der CRS-Regeln** auf **Nur protokollieren**: Anfragen werden dann nur aufgezeichnet.

Können Sie sich nicht mehr anmelden, schalten Sie die CRS-Regeln auf der Konsole ab, melden Sie sich an und schalten Sie danach die Regel ab:

```
vendor/bin/contao-console ispprotect:settings:set waf.mode off
```

Datenschutz und externe Dienste

Das Bundle läuft auf Ihrem Server und speichert seine Daten in Ihrer Datenbank. Dieses Kapitel listet alles auf, was den Server verlässt.

Kontakt zu externen Diensten

Dienst	Wann	Was gesendet wird
packagist.org	**Auf bekannte Sicherheitslücken prüfen** ist eingeschaltet	Die Namen der installierten Pakete. Keine Versionen: Sie werden auf Ihrem Server verglichen.
Scan-Dienst	**Remote-Scan** ist nicht **Aus**	Siehe unten.
OWASP-CRS-Regeln (GitHub)	Sie klicken auf **Regeln installieren** oder **Regeln aktualisieren**	Nur die Download-Anfrage für das Regelarchiv des CRS-Projekts, an `github.com` und den Download-Host, auf den GitHub weiterleitet. Nichts über Ihre Website, deren Besucher oder deren Anfragen. Der Download wird mit einer im Bundle eingebauten Prüfsumme verglichen.
Lizenzportal	Im Modus **Gehosteter Scan-Dienst (Lizenz)**, wenn Sie eine Lizenz verbinden, erneuern oder trennen, und wenn Sie das Bundle entfernen	Siehe unten.

Das Bundle nimmt keinen weiteren Kontakt zu externen Diensten auf. Es sendet keine Nutzungsdaten und keine Daten an seine Autoren.

Scan-Dienst

Mit **Lokaler Scan-Dienst (Socket)** verlässt nichts den Server. Mit **Eigener Scan-Dienst** sendet das Bundle an die Adresse, die Sie eintragen, und mit **Gehosteter Scan-Dienst (Lizenz)** an den ISPProtect-Scan-Dienst unter `https://scan.ispprotect.com`. In beiden Modi sendet es für jede Code-Datei die SHA-256-Prüfsumme und den Dateinamen oder nur `file.` mit der Endung. Es lädt Dateien hoch, die der Dienst nicht kennt, bis zu **Upload-Grenze je Scan (MB)**. Dateien mit Geheimnissen, etwa Schlüssel, `.env`-Dateien und Datenbank-Dumps, werden nie gesendet. Einige PHP-Konfigurationsdateien werden nur in geschwärzter Form gesendet, wobei alle Zeichenketten, Zahlen und Kommentare ersetzt sind. Die Liste steht unter Remote-Scan und Lizenz.

Lizenzportal

Aktion	Gesendete Daten
Verbinden	Der Lizenzschlüssel, der Produktname, eine zufällige Installations-ID, der Hostname der Website, die Plattform `contao` und die Version des Bundles
Erneuern	Der Lizenzschlüssel, die Installations-ID, der Hostname und die Version
Trennen, Entfernen	Der Lizenzschlüssel und die Installations-ID

Die Installations-ID ist ein zufälliger Wert, den das Bundle erzeugt. Lizenzanfragen gehen an `https://license.ispprotect.com`, nicht an die Konto-Konsole unter `https://console.ispprotect.com`. Sie warten 15 Sekunden, beim Entfernen des Bundles 5 Sekunden.

Daten in Ihrer Datenbank

- Das Ereignisprotokoll enthält Ereignisse mit Zeit, Adresse, Benutzername und Details. E-Mail-Adressen werden nur für Backend-Benutzer gespeichert. Einträge werden nach **Protokolleinträge aufbewahren (Tage)** entfernt. **Adressen im Protokoll kürzen** kürzt Adressen vor dem Speichern: bei einer IPv4-Adresse wird die letzte der vier Zahlen auf 0 gesetzt, von einer IPv6-Adresse werden nur die ersten 48 Bit behalten.

- Die Zähler des Anmeldeschutzes enthalten Adressen und Benutzernamen. Sperren geschützter Administrator-Adressen enthalten nur einen Hash der Adresse.
- Konten von Backend-Benutzern, Gruppen und Mitgliedern werden nur mit Feldnamen protokolliert, ohne Werte.
- Passwörter und Passwort-Hashes werden nie gelesen oder gespeichert.
- Der Zugangstoken und der Lizenzschlüssel werden verschlüsselt gespeichert, siehe Remote-Scan und Lizenz.

Wenn Sie das Bundle entfernen, werden alle diese Daten gelöscht, siehe Das Bundle entfernen.

Das Bundle entfernen

Entfernen Sie das Bundle in zwei Schritten: zuerst seine Daten, dann den Code.

Die Daten löschen

```
vendor/bin/contao-console ispprotect:uninstall
```

Der Befehl tut Folgendes:

1. Ist ein Lizenzschlüssel gespeichert, gibt er die Website beim Lizenzportal frei und sagt, ob das geklappt hat. Konnte das Portal nicht erreicht werden, zählt die Website weiter zum Website-Limit der Lizenz, bis Sie sie in Ihrem Konto im Lizenzportal freigeben.
2. Er löscht alle Tabellen des Bundles: Einstellungen, Adresslisten, Sperren, Zähler, Ereignisprotokoll, Scans, Dateien, Funde, die Tabelle für Zwei-Faktor-Daten und die Daten des Remote-Scans.
3. Er leert den Cache-Pool des Bundles.

Er entfernt keine Dateien und ändert nichts sonst in Contao. Der Befehl fragt nach einer Bestätigung. Ohne Terminal braucht er `--force` (oder `-f`) und bricht sonst mit Exit-Code 1 ab. Lehnen Sie ab, löscht er nichts und endet ebenfalls mit Exit-Code 1.

> Das Löschen kann nicht rückgängig gemacht werden. Danach sind das Ereignisprotokoll und die Funde weg.

Führen Sie zwischen den beiden Schritten nicht `contao:migrate` aus. Solange das Bundle installiert ist, legt es die leeren Tabellen wieder an.

Den Code entfernen

```
composer remove ispprotect/contao-web-security-bundle
```

Leeren Sie danach den Cache von Contao. Sie können das Bundle auch mit dem Contao Manager entfernen.