UNITED SECURITY PROVIDERS
ZERO TRUST UNIVERSE

# PENTESTING IM ZEITALTER VON KI

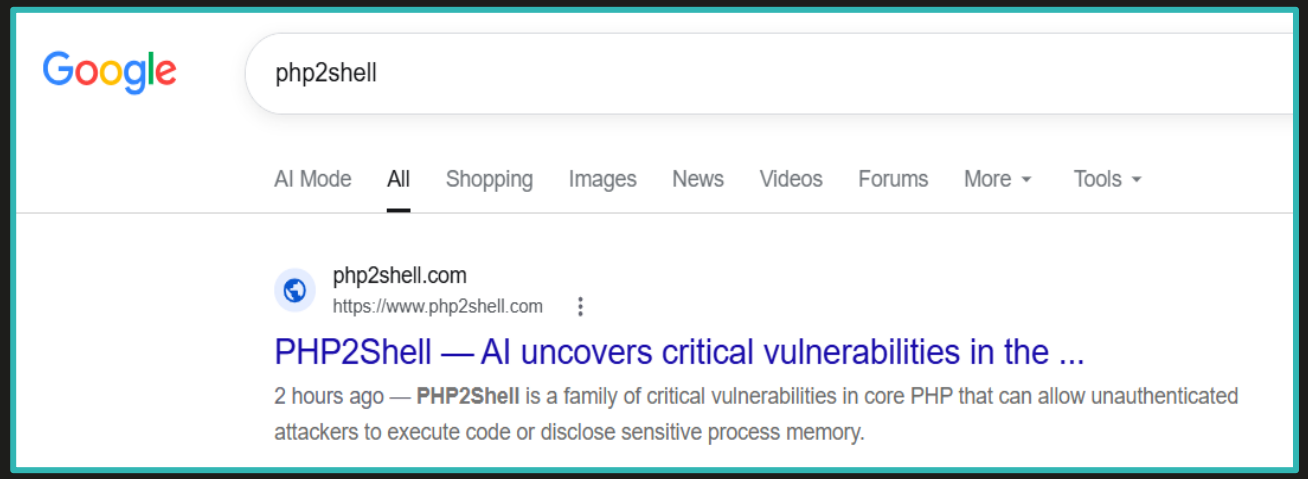
## WAS AUF DER PACKUNG STEHT UND WAS DRIN IST.



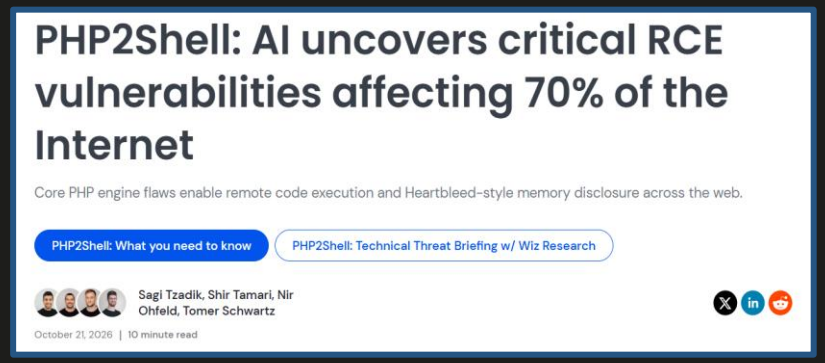
30.10.2026

LEA ZIMMERLI

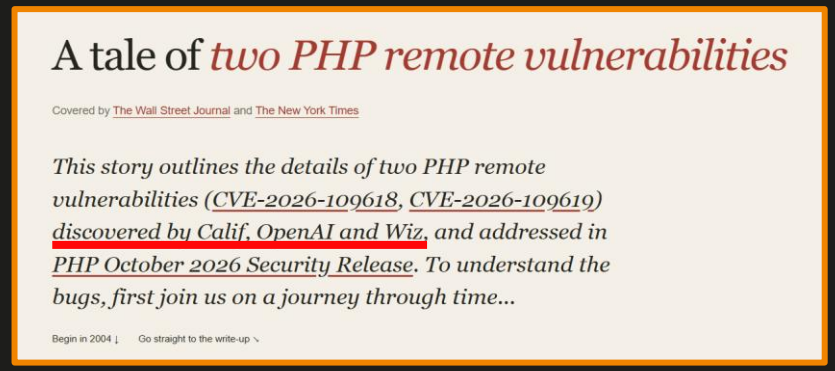
# PHP2SHELL




Source: [1]




Source: [3]




Source: [5]

## Die Timeline

**3. Aug.**
Ryan Austin von Calif findet die RCE-Pfade.

**11.-14. Aug.**
Er meldet den Fehler und einen funktionierenden RCE-Proof-of-Concept an PHP.

**19.-24. Aug.** Wiz findet unabhängig dieselbe Fehlerfamilie mit Wiz Atlas, Gemini 4 Argon, und GPT-5.6 Sol

© UNITED SECURITY PROVIDERS AG

# DAS POTENZIAL VON AI PENTESTING

## #1

Zum ersten Mal überhaupt, hat ein autonomer Penetrationstester, XBOW, den ersten Platz in der HackerOne US-Rangliste erreicht.[6]

132/1060: überprüft und behoben

417/1060: Duplikate oder informativ

Ca 51% valide Findings nachdem sie manuell überprüft wurden

## 2 von 11

ARTEMIS (Stanford, CMU, Gray Swan) schlägt in einem Live-Netz mit ca. 8'000 Hosts 9 von 10 Menschen.[7]

80% der Menschen haben eine kritische RCE-Schwachstelle gefunden, die ARTEMIS nicht gefunden hat.

## 82 %

gültige Meldungen bei ARTEMIS.

Laufkosten ab CHF 14* pro Stunde, Profis ca. CHF 48.

Die Konfiguration, welche 82% gültige Meldungen hatte, kostet CHF 47, die für CHF 14 nur 55%.

**WIR MÜSSEN KI-PENTESTING NUR EINSCHALTEN, DANN LÄUFTS SCHON.(?)**

*Preise in USD, umgerechnet zu CHF 0.80.

© UNITED SECURITY PROVIDERS AG

# DREI STUFEN, EIN ETIKETT

## STUFE 1: KI-SCAN

- Tool scannt automatisch.
- Kein Ausnutzen, viele False Positives.
- Kein Pentest im Audit-Sinn, aber gute Basis-Hygiene.

**PREIS**

ca. CHF 31–151 pro Monat [8]

**Fällt als Pentest-Ersatz raus**

## STUFE 2: KI-UNTERSTÜTZT

- Mensch führt, KI hilft bei Recon, Code und Bericht.
- Beispiel: PHP2Shell.
- Validierte Funde, ein Name steht hinter dem Bericht.

**PREIS**

CHF ≈15’000

Schätzung aus unserer Erfahrung,
4 verschiedene Rollen, 2 Tenants, OWASP Web&API

## STUFE 3: KI-AGENT

- Agent plant und führt Angriffsschritte selbst aus.
- Mensch richtet ein, prüft und gibt frei.
- Mehrere Kaufmodelle unter einem Etikett.

**PREIS**

Alles von CHF 32 [9] pro Monat
bis CHF 24’000 [10] pro Test

Preise in USD, umgerechnet zu CHF 0.80.

© UNITED SECURITY PROVIDERS AG

# AGENT IST NICHT GLEICH AGENT

## SELBST BETRIEBENES ABO

**BEISPIEL**

Penligent Pro:

**72[14] CHF pro Monat**

Vgl. Vor einer Woche:
**32[9] CHF pro Monat**,

**DIE FALLE**

Eine Lizenz ist kein fertiger Service. Betrieb und Prüfung bleiben bei Ihnen.

## AUTONOMER SERVICE

**BEISPIEL**

pwn.ai:
**2’400 bis 4’800[11] CHF pro Test.**

XBOW bis Juli 2026:
**3’200 bis 6’400[12] CHF pro Test**, heute auf Anfrage.

**DIE FALLE**

Annehmen, jede Anwendung sei gleich komplex. Zuständigkeit der Aufgabenbereiche unterschiedlich.

## HYBRID ENGAGEMENT

**BEISPIEL**

Stingrai Hybrid:
**5’440[15] CHF pro Test**

Synack:
**8’226[16] CHF pro Test**

**DIE FALLE**

Das Hybrid-Engagement mit einem Agent-Abo vergleichen und vom Abo denselben Schutz erwarten.

© UNITED SECURITY PROVIDERS AG

# WO DER AGENT IM PROZESS SITZT

| | SCOPING | SETUP | TESTLAUF | VALIDIERUNG | BERICHT | DEBRIEFING |
|---|---|---|---|---|---|---|
| Selbst betriebenes Abo | Kunde | Kunde | Agent | Kunde | Kunde | Kunde |
| Autonomer Service | Kunde + Anbieter | Kunde + Anbieter | Agent | Kunde + Anbieter | Kunde + Anbieter | Kunde |
| Hybrid-Engagement | Kunde + Anbieter | Kunde + Anbieter | Agent + Tester | Anbieter | Anbieter | Anbieter |

**Der Agent deckt nur den Testlauf ab.**

Die Kosten für den Kunden liegen in der Vor- und Nachbearbeitung vom Agent-Test.

© UNITED SECURITY PROVIDERS AG

# SO RECHNEN SIE

PREIS ANBIETER FÜR AGENT (SERVICE) + AUFWAND KUNDE: TAGE × TAGESSATZ = GESAMTKOSTEN

| Phase | Welche Aufwände gibt es? | Tage |
|---|---|---|
| Scoping | Umfang festlegen (Anwendung, Rollen, Mandanten, APIs, Umgebungen)? | 0.25 |
| | Ausschlüsse und bekannte fragile Funktionen festlegen | 0.1 |
| | Abrechnungseinheit und Preisgrenzen definieren (Anwendung, Credits, Überschreitung)? | 0.1 |
| | Abschluss, Stoppbedingungen und Ausgabenlimit festlegen | 0.1 |
| Setup | Testkonten erstellen | 0.5 |
| | Seed-Daten erstellen | 0.5 |
| | Testumgebung aufsetzen | 1 |
| | Zugangswege einrichten (VPN, Jump Host, IP-Freigabe, MFA)? | 0.5 |
| | Agenten konfigurieren | 1 |
| Testlauf | Test überwachen und stoppen bei Problemen | 0.25 |
| Validierung | Funde prüfen (Duplikate, Fehlalarme) | 1 |
| Bericht & Debrief. | Bericht erstellen, Besprechung der Resultate | 0.75 |

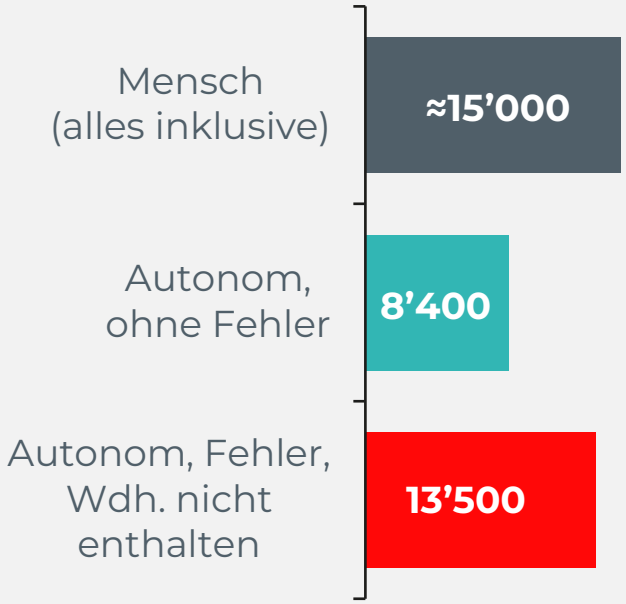
Alle Tage sind Annahmen für einen autonomen Service

© UNITED SECURITY PROVIDERS AG

# RECHENBEISPIEL BUCHUNGSPLATTFORM

Preis des Anbieters pwn.ai: 2’400-4’800 ≈ 3’600

| Schritt | Wer? | Tage | CHF |
|---|---|---|---|
| **1 Aufwand, den der Kunde immer hat** | | | |
| Umfang festlegen (Anwendung, Rollen, Mandanten, APIs, Umgebungen) | **Kunde** | 0.25 | 250 |
| Ausschlüsse und bekannte fragile Funktionen festlegen | **Kunde** | 0.1 | 100 |
| Abrechnungseinheit und Preisgrenzen definieren | **Kunde** | 0.1 | 100 |
| Abschluss, Stoppbedingungen und Ausgabenlimit festlegen | **Kunde** | 0.1 | 100 |
| Testkonten erstellen | **Kunde** | 0.5 | 500 |
| Seed-Daten erstellen | **Kunde** | 0.5 | 500 |
| Testumgebung aufsetzen | **Kunde** | 1 | 1’000 |
| Agent | **Kunde** | - | 3’600 |
| **2 Variabel: Ist es im Preis enthalten?** | | | |
| Wer richtet Zugangswege ein (VPN, Jump Host, IP-Freigabe, MFA)? | **Kunde** | 0.5 | 500 |
| Agenten konfigurieren | **Anbieter** | 1 | 0 |
| Test überwachen und bei Problemen stoppen | **Anbieter** | 0.25 | 0 |
| Funde prüfen (Duplikate, Fehlalarme) | **Kunde** | 1 | 1’000 |
| Bericht erstellen (Stingrai: same day results) | **Kunde** | 0.5 | 500 |
| Besprechung der Resultate | **Kunde** | 0.25 | 250 |
| **Gesamtkosten ohne Fehler** | | | **8’400** |
| **3 Fehler: Wer löst ihn, ist die Wiederholung enthalten?** | | | |
| Fehler aufgetreten? Wer löst ihn? | **Kunde** | 1.5 | 1500 |
| Wiederholung im Angebot enthalten? (Stingrai: automated rerun) | **Nein** | | 3’600 |
| Zweiten Lauf prüfen | **Anbieter** | 0.25 | 0 |
| **Gesamtkosten mit Fehler, Wiederholung nicht enthalten** | | | **13’500** |




Alle Tage sind Annahmen.
Interner Tagessatz CHF 1’000.

© UNITED SECURITY PROVIDERS AG

# DIE STUFEN IM VERGLEICH

| STUFE | PREIS (CHF) | VORTEILE | NACHTEILE | RISIKO | UMFANG |
|---|---|---|---|---|---|
| **KI-Scan** | 31-151 pro Monat | günstig, wiederholbar, breit | viele False Positives, kein Nachweis | Scheinsicherheit | bekannte Schwachstellen |
| **KI-unterstützt (Mensch)** | ≈15’000 | Tiefe, Geschäftslogik, validiert | teuer, Moment-aufnahme | Verpasste Schwachstellen | ganze Anwendung inkl. Rollen |
| **Agent-Service** | 8’400-13’500 | schnell, wiederholbar | Fehlerläufe, Prüfaufwand, blinde Flecken | stiller Ausfall, Produktions-risiko, Daten beim Modell-anbieter, verpasste Schwachstellen | ein Target, Rollen begrenzt |

© UNITED SECURITY PROVIDERS AG

# GRENZEN AUTONOMER AGENTEN

## GESCHÄFTSLOGIK

Ungeschriebene Regeln kennt der Agent nicht und kann sie demnach nicht beurteilen.

## FAST NUR WEB

Meist auf Web-Anwendungen und APIs beschränkt.

## BLINDE FLECKEN IM SETUP

Einmal konfiguriert, selten wieder geprüft.

## BEISPIEL: GESCHÄFTSLOGIK

**Regel:** Rückerstattung nur bei Storno mehr als 24 Stunden vor dem Termin.

**Fehler:** Wer nach der Stornierung neu bucht, behält die Rückerstattung.

Der Agent kennt die Regel nicht, es sei denn, jemand schreibt sie auf.

## BEISPIEL: BLINDER FLECK IM SCOPE

Ein Target wird ausgeschlossen weil darauf kritische Dienste laufen

Die App im Scope sendet aber bei jeder Stornierung eine Anfrage dorthin.

Der Agent testet diese Verbindung nie weil sie nicht im Scope ist. Beim Retest bleibt die Lücke ebenfalls unsichtbar.

© UNITED SECURITY PROVIDERS AG

# PHP2SHELL

## WAS EIN AGENT EMPFIEHLT

**Frage:** «Mein System ist von PHP2Shell betroffen, was soll ich tun?”

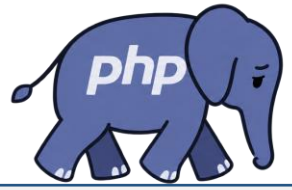
**Grok, Claude, ChatGPT:** Patchen. Überwachen. Regelmässig scannen.

## WAS EIN MENSCH EMPFIEHLT

**Warum läuft ein 22 Jahre alter Interpreter, teils ohne Support, am Internet?**

Veraltete Stacks ablösen, Angriffsfläche verkleinern, Worker isolieren, Migration planen.






**~70 %** der internetnahen PHP-Hosts laufen auf PHP Version 8.1 und älter, für die es keinen Patch gibt.[13]

**Der Agent liefert den Fund. Die Empfehlung braucht ein Urteil.**

© UNITED SECURITY PROVIDERS AG

# WIE USP KI IM PENTEST EINSETZT: ISFET

## WAS ISFET IST

### Ein KI-Agent für die Aufklärung. Kein Ersatz für den Pentester.

- Prototyp mit festen Phasen, autorisiertes Ziel, wenig menschliche Eingabe.
- Modell austauschbar (GPT-5*, Claude, DeepSeek, online oder lokal, etc.).

## WO DER MEHRWERT LIEGT

### Nicht das schnelle Abarbeiten von Tools wie nmap oder nuclei, sondern die Denkschicht darüber.

- Funde verschiedener Werkzeuge verknüpfen
- Erklärung eines leeren Scans. Stille ist kein Beweis für Sicherheit.
- Priorisieren:  Aus viel Rauschen wird eine kurze Liste für den Menschen.

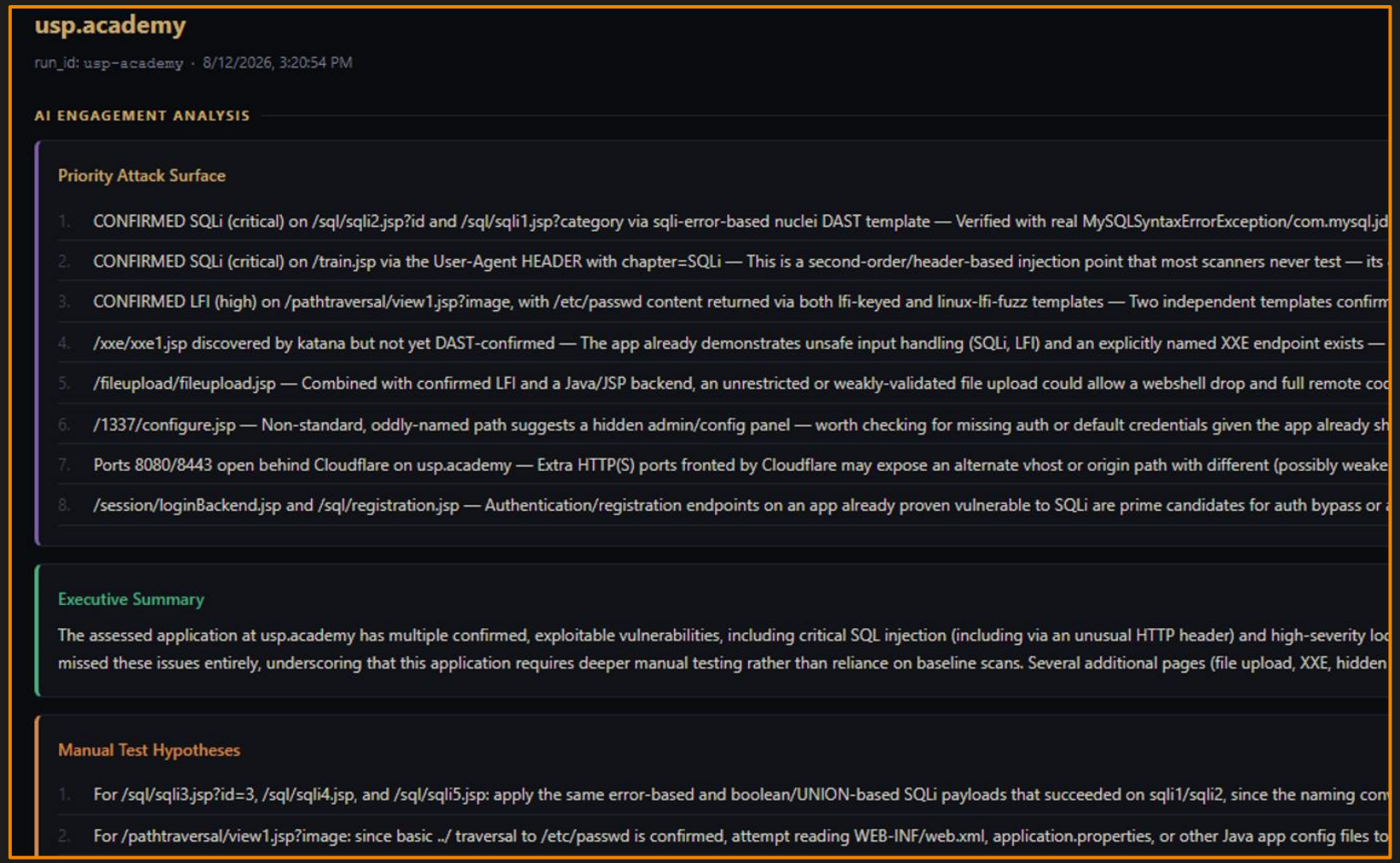
## DER BEWEIS

SQL-Injection im User-Agent-Header (kritisch). Der passive Scan hat sie nicht gefunden.

Quelle: eigener Prototyp «Isfet», Testlauf an einer Trainingsanwendung. Entspricht Stufe 2: Der Mensch führt, die KI unterstützt.

© UNITED SECURITY PROVIDERS AG

# WIE USP KI IM PENTEST EINSETZT: ISFET




Quelle: eigener Prototyp «Isfet», Testlauf an einer Trainingsanwendung. Entspricht Stufe 2: Der Mensch führt, die KI unterstützt.

© UNITED SECURITY PROVIDERS AG

# REFERENCES


1) https://www.google.com/search?q=php2shell&oq=php2shell, Accessed 23.10.2026
2) https://www.wsj.com/tech/cybersecurity/ai-just-found-a-bug-that-puts-up-to-70-of-the-worlds-websites-at-risk-fd0902ea, Accessed 23.10.2026
3) https://www.wiz.io/blog/php2shell-php-rce, Accessed: 23.10.2026
4) https://www.nytimes.com/2026/10/21/us/politics/php-vulnerability-ai-openai-cybersecurity.html, Accessed: 23.10.2026
5) https://calif.io/php2shell/, Accessed: 23.10.2026
6) https://xbow.com/blog/top-1-how-xbow-did-it, Accessed: 23.10.2026
7) https://arxiv.org/abs/2512.09882, Accessed: 23.10.2026
8) https://hostedscan.com/pricing, Basic: 39$ Premium: 109$, Professional 189$, Accessed: 23.10.2026
9) https://www.penligent.ai/pricing, Pro: 40$, Accessed: 23.10.2026
10) https://www.aikido.dev/pricing?product=pentest, Rightsized Pentest: 45-25'000€ Accessed: 23.10.2026
11) https://pwn.ai/pricing, Starter: 3'000$, Pro: 6'000$, Accessed: 29.10.2026
12) https://web.archive.org/web/20260722210349/https://xbow.com/pricing, Accessed: 23.10.2026
13) https://mallory.ai/blog/php-rce-rapid-response, Accessed: 23.10.2026
14) https://www.penligent.ai/pricing, Pro: 89.92$, Accessed: 27.10.2026
15) https://www.stingrai.io/pricing, Hybrid Pentest: 6'800$, Accessed: 27.10.2026
16) https://www.synack.com/pricing, SynackST: 10'283$ , Accessed: 27.10.2026


© UNITED SECURITY PROVIDERS AG

FRAGEN?

UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

# VIELEN DANK!




LEA ZIMMERLI

Pentesterin

Hauptsitz

Bern

Stauffacherstrasse 65/15 (Businesspark Bern)

3014 Bern

Zürich

Baslerstrasse 60 (Baslerpark)

8048 Zürich

+41 31 959 02 02

info@united-security-providers.ch

www.united-security-providers.ch