🛡️ Verantwortungsvolle Schwachstellenmeldung mit security.txt

Die `security.txt` ist eine standardisierte Textdatei nach RFC 9116. Sie gibt Sicherheitsforschenden einen eindeutigen, öffentlich auffindbaren Kontakt, über den sie entdeckte Schwachstellen einer Website sicher melden können, statt lange nach einer Ansprechperson suchen zu müssen. Das BSI empfiehlt die Umsetzung ausdrücklich.

📁 Ablageort: `https://domain.tld/.well-known/security.txt`

Pflichtfeld · Empfohlen · Optional — RFC 9116

✉️ Contact

Pflicht

Wie Sicherheitsforschende euch erreichen können, um eine Schwachstelle zu melden. Mehrfach angebbar, Reihenfolge = Präferenz.

```
Contact: mailto:security@example.com
```

📅 Expires

Pflicht

Ab wann die Datei als veraltet gilt. Darf nur einmal vorkommen. Empfehlung: unter einem Jahr in der Zukunft.

```
Expires: 2027-02-25T00:00:00Z
```

🔗 Canonical

Empfohlen

Die offizielle URL dieser Datei selbst. Bestätigt, dass eine abgerufene Kopie authentisch ist, besonders bei Signatur wichtig.

```
Canonical: https://example.com/.well-known/security.txt
```

🔒 Encryption

Empfohlen

Link zu einem PGP-Schlüssel für verschlüsselte Meldungen. Der Schlüssel selbst darf nicht direkt im Feld stehen, nur ein Link darauf.

```
Encryption: https://example.com/pgp-key.txt
```

📄 Policy

Empfohlen

Link zur Vulnerability-Disclosure-Policy. Erklärt Meldenden den Ablauf, erlaubte Tests und ob es eine Bug-Bounty gibt.

```
Policy: https://example.com/security-policy.html
```

🏆 Acknowledgments

Optional

Link zu einer Seite, die meldende Sicherheitsforschende öffentlich würdigt, eine Art Hall of Fame.

```
Acknowledgments: https://example.com/hall-of-fame.html
```

🌐 Preferred-Languages

Optional

In welchen Sprachen Meldungen gerne entgegengenommen werden. Darf nur einmal vorkommen, kommagetrennte Liste. Ohne Angabe wird Englisch angenommen.

```
Preferred-Languages: de, en
```

💼 Hiring

Optional

Link zu offenen Security-Stellenangeboten. Nützlich, da genau die Zielgruppe, die diese Datei liest, potenziell an solchen Jobs interessiert ist.

```
Hiring: https://example.com/jobs.html
```

Technische Hinweise zur Umsetzung

🔤 Zeichenkodierung

Die Datei muss als reiner Text im Format `text/plain` mit Kodierung UTF-8 ausgeliefert werden. Der Webserver sollte diesen Content-Type per HTTP-Header senden, nicht als Zeile in der Datei selbst.

```
Content-Type: text/plain; charset=utf-8
```

⚙️ Steuerung über .htaccess

Auf Apache-Servern lässt sich der korrekte Content-Type sowie eine Weiterleitung vom Legacy-Pfad zentral über die .htaccess-Datei setzen, ohne die Server-Hauptkonfiguration anzufassen.

```
AddType text/plain .txt
Redirect 301 /security.txt /.well-known/security.txt
```

🕰️ Legacy-Pfad

Zusätzlich zum verbindlichen Pfad unter .well-known kann aus Kompatibilitätsgründen auch eine Kopie im Wurzelverzeichnis liegen. Existieren beide, ist die Version unter .well-known maßgeblich.

```
https://domain.tld/security.txt
```

💬 Kommentare

Zeilen, die mit einer Raute beginnen, gelten als Kommentar und werden von Auswertenden ignoriert. Praktisch für kurze Erläuterungen im Quelltext.

```
# Zuletzt aktualisiert am 2026-08-25
```

✍️ Digitale Signatur (OpenPGP)

Die gesamte Datei kann per OpenPGP cleartext signiert werden, das ist keine eigene Zeile, sondern eine Hülle um den gesamten Inhalt. So lässt sich nachweisen, dass die Datei wirklich vom Betreiber stammt und nicht manipuliert wurde. In Kombination mit Signatur wird ein Canonical-Feld dringend empfohlen, damit auch der Speicherort mit abgesichert ist.

```
gpg --clearsign security.txt
```

📏 Größenlimits

Die Spezifikation empfiehlt, die Datei kompakt zu halten, damit Auswertende sie robust verarbeiten können. Richtwerte: unter 32 KB Gesamtgröße, unter 2.048 Zeichen pro Feld und unter 1.000 Zeilen.

```
max. 32 KB · max. 2.048 Zeichen je Feld · max. 1.000 Zeilen
```

🔓 Nur über HTTPS

Der Abruf der Datei muss zwingend über HTTPS erfolgen, damit der Inhalt nicht auf dem Übertragungsweg manipuliert werden kann. Ein Abruf über unverschlüsseltes HTTP gilt als nicht konform.

```
https:// statt http://
```

📍 Geltungsbereich

Eine security.txt gilt nur für genau die Domain oder IP-Adresse, unter der sie abgerufen wurde, nicht automatisch für Subdomains oder die übergeordnete Domain. Jede Subdomain benötigt bei Bedarf ihre eigene Datei.

```
shop.example.com ≠ example.com
```

✅ Datei online prüfen

Nach dem Einrichten lohnt sich ein Test mit einem Online-Validator, um Formatfehler und fehlende Pflichtfelder frühzeitig zu erkennen.

```
securitytxt.org
```

⚠️ Häufiger Fehler: HTTP-Response-Header wie Content-Type gehören in die Server-Konfiguration, nicht als Zeile in den Dateiinhalt. Eine Zeile wie „Content-Type: …" in der Datei selbst ist kein gültiges RFC-9116-Feld und wird ignoriert.