
**ePrivacyseal GmbH**

**Kriterienkatalog**

**„ePrivacy Pentesting“**

**Januar 2026**

Das Zertifikate „ePrivacy Pentesting“ für Datensicherheit der ePrivacyseal GmbH bestätigt dem jeweiligen Antragsteller, dass sein Angebot mit den im nachfolgenden Kriterienkatalog näher spezifizierten Kriterien im Einklang steht, die sich an den Anforderungen an Datensicherheit auf der Basis des deutschen Datenschutzrechtes, an der Datenschutz-grundverordnung und dem aktuellen Stand der Technik orientieren.

## Prüfgegenstand

Die Zertifizierung bezieht sich ausschließlich auf die sicherheitstechnische Integrität der geprüften Anwendung oder Infrastruktur zum Zeitpunkt des Tests. Bestätigt wird:

- Durchführung eines umfassenden Penetrationstests auf Basis etablierter Standards
- Keine identifizierten hohen oder kritischen Schwachstellen bzw. deren vollständige Behebung im Rahmen eines Nachtests
- Erfüllung organisatorischer, technischer und dokumentarischer Mindest-anforderungen gemäß diesem Katalog

Der Test erfolgte unter Berücksichtigung der höchsten Sicherheitsstandards und branchenüblicher Best Practices, wie in diesem Dokument spezifiziert

Im Einzelnen wird damit die Einhaltung folgender Anforderungen bestätigt:

# 1. Allgemeine und organisatorische Kriterien

- Der Pentest darf keine hohen oder kritischen Schwachstellen identifiziert haben oder diese sind im Rahmen eines Nachtests als behoben bestätigt worden.
- Zur Durchführung des Pentests wurde eine entsprechend gesichertes Management-System genutzt.
- Identifizierte Schwachstellen werden revisionssicher gespeichert.
- Identifizierte Schwachstellen wurden nach CVSS im Risiko eingeschätzt.
- Ausschließlich qualifizierte Analysten wurden für das Projekt eingesetzt.
- Der Dienstleister ist ISO27001 zertifiziert.
- Der Scope des Pentests wurde klar und sinnvoll festgelegt.
- Sicherstellung der Aktualität und Korrektheit der eingesetzten Werkzeuge.
- Durchführung in Übereinstimmung mit ethischen Standards und rechtlichen Rahmenbedingungen.
- Möglichkeit der Reproduktion der Testergebnisse unter gleichen Bedingungen.
- Sicherstellung der Transparenz und Nachvollziehbarkeit der Testverfahren.
- Strikte Wahrung der Vertraulichkeit während des gesamten Testprozesses.
- Der Pentest wurde nach anerkannten Standards wie BSI oder OWASP durchgeführt.
- Es wurden verifizierte und bewährte Tools eingesetzt.
- Das Pentest-Projekt wurde in einem angemessenen Umfang von mindestens 5 Personentagen durchgeführt.
- Der Pentest-Bericht soll ein Management Summary sowie detaillierte Informationen zu den identifizierten Schwachstellen enthalten.

# 2. Anwendungsspezifische Kriterien

## Information Gathering

- Es sind keine sensiblen Informationen über Suchmaschinen oder externe Quellen auffindbar
- Der Webserver wurde korrekt identifiziert und gibt keine unnötigen Bannerinformationen preis.
- Metadaten und Konfigurationsdateien enthalten keine vertraulichen Informationen.
- Alle auf dem Webserver laufenden Anwendungen sind anonymisiert.
- Webseiten enthalten keine sensiblen Inhalte, Kommentare oder Debug-Informationen.
- Alle möglichen Eingabepunkte der Anwendung sind anonymisiert.
- Anwendungspfade und Navigationslogik sind anonymisiert.
- Das verwendete Webframework ist anonymisiert
- Alle fingerprints sind deaktiviert.
- Die logische und technische Architektur der Anwendung ist anonymisiert

## Configuration and Deployment Management

- Netzwerkkonfiguration ist sicher und bietet keine unnötigen offenen Ports.
- Serverkonfigurationen entsprechen gängigen Sicherheitsrichtlinien.
- Dateiendungen geben keine sensitiven Daten preis.
- Alte oder vergessene Dateien enthalten keine schützenswerten Inhalte.
- Adminschnittstellen sind geschützt und nicht öffentlich erreichbar.
- Nur notwendige HTTP-Methoden sind aktiviert.
- HSTS ist implementiert und korrekt konfiguriert.
- Cross-Domain-Policy-Dateien sind restriktiv konfiguriert.
- Dateiberechtigungen verhindern unautorisierten Zugriff.
- Subdomains sind geschützt gegen Übernahme.
- Cloud-Speicher ist sicher konfiguriert und nicht öffentlich einsehbar.

## Identity Management

- Rollen und Rechte sind klar definiert und korrekt zugewiesen.
- Der Registrierungsprozess erfordert Identitätsnachweis und Validierung.
- Account-Provisionierung erfolgt ausschließlich über sichere Prozesse.
- Benutzeridentitäten können nicht durch Fehlerausgaben oder Seiteneffekte erschlossen werden.
- Die Vergabe von Benutzernamen folgt strengen Richtlinien.

## Authentication

- Zugangsdaten werden ausschließlich verschlüsselt übertragen.
- Standardkennwörter sind deaktiviert oder entfernt.

- Login-Versuche sind gegen Bruteforce und Enumeration geschützt.
- Authentifizierungsmechanismen sind robust gegen Umgehung.
- "Remember Me"-Funktionen speichern keine sensiblen Informationen im Klartext.
- Der Browser speichert keine Passwörter oder Sessiondaten unsicher.
- Passwortanforderungen erfüllen definierte Sicherheitsstandards.
- Sicherheitsfragen lassen sich nicht erraten oder umgehen.
- Passwortänderungs- und Reset-Funktionen sind durch Token und Validierung geschützt.
- Authentifizierungsmechanismen alternativer Kanäle sind gleich stark abgesichert.

## Authorization

- Verzeichnispfade und Dateizugriffe sind gegen Directory Traversal abgesichert.
- Autorisierung kann nicht durch Parameter-Manipulation umgangen werden.
- Rechteeskalation durch Benutzerwechsel ist ausgeschlossen.
- Direkte Objektreferenzen sind nur für berechtigte Benutzer aufrufbar.

## Session Management

- Sessiondaten werden sicher verarbeitet und übertragen.
- Cookies besitzen die Attribute HttpOnly, Secure, SameSite.
- Schutz gegen Session-Fixation ist aktiv.
- Sessionvariablen sind vor externem Zugriff geschützt.
- CSRF-Schutzmechanismen sind vorhanden und aktiv.
- Logout löscht die Session vollständig.
- Sessions verfallen nach festgelegter Inaktivitätsdauer.
- Sessionpuzzling ist technisch ausgeschlossen.
- Session-Hijacking wird durch Token-Management verhindert.

## Input Validation

- Cross-Site Scripting ist durch Eingabevalidierung und Output-Encoding ausgeschlossen.
- HTTP-Verben und -Parameter sind auf erwartete Werte beschränkt.
- SQL-Injections sind durch sichere Abfragen verhindert.
- Datenbankspezifische Angriffsvektoren sind vollständig geprüft und ausgeschlossen.
- LDAP-, XML-, SSI- und XPath-Injections sind technisch nicht möglich.
- Code-, Datei- und Befehlsinjektionen werden zuverlässig verhindert.
- Lokale und entfernte Dateiinbindungen sind ausgeschlossen.
- HTTP Request Smuggling kann nicht durchgeführt werden.
- Host Header Manipulation ist ohne Auswirkung auf Anwendung oder Logik.
- Template-Injections sind durch Eingabekontrolle ausgeschlossen.
- Server-Side Request Forgery wird durch strikte Zielvalidierung verhindert.

## Error Handling

- Fehlerbehandlung gibt keine technischen Details oder Stack Traces preis.
- Fehlermeldungen ermöglichen keine Rückschlüsse auf interne Logik oder Komponenten.

## Cryptography

- Transportverschlüsselung erfüllt aktuelle Standards.
- Nur sichere Cipher Suites und TLS-Versionen sind aktiviert.
- Padding-Oracle-Schwachstellen sind ausgeschlossen.
- Keine sensiblen Daten werden unverschlüsselt übertragen.
- Kryptografie verwendet starke, zeitgemäße Algorithmen.

## Business Logic

- Eingaben und Prozesse entsprechen definierten Geschäftsregeln.
- Benutzeraktionen können nicht manipuliert oder gefälscht werden.
- Integritätsprüfungen verhindern unzulässige Zustandsänderungen.
- Zeitliche Abhängigkeiten und Prozessfolgen sind abgesichert.
- Funktionsnutzung ist durch Limits oder Schwellenwerte eingeschränkt.
- Umgehung von Workflows ist nicht möglich.
- Schutzmaßnahmen verhindern absichtliche Fehl- oder Zweckentfremdung.
- Hochgeladene Dateien werden auf erlaubte Typen und Inhalte geprüft.
- Schadhafte Uploads werden zuverlässig erkannt und abgewiesen.

## Client-side Testing

- DOM-Manipulation führt nicht zu Sicherheitslücken.
- JavaScript-Schnittstellen sind auf sichere Datenverarbeitung ausgelegt.
- HTML- und CSS-Injections sind technisch ausgeschlossen.
- Client-seitige Redirects lassen sich nicht manipulieren.
- Lokaler Speicher enthält keine sensitiven Informationen.
- CORS ist restriktiv konfiguriert.
- Schutzmechanismen gegen Clickjacking sind aktiv.
- Kommunikationsschnittstellen wie WebSockets und Messaging sind abgesichert.
- Fremde Skriptquellen erfordern explizite Vertrauensstellung.

## API Testing

- GraphQL-Interfaces lassen keine unautorisierte Schema-Abfrage zu.
- Datenexfiltration durch unbeschränkte Queries ist ausgeschlossen.
- Alle API-Endpunkte sind authentifiziert und autorisiert.
- Rate Limiting und Zugriffsbeschränkungen sind aktiv.

# 3. Prüfungen

## Information Gathering

- Überprüfung auf Informationslecks über Suchmaschinen
- Durchsuchen von Suchmaschinen
- Überprüfung von Cache-Versionen
- Analyse von Suchergebnissen
- Identifikation des Webservers ohne Preisgabe von Bannerinformationen
- Analyse der HTTP-Antwort-Header
- Beobachtung von Fehlerseiten
- Überprüfung auf öffentlich zugängliche Statusseiten
- Überprüfung von Metadaten und Konfigurationsdateien
- Zugriff auf Metadateien
- Analyse auf Entwicklungsspuren
- Anonymisierung der auf dem Webserver laufenden Anwendungen
- Überprüfung der URL-Struktur
- Beobachtung des Verhaltens der Anwendung
- Überprüfung von Standardverzeichnissen

**Überprüfung des Webseiteninhalts auf Informationslecks**

- Analyse des Quellcodes
- Überprüfung eingebundener Skripte
- Anonymisierung aller möglichen Eingabepunkte der Anwendung
- Überprüfung der URL-Parameter
- Beobachtung der Formularfelder
- Überprüfung von Datei-Upload-Funktionen

**Anonymisierung von Anwendungspfaden und Navigationslogik**

- Überprüfung der URL-Struktur
- Beobachtung der Navigation
- Überprüfung von Weiterleitungen

**Anonymisierung des verwendeten Webframeworks**

- Überprüfung der URL-Struktur
- Beobachtung von Fehlermeldungen
- Überprüfung von Standardverzeichnissen
- Deaktivierung aller Fingerprints
- Überprüfung der HTTP-Header
- Beobachtung von Fehlermeldungen
- Überprüfung von Standardverzeichnissen

**Anonymisierung der logischen und technischen Architektur der Anwendung**

- Überprüfung der URL-Struktur
- Beobachtung der Navigation
- Überprüfung von Weiterleitungen

## Configuration and Deployment Management

- Sichere Netzwerkkonfiguration ohne unnötige offene Ports
- Serverkonfiguration gemäß gängiger Sicherheitsrichtlinien
- Dateiendungen geben keine sensiblen Daten preis
- Alte oder vergessene Dateien enthalten keine schützenswerten Inhalte
- Adminschnittstellen sind geschützt und nicht öffentlich erreichbar
- Nur notwendige HTTP-Methoden sind aktiviert
- HSTS ist implementiert und korrekt konfiguriert
- Cross-Domain-Policy-Dateien sind restriktiv konfiguriert
- Dateiberechtigungen verhindern unautorisierten Zugriff
- Subdomains sind geschützt gegen Übernahme
- Cloud-Speicher ist sicher konfiguriert und nicht öffentlich einsehbar

## Identity Management

- Rollen und Rechte sind klar definiert und korrekt zugewiesen
- Der Registrierungsprozess erfordert Identitätsnachweis und Validierung
- Account-Provisionierung erfolgt ausschließlich über sichere Prozesse
- Benutzeridentitäten können nicht durch Fehlerausgaben oder Seiteneffekte erschlossen werden
- Die Vergabe von Benutzernamen folgt strengen Richtlinien

## Authentication

- Zugangsdaten werden ausschließlich verschlüsselt übertragen
- Standardkennwörter sind deaktiviert oder entfernt
- Login-Versuche sind gegen Bruteforce und Enumeration geschützt
- Authentifizierungsmechanismen sind robust gegen Umgehung
- "Remember Me"-Funktionen speichern keine sensiblen Informationen im Klartext
- Der Browser speichert keine Passwörter oder Sessiondaten unsicher
- Passwortanforderungen erfüllen definierte Sicherheitsstandards
- Sicherheitsfragen lassen sich nicht erraten oder umgehen
- Passwortänderungs- und Reset-Funktionen sind durch Token und Validierung geschützt
- Authentifizierungsmechanismen alternativer Kanäle sind gleich stark abgesichert

## Authorization

- Verzeichnispfade und Dateizugriffe sind gegen Directory Traversal abgesichert
- Autorisierung kann nicht durch Parameter-Manipulation umgangen werden
- Rechteeskalation durch Benutzerwechsel ist ausgeschlossen
- Direkte Objektreferenzen sind nur für berechtigte Benutzer aufrufbar

## Session Management

- Sessiondaten werden sicher verarbeitet und übertragen
- Cookies besitzen die Attribute HttpOnly, Secure, SameSite
- Schutz gegen Session-Fixation ist aktiv
- Sessionvariablen sind vor externem Zugriff geschützt
- CSRF-Schutzmechanismen sind vorhanden und aktiv
- Logout löscht die Session vollständig
- Sessions verfallen nach festgelegter Inaktivitätsdauer
- Sessionpuzzling ist technisch ausgeschlossen
- Session-Hijacking wird durch Token-Management verhindert

## Input Validation

- Cross-Site Scripting (XSS) ist durch Eingabevalidierung und Output-Encoding
- HTTP-Verben und -Parameter sind auf erwartete Werte beschränkt
- SQL-Injections sind durch sichere Abfragen verhindert
- Datenbankspezifische Angriffsvektoren sind vollständig geprüft und ausgeschlossen
- LDAP-, XML-, SSI- und XPath-Injections sind technisch nicht möglich
- Code-, Datei- und Befehlsinjektionen werden zuverlässig verhindert
- Lokale und entfernte Dateiinbindungen sind ausgeschlossen
- HTTP Request Smuggling kann nicht durchgeführt werden
- Host Header Manipulation ist ohne Auswirkung auf Anwendung oder Logik
- Template-Injections sind durch Eingabekontrolle ausgeschlossen
- Server-Side Request Forgery wird durch strikte Zielvalidierung verhindert

## Error Handling

- Fehlermeldungen ermöglichen keine Rückschlüsse auf interne Logik oder Komponenten

## Cryptography

- Transportverschlüsselung erfüllt aktuelle Standards
- Nur sichere Cipher Suites und TLS-Versionen sind aktiviert
- Padding-Oracle-Schwachstellen sind ausgeschlossen
- Keine sensiblen Daten werden unverschlüsselt übertragen
- Kryptografie verwendet starke, zeitgemäße Algorithmen

## Business Logic

- Eingaben und Prozesse entsprechen definierten Geschäftsregeln
- Benutzeraktionen können nicht manipuliert oder gefälscht werden
- Integritätsprüfungen verhindern unzulässige Zustandsänderungen
- Zeitliche Abhängigkeiten und Prozessfolgen sind abgesichert
- Funktionsnutzung ist durch Limits oder Schwellenwerte eingeschränkt
- Umgehung von Workflows ist nicht möglich
- Schutzmaßnahmen verhindern absichtliche Fehl- oder Zweckentfremdung
- Hochgeladene Dateien werden auf erlaubte Typen und Inhalte geprüft
- Schadhafte Uploads werden zuverlässig erkannt und abgewiesen

## Client-side Testing

- DOM-Manipulation führt nicht zu Sicherheitslücken
- JavaScript-Schnittstellen sind auf sichere Datenverarbeitung ausgelegt
- HTML- und CSS-Injections sind technisch ausgeschlossen
- Client-seitige Redirects lassen sich nicht manipulieren
- Lokaler Speicher enthält keine sensitiven Informationen
- CORS ist restriktiv konfiguriert
- Schutzmechanismen gegen Clickjacking sind aktiv
- Kommunikationsschnittstellen wie WebSockets und Messaging sind abgesichert
- Fremde Skriptquellen erfordern explizite Vertrauensstellung

## API Testing

- GraphQL-Interfaces lassen keine unautorisierte Schema-Abfrage zu
- Datenexfiltration durch unbeschränkte Queries ist ausgeschlossen
- Alle API-Endpunkte sind authentifiziert und autorisiert
- Rate Limiting und Zugriffsbeschränkungen sind aktiv

Hamburg, ePrivacy GmbH