Vorlage für die Erstellung des Prüfberichtes zum Penetrationstest unter Berücksichtigung des OWASP Testing Guides (Open Web Application Security Project)

(Stand: 15.06.2023)

Inhalt

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

1. Zielsetzung

1.1 Allgemeines

1.2 Abgrenzung

2. Management Summary

3. Ergebnisse der Analyse

Verantwortlicher Analyst	
Ansprechpartner beim Auftraggeber	
Untersuchungsobjekte	
Durchführungszeitraum	

3.1 Rahmenbedingungen

3.1.1 Beschreibung des Zielsystems

Kurze Beschreibung, was das Ziel des Servers ist, wo er platziert ist (DMZ / Intranet) und weitere relevante Informationen.

3.1.2 Verfügbare Informationen

Beschreibung des Vorgehens (Black-, Grey- oder Whitebox-Test) und der zur Verfügung gestellten Informationen (Netzpläne, Zugangsdaten, etc.)

3.1.3 Tools

Liste der im Rahmen der Analyse verwendeten Tools.

3.2 Ergebnisse Port- und Schwachstellenscan

In diesem Kapitel sind alle Ergebnisse der durchzuführenden Port-Scans (bspw. mit nmap) und der durchgeführten Schwachstellenscans (bspw. mit Nessus) aufzuführen.

Das Zielobjekt der Analyse ist das zu untersuchende Portal (anhand einer oder mehrerer IP-Adressen und / oder DNS-Namen identifiziert). Alle direkt dem Zielobjekt zuzuordnenden Systeme müssen hinsichtlich aller TCP-Ports und aller UDP-Ports geprüft werden.

Die identifizierten Ports müssen incl. der ggf. identifizierten Diensterkennungen und Schwachstellen dokumentiert werden. Die Dokumentation muss dabei zunächst basierend auf IP-Adressen und danach basierend auf Port-Nummern (erst TCP, dann UDP) erfolgen. Ports, auf denen kein lauschender Dienst identifiziert wurde, müssen nicht dokumentiert werden. Im Rahmen der Auswertung wird davon ausgegangen, dass nicht dokumentierte Ports während der Analyse nicht erreichbar waren.

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 -0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

Die während der Analysen verwendeten Einstellungen der genutzten Tools müssen im Anhang des Berichtes dokumentiert werden.

3.3 Ergebnisse der Analyse nach OWASP Testing-Guide

Die Dokumentation der Prüfergebnisse muss basierend auf dem jeweils aktuellen OWASP Testing-Guide erfolgen. Zu diesem OWASP-Prüfpunkt muss dabei dokumentiert werden, ob eine Schwachstelle identifiziert werden konnte oder nicht.

Im Folgenden wird ein Beispiel anhand des zum Erstelldatum des vorliegenden Berichts gültigen OWASP Testing-Guides 4.2 gegeben.

3.3.1 Informationssammlung

- **Suchmaschinen Information Leakage (WSTG-INFO-01)**
- **Webserver-Fingerprinting (WSTG-INFO-02)**
- **Webserver Metadateien (WSTG-INFO-03)**
- **Identifikation weiterer Web-Anwendungen (WSTG-INFO-04)**
- **Webseiten-Kommentare und -Metadaten (WSTG-INFO-05)**
- **Identifikation der Zugangspunkte des Portals (WSTG-INFO-06)**
- **Applikationsstruktur (WSTG-INFO-07)**
- **Web-Applikations-Framework-Fingerprinting (WSTG-INFO-08)**
- **Web-Applikations-Fingerprinting (WSTG-INFO-09)**
- **Applikationsarchitektur (WSTG-INFO-10)**

3.3.2 Konfiguration und Verteilung des untersuchten Portals

- **Netzwerk/Infrastruktur Konfiguration (WSTG-CONF-01)**
- **Konfiguration der Applikation (WSTG-CONF-02)**
- **Behandlung von Dateiendungen (WSTG-CONF-03)**
- **Identifikation von Backup- oder unreferenzierten Dateien (WSTG-CONF-04)**
- **Identifikation von Infrastruktur- und Administrativen-Schnittstellen (WSTG-CONF-05)**
- **Genutzte HTTP-Methoden (WSTG-CONF-06)**
- **HTTP Strict Transport Security Header (WSTG-CONF-07)**

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

- **RIA (Rich Internet Applications) Cross Domain Policy (WSTG-CONF-08)**
- **Dateiberechtigung, Benutzer- und Zugriffsrechteverwaltung (WSTG-CONF-09)**
- **Übernahme einer Subdomain (WSTG-CONF-10)**
- **Cloud Speicher (WSTG-CONF-11)**

3.3.3 Identitätsmanagement

- **Rollen Definitionen (WSTG-IDENT-01)**

  Die folgende Matrix beschreibt die definierten (z.B. durch eine Dokumentation vorgegebenen)

  Rollen und deren Berechtigungen auf die unterschiedlichen Objekte:

  R – Read Zugriffsrechte

  W – Write- Zugriffsrechte

  E – Execute Zugriffsrechte

  Abweichungen zwischen Definition und IST-Stand sind in rot zu markieren.

Bereich	Objekt	Administrator	Standard-Benutzer		
Administration	Benutzerberechtigung	RW	R		
Benutzerkonto	Passwortänderung	RWE	RWE		

- **Benutzerregistrierungsprozess (WSTG-IDNT-02)**
- **Account-Provisionierungsprozess (WSTG-IDNT-03)**
- **Benutzer-Account Identifikation (WSTG-IDNT-04)**
- **Benutzernamen-Policy (WSTG-IDNT-05)**

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 -0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

3.3.4 Authentisierungsmechanismen

- **Nutzung von verschlüsselten Verbindungen zum Transport von Anmeldedaten (WSTGATHN-01)**
- **Identifikation von Standard-Zugangsdaten (WSTG-ATHN-02)**
- **Schwache Lock-Out Mechanismen (WSTG-ATHN-03)**
- **Umgehung des Authentisierungsschemas (WSTG-ATHN-04)**
- **Passwort-Speicherung (WSTG-ATHN-05)**
- **Browser Cache-Management (WSTG-ATHN-06)**
- **Passwort-Policy (WSTG-ATHN-07)**
- **Sicherheitsfragen und -Antworten (WSTG-ATHN-08)**
- **Passwort-Änderung und -Reset (WSTG-ATHN-09)**
- **Schwache Authentisierung in alternativen Kanälen (WSTG-ATHN-10)**

3.3.5 Autorisierungmechanismen

- **Directory / Path-Traversal (WSTG-ATHZ-01)**
- **Umgehen des Autorisierungsschemas (WSTG-ATHZ-02)**
- **Privilege Escalation (WSTG-ATHZ-03)**
- **Unsichere direkte Objektreferenzen (WSTG-ATHZ-04)**

3.3.6 Session Management

- **Session Management Schema (WSTG-SESS-01)**
- **Parametrisierung der Session Cookies (WSTG-SESS-02)**
- **Session Fixation (WSTG-SESS-03)**
- **Exponierte Session Variablen (WSTG-SESS-04)**
- **Cross-Site-Request-Forgery (WSTG-SESS-05)**
- **Logout Funktionalität (WSTG-SESS-06)**
- **Session Timeout (WSTG-SESS-07)**

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

- **Session-Puzzling (WSTG-SESS-08)**
- **Session-Hijacking (WSTG-Sess-09)**

3.3.7 Eingabedatenvalidierung

- **Reflected Cross-Site-Scripting (WSTG-INPV-01)**
- **Stored Cross-Site-Scripting (WSTG-INPV-02)**
- **HTTP-Verb-Tampering (WSTG-INPV-03)**
- **HTTP-Parameter-Pollution (WSTG-INPV-04)**
- **SQL-Injection (WSTG-INPV-05)**
- **Oracle**
- **MySQL**
- **SQL Server**
- **PostgreSQL**
- **MS Access**
- **NoSQL Injection**
- **ORM Injection**
- **Client-side**
- **LDAP Injection (WSTG-INPV06)**
- **XML-Injection (WSTG-INPV-08)**
- **SSI-Injection (WSTG-INPV-09)**
- **XPath-Injection (WSTG-INPV-10**
- **IMAP/SMTP-Injection (WSTG-INPV-11)**
- **Code Injection (WSTG-INPV-12)**
- **Lokale Datei**
- **Remote Datei**
- **Command Injection (WSTG-INPV-12)**

GGL | Gemeinsame Glücksspielbehörde
der Länder | Anstalt des öffentlichen Rechts |
Hansering 15 | 06108 Halle (Saale)

Vorstand:
Ronald Benter

Telefon: (0345) 52352 -0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

- **Format String Injection (WSTG-INPV-13)**
- **Inkubierte Schwachstelle (WSTG-INPV-14)**
- **HTTP Splitting/Smuggling (WSTG-INPV-15)**
- **HTTP Incoming Requests (WSTG-INPV-16)**
- **Host Header Injection (WSTG-INPV-17)**
- **Server-side Template Injection (WSTG-INPV-18)**
- **Server-side Request Forgery (WSTG-INPV-19)**

3.3.8 Fehlerbehandlung

- **Fehlermeldungen (WSTG-ERRH-01)**
- **Stack Traces (WSTG-ERRH-02)**

3.3.9 Verschlüsselung

- **Verwendete Verschlüsslungsmechanismen (WSTG-CRYP-01)**
- **Padding Oracle (WSTG-CRYP-02)**
- **Unsichere Nutzung von Verschlüsselung (WSTG-CRYP-03)**
- **Schwache Verschlüsselung (WSTG-CRYP-04)**

3.3.10 Business-Logik

- **Business-Logik Datenvalidierung (WSTGBUSL-01)**
- **Gefälschte Anfragen (WSTG-BUSL-02)**
- **Integritätsprüfungen (WSTG-BUSL-03)**
- **Prozess-Timing (WSTG-BUSL-04)**
- **Funktionslimits (WSTG-BUSL-05)**
- **Umgehung von Workflows (WSTG-BUSL-06)**
- **Schutz vor Applikationsmissbrauch (WSTG-BUSL-07)**
- **Upload Unerwarteter Dateitypen (WSTG-BUSL-08)**
- **Upload Bösartiger Dateitypen (WSTG-BUSL-09)**

GGL | Gemeinsame Glücksspielbehörde
der Länder | Anstalt des öffentlichen Rechts |
Hansering 15 | 06108 Halle (Saale)

Vorstand:
Ronald Benter

Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

3.3.11 Client-Seitige Schwachstellen

- **DOM-basiertes Cross Site Scripting (WSTG-CLNT-01)**
- **JavaScript Injection (WSTG-CLNT-02)**
- **HTML Injection (WSTG-CLNT-03)**
- **Client-Seitige URL Weiterleitung (WSTG-CLNT-04)**
- **CSS Injection (WSTG-CLNT-05)**
- **Client-Seitige Resource Manipulation (WSTG-CLNT-06)**
- **Cross Origin Ressource Sharing (WSTG-CLNT-07)**
- **Cross-Site Flashing (WSTG-CLNT-08)**
- **Clickjacking (WSTG-CLNT-09)**
- **WebSockets (WSTG-CLNT-10)**
- **Web Messaging (WSTG-CLNT-11)**
- **Browser Speicher (WSTG-CLNT-12)**
- **Cross Site Script Inclusion (WSTG-CLNT-13)**

3.3.12 API Testing

- **GraphQL (WSTG-APIT-01**

3.3.13 Weitere Schwachstellen

In diesem Abschnitt können weitere Schwachstellen aufgeführt werden, die nicht in das OWASP Bewertungsschema passen. Jede Schwachstelle ist zu erfassen und zu bewerten.

3.4 Übersicht

In der unten aufgeführten Tabelle sind die im Rahmen der Analyse identifizierten Schwachstellen auszuführen. Dabei ist für jede Schwachstelle die zugehörige Schwachstelle, die Seiten, auf der die Schwachstelle dokumentiert wurde, der CVSS-String und der CVSS-Score zu beschreiben. Dabei ist das CVSS in der Version 3.0 zu verwenden. Sollte in einem Kapitel mehr als eine Schwachstelle identifiziert worden sein, ist die entsprechende Zeile zu kopieren.

Die Freigabe der Anwendung erfolgt maßgeblich basierend auf den Ergebnissen dieser Übersichtstabelle, wobei die Freigabe verweigert wird, sollte ein CVSS Base-Score den Wert von 7 oder die Summe der CVSS Base-Scores den Wert von 70 überschreiten.

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 -0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

		Identifizierte Schwachstelle			
		ID	Seite	CVSS	
				String	Score
Port- und Schwachstellenscan					0
Information Gathering	WSTG-INFO-01				0
	WSTG-INFO-02				0
	WSTG-INFO-03				0
	WSTG-INFO-04				0
	WSTG-INFO-05				0
	WSTG-INFO-06				0
	WSTG-INFO-07				0
	WSTG-INFO-08				0
	WSTG-INFO-09				0
	WSTG-INFO-010				0
Configuration and Management	WSTG-CONF-01				0
	WSTG-CONF-02				0
	WSTG-CONF-03				0
	WSTG-CONF-04				0
	WSTG-CONF-05				0
	WSTG-CONF-06				0
	WSTG-CONF-07				0
	WSTG-CONF-08				0
	WSTG-CONF-09				0
	WSTG-CONF-10				0
	WSTG-CONF-11				0
Identity Manage-ment	WSTG-IDENT-01				0
	WSTG-IDENT-02				0
	WSTG-IDENT-03				0
	WSTG-IDENT-04				0
	WSTG-IDENT-05				0
Authentication	WSTG-ATHN-01				0
	WSTG-ATHN-02				0
	WSTG-ATHN-03				0
	WSTG-ATHN-04				0
	WSTG-ATHN-05				0
	WSTG-ATHN-06				0
	WSTG-ATHN-07				0
	WSTG-ATHN-08				0
	WSTG-ATHN-09				0
	WSTG-ATHN-10				0
Authori-za-tion	WSTG-ATHZ-01				0
	WSTG-ATHZ-02				0
	WSTG-ATHZ-03				0
	WSTG-ATHZ-04				0
Session Management	WSTG-SESS-01				0
	WSTG-SESS-02				0
	WSTG-SESS-03				0
	WSTG-SESS-04				0
	WSTG-SESS-05				0
	WSTG-SESS-06				0
	WSTG-SESS-07				0

Abbildung 1

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

	WSTG-SESS-08				0
Input Validation	WSTG-INPV-01				0
	WSTG-INPV-02				0
	WSTG-INPV-03				0
	WSTG-INPV-04				0
	WSTG-INPV-05				0
	WSTG-INPV-06				0
	WSTG-INPV-07				0
	WSTG-INPV-08				0
	WSTG-INPV-09				0
	WSTG-INPV-10				0
	WSTG-INPV-11				0
	WSTG-INPV-12				0
	WSTG-INPV-13				0
	WSTG-INPV-14				0
	WSTG-INPV-15				0
	WSTG-INPV-16				0
	WSTG-INPV-17				
	WSTG-INPV-18				
	WSTG-INPV-19				
Error Handling	WSTG-ERRH-01				0
	WSTG-ERRH-02				0
Weak Cryptography	WSTG-CRYP-01				0
	WSTG-CRYP-02				0
	WSTG-CRYP-03				0
	WSTG-CRYP-04				
Business Logic	WSTG-BUSL-01				0
	WSTG-BUSL-02				0
	WSTG-BUSL-03				0
	WSTG-BUSL-04				0
	WSTG-BUSL-05				0
	WSTG-BUSL-06				0
	WSTG-BUSL-07				0
	WSTG-BUSL-08				0
	WSTG-BUSL-09				0
Client Side	WSTG-CLNT-01				0
	WSTG-CLNT-02				0
	WSTG-CLNT-03				0
	WSTG-CLNT-04				0
	WSTG-CLNT-05				0
	WSTG-CLNT-06				0
	WSTG-CLNT-07				0
	WSTG-CLNT-08				0
	WSTG-CLNT-09				0
	WSTG-CLNT-10				0
	WSTG-CLNT-11				0
	WSTG-CLNT-12				0
	WSTG-CLNT-13				
Zusätzliche Tests					0
weitere Schwachstellen					0
höchster CVSS-Score					0

Abbildung 2

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 -0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de

Summe CVSS-Scores				0

Abbildung 3

4. Maßnahmenempfehlung

Während der Analyse ist für jede Schwachstelle eine Maßnahme zu empfehlen, die die der Schwachstelle oder den Auswirkungen der Schwachstelle entgegenwirkt. Die Maßnahmen stellen Empfehlungen dar, die in Zusammenarbeit mit den IT-Mitarbeitern der Betreiber verfeinert werden müssen.

Die Priorisierung der Maßnahmen leitet sich direkt aus der Kritizität der Schwachstellen und dem identifizierten Risiko ab und erfolgt anhand der Kategorien **zeitnah, kurzfristig, mittelfristig** und **langfristig**, die wie folgt definiert werden:

Zeitnah: Reaktion unmittelbar

kurzfristig: Reaktion innerhalb von vier Wochen

mittelfristig: Reaktion innerhalb von drei Monaten

langfristig: Reaktion innerhalb von sechs Monate

GGL | Gemeinsame Glücksspielbehörde der Länder | Anstalt des öffentlichen Rechts | Hansering 15 | 06108 Halle (Saale)
Vorstand: Ronald Benter
Telefon: (0345) 52352 - 0
E-Mail: info@gluecksspiel-behoerde.de
Web: www.gluecksspiel-behoerde.de