OWASP Security Testing Checklist – Plan testowania bezpieczeństwa aplikacji webowej

Wstęp i jak używać tego dokumentu

Niniejsza checklista łączy trzy kluczowe standardy OWASP:[1][2]

Standard	Rola w procesie testowania
OWASP Development Guide	Ogólne kontrole bezpieczeństwa na etapie projektowania i kodu[3][4]
OWASP Top Ten (2021)	10 najgroźniejszych kategorii podatności – priorytetowe obszary testów[5][6]
OWASP ASVS 4.0 (Application Security Verification Standard)	Szczegółowy framework wymagań z 3 poziomami weryfikacji[1][7]

Poziomy ASVS – wybierz odpowiedni dla Twojej aplikacji

Poziom	Opis	Dla kogo
L1 – Podstawowy	Minimum dla każdej aplikacji; weryfikacja zautomatyzowana i dynamiczna[8][9]	Strony marketingowe, wewnętrzne narzędzia, prototypy
L2 – Standardowy	Zalecany dla większości aplikacji; wymaga testów manualnych i code review[8][10]	Aplikacje z danymi użytkowników, e-commerce, SaaS
L3 – Zaawansowany	Najwyższy poziom; formalny threat modeling, pełny pentest z dostępem do kodu[8][9]	Bankowość, e-zdrowie, systemy rządowe, identity providerzy

> Poziomy ASVS są **kumulatywne** – L2 zawiera wszystkie wymagania L1, a L3 zawiera L1+L2.[^8]

FAZA 0 – Przygotowanie i zakres

Przed przystąpieniem do testów wykonaj poniższe kroki zgodnie z OWASP Testing Framework (WSTG):[11][12]

- [ ] Zdefiniuj zakres testów (domeny, środowiska, konta testowe, ograniczenia)
- [ ] Uzyskaj pisemną autoryzację do testowania
- [ ] Przygotuj środowisko testowe (proxy, konta o różnych uprawnieniach)
- [ ] Przeprowadź rekonesans: zbuduj mapę aplikacji, zidentyfikuj endpointy, role, parametry
- [ ] Ustal poziom ASVS (L1/L2/L3) adekwatny do krytyczności aplikacji[^13]
- [ ] Wykonaj threat modeling (opcjonalnie, wymagane przy L3)[^11]

FAZA 1 – Zbieranie informacji (WSTG-INFO)

Źródło: OWASP WSTG Information Gathering[14][11]

ID	Test	Narzędzie
WSTG-INFO-01	Rekonesans przez wyszukiwarki (Google Dorks, Shodan)	theHarvester, Shodan
WSTG-INFO-02	Fingerprint serwera webowego	Nmap, Nikto, Wappalyzer
WSTG-INFO-03	Przegląd metaplików webservera (robots.txt, sitemap.xml)	curl, OWASP ZAP
WSTG-INFO-04	Enumeracja aplikacji na serwerze	Nmap, Gobuster
WSTG-INFO-05	Analiza treści strony pod kątem wycieku informacji	OWASP ZAP, Burp Suite
WSTG-INFO-06	Identyfikacja punktów wejścia aplikacji	Burp Suite Spider, OWASP ZAP
WSTG-INFO-07	Mapowanie ścieżek wykonania	Burp Suite, OWASP ZAP
WSTG-INFO-08	Fingerprint frameworka webowego	Wappalyzer, WhatWeb
WSTG-INFO-09	Fingerprint aplikacji webowej	WhatWeb, Nikto
WSTG-INFO-10	Mapowanie architektury aplikacji	Manualne + diagram

FAZA 2 – Konfiguracja i zarządzanie deploymentem (WSTG-CONF)

Powiązanie: OWASP Top Ten A05 – Security Misconfiguration[5][6] */ ASVS V14 – Configuration*[15][16]

ID	Test	Narzędzie
WSTG-CONF-01	Test konfiguracji infrastruktury sieciowej	Nmap, Nessus
WSTG-CONF-02	Test konfiguracji platformy aplikacji	Nikto, OWASP ZAP
WSTG-CONF-03	Obsługa rozszerzeń plików (wycieki .bak, .sql, .env)	Gobuster, Dirb
WSTG-CONF-04	Stare pliki backupu i nieużywane zasoby	Gobuster, Nikto
WSTG-CONF-05	Enumeracja interfejsów administracyjnych (/admin, /console)	Gobuster, Burp Suite
WSTG-CONF-06	Test metod HTTP (PUT, DELETE, TRACE)	curl, Burp Suite
WSTG-CONF-07	HTTP Strict Transport Security (HSTS)	SecurityHeaders.com, OWASP ZAP
WSTG-CONF-08	Cross-domain policy (Flash/RIA)	Manualne

ID	Test	Narzędzie
WSTG-CONF-09	Uprawnienia plików i katalogów	Manualne
WSTG-CONF-10	Subdomain Takeover	Subjack, Sublist3r
WSTG-CONF-11	Cloud Storage (S3, Azure Blob – publiczny dostęp)	S3Scanner, Prowler
WSTG-CONF-12	Content Security Policy (CSP)	CSP Evaluator, OWASP ZAP
WSTG-CONF-14	Inne nagłówki bezpieczeństwa HTTP (X-Frame-Options, CORS)	SecurityHeaders.com, Burp Suite

Checklista nagłówków HTTP (OWASP Dev Guide)[^17]

- [ ] `Strict-Transport-Security` – obecny i prawidłowo skonfigurowany
- [ ] `Content-Security-Policy` – zdefiniowany, bez `unsafe-inline`
- [ ] `X-Content-Type-Options: nosniff`
- [ ] `X-Frame-Options: DENY` lub `SAMEORIGIN`
- [ ] `Referrer-Policy` – skonfigurowany
- [ ] `Permissions-Policy` – ograniczone uprawnienia przeglądarki
- [ ] Brak nagłówków ujawniających wersje (Server, X-Powered-By)

FAZA 3 – Zarządzanie tożsamością (WSTG-IDNT / ASVS V2)

Powiązanie: OWASP Top Ten A07 – Identification and Authentication Failures[5][6] / ASVS V2 Authentication[^15]

ID	Test	Narzędzie
WSTG-IDNT-01	Test definicji ról użytkowników	Manualne
WSTG-IDNT-02	Test procesu rejestracji użytkownika	Manualne, Burp Suite
WSTG-IDNT-04	Enumeracja kont użytkowników	Burp Suite Intruder
WSTG-IDNT-05	Słaba polityka nazw użytkowników	Manualne

FAZA 4 – Uwierzytelnianie (WSTG-ATHN / ASVS V2)

Powiązanie: OWASP Top Ten A07[^5] / ASVS V2 – Authentication (L1–L3)[15][18]

ID	Test	Narzędzie
WSTG-ATHN-01	Credentials transportowane po HTTPS	Burp Suite, OWASP ZAP
WSTG-ATHN-02	Domyślne dane logowania	Hydra, Burp Suite Intruder

ID	Test	Narzędzie
WSTG-ATHN-03	Mechanizm blokowania konta (brute-force)	Burp Suite Intruder
WSTG-ATHN-04	Bypass schematu uwierzytelniania	Manualne, Burp Suite
WSTG-ATHN-05	Funkcja "Zapamiętaj mnie"	Burp Suite, DevTools
WSTG-ATHN-06	Cache przeglądarki (wrażliwe dane)	Manualne, DevTools
WSTG-ATHN-07	Siła polityki haseł	Manualne, Burp Suite
WSTG-ATHN-09	Zmiana / reset hasła	Burp Suite, Manualne
WSTG-ATHN-11	Testowanie MFA (Multi-Factor Authentication)	Manualne, Burp Suite

Checklista uwierzytelniania (OWASP Dev Guide)[4][17]

- [ ] Nowy token sesji generowany po zalogowaniu (ASVS 3.2.1 – L1/L2/L3)[^10]
- [ ] Hasła przechowywane z silnym algorytmem (bcrypt, Argon2, scrypt)
- [ ] Blokada konta po N nieudanych próbach
- [ ] Funkcja resetowania hasła bezpieczna (bez enumeracji, z tokenem jednorazowym)
- [ ] MFA dostępne i nie do obejścia przez alternative channel

FAZA 5 – Autoryzacja i kontrola dostępu (WSTG-ATHZ / ASVS V4)

Powiązanie: OWASP Top Ten A01 – Broken Access Control (najgroźniejsza kategoria)[5][6] / ASVS V4 Access Control[^15]

ID	Test	Narzędzie
WSTG-ATHZ-01	Directory traversal / File inclusion	Burp Suite, dotdotpwn
WSTG-ATHZ-02	Bypass schematu autoryzacji	Burp Suite, Manualne
WSTG-ATHZ-03	Privilege escalation (normalny użytkownik → admin)	Burp Suite, Autorize (plugin)
WSTG-ATHZ-04	Insecure Direct Object References (IDOR)	Burp Suite, Autorize
WSTG-ATHZ-05	Słabości OAuth 2.0	Manualne, Burp Suite

Checklista kontroli dostępu (OWASP Dev Guide + ASVS V4)[^4]

- [ ] Autoryzacja wymuszana server-side na każdym żądaniu
- [ ] Zasada domyślnego odmawiania dostępu (deny by default)
- [ ] RBAC/ABAC z centralnym egzekwowaniem polityki
- [ ] Test IDOR: podmiana ID w żądaniach API między kontami
- [ ] Weryfikacja dostępu do /admin, /api/admin jako zwykły użytkownik
- [ ] Weryfikacja dostępu do zasobów po wylogowaniu

FAZA 6 – Zarządzanie sesją (WSTG-SESS / ASVS V3)

Powiązanie: OWASP Top Ten A07[^5] / ASVS V3 Session Management[^15]

ID	Test	Narzędzie
WSTG-SESS-01	Schemat zarządzania sesją (entropia tokenów)	Burp Suite Sequencer
WSTG-SESS-02	Atrybuty cookies (Secure, HttpOnly, SameSite)	DevTools, Burp Suite
WSTG-SESS-03	Session Fixation	Manualne, Burp Suite
WSTG-SESS-04	Ujawnione zmienne sesji	Manualne, Burp Suite
WSTG-SESS-05	Cross-Site Request Forgery (CSRF)	OWASP ZAP, Burp Suite
WSTG-SESS-06	Funkcja wylogowania (unieważnienie sesji)	Manualne
WSTG-SESS-07	Timeout sesji	Manualne
WSTG-SESS-09	Session Hijacking	Burp Suite, Manualne
WSTG-SESS-10	JSON Web Tokens (JWT)	jwt.io, Burp JWT Editor
WSTG-SESS-11	Concurrent sessions	Manualne

FAZA 7 – Walidacja danych wejściowych / Injection (WSTG-INPV)

Powiązanie: OWASP Top Ten A03 – Injection[5][6] / ASVS V5 – Validation, Sanitization & Encoding[^15]

ID	Test	Narzędzie
WSTG-INPV-01	Reflected Cross-Site Scripting (XSS)	OWASP ZAP, Burp Suite, XSStrike
WSTG-INPV-02	Stored Cross-Site Scripting (XSS)	OWASP ZAP, Burp Suite
WSTG-INPV-03	HTTP Verb Tampering	Burp Suite, curl
WSTG-INPV-04	HTTP Parameter Pollution	Manualne, Burp Suite
WSTG-INPV-05	SQL Injection	SQLMap, Burp Suite
WSTG-INPV-06	LDAP Injection	Manualne, Burp Suite
WSTG-INPV-07	XML Injection / XXE	Burp Suite, OWASP ZAP
WSTG-INPV-11	Code Injection	Manualne, Burp Suite
WSTG-INPV-12	Command Injection	Manualne, Commix
WSTG-INPV-13	Format String Injection	Manualne, Burp Suite
WSTG-INPV-17	Host Header Injection	Manualne, Burp Suite
WSTG-INPV-18	Server-Side Template Injection (SSTI)	Burp Suite, tplmap
WSTG-INPV-19	Server-Side Request Forgery (SSRF)	Burp Suite, Collaborator
WSTG-INPV-20	Mass Assignment	Manualne, Burp Suite

Checklista walidacji danych (OWASP Dev Guide)[17][4]

- [ ] Walidacja wszystkich danych wejściowych po stronie serwera (nie tylko klient)
- [ ] Whitelist dozwolonych wartości – nie blacklist
- [ ] Parametryzowane zapytania SQL (prepared statements) – brak dynamicznego SQL
- [ ] Kodowanie danych wyjściowych przed umieszczeniem w HTML/JS/CSS/URL
- [ ] Upload plików: walidacja MIME type, nazwy, rozmiaru i zawartości
- [ ] Dezaktywacja external entity processing w parserach XML

FAZA 8 – Kryptografia (WSTG-CRYP / ASVS V6, V9)

Powiązanie: OWASP Top Ten A02 – Cryptographic Failures[5][6] / ASVS V6 Stored Cryptography, V9 Communications Security[^15]

ID	Test	Narzędzie
WSTG-CRYP-01	Słabe TLS/SSL (wersja, szyfry, klucze)	testssl.sh, SSLLabs
WSTG-CRYP-02	Padding Oracle Attack	Manualne, Burp Suite
WSTG-CRYP-03	Wrażliwe dane w niezaszyfrowanym kanale	Wireshark, Burp Suite
WSTG-CRYP-04	Słabe algorytmy szyfrowania (MD5, SHA1, DES)	Manualne, code review

Checklista kryptografii (OWASP Dev Guide + ASVS V6)[4][17]

- [ ] TLS 1.2 minimum, preferowane TLS 1.3
- [ ] Brak przestarzałych szyfrów (RC4, 3DES, NULL ciphers)
- [ ] Ważny certyfikat SSL/TLS z poprawnym CN
- [ ] Dane wrażliwe (hasła, PII, karty) szyfrowane at-rest[^19]
- [ ] Brak zakodowanych na stałe kluczy kryptograficznych w kodzie
- [ ] Bezpieczne generowanie liczb losowych (CSPRNG)

FAZA 9 – Obsługa błędów i logowanie (WSTG-ERRH / ASVS V7)

Powiązanie: OWASP Top Ten A09 – Security Logging and Monitoring Failures[5][6] / ASVS V7 Error Handling and Logging[^15]

ID	Test	Narzędzie
WSTG-ERRH-01	Nieprawidłowa obsługa błędów (stack trace, ścieżki, wersje)	Manualne, Burp Suite
WSTG-ERRH-02	Wycieki stack trace do użytkownika	Manualne

Checklista logowania (OWASP Dev Guide)[17][4]

- [ ] Aplikacja nie wyświetla stack trace / szczegółów wewnętrznych użytkownikowi
- [ ] Błędy logowane po stronie serwera z wystarczającym kontekstem
- [ ] Logowanie zdarzeń bezpieczeństwa: logowania, nieudane próby, zmiany uprawnień
- [ ] Logi chronione przed modyfikacją (write-only, centralne SIEM)
- [ ] Alerty na anomalie (np. nagły wzrost błędów 403/404)
- [ ] Brak danych wrażliwych w logach (hasła, tokeny, PII)

FAZA 10 – Logika biznesowa (WSTG-BUSL / ASVS V11)

Powiązanie: ASVS V11 Business Logic[15][16]

ID	Test	Narzędzie
WSTG-BUSL-01	Walidacja danych w logice biznesowej	Manualne, Burp Suite
WSTG-BUSL-02	Możliwość fałszowania żądań	Burp Suite
WSTG-BUSL-03	Weryfikacja integralności danych	Manualne
WSTG-BUSL-04	Timing attacks / race conditions	Burp Suite Turbo Intruder
WSTG-BUSL-05	Limity użycia funkcji (np. kupon jednorazowy)	Manualne
WSTG-BUSL-06	Pomijanie kroków workflow (np. checkout bez płatności)	Manualne, Burp Suite
WSTG-BUSL-08	Upload nieoczekiwanych typów plików	Manualne, Burp Suite
WSTG-BUSL-09	Upload złośliwych plików	Manualne
WSTG-BUSL-10	Test funkcjonalności płatności	Manualne

FAZA 11 – Testowanie API (WSTG-APIT / ASVS V13)

Powiązanie: OWASP Top Ten A01, A03[^5] / ASVS V13 API and Web Service[^15]

ID	Test	Narzędzie
WSTG-APIT-01	API Reconnaissance (enumeracja endpointów)	Burp Suite, Swagger/OpenAPI
WSTG-APIT-02	Broken Object Level Authorization (BOLA/IDOR)	Burp Suite, Autorize
WSTG-APIT-99	Testowanie GraphQL (introspection, query depth)	GraphQL Voyager, Burp Suite

Checklista API (OWASP Dev Guide + ASVS V13)[19][4]

- [ ] Walidacja nagłówka `Content-Type` (V4.1.1 – L1)[^19]
- [ ] Wyłączona introspection GraphQL w środowisku produkcyjnym (V4.3.2 – L2)[^19]
- [ ] Ograniczenie głębokości zapytań GraphQL (V4.3.1 – L2)[^19]

- [ ] Uwierzytelnianie WebSocket (V4.4.1 – L2)[^19]
- [ ] Wersjonowanie API + dokumentacja (OpenAPI/Swagger)
- [ ] Rate limiting i throttling na endpointach API
- [ ] Brak wrażliwych danych w odpowiedziach API (IDOR)

FAZA 12 – Komponenty i zależności (ASVS V12 / Top Ten A06)

Powiązanie: OWASP Top Ten A06 – Vulnerable and Outdated Components[5][6]

Checklista (OWASP Dev Guide)[4][17]

- [ ] Inwentaryzacja wszystkich bibliotek i zależności (npm audit, composer audit)
- [ ] Aktualizacja komponentów z known CVE
- [ ] Usunięcie nieużywanych zależności
- [ ] Weryfikacja integralności paczek (Subresource Integrity dla CDN)
- [ ] Monitorowanie podatności w czasie (Dependabot, Snyk, OWASP Dependency-Check)

FAZA 13 – Testowanie klienta (WSTG-CLIENT)

Powiązanie: ASVS V3 Web Frontend Security[^19]

ID	Test	Narzędzie
WSTG-CLNT-01	DOM-Based XSS	Burp Suite, DOMInvader
WSTG-CLNT-04	Client-Side URL Redirect	Manualne, Burp Suite
WSTG-CLNT-05	CSS Injection	Manualne
WSTG-CLNT-07	Cross-Origin Resource Sharing (CORS)	Manualne, Burp Suite
WSTG-CLNT-09	Clickjacking	Clickjacking Tester, Burp Suite
WSTG-CLNT-10	WebSockets	Burp Suite
WSTG-CLNT-12	Browser Storage (localStorage/sessionStorage)	DevTools
WSTG-CLNT-14	Reverse Tabnabbing	Manualne

FAZA 14 – Projekt i architektura (ASVS V1 / Top Ten A04)

Powiązanie: OWASP Top Ten A04 – Insecure Design[20][5] / ASVS V1 Architecture, Design and Threat Modeling[^15]

Checklista (OWASP Dev Guide)[3][4]

- [ ] Przeprowadzono threat modeling (STRIDE, OWASP Threat Dragon, Cornucopia)[^17]
- [ ] Stosowane zasady Security by Design i Least Privilege
- [ ] Separacja warstw (frontend/backend/baza danych)
- [ ] Aplikacja nie ujawnia szczegółów implementacji w odpowiedziach HTTP
- [ ] Frameworki i biblioteki bezpieczeństwa używane zamiast własnych implementacji
- [ ] Dokumentacja architektury bezpieczeństwa istnieje i jest aktualna

FAZA 15 – Integralność oprogramowania (Top Ten A08)

Powiązanie: OWASP Top Ten A08 – Software and Data Integrity Failures[6][5]

Checklista

- [ ] Weryfikacja podpisów cyfrowych dla aktualizacji oprogramowania
- [ ] Sprawdzenie pipeline CI/CD pod kątem nieautoryzowanych modyfikacji
- [ ] Subresource Integrity (SRI) dla zasobów CDN
- [ ] Weryfikacja deserializacji danych (brak unsafe deserialization)
- [ ] Analiza łańcucha dostaw (supply chain) dla paczek zewnętrznych

Rekomendowane narzędzia testowe

Narzędzia open-source (bezpłatne)

Narzędzie	Kategoria	Zastosowanie
OWASP ZAP (Zed Attack Proxy)	DAST	Automatyczne i manualne skanowanie, proxy, fuzzing, CI/CD[21][22]
Burp Suite Community	Proxy / Manual Testing	Przechwytywanie i modyfikacja HTTP/HTTPS, repeater, intruder[22][23]
SQLMap	Injection Testing	Automatyczne wykrywanie i eksploatacja SQL Injection[24][25]
Nikto	Web Scanner	Szybkie skanowanie pod kątem nagłówków, wersji, misconfiguracji[26][25]
Nmap	Network Recon	Skanowanie portów, fingerprint usług, wykrywanie wersji[27][24]
w3af	DAST	Framework do skanowania i eksploatacji aplikacji webowych[22][23]
testssl.sh	SSL/TLS Testing	Analiza konfiguracji TLS, szyfry, certyfikat

Narzędzie	Kategoria	Zastosowanie
Gobuster / Dirb	Directory Brute-Force	Enumeracja katalogów i plików
Sublist3r / Subjack	Recon	Enumeracja subdomen, subdomain takeover
XSStrike	XSS Testing	Zaawansowane wykrywanie XSS
Commix	Command Injection	Automatyczna eksploatacja command injection
tplmap	SSTI Testing	Server-Side Template Injection
SonarQube (Community)	SAST	Analiza statyczna kodu, wykrywanie podatności w kodzie źródłowym[^23]
OWASP Dependency-Check	SCA	Wykrywanie podatnych zależności (CVE)[^6]
jwt.io / Burp JWT Editor	JWT Testing	Analiza i modyfikacja tokenów JWT

Narzędzia komercyjne (płatne)

Narzędzie	Kategoria	Zastosowanie
Burp Suite Professional	Proxy / DAST	Pełny zestaw: aktywny skaner, Collaborator, Turbo Intruder[23][28]
Acunetix	DAST	Automatyczne skanowanie OWASP Top 10, API[21][29]
HCL AppScan	DAST/SAST	Kompleksowe skanowanie enterprise[21][22]
Nessus	Vulnerability Scanner	Skanowanie infrastruktury, CVE detection[^27]
Snyk	SCA / SAST	Integracja z CI/CD, monitoring zależności w czasie rzeczywistym[^25]

Dystrybucje środowisk testowych

Środowisko	Opis
Kali Linux	System z ponad 600 narzędziami pentestingowymi; zawiera ZAP, Burp, Nikto, SQLMap[^23]
Parrot OS Security	Alternatywa dla Kali, lżejszy system
DVWA / WebGoat / Juice Shop	Celowo podatne aplikacje do ćwiczenia technik testowania

Workflow testowania – podsumowanie etapów

```
 Autoryzacja i zakres
       ↓
[^1] Rekonesans (INFO)
       ↓
[^2] Konfiguracja serwera (CONF)
       ↓
[^3] Tożsamość i uwierzytelnianie (IDNT + ATHN)
       ↓
[^4] Autoryzacja i kontrola dostępu (ATHZ)
       ↓
[^5] Zarządzanie sesją (SESS)
       ↓
[^6] Walidacja wejść / Injection (INPV)
       ↓
[^7] Kryptografia (CRYP)
       ↓
[^8] API Testing (APIT)
       ↓
[^9] Frontend / Client-side (CLIENT)
       ↓
[^10] Logika biznesowa (BUSL)
       ↓
[^11] Błędy i logowanie (ERRH)
       ↓
[^12] Komponenty i zależności
       ↓
[^13] Raport z wynikami (severity, repro steps, remediation)
```

Szablon statusu testów

Dla każdego testu z checklisty stosuj jeden ze statusów:

Status	Znaczenie
✅ PASS	Test zaliczony – kontrola wdrożona poprawnie
❌ FAIL	Podatność znaleziona – wymaga naprawy
⚠️ PARTIAL	Częściowo wdrożone – wymaga poprawy
N/A	Nie dotyczy tej aplikacji

Przydatne zasoby OWASP

- OWASP WSTG (Web Security Testing Guide) – szczegółowe techniki testowania[^12]
- OWASP ASVS na GitHub – oficjalny standard z wymaganiami[^30]
- OWASP Developer Guide – przewodnik dla developerów[^2]
- OWASP Top Ten 2021 – lista 10 krytycznych podatności[^6]

- OWASP Cheat Sheet Series – praktyczne ściągawki per technologia

References

1. OWASP Application Security Verification Standard (ASVS) - The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web...
2. OWASP Developer Guide - The OWASP Developer Guide provides an introduction to security concepts and an initial reference for...
3. Overview - OWASP Developer Guide - The checklists that follow are general lists that are categorized to follow the controls listed in t...
4. Web Application Checklist - Web Application Checklist on the main website for The OWASP Foundation. OWASP is a nonprofit foundat...
5. OWASP Top Security Risks & Vulnerabilities 2021 Edition - Sucuri - OWASP Top Ten is the list of the 10 most common application vulnerabilities. It also shows their ris...
6. OWASP Top 10:2021 - OWASP Top 10:2021
7. Essential OWASP Application Security Verification Standard - The ASVS 4.0 covers a comprehensive list of controls that an application must adhere to in order to ...
8. OWASP ASVS: A Comprehensive Overview - Codific - 25 November, 2025 As software systems grow more complex, proving that they are secure has [...]
9. How to Use OWASP ASVS to Protect Web Applications | Jit - Jit.io - Learn about the structure of OWASP Application Security Verification Standard (ASVS) guidelines and ...
10. Implementing OWASP ASVS - SoftwareMill - Implementing OWASP ASVS standard in an existing project, from a backend developer perspective.
11. Web Application Security Testing - WSTG - v4.2 | OWASP Foundation - Guardsquare's software integrates seamlessly across the development cycle: from app security testing...
12. WSTG - v4.2 - OWASP Foundation - 4. Web Application Security Testing · 1 Test Network Infrastructure Configuration · 2 Test Applicati...
13. ASVS - OWASP Developer Guide - OWASP Foundation Developer Guide project
14. wstg/checklists/checklist.md at master · OWASP/wstg - GitHub - The Web Security Testing Guide is a comprehensive Open Source guide to testing the security of web a...
15. OWASP ASVS Explained: Web App Security Verification Standard - Learn the OWASP Application Security Verification Standard (ASVS): its levels, control chapters, use...
16. ASVS - OWASP Developer Guide - The ASVS is an open standard that sets out the coverage and 'level of rigor' expected when it comes ...
17. [PDF] Developer Guide - OWASP Foundation - The ESAPI is an open source web application security control library that makes it easier for Java p...
18. Understanding the OWASP Application Security Verification Standard - The OWASP ASVS framework provides a comprehensive security standard for all types of web apps and we...

19. asvs-requirements - Skill - Smithery - OWASP ASVS 5.0 requirements database for security audits. Provides chapter structure, control object...
20. OWASP Top Ten 2024 – The Complete Guide - Reflectiz - OWASP 2024 is a big deal because this list of the 10 most serious web app security vulnerabilities r...
21. Testing Tools Resource - WSTG - Stable | OWASP Foundation - NGS Typhon · HCL AppScan · Burp Intruder · Acunetix Web Vulnerability Scanner · MaxPatrol Security S...
22. Testing Tools Resource - WSTG - v4.2 | OWASP Foundation - Commercial Black-Box Testing Tools · NGS Typhon · HCL AppScan · Burp Intruder · Acunetix Web Vulnera...
23. The 6 best OWASP security testing tools in 2026 - Comparison table ; OWASP ZAP, Free DAST, Flexible, open-source, proxy-based, Budget-friendly setups ...
24. 10 Best Pen Testing Tools for Cybersecurity in 2026 - ZeroThreat - Best 10 Pentesting Tools for Experts in 2026 · 10. Nessus · 9. Nikto · 8. w3af · 7. OWASP ZAP · 6. B...
25. Top 8 penetration testing tools | Snyk - Top 8 penetration testing tools · 1. Metasploit framework · 2. Nmap · 3. sqlmap · 4. Burp Suite · 5....
26. Top 10 Web Application Penetration Testing Tools (2025) | Strobes - OWASP ZAP – A free alternative that scans for common web vulnerabilities like SQL injection and XSS....
27. Top 15 Penetration Testing Tools In 2026 - CloudSEK - The top penetration testing tools in 2026 include Metasploit, Burp Suite, Nmap, and Nessus for relia...
28. Essential OWASP Security Tools Overview | PDF | Penetration Test - The document presents essential web application security tools, including OWASP ZAP, Burp Suite, and...
29. Testing Tools Resource - WSTG - v4.1 | OWASP Foundation - NGS Typhon · IBM AppScan · Burp Intruder · Acunetix Web Vulnerability Scanner · MaxPatrol Security S...
30. OWASP/ASVS: Application Security Verification Standard - GitHub - The primary aim of the OWASP Application Security Verification Standard (ASVS) Project is to provide...