15 February 2026

Penetration Test Report

For Acme Corp Web App

Table of Contents

1. Executive Summary

- 1.1 Confidentiality Statement
- 1.2 Report Overview
- 1.3 Key Findings & Business Impact

2. Findings

- 2.1 Vulnerability Distribution
- 2.2 Master Findings Table
- 2.3 Detailed Findings

Appendices

- A. Scope & Methodology
- B. Vulnerability Coverage
- C. Glossary

1. Executive Summary

1.1 Confidentiality Statement

This document is the exclusive property of Acme Corp Web App and Agent Breach. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of both Acme Corp Web App and Agent Breach. Acme Corp Web App may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

1.2 Report Overview

On 15 February 2026, Agent Breach conducted web application penetration tests for Acme Corp Web App to evaluate its security posture and determine its exposure to a targeted attack. The primary goal of this engagement was to proactively discover vulnerabilities that could lead to the compromise of systems or sensitive information.

The assessment aimed to simulate a real-world attacker to identify risks that could impact the confidentiality of private data and the integrity of information systems. The configured scope was limited to the production web application hosted at https://example.com and its associated API endpoints. A **Deep** scan profile was used.

Total scan duration: **5.7 minutes**.

1.3 Key Findings & Business Impact

HIGH — **Missing HSTS on HTTPS Endpoint**

A successful exploitation could result in unauthorized access to customer accounts, theft of proprietary business data, and exposure of personally identifiable information (PII), leading to potential GDPR, CCPA, and other regulatory compliance violations with substantial fines. Customers discovering their data was compromised through an unencrypted connection would suffer significant reputational damage and loss of trust in Acme Corp's security practices. The financial impact includes breach notification costs, potential lawsuits, regulatory penalties, and long-term customer attrition.

HIGH — **Missing Security Header: Content-Security-Policy**

A successful XSS attack exploiting this vulnerability could result in large-scale user data breaches, leading to regulatory fines under GDPR, CCPA, and other privacy laws, plus mandatory breach notification costs. Your organization faces reputational damage as customers lose trust in your security practices, potentially resulting in customer churn and loss of business. Additionally, you may face legal liability if user data is compromised, and compliance audits will flag this as a critical gap in your security posture.

HIGH — **Missing Security Header: Strict-Transport-Security**

A successful attack could result in customer data breaches, leading to regulatory fines under GDPR, CCPA, and other privacy laws, as well as mandatory breach notification costs. Your organization faces reputational damage, loss of customer trust, and potential legal liability if customer data is compromised through this preventable vulnerability. Additionally, compliance frameworks like PCI-DSS, SOC 2, and industry-specific standards increasingly require HSTS

implementation, so this gap could cause audit failures and certification issues.

HIGH — Unrestricted File Upload (6 instances)

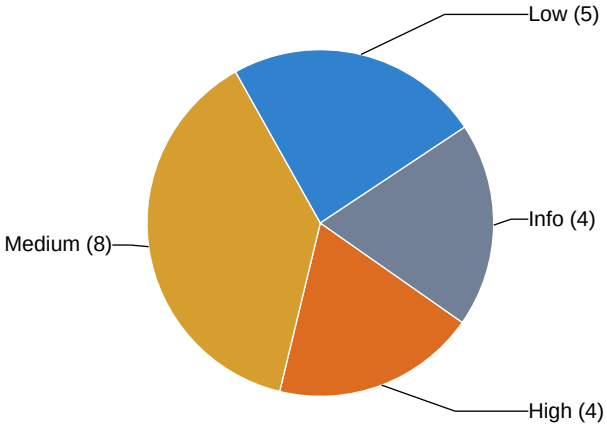
A successful exploit could result in theft of customer data (triggering GDPR, CCPA, and other compliance violations with substantial fines), operational downtime, and severe reputational damage that erodes customer trust. Your organization could face legal liability, mandatory breach notifications, regulatory investigations, and loss of business as customers migrate to competitors. The financial impact includes incident response costs, potential ransom demands, regulatory penalties, and long-term revenue loss from damaged reputation.

MEDIUM — Missing Security Header: X-Frame-Options

A successful clickjacking attack could lead to direct financial losses through fraudulent transactions, regulatory fines for failing to implement standard security controls, and significant reputational damage when customers discover they've been victimized. Compliance frameworks like PCI-DSS, HIPAA, and GDPR expect organizations to implement standard security headers, making this vulnerability a potential audit failure. The cost of remediation is negligible compared to the potential liability from a breach or compliance violation.

2. Findings

2.1 Vulnerability Distribution



- **High-severity** issues (4) could result in unauthorized access, data exposure, or significant system manipulation.

- **Medium-severity** issues (8) may enable unauthorized actions, information disclosure, or user manipulation.

- **Low-severity** issues (5) represent limited-impact weaknesses or informational findings.

Severity	Count
Critical	0
High	4
Medium	8
Low	5
Info	4
Total	**21**

2.2 Master Findings Table

ID	Title	State	Severity
PT-1	Missing HSTS on HTTPS Endpoint	Unresolved	High
PT-2	Missing Security Header: Content-Security-Policy	Unresolved	High
PT-3	Missing Security Header: Strict-Transport-Security	Unresolved	High
PT-4	Unrestricted File Upload (6 instances)	Unresolved	High
PT-5	Missing Security Header: X-Frame-Options	Unresolved	Medium
PT-6	Open Port 80/tcp (http)	Unresolved	Medium
PT-7	Missing Security Header: X-Content-Type-Options	Unresolved	Medium
PT-8	Clickjacking: Missing X-Frame-Options Header	Unresolved	Medium
PT-9	Rate Limiting Not Implemented	Unresolved	Medium
PT-10	Missing DMARC Record	Unresolved	Medium
PT-11	Missing SPF Record	Unresolved	Medium
PT-12	Missing Security Header: Permissions-Policy	Unresolved	Medium
PT-13	Server Information Disclosure	Unresolved	Low
PT-14	Clickjacking: Missing CSP frame-ancestors	Unresolved	Low
PT-15	RBAC: Weak Permission Boundaries	Unresolved	Low
PT-16	Missing Security Header: Referrer-Policy	Unresolved	Low
PT-17	Weak Password Policy	Unresolved	Low
PT-18	covery: 3 subdomains found for example.com	Unresolved	Info
PT-19	Discovered Subdomain: backcast.example.com	Unresolved	Info
PT-20	Discovered Subdomain: api.example.com	Unresolved	Info
PT-21	Discovered Subdomain: era5.example.com	Unresolved	Info

2.3 Detailed Findings

PT-1 — Missing HSTS on HTTPS Endpoint

HIGH

Identified on: February 15, 2026

CVSS	7.5
Type	Missing Hsts Https
URL	https://example.com/
Method	GET

Description

HTTPS endpoint missing Strict-Transport-Security header

Business Impact

A successful exploitation could result in unauthorized access to customer accounts, theft of proprietary business data, and exposure of personally identifiable information (PII), leading to potential GDPR, CCPA, and other regulatory compliance violations with substantial fines. Customers discovering their data was compromised through an unencrypted connection would suffer significant reputational damage and loss of trust in Acme Corp's security practices. The financial impact includes breach notification costs, potential lawsuits, regulatory penalties, and long-term customer attrition.

Remediation

Add Strict-Transport-Security header to all HTTPS responses.

PT-2 — Missing Security Header: Content-Security-Policy

HIGH

Identified on: February 15, 2026

CVSS	7.5
CWE	CWE-693
Type	Missing Security Header Content Security Policy
URL	https://example.com/
Method	GET

Description

Content Security Policy helps prevent XSS attacks. Header is missing.

Business Impact

A successful XSS attack exploiting this vulnerability could result in large-scale user data breaches, leading to regulatory fines under GDPR, CCPA, and other privacy laws, plus mandatory breach notification costs. Your organization faces reputational damage as customers lose trust in your security practices, potentially resulting in customer churn and loss of business. Additionally, you may face legal liability if user data is compromised, and compliance audits will flag this as a critical gap in your security posture.

Remediation

Add Content-Security-Policy header with value: default-src 'self'; script-src 'self'; object-src 'none';

PT-3 — Missing Security Header: Strict-Transport-Security

HIGH

Identified on: February 15, 2026

CVSS	7.5
CWE	CWE-693
Type	Missing Security Header Strict Transport Security
URL	https://example.com/
Method	GET

Description

Forces HTTPS connections (HSTS). Header is missing.

Business Impact

A successful attack could result in customer data breaches, leading to regulatory fines under GDPR, CCPA, and other privacy laws, as well as mandatory breach notification costs. Your organization faces reputational damage, loss of customer trust, and potential legal liability if customer data is compromised through this preventable vulnerability. Additionally, compliance frameworks like PCI-DSS, SOC 2, and industry-specific standards increasingly require HSTS implementation, so this gap could cause audit failures and certification issues.

Remediation

Add Strict-Transport-Security header with value: max-age=31536000; includeSubDomains; preload

PT-4 — Unrestricted File Upload (6 instances)

HIGH

Identified on: February 15, 2026

CVSS	9.8
CWE	CWE-434
Type	Unrestricted File Upload
URL	https://example.com/
Method	POST

Description

Detected 6 instances of this issue on the same endpoint. Affected variants include: • The application accepted a potentially dangerous file upload. Filename: test.phtml, Content-Type: application/x-php. Test: PHP alternate extension. • The application accepted a potentially dangerous file upload. Filename: test.php5, Content-Type: application/x-php. Test: PHP5 extension bypass. • The application accepted a potentially dangerous file upload. Filename: test.jpg.php, Content-Type: image/jpeg. Test: Reverse double extension. • The application accepted a potentially dangerous file upload. Filename: test.php.jpg, Content-Type: image/jpeg. Test: Double extension bypass. • The application accepted a potentially dangerous file upload. Filename: test.svg, Content-Type: image/svg+xml. Test: SVG with embedded XSS. … and 1 more.

Business Impact

A successful exploit could result in theft of customer data (triggering GDPR, CCPA, and other compliance violations with substantial fines), operational downtime, and severe reputational damage that erodes customer trust. Your organization could face legal liability, mandatory breach notifications, regulatory investigations, and loss of business as customers migrate to competitors. The financial impact includes incident response costs, potential ransom demands, regulatory penalties, and long-term revenue loss from damaged reputation.

How to Exploit

6 instance(s) detected:

- **Unrestricted File Upload: PHP alternate extension** [HIGH]

  The application accepted a potentially dangerous file upload. Filename: test.phtml, Content-Type: application/x-php. Test: PHP alternate extension.

- **Unrestricted File Upload: PHP5 extension bypass** [HIGH]

  The application accepted a potentially dangerous file upload. Filename: test.php5, Content-Type: application/x-php. Test: PHP5 extension bypass.

- **Unrestricted File Upload: Reverse double extension** [HIGH]

  The application accepted a potentially dangerous file upload. Filename: test.jpg.php, Content-Type: image/jpeg. Test: Reverse double extension.

- **Unrestricted File Upload: Double extension bypass** [MEDIUM]

  The application accepted a potentially dangerous file upload. Filename: test.php.jpg, Content-Type: image/jpeg. Test: Double extension bypass.

- **Unrestricted File Upload: SVG with embedded XSS** [LOW]

  The application accepted a potentially dangerous file upload. Filename: test.svg, Content-Type: image/svg+xml. Test: SVG with embedded XSS.

- **Unrestricted File Upload: HTML file upload (stored XSS)** [LOW]

  The application accepted a potentially dangerous file upload. Filename: test.html, Content-Type: text/html. Test: HTML file upload (stored XSS).

Remediation

Validate file uploads server-side: check file extension against an allowlist, validate the MIME type, scan file content for executable code, store uploads outside the web root, and rename files on save.

PT-5 — Missing Security Header: X-Frame-Options

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Frame Options
URL	https://example.com/
Method	GET

Description

Prevents clickjacking attacks. Header is missing.

Business Impact

A successful clickjacking attack could lead to direct financial losses through fraudulent transactions, regulatory fines for failing to implement standard security controls, and significant reputational damage when customers discover they've been victimized. Compliance frameworks like PCI-DSS, HIPAA, and GDPR expect organizations to implement standard security headers, making this vulnerability a potential audit failure. The cost of remediation is negligible compared to the potential liability from a breach or compliance violation.

Remediation

Add X-Frame-Options header with value: DENY or SAMEORIGIN

PT-6 — Open Port 80/tcp (http)

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
Type	Open Port
URL	34.195.134.6:80
Method	NETWORK_SCAN

Description

Port 80/tcp is open and running http None

Business Impact

Exposed HTTP traffic can lead to customer data breaches, resulting in regulatory fines under GDPR, HIPAA, or PCI-DSS compliance requirements, and potential lawsuits. A successful attack could damage your organization's reputation, erode customer trust, and result in significant financial losses from incident response, remediation, and lost business. For e-commerce or financial services, this vulnerability directly threatens transaction security and customer confidence.

PT-7 — Missing Security Header: X-Content-Type-Options

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Content Type Options
URL	https://example.com/
Method	GET

Description

Prevents MIME type sniffing. Header is missing.

Business Impact

A successful MIME type sniffing attack could result in unauthorized access to sensitive customer data, leading to regulatory fines under GDPR, CCPA, or industry-specific standards like PCI-DSS. Beyond compliance penalties, the organization faces reputational damage, loss of customer trust, and potential legal liability if user data is compromised. Financial impact includes incident response costs, notification expenses, and potential loss of business from affected customers.

Remediation

Add X-Content-Type-Options header with value: nosniff

PT-8 — Clickjacking: Missing X-Frame-Options Header

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-1021
Type	Clickjacking Missing X Frame Options
URL	https://example.com/
Method	GET

Description

Missing X-Frame-Options header, vulnerable to clickjacking

Business Impact

A successful clickjacking attack could result in unauthorized financial transactions, compromised user accounts, and loss of customer trust—particularly damaging for financial or e-commerce platforms. Regulatory compliance frameworks (PCI-DSS, HIPAA, GDPR) often require protection against clickjacking, making this vulnerability a potential compliance violation with associated fines. Reputational damage occurs when customers discover they've been manipulated into performing actions on your platform, leading to negative publicity and customer churn.

Remediation

Add X-Frame-Options: DENY or X-Frame-Options: SAMEORIGIN header.

PT-9 — Rate Limiting Not Implemented

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-307
Type	No Rate Limiting
URL	https://example.com/
Method	GET

Description

No rate limiting detected. Sent 20 successful requests rapidly.

Business Impact

A successful attack could result in unauthorized access to customer data, leading to potential GDPR, CCPA, or other regulatory fines (up to 4% of revenue under GDPR). Your reputation and customer trust could suffer significantly if users learn their accounts were compromised through brute-force attacks, and you may face legal liability for inadequate security controls. Service disruptions from DoS attacks directly impact revenue, customer satisfaction, and operational costs for incident response and recovery.

Remediation

- Implement rate limiting.
- Use token bucket or sliding window algorithm.
- Return 429 status code when limit exceeded.

PT-10 — Missing DMARC Record

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
Type	Missing Dmarc
URL	example.com

Description

No DMARC record found

Business Impact

Your organization faces significant reputational damage as customers and partners may lose trust after receiving phishing emails spoofed from your domain. You could face regulatory compliance violations (GDPR, SOC 2, industry standards) and potential legal liability if customers are harmed by spoofed emails. Financial losses can result from incident response costs, customer churn, and potential fines from regulatory bodies.

Remediation

Add DMARC record to prevent email spoofing.

PT-11 — Missing SPF Record

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
Type	Missing Spf
URL	example.com

Description

No SPF record found

Business Impact

Missing SPF records expose your organization to significant reputational damage—customers may lose trust if they receive phishing emails appearing to come from your domain. You face compliance risks under regulations like GDPR, HIPAA, and SOC 2, which require email security controls. Financial losses can result from successful phishing attacks, fraud, ransomware infections, or regulatory fines, while your legitimate emails may be marked as spam due to authentication failures.

Remediation

Add SPF record to prevent email spoofing.

PT-12 — Missing Security Header: Permissions-Policy

MEDIUM

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header Permissions Policy
URL	https://example.com/
Method	GET

Description

Controls browser features and APIs. Header is missing.

Business Impact

This vulnerability exposes your organization to significant privacy breach liability, potential GDPR/CCPA violations, and regulatory fines if user data is harvested without proper consent. A publicized incident involving unauthorized camera or microphone access would severely damage customer trust and brand reputation, potentially leading to user churn and negative media coverage. Additionally, you may face legal action from affected users and increased compliance scrutiny from regulators.

Remediation

Add Permissions-Policy header with value: geolocation=(), microphone=(), camera=()

PT-13 — Server Information Disclosure

LOW

Identified on: February 15, 2026

CVSS	3.0
Type	Server Information Disclosure
URL	https://example.com/
Method	GET

Description

Server header exposes server information: Apache/2.4.18 (Ubuntu)

Business Impact

Exposed server information can damage your organization's security posture and reputation if discovered during security audits or by competitors. It may trigger compliance violations in regulated industries (healthcare, finance) where security hardening is required. Additionally, it increases the likelihood of successful targeted attacks, which could lead to data breaches, operational downtime, and associated financial and legal consequences.

Remediation

Remove or obfuscate Server header to prevent information disclosure.

PT-14 — Clickjacking: Missing CSP frame-ancestors

LOW

Identified on: February 15, 2026

CVSS	3.0
Type	Clickjacking Missing Csp
URL	https://example.com/
Method	GET

Description

Missing Content-Security-Policy frame-ancestors directive

Business Impact

Clickjacking attacks could lead to financial fraud, customer account compromise, or regulatory violations depending on your industry (especially critical for financial services and healthcare). Exploitation could damage customer trust and brand reputation if users report unauthorized transactions or data access linked to your platform. Additionally, compliance frameworks like PCI-DSS and various data protection regulations expect organizations to implement standard security controls like CSP headers.

Remediation

Add Content-Security-Policy: frame-ancestors 'none' or frame-ancestors 'self'.

PT-15 — RBAC: Weak Permission Boundaries

LOW

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-284
Type	Rbac Weak Boundaries
URL	https://example.com/
Method	GET

Description

Can use POST method when should only allow GET

Business Impact

Exploiting this vulnerability could result in data integrity issues, compliance violations (GDPR, HIPAA, SOC 2), and potential financial penalties if sensitive data is modified or deleted. Additionally, unauthorized modifications could damage customer trust, trigger incident response costs, and create legal liability if the breach affects user data or business operations.

Remediation

Enforce method-level permissions. Verify user has permission for specific HTTP methods.

PT-16 — Missing Security Header: Referrer-Policy

LOW

Identified on: February 15, 2026

CVSS	3.0
CWE	CWE-693
Type	Missing Security Header Referrer Policy
URL	https://example.com/
Method	GET

Description

Controls referrer information leakage. Header is missing.

Business Impact

Uncontrolled referrer leakage can result in privacy violations affecting user trust and potentially triggering GDPR or similar privacy regulation scrutiny. Competitors or malicious actors could map your application architecture and identify vulnerabilities by analyzing leaked URLs. This oversight, while low-severity individually, signals incomplete security practices that could undermine compliance certifications or customer confidence in your security posture.

Remediation

Add Referrer-Policy header with value: strict-origin-when-cross-origin

PT-17 — Weak Password Policy

LOW

Identified on: February 15, 2026

CVSS	5.0
CWE	CWE-521
Type	Weak Password Policy
URL	https://example.com/

Description

Weak password 'password' was accepted during registration

Business Impact

A breach resulting from weak passwords can lead to significant financial losses through regulatory fines (GDPR, HIPAA, PCI-DSS compliance violations), customer notification costs, and potential lawsuits. The organization faces reputational damage as customers lose trust in the platform's security, potentially resulting in user churn and lost business. Additionally, compromised accounts can be used for fraud, identity theft, or to access confidential business information, creating cascading business disruptions.

Remediation

Enforce strong password policy. Require minimum length, complexity, and check against common password lists.

PT-18 — Subdomain Discovery: 3 subdomains found for example.com

INFO

Identified on: February 15, 2026

CWE	CWE-200
Type	Subdomain Discovery
URL	https://example.com
Method	SUBDOMAIN_ENUMERATIO

Description

Subfinder discovered 3 subdomains for example.com Each subdomain increases the attack surface and should be reviewed.

Business Impact

Unmanaged subdomains create compliance violations (HIPAA, SOC 2, ISO 27001 require complete asset inventory), increase breach likelihood, and can result in regulatory fines and customer trust erosion. If a subdomain is compromised and used to distribute malware or phishing content, your organization bears reputational and legal liability. The cost of incident response and breach notification can far exceed the minimal effort required to properly inventory and secure these assets.

How to Exploit

Remediation

- Review all discovered subdomains.
- Remove or restrict access to unused subdomains.
- Ensure all subdomains have proper security configurations.

PT-19 — Discovered Subdomain: backcast.example.com

INFO

Identified on: February 15, 2026

Type	Subdomain Discovery
URL	https://backcast.example.com
Method	SUBDOMAIN_ENUMERATIO

Description

Subdomain backcast.example.com discovered for domain example.com

Business Impact

An unmonitored subdomain could lead to data breaches affecting customer information or intellectual property, resulting in regulatory fines (GDPR, CCPA) and mandatory breach notifications. Reputational damage occurs when customers learn their data was compromised through a forgotten system, eroding trust and potentially causing customer churn. Incident response costs and legal liability can be substantial if the breach involves sensitive personal or financial data.

PT-20 — Discovered Subdomain: api.example.com

INFO

Identified on: February 15, 2026

Type	Subdomain Discovery
URL	https://api.example.com
Method	SUBDOMAIN_ENUMERATIO

Description

Subdomain api.example.com discovered for domain example.com

Business Impact

An exposed or compromised API could lead to unauthorized access to sensitive customer data, resulting in GDPR, HIPAA, or other regulatory compliance violations and substantial fines. A data breach through this vector would damage customer trust and brand reputation, potentially leading to customer churn and loss of revenue. The organization may also face legal liability, incident response costs, and mandatory breach notification expenses if personal or financial data is compromised.

PT-21 — Discovered Subdomain: era5.example.com

INFO

Identified on: February 15, 2026

Type	Subdomain Discovery
URL	https://era5.example.com
Method	SUBDOMAIN_ENUMERATIO

Description

Subdomain era5.example.com discovered for domain example.com

Business Impact

An unmanaged subdomain could expose sensitive data (customer information, intellectual property, or credentials), leading to regulatory fines under GDPR, HIPAA, or other compliance frameworks. This discovery could indicate gaps in your asset management processes, damaging stakeholder confidence and potentially triggering mandatory breach notifications if data exposure occurs. Reputational damage from a breach traced to a forgotten subdomain signals poor security hygiene to customers and partners.

Appendices

A. Scope & Methodology

Methodologies

The assessment utilized Agent Breach's AI-powered security analysis platform combined with industry-standard penetration testing methodologies:

- AI-Powered Security Analysis Engine
- OWASP Testing Guide v4.2
- PTES (Penetration Testing Execution Standard)
- NIST SP 800-115
- Automated Vulnerability Assessment (OWASP ASVS)

Scope

Target URL: https://example.com

Scan Profile: Deep

Testing Type: Automated Dynamic Application Security Testing (DAST)

Tools Executed

AMASS, API_FUZZER, BRUTE_FORCE, BUSINESS_LOGIC, CLICKJACKING, CLOUD_SECURITY, CORS, CSRF, DESERIALIZATION, DIRB, DNS_SECURITY, FILE_UPLOAD, GRAPHQL, IDOR, JWT_SECURITY, LDAP_INJECTION, NIKTO, NMAP, NUCLEI, PASSWORD_POLICY, RACE_CONDITION, RATE_LIMIT, RBAC, SECURITY_HEADERS, SQLMAP, SSLYZE, SSRF, SUBFINDER, TEMPLATE_INJECTION, TESTSSL, THEHARVESTER, WEBSOCKET, WFUZZ, WHATWEB, WPSCAN, XSSTRIKE

Test Execution Summary

Tool	Action	Status	Findings	Duration (s)
nuclei	run_nuclei	SUCCESS	0	0.9
nikto	run_nikto	SUCCESS	0	0.1
wpscan	run_wpscan	SUCCESS	0	9.1
whatweb	detect_technologies	SUCCESS	1	10.4
sqlmap	run_sqli_scan	SUCCESS	0	19.2
xsstrike	scan_xss	SUCCESS	0	0.0
template_injection	test_template_injection	SUCCESS	0	44.8

ldap_injection	test_ldap_injection	SUCCESS	0	33.6
api_fuzzer	fuzz_api	SUCCESS	0	0.0
wfuzz	fuzz_web_application	SUCCESS	0	1.4
jwt_security	test_jwt_security	SUCCESS	1	0.0
rbac	test_rbac	SUCCESS	1	18.0
idor	test_idor	SUCCESS	1	0.0
brute_force	brute_force_login	SUCCESS	0	11.5
password_policy	test_password_policy	SUCCESS	2	0.9
cors	test_cors	SUCCESS	0	4.2
security_headers	test_security_headers	SUCCESS	9	0.5
sslyze	run_ssl_scan	SUCCESS	0	33.3
testssl	run_testssl	SUCCESS	0	0.2
dns_security	test_dns_security	SUCCESS	2	0.0
clickjacking	test_clickjacking	SUCCESS	2	0.5
csrf	test_csrf	SUCCESS	1	0.5
ssrf	test_ssrf	SUCCESS	3	13.0
file_upload	test_file_upload	SUCCESS	12	1.7
deserialization	test_deserialization	SUCCESS	0	11.2
websocket	test_websocket_security	SUCCESS	0	0.1
rate_limit	test_rate_limiting	SUCCESS	2	7.2
business_logic	test_business_logic	SUCCESS	0	2.8
race_condition	test_race_condition	SUCCESS	1	0.5
dirb	enumerate_directories	SUCCESS	0	0.0
subfinder	discover_subdomains	SUCCESS	4	2.1
amass	enumerate_subdomains_amass	SUCCESS	0	0.0
graphql	discover_graphql	SUCCESS	0	0.0
theharvester	run_theharvester	FAILED	0	3.0
nmap	run_nmap	SUCCESS	2	23.6
cloud_security	test_cloud_security	SUCCESS	1	12.4

B. Vulnerability Coverage

OWASP Top 10 Compliance

The assessment covers all vulnerability categories defined in the OWASP Top 10, ensuring detection of the most critical web application security risks.

Category	Findings
Injection	0
Broken Authentication	1
Sensitive Data Exposure	1
XML External Entities	0
Broken Access Control	1
Security Misconfiguration	2
Cross-Site Scripting	0
Insecure Deserialization	0
Known Vulnerabilities	0
Insufficient Logging	0

Tested Vulnerability Classes

Injection & Execution	Authentication & Access Control
SQL, NoSQL, XPath & LDAP Injection	Broken or Improper Authentication
Cross-Site Scripting (XSS)	Insecure Direct Object Reference (IDOR)
Server-Side Request Forgery (SSRF)	Improper Access Control
Server-Side Template Injection (SSTI)	Cross-Site Request Forgery (CSRF)
Local File Inclusion (LFI)	Unrestricted File Uploads
Insecure Deserialization	Open Redirects
Business Logic Flaws	Improper JWT Verification
Web Cache Poisoning	Hard-Coded Credentials

C. Glossary

Term	Definition
Authentication	The process of verifying the identity of a user, device, or system before granting access to resources.
Authorization	The process of determining what permissions an authenticated user has and what resources they can access.
CVSS	Common Vulnerability Scoring System — a standardized method for rating the severity of security vulnerabilities (0-10 scale).
CWE	Common Weakness Enumeration — a community-developed list of software and hardware weakness types.
DAST	Dynamic Application Security Testing — testing a running application for vulnerabilities from the outside.
IDOR	Insecure Direct Object Reference — when an application provides direct access to objects based on user-supplied input without proper authorization checks.
PII	Personally Identifiable Information — any data that could potentially identify a specific individual.
SQL Injection	A code injection technique where malicious SQL statements are inserted into application data entry points.
SSRF	Server-Side Request Forgery — an attack that forces a server to make requests to unintended locations.
XSS	Cross-Site Scripting — a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users.
WAF	Web Application Firewall — a security device that monitors, filters, and blocks HTTP traffic to and from a web application.