Agent Breach

OWASP WSTG Security Assessment Report

Target: Hack This Site

URL: https://www.hackthissite.org/

Scan Date: 2026-05-29 17:32 UTC

Scan Profile: deep

This report includes findings with severity: Critical, High, Medium only.

1. Executive Summary

Total findings: 51 | Risk Score: 54.72549019607843/100

This report follows the OWASP Web Security Testing Guide (WSTG) v4.2 structure. Findings are mapped to the corresponding WSTG test categories where applicable.

Severity Breakdown

Severity	Count
Critical	1
High	5
Medium	45
Low	0
Info	0
Total	51

2. Scope and Methodology

The assessment was conducted using Agent Breach's automated testing platform, which combines 30+ specialised security testing engines. Tests were mapped to OWASP WSTG categories including information gathering, configuration management, identity management, authentication, authorisation, session management, input validation, error handling, cryptography, and business logic testing.

3. Findings by WSTG Category

WSTG-CONF — Configuration and Deployment Management (6 findings)

[MEDIUM] CORS: Wildcard Origin Allowed

CORS policy allows wildcard origin (*)

Affected URL: https://hackthissite.org

CVSS: 5.0 | CWE: CWE-942

[MEDIUM] CORS: Wildcard Origin Allowed

CORS policy allows wildcard origin (*)

Affected URL: https://www.hackthissite.org/

CVSS: 5.0 | CWE: CWE-942

[MEDIUM] Clickjacking: Missing X-Frame-Options Header

Missing X-Frame-Options header, vulnerable to clickjacking

Affected URL: https://hackthissite.org

CVSS: 5.0 | CWE: CWE-1021

[MEDIUM] Clickjacking: Missing X-Frame-Options Header

Missing X-Frame-Options header, vulnerable to clickjacking

Affected URL: https://www.hackthissite.org

CVSS: 5.0 | CWE: CWE-1021

[MEDIUM] CORS: Wildcard Origin Allowed

CORS policy allows wildcard origin (*)

Affected URL: https://www.hackthissite.org

CVSS: 5.0 | CWE: CWE-942

[MEDIUM] Clickjacking: Missing X-Frame-Options Header

Missing X-Frame-Options header, vulnerable to clickjacking

Affected URL: https://www.hackthissite.org/

CVSS: 5.0 | CWE: CWE-1021

WSTG-ATHN — Authentication (2 findings)

[MEDIUM] Weak Password Policy

Weak password 'password' was accepted during registration

Affected URL: https://www.hackthissite.org

CVSS: 5.0 | CWE: CWE-521

[MEDIUM] Weak Password Policy

Weak password 'password' was accepted during registration

Affected URL: https://www.hackthissite.org/

CVSS: 5.0 | CWE: CWE-521

WSTG-SESS — Session Management (1 finding)

[MEDIUM] CSRF: Missing SameSite Cookie Attribute

Cookie missing SameSite attribute, may be vulnerable to CSRF

Affected URL: https://hackthissite.org

CVSS: 5.0 | CWE: CWE-352

WSTG-INPV — Input Validation (5 findings)

[CRITICAL] SQL Injection (Union-Based) in parameter 'id' (5 instances)

Detected 5 instances of this issue on the same endpoint. Affected variants include: • Union-based SQL injection detected in parameter 'id'. Successfully injected UNION SELECT with 10 columns and the marker string was reflected in the response body. An attacker can extract arbitrary data from the database. • Union-based SQL injection detected in parameter 'q'. Successfully injected UNION SELECT with 10 columns and the marker string was reflected in the response body. An attacker can extract arbit...

Affected URL: https://hp.hackthissite.org

CVSS: 9.8 | CWE: CWE-89

[HIGH] SQL Injection (Boolean-Blind) in parameter 'id'

Boolean-based blind SQL injection detected in parameter 'id'. True condition ('1 AND 1=1') and false condition ('1 AND 1=2') produce consistently different responses (length diff round-1: 152, round-2: 132 bytes).

Affected URL: https://ip100.ip-137-74-187.eu

CVSS: 8.6 | CWE: CWE-89

[HIGH] Unrestricted File Upload (2 instances)

Detected 2 instances of this issue on the same endpoint. Affected variants include: • 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.svg, Content-Type: image/svg+xml. Test: SVG with embedded XSS.

Affected URL: https://hackthissite.org

CVSS: 9.8 | CWE: CWE-434

[HIGH] Unrestricted File Upload (3 instances)

Detected 3 instances of this issue on the same endpoint. Affected variants include: • 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 wi...

Affected URL: https://www.hackthissite.org

CVSS: 9.8 | CWE: CWE-434

[HIGH] SQL Injection (Boolean-Blind) in parameter 'item'

Boolean-based blind SQL injection detected in parameter 'item'. True condition ('1) AND (1=1) --') and false condition ('1) AND (1=2) --') produce consistently different responses (length diff round-1: 191, round-2: 149 bytes).

Affected URL: https://www.hackthissite.org

CVSS: 8.6 | CWE: CWE-89

WSTG-BUSL — Business Logic (1 finding)

[MEDIUM] Rate Limiting Not Implemented

No rate limiting detected. Sent 20 successful requests rapidly.

Affected URL: https://hackthissite.org

CVSS: 5.0 | CWE: CWE-307

Other Findings (36)

[HIGH] Public S3 Bucket Found

S3 bucket hp-uploads is publicly accessible

[MEDIUM] Missing Security Header: X-Frame-Options

Prevents clickjacking attacks. Header is missing.

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Open Port 80/tcp (http-proxy)

Port 80/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Misconfigured Content-Security-Policy: Unsafe Directives

Content-Security-Policy contains unsafe directives: *

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Missing Security Header: Permissions-Policy

Controls browser features and APIs. Header is missing.

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Missing Security Header: Permissions-Policy

Controls browser features and APIs. Header is missing.

[MEDIUM] Missing Security Header: X-Content-Type-Options

Prevents MIME type sniffing. Header is missing.

[MEDIUM] Missing Security Header: X-Frame-Options

Prevents clickjacking attacks. Header is missing.

[MEDIUM] Open Port 443/tcp (http-proxy)

Port 443/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Missing Security Header: X-Content-Type-Options

Prevents MIME type sniffing. Header is missing.

[MEDIUM] Open Port 80/tcp (http-proxy)

Port 80/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Open Port 443/tcp (http-proxy)

Port 443/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Misconfigured Content-Security-Policy: Unsafe Directives

Content-Security-Policy contains unsafe directives: *

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Open Port 80/tcp (http-proxy)

Port 80/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Open Port 80/tcp (http-proxy)

Port 80/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Missing Security Header: Permissions-Policy

Controls browser features and APIs. Header is missing.

[MEDIUM] Open Port 443/tcp (http-proxy)

Port 443/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Open Port 80/tcp (http-proxy)

Port 80/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Missing Security Header: X-Content-Type-Options

Prevents MIME type sniffing. Header is missing.

[MEDIUM] Misconfigured Content-Security-Policy: Unsafe Directives

Content-Security-Policy contains unsafe directives: *

[MEDIUM] Open Port 443/tcp (http-proxy)

Port 443/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Open Port 443/tcp (http-proxy)

Port 443/tcp is open and running http-proxy 1.3.1 - 1.9.0

[MEDIUM] Missing DMARC Record

No DMARC record found

[MEDIUM] Missing SPF Record

No SPF record found

[MEDIUM] Missing Security Header: X-Frame-Options

Prevents clickjacking attacks. Header is missing.

4. Risk Rating Methodology

Findings are rated using the OWASP Risk Rating Methodology, considering likelihood and impact factors. Severity levels map as follows: Critical (CVSS 9.0-10.0), High (7.0-8.9), Medium (4.0-6.9), Low (0.1-3.9), Info (informational).

Report generated by Agent Breach on 2026-06-13 10:30 UTC