Agent Breach

29 May 2026

Penetration Test Report

For Hack This Site

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

Table of Contents

1. Executive Summary

1.1 Confidentiality Statement

This document is the exclusive property of Hack This Site 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 Hack This Site and Agent Breach. Hack This Site may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

1.2 Report Overview

On 29 May 2026, Agent Breach conducted web application penetration tests for Hack This Site 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://www.hackthissite.org/ and its associated API endpoints. A **Deep** scan profile was used.

Total scan duration: **70.7 minutes**.

1.3 Key Findings & Business Impact

CRITICAL — **SQL Injection (Union-Based) in parameter 'id' (5 instances)**

A successful SQL injection attack could result in a massive data breach exposing customer personal information, leading to GDPR, CCPA, and other regulatory fines (potentially millions of dollars). Your organization would face severe reputational damage, loss of customer trust, and potential legal liability from affected users. Additionally, incident response, forensics, notification costs, and potential business interruption could result in significant financial losses.

HIGH — **SQL Injection (Boolean-Blind) in parameter 'id'**

A successful exploitation could result in a data breach exposing customer personal information, leading to regulatory fines under GDPR, CCPA, and other privacy laws—potentially costing millions of dollars. Your organization would face severe reputational damage, loss of customer trust, and potential legal liability if customer data is compromised. Additionally, operational disruption from incident response, forensics, and system remediation could impact business continuity and revenue.

HIGH — **Public S3 Bucket Found**

A public S3 bucket exposure can result in regulatory fines (GDPR, HIPAA, PCI-DSS violations), loss of customer trust, and potential lawsuits if personal data is compromised. Your organization could face significant reputational damage and operational disruption if sensitive intellectual property or customer information is leaked. Financial impact includes breach notification costs, incident response, potential ransom demands, and loss of business.

HIGH — **Unrestricted File Upload (2 instances)**

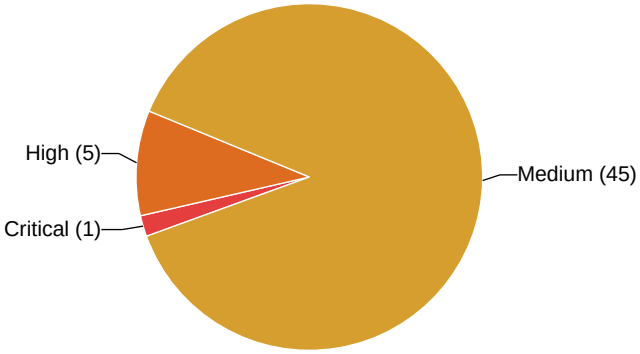
A successful exploit could result in a complete data breach exposing customer information, leading to regulatory fines (GDPR, CCPA, etc.), mandatory breach notifications, and potential lawsuits. Your organization's reputation would suffer significant damage, eroding customer trust and potentially causing loss of business. Additionally, your infrastructure could be used to launch attacks on other organizations, creating legal liability and incident response costs that could reach hundreds of thousands of dollars.

HIGH — Unrestricted File Upload (3 instances)

A successful exploit could result in a complete data breach exposing customer information, leading to regulatory fines (GDPR, CCPA), mandatory breach notifications, and potential lawsuits. Your organization's reputation and customer trust would be severely damaged, potentially resulting in loss of business and market share. Incident response, forensics, system rebuilds, and legal costs could easily reach hundreds of thousands of dollars.

2. Findings

2.1 Vulnerability Distribution



- **Critical-severity** issues (1) require immediate remediation as they allow direct system compromise or data breach.

- **High-severity** issues (5) could result in unauthorized access, data exposure, or significant system manipulation.

- **Medium-severity** issues (45) may enable unauthorized actions, information disclosure, or user manipulation.

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

2.2 Master Findings Table

ID	Title	State	Severity
PT-1	SQL Injection (Union-Based) in parameter 'id' (5 instances)	Unresolved	Critical
PT-2	SQL Injection (Boolean-Blind) in parameter 'id'	Unresolved	High
PT-3	Public S3 Bucket Found	Unresolved	High
PT-4	Unrestricted File Upload (2 instances)	Unresolved	High
PT-5	Unrestricted File Upload (3 instances)	Unresolved	High
PT-6	SQL Injection (Boolean-Blind) in parameter 'item'	Unresolved	High
PT-7	Missing Security Header: X-Frame-Options	Unresolved	Medium
PT-8	Missing SPF Record	Unresolved	Medium
PT-9	Missing DMARC Record	Unresolved	Medium
PT-10	Open Port 80/tcp (http-proxy)	Unresolved	Medium
PT-11	CSRF: Missing SameSite Cookie Attribute	Unresolved	Medium
PT-12	Misconfigured Content-Security-Policy: Unsafe Directives	Unresolved	Medium
PT-13	Missing SPF Record	Unresolved	Medium
PT-14	CORS: Wildcard Origin Allowed	Unresolved	Medium
PT-15	Missing Security Header: Permissions-Policy	Unresolved	Medium
PT-16	Missing DMARC Record	Unresolved	Medium
PT-17	Weak Password Policy	Unresolved	Medium
PT-18	Missing Security Header: Permissions-Policy	Unresolved	Medium
PT-19	Missing Security Header: X-Content-Type-Options	Unresolved	Medium
PT-20	Missing Security Header: X-Frame-Options	Unresolved	Medium
PT-21	Open Port 443/tcp (http-proxy)	Unresolved	Medium
PT-22	Missing SPF Record	Unresolved	Medium
PT-23	Missing Security Header: X-Content-Type-Options	Unresolved	Medium
PT-24	CORS: Wildcard Origin Allowed	Unresolved	Medium
PT-25	Open Port 80/tcp (http-proxy)	Unresolved	Medium

PT-26	Open Port 443/tcp (http-proxy)	Unresolved	Medium
PT-27	Missing DMARC Record	Unresolved	Medium
PT-28	Missing SPF Record	Unresolved	Medium
PT-29	Misconfigured Content-Security-Policy: Unsafe Directives	Unresolved	Medium
PT-30	Missing DMARC Record	Unresolved	Medium
PT-31	Open Port 80/tcp (http-proxy)	Unresolved	Medium
PT-32	Open Port 80/tcp (http-proxy)	Unresolved	Medium
PT-33	Missing DMARC Record	Unresolved	Medium
PT-34	Missing Security Header: Permissions-Policy	Unresolved	Medium
PT-35	Open Port 443/tcp (http-proxy)	Unresolved	Medium
PT-36	Rate Limiting Not Implemented	Unresolved	Medium
PT-37	Open Port 80/tcp (http-proxy)	Unresolved	Medium
PT-38	Missing DMARC Record	Unresolved	Medium
PT-39	Clickjacking: Missing X-Frame-Options Header	Unresolved	Medium
PT-40	Missing Security Header: X-Content-Type-Options	Unresolved	Medium
PT-41	Clickjacking: Missing X-Frame-Options Header	Unresolved	Medium
PT-42	Misconfigured Content-Security-Policy: Unsafe Directives	Unresolved	Medium
PT-43	CORS: Wildcard Origin Allowed	Unresolved	Medium
PT-44	Clickjacking: Missing X-Frame-Options Header	Unresolved	Medium
PT-45	Open Port 443/tcp (http-proxy)	Unresolved	Medium
PT-46	Missing SPF Record	Unresolved	Medium
PT-47	Open Port 443/tcp (http-proxy)	Unresolved	Medium
PT-48	Missing DMARC Record	Unresolved	Medium
PT-49	Missing SPF Record	Unresolved	Medium
PT-50	Weak Password Policy	Unresolved	Medium
PT-51	Missing Security Header: X-Frame-Options	Unresolved	Medium

2.3 Detailed Findings

PT-1 — SQL Injection (Union-Based) in parameter 'id' (5 instances)

CRITICAL

Identified on: May 29, 2026

CVSS	9.8
CWE	CWE-89
Type	Sql Injection
URL	https://hp.hackthissite.org
Method	GET

Description

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 arbitrary data from the database. • Union-based SQL injection detected in parameter 'user'. 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 'item'. 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 'cat'. 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.

Business Impact

A successful SQL injection attack could result in a massive data breach exposing customer personal information, leading to GDPR, CCPA, and other regulatory fines (potentially millions of dollars). Your organization would face severe reputational damage, loss of customer trust, and potential legal liability from affected users. Additionally, incident response, forensics, notification costs, and potential business interruption could result in significant financial losses.

How to Exploit

Step 1: Navigate to https://hp.hackthissite.org

Step 2: Set parameter 'id' to payload: ' UNION SELECT 'agentbreach_sqli_marker_8x7k',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL --

Step 3: Observe union-based SQL injection indicator in the response

5 instance(s) detected:

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

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.

Parameter: id

• **SQL Injection (Union-Based) in parameter 'q'** [CRITICAL]

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 arbitrary data from the database.

Parameter: q

• **SQL Injection (Union-Based) in parameter 'user'** [CRITICAL]

Union-based SQL injection detected in parameter 'user'. 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.

Parameter: user

• **SQL Injection (Union-Based) in parameter 'item'** [CRITICAL]

Union-based SQL injection detected in parameter 'item'. 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.

Parameter: item

• **SQL Injection (Union-Based) in parameter 'cat'** [CRITICAL]

Union-based SQL injection detected in parameter 'cat'. 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.

Parameter: cat

Remediation

- Use parameterized queries (prepared statements) for all database access.
- Never concatenate user input into SQL strings.
- Apply input validation and use an ORM where possible.

References

- https://owasp.org/www-community/attacks/SQL_Injection
- https://cwe.mitre.org/data/definitions/89.html
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

PT-2 — SQL Injection (Boolean-Blind) in parameter 'id'

HIGH

Identified on: May 29, 2026

CVSS	8.6
CWE	CWE-89
Type	Sql Injection
URL	https://ip100.ip-137-74-187.eu
Method	GET

Description

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).

Business Impact

A successful exploitation could result in a data breach exposing customer personal information, leading to regulatory fines under GDPR, CCPA, and other privacy laws—potentially costing millions of dollars. Your organization would face severe reputational damage, loss of customer trust, and potential legal liability if customer data is compromised. Additionally, operational disruption from incident response, forensics, and system remediation could impact business continuity and revenue.

How to Exploit

Step 1: Navigate to https://ip100.ip-137-74-187.eu

Step 2: Set parameter 'id' to payload: 1 AND 1=1

Step 3: Observe boolean-blind SQL injection indicator in the response

```
curl -ks 'https://ip100.ip-137-74-187.eu?id=1+AND+1%3D1'
```

```
Payload: 1 AND 1=1
```

Remediation

- Use parameterized queries (prepared statements) for all database access.
- Never concatenate user input into SQL strings.
- Apply input validation and use an ORM where possible.

References

- https://owasp.org/www-community/attacks/SQL_Injection
- https://cwe.mitre.org/data/definitions/89.html
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

PT-3 — Public S3 Bucket Found

HIGH

Identified on: May 29, 2026

CVSS	7.5
CWE	CWE-284
Type	Public S3 Bucket
URL	https://hp-uploads.s3.amazonaws.com

Description

S3 bucket hp-uploads is publicly accessible

Business Impact

A public S3 bucket exposure can result in regulatory fines (GDPR, HIPAA, PCI-DSS violations), loss of customer trust, and potential lawsuits if personal data is compromised. Your organization could face significant reputational damage and operational disruption if sensitive intellectual property or customer information is leaked. Financial impact includes breach notification costs, incident response, potential ransom demands, and loss of business.

Remediation

- Make S3 bucket private.
- Use bucket policies to restrict access.
- Enable bucket versioning and logging.

PT-4 — Unrestricted File Upload (2 instances)

HIGH

Identified on: May 29, 2026

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

Description

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.

Business Impact

A successful exploit could result in a complete data breach exposing customer information, leading to regulatory fines (GDPR, CCPA, etc.), mandatory breach notifications, and potential lawsuits. Your organization's reputation would suffer significant damage, eroding customer trust and potentially causing loss of business. Additionally, your infrastructure could be used to launch attacks on other organizations, creating legal liability and incident response costs that could reach hundreds of thousands of dollars.

How to Exploit

2 instance(s) detected:

- **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: 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.

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 — Unrestricted File Upload (3 instances)

HIGH

Identified on: May 29, 2026

CVSS	9.8
CWE	CWE-434
Type	Unrestricted File Upload
URL	https://www.hackthissite.org
Method	POST

Description

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 with embedded XSS.

Business Impact

A successful exploit could result in a complete data breach exposing customer information, leading to regulatory fines (GDPR, CCPA), mandatory breach notifications, and potential lawsuits. Your organization's reputation and customer trust would be severely damaged, potentially resulting in loss of business and market share. Incident response, forensics, system rebuilds, and legal costs could easily reach hundreds of thousands of dollars.

How to Exploit

3 instance(s) detected:

- **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.

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-6 — SQL Injection (Boolean-Blind) in parameter 'item'

HIGH

Identified on: May 29, 2026

CVSS	8.6
CWE	CWE-89
Type	Sql Injection
URL	https://www.hackthissite.org
Method	GET

Description

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).

Business Impact

A successful SQL injection attack could result in a data breach exposing customer personal information, leading to regulatory fines (GDPR, CCPA, etc.), legal liability, and mandatory breach notifications. Your organization's reputation and customer trust could suffer significantly, potentially resulting in loss of business and competitive disadvantage. Financial impact includes incident response costs, forensic investigations, remediation efforts, and potential lawsuits from affected customers.

How to Exploit

Step 1: Navigate to https://www.hackthissite.org

Step 2: Set parameter 'item' to payload: 1) AND (1=1) --

Step 3: Observe boolean-blind SQL injection indicator in the response

```
curl -ks 'https://www.hackthissite.org?item=1%29+AND+%281%3D1%29+--'
```

```
Payload: 1) AND (1=1) --
```

Remediation

- Use parameterized queries (prepared statements) for all database access.
- Never concatenate user input into SQL strings.
- Apply input validation and use an ORM where possible.

References

- https://owasp.org/www-community/attacks/SQL_Injection
- https://cwe.mitre.org/data/definitions/89.html
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

PT-7 — Missing Security Header: X-Frame-Options

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Frame Options
URL	https://www.hackthissite.org/
Method	GET

Description

Prevents clickjacking attacks. Header is missing.

Remediation

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

PT-8 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	ip101.ip-137-74-187.eu

Description

No SPF record found

Business Impact

Email spoofing can result in significant financial losses through BEC fraud, where attackers impersonate executives to authorize fraudulent wire transfers or payments. Your organization's reputation can be severely damaged if customers receive phishing emails appearing to come from you, leading to loss of trust and potential customer churn. You may also face compliance violations under regulations like GDPR, HIPAA, or industry standards (PCI-DSS, SOC 2) that require email authentication controls, resulting in audit failures or regulatory penalties.

Remediation

Add SPF record to prevent email spoofing.

PT-9 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	ip102.ip-137-74-187.eu

Description

No DMARC record found

Business Impact

Your organization faces significant reputational damage as customers may lose trust after receiving phishing emails from your spoofed domain. You could face compliance violations under regulations like GDPR, HIPAA, or industry standards (PCI-DSS) that require email authentication controls. Financial losses can result from successful phishing attacks targeting employees or customers, plus costs associated with incident response and remediation.

Remediation

Add DMARC record to prevent email spoofing.

PT-10 — Open Port 80/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.103:80
Method	NETWORK_SCAN

Description

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

Business Impact

Exposed proxy services can lead to data breaches affecting customer information, intellectual property, or financial records—resulting in regulatory fines (GDPR, HIPAA, PCI-DSS) and mandatory breach notifications. Your organization's reputation and customer trust could suffer significantly if users' traffic is compromised or if your infrastructure is used to attack others. Financial losses include incident response costs, legal fees, potential ransom demands, and loss of business due to service disruption or loss of customer confidence.

PT-11 — CSRF: Missing SameSite Cookie Attribute

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-352
Type	Csrf Missing Samesite
URL	https://hackthissite.org

Description

Cookie missing SameSite attribute, may be vulnerable to CSRF

Business Impact

A successful CSRF attack could result in unauthorized transactions, data manipulation, or account takeovers affecting multiple users simultaneously, leading to direct financial losses and potential regulatory fines under GDPR, PCI-DSS, or other compliance frameworks. Customer trust and brand reputation suffer significantly when users discover their accounts were compromised through security oversights. Legal liability and incident response costs can be substantial, particularly if the vulnerability was known but unpatched.

Remediation

Set SameSite=Strict or SameSite=Lax on all cookies.

PT-12 — Misconfigured Content-Security-Policy: Unsafe Directives

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Misconfigured Content Security Policy
URL	https://www.hackthissite.org
Method	GET

Description

Content-Security-Policy contains unsafe directives: *

Business Impact

Failure to remediate this medium severity vulnerability could result in data breaches, compliance violations, reputation damage, and financial losses.

Remediation

Remove unsafe directives from CSP. Use nonces or hashes instead of 'unsafe-inline'.

PT-13 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	ip102.ip-137-74-187.eu

Description

No SPF record found

Business Impact

Email spoofing attacks can result in significant financial losses through wire fraud, credential theft, and ransomware infections. Your organization faces reputational damage when customers receive fraudulent emails appearing to come from your domain, eroding trust and brand credibility. Additionally, you may face compliance violations under regulations like GDPR, HIPAA, or industry standards (PCI-DSS) that require email authentication controls.

Remediation

Add SPF record to prevent email spoofing.

PT-14 — CORS: Wildcard Origin Allowed

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-942
Type	Cors Wildcard
URL	https://hackthissite.org
Method	GET

Description

CORS policy allows wildcard origin (*)

Business Impact

A successful exploit could lead to unauthorized data access affecting customer privacy and triggering regulatory fines under GDPR, CCPA, or industry-specific regulations like HIPAA or PCI-DSS. Customer trust and brand reputation suffer significantly when users discover their accounts were compromised through your security misconfiguration. Financial losses include incident response costs, potential legal liability, mandatory breach notifications, and loss of customer confidence that impacts revenue.

Remediation

Use specific allowed origins instead of wildcard. Maintain allowlist of trusted domains.

PT-15 — Missing Security Header: Permissions-Policy

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header Permissions Policy
URL	https://www.hackthissite.org
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 fines for unauthorized data collection, and severe reputational damage if users discover their cameras or microphones were accessed without consent. Regulatory bodies and privacy advocates increasingly scrutinize companies that fail to implement basic security headers, and a breach involving device access could result in class-action lawsuits. Additionally, loss of user trust directly impacts customer retention and brand value.

Remediation

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

PT-16 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	forums.hackthissite.org

Description

No DMARC record found

Remediation

Add DMARC record to prevent email spoofing.

PT-17 — Weak Password Policy

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-521
Type	Weak Password Policy
URL	https://www.hackthissite.org

Description

Weak password 'password' was accepted during registration

Remediation

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

PT-18 — Missing Security Header: Permissions-Policy

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header Permissions Policy
URL	https://www.hackthissite.org/
Method	GET

Description

Controls browser features and APIs. Header is missing.

Remediation

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

PT-19 — Missing Security Header: X-Content-Type-Options

MEDIUM

Identified on: May 29, 2026

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

Description

Prevents MIME type sniffing. Header is missing.

Remediation

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

PT-20 — Missing Security Header: X-Frame-Options

MEDIUM

Identified on: May 29, 2026

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

Description

Prevents clickjacking attacks. Header is missing.

Remediation

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

PT-21 — Open Port 443/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.104:443
Method	NETWORK_SCAN

Description

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

Business Impact

A compromised proxy could lead to theft of sensitive customer data, intellectual property, or financial information, resulting in regulatory fines (GDPR, HIPAA, PCI-DSS) and loss of customer trust. Your organization could face reputational damage, legal liability, and operational disruption if systems are compromised or taken offline. The financial impact includes incident response costs, potential ransom demands, and long-term loss of business due to damaged reputation.

PT-22 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	www.hackthissite.org

Description

No SPF record found

Remediation

Add SPF record to prevent email spoofing.

PT-23 — Missing Security Header: X-Content-Type-Options

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Content Type Options
URL	https://www.hackthissite.org
Method	GET

Description

Prevents MIME type sniffing. Header is missing.

Remediation

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

PT-24 — CORS: Wildcard Origin Allowed

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-942
Type	Cors Wildcard
URL	https://www.hackthissite.org/
Method	GET

Description

CORS policy allows wildcard origin (*)

Remediation

Use specific allowed origins instead of wildcard. Maintain allowlist of trusted domains.

PT-25 — Open Port 80/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.104:80
Method	NETWORK_SCAN

Description

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

PT-26 — Open Port 443/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.100:443
Method	NETWORK_SCAN

Description

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

PT-27 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	ip100.ip-137-74-187.eu

Description

No DMARC record found

Remediation

Add DMARC record to prevent email spoofing.

PT-28 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	ip100.ip-137-74-187.eu

Description

No SPF record found

Remediation

Add SPF record to prevent email spoofing.

PT-29 — Misconfigured Content-Security-Policy: Unsafe Directives

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Misconfigured Content Security Policy
URL	https://hackthissite.org
Method	GET

Description

Content-Security-Policy contains unsafe directives: *

Business Impact

Failure to remediate this medium severity vulnerability could result in data breaches, compliance violations, reputation damage, and financial losses.

Remediation

Remove unsafe directives from CSP. Use nonces or hashes instead of 'unsafe-inline'.

PT-30 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	www.hackthissite.org

Description

No DMARC record found

Remediation

Add DMARC record to prevent email spoofing.

PT-31 — Open Port 80/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.101:80
Method	NETWORK_SCAN

Description

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

PT-32 — Open Port 80/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.100:80
Method	NETWORK_SCAN

Description

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

PT-33 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	ip103.ip-137-74-187.eu

Description

No DMARC record found

Remediation

Add DMARC record to prevent email spoofing.

PT-34 — Missing Security Header: Permissions-Policy

MEDIUM

Identified on: May 29, 2026

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

Description

Controls browser features and APIs. Header is missing.

Remediation

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

PT-35 — Open Port 443/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.101:443
Method	NETWORK_SCAN

Description

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

Business Impact

This vulnerability could lead to unauthorized access to sensitive customer or employee data, resulting in GDPR, HIPAA, or PCI-DSS compliance violations with substantial fines. A successful breach could damage your organization's reputation, erode customer trust, and result in legal liability if customer data is compromised. The proxy could also be weaponized for distributed attacks, potentially resulting in your IP address being blacklisted and affecting legitimate business operations.

PT-36 — Rate Limiting Not Implemented

MEDIUM

Identified on: May 29, 2026

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

Description

No rate limiting detected. Sent 20 successful requests rapidly.

Business Impact

Uncontrolled API abuse can result in unexpected infrastructure costs from excessive server usage, potential data breaches if credentials are compromised through brute force, and compliance violations (GDPR, PCI-DSS require reasonable security controls). A public incident involving account takeovers or data theft due to missing rate limiting can severely damage customer trust and brand reputation, potentially resulting in customer churn and regulatory fines.

Remediation

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

PT-37 — Open Port 80/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.102:80
Method	NETWORK_SCAN

Description

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

Business Impact

A compromised proxy service could lead to data breaches affecting customers or employees, resulting in regulatory fines (GDPR, HIPAA, PCI-DSS), legal liability, and mandatory breach notifications. Your organization's reputation could suffer significantly, leading to loss of customer trust and business. Additionally, attackers could use the compromised proxy to launch attacks against your partners or customers, making your company liable for downstream damages.

PT-38 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	hp.hackthissite.org

Description

No DMARC record found

Business Impact

Your organization faces significant reputational damage if customers receive phishing emails appearing to come from your domain, potentially eroding trust and customer relationships. You may face compliance violations depending on your industry (financial services, healthcare, etc. often have email authentication requirements), resulting in regulatory fines or audit failures. Financial losses can occur through customer fraud, support costs from handling compromised accounts, and potential legal liability if your spoofed domain is used in successful attacks against third parties.

Remediation

Add DMARC record to prevent email spoofing.

PT-39 — Clickjacking: Missing X-Frame-Options Header

MEDIUM

Identified on: May 29, 2026

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

Description

Missing X-Frame-Options header, vulnerable to clickjacking

Business Impact

Clickjacking attacks can result in unauthorized transactions, compromised user accounts, and loss of customer trust. Regulatory compliance frameworks (GDPR, PCI-DSS, SOC 2) often require protection against clickjacking, making this vulnerability a compliance violation. Publicized clickjacking incidents damage brand reputation and can lead to financial losses through fraud, legal liability, and customer churn.

Remediation

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

PT-40 — Missing Security Header: X-Content-Type-Options

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Content Type Options
URL	https://www.hackthissite.org/
Method	GET

Description

Prevents MIME type sniffing. Header is missing.

Business Impact

A successful MIME type sniffing attack could result in unauthorized access to customer accounts, leading to potential data breaches and regulatory fines under GDPR, CCPA, or industry-specific standards like PCI-DSS. Reputation damage is significant—customers lose trust in your security posture when vulnerabilities are exploited, potentially leading to customer churn and negative media coverage. The cost of incident response, forensics, and remediation can range from thousands to millions of dollars depending on breach scope.

Remediation

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

PT-41 — Clickjacking: Missing X-Frame-Options Header

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-1021
Type	Clickjacking Missing X Frame Options
URL	https://www.hackthissite.org
Method	GET

Description

Missing X-Frame-Options header, vulnerable to clickjacking

Business Impact

Clickjacking attacks can result in direct financial losses through fraudulent transactions and significant reputational damage when users blame your company for unauthorized actions on their accounts. Depending on your industry (finance, healthcare, e-commerce), this vulnerability may violate compliance requirements like PCI-DSS, HIPAA, or GDPR, leading to regulatory fines and legal liability. Customer trust erodes quickly when accounts are compromised through your application, even if the attack originated externally.

Remediation

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

PT-42 — Misconfigured Content-Security-Policy: Unsafe Directives

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Misconfigured Content Security Policy
URL	https://www.hackthissite.org/
Method	GET

Description

Content-Security-Policy contains unsafe directives: *

Business Impact

Failure to remediate this medium severity vulnerability could result in data breaches, compliance violations, reputation damage, and financial losses.

Remediation

Remove unsafe directives from CSP. Use nonces or hashes instead of 'unsafe-inline'.

PT-43 — CORS: Wildcard Origin Allowed

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-942
Type	Cors Wildcard
URL	https://www.hackthissite.org
Method	GET

Description

CORS policy allows wildcard origin (*)

Business Impact

This vulnerability exposes your organization to data breaches affecting customer information, financial records, or intellectual property, resulting in regulatory fines (GDPR, CCPA, HIPAA), mandatory breach notifications, and loss of customer trust. A successful attack could damage your reputation, lead to customer churn, and result in legal liability if user data is compromised. The financial impact includes incident response costs, potential regulatory penalties, and long-term brand damage.

Remediation

Use specific allowed origins instead of wildcard. Maintain allowlist of trusted domains.

PT-44 — Clickjacking: Missing X-Frame-Options Header

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-1021
Type	Clickjacking Missing X Frame Options
URL	https://www.hackthissite.org/
Method	GET

Description

Missing X-Frame-Options header, vulnerable to clickjacking

Business Impact

Clickjacking attacks can result in direct financial losses through fraudulent transactions, regulatory fines for failing to implement standard security controls, and severe reputational damage when customers discover they've been deceived. Compliance frameworks (PCI-DSS, HIPAA, GDPR) expect organizations to implement basic security headers, making this vulnerability a compliance violation. A successful attack could erode customer trust and expose the organization to liability lawsuits.

Remediation

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

PT-45 — Open Port 443/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.102:443
Method	NETWORK_SCAN

Description

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

Business Impact

A data breach through this exposure could result in significant financial penalties under regulations like GDPR, HIPAA, or PCI-DSS, potentially costing hundreds of thousands of dollars. Your organization could face reputational damage and loss of customer trust if sensitive data is compromised, and you may be held liable if attackers use your proxy to attack third parties. Additionally, incident response, forensics, and remediation costs could strain IT budgets and divert resources from strategic initiatives.

PT-46 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	ip103.ip-137-74-187.eu

Description

No SPF record found

Business Impact

Missing SPF records expose your organization to brand damage and reputation harm when customers receive phishing emails impersonating your company. You may face compliance violations under regulations like GDPR, HIPAA, or industry standards (PCI-DSS, SOC 2) that require email authentication controls. Financial losses can result from successful BEC attacks, fraud, data breaches initiated through phishing, and the costs of incident response and customer notification.

Remediation

Add SPF record to prevent email spoofing.

PT-47 — Open Port 443/tcp (http-proxy)

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Open Port
URL	137.74.187.103:443
Method	NETWORK_SCAN

Description

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

Business Impact

Exploitation could lead to unauthorized access to customer data, resulting in GDPR, HIPAA, or PCI-DSS compliance violations and associated fines. A data breach through this vector would damage customer trust and brand reputation, potentially resulting in loss of business and legal liability. Financial impact includes incident response costs, notification expenses, regulatory penalties, and potential lawsuits from affected parties.

PT-48 — Missing DMARC Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Dmarc
URL	ip101.ip-137-74-187.eu

Description

No DMARC record found

Business Impact

Your organization faces significant reputational damage if customers receive phishing emails appearing to come from you, potentially eroding trust and brand value. You may face regulatory compliance issues, as many standards (HIPAA, PCI-DSS, SOC 2) increasingly require DMARC implementation. Financial losses can occur through direct fraud, incident response costs, and potential legal liability if your domain is used to compromise third parties.

Remediation

Add DMARC record to prevent email spoofing.

PT-49 — Missing SPF Record

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
Type	Missing Spf
URL	hp.hackthissite.org

Description

No SPF record found

Business Impact

Missing SPF records expose your organization to brand impersonation, which can result in customer trust erosion, financial fraud, and potential data breaches through phishing campaigns. You may face compliance violations under regulations like GDPR, HIPAA, or industry standards (PCI-DSS) that require email authentication controls. The reputational damage from customers receiving convincing phishing emails impersonating your company can be severe and costly to recover from.

Remediation

Add SPF record to prevent email spoofing.

PT-50 — Weak Password Policy

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-521
Type	Weak Password Policy
URL	https://www.hackthissite.org/

Description

Weak password 'password' was accepted during registration

Business Impact

A successful attack exploiting weak passwords can result in significant data breaches, leading to regulatory fines (GDPR, HIPAA, PCI-DSS violations), loss of customer trust, and reputational damage that takes years to recover from. Organizations may face legal liability, mandatory breach notifications, and costly incident response efforts. Additionally, compromised accounts can be used for fraud, ransomware deployment, or lateral movement within the network, multiplying the financial impact.

Remediation

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

PT-51 — Missing Security Header: X-Frame-Options

MEDIUM

Identified on: May 29, 2026

CVSS	5.0
CWE	CWE-693
Type	Missing Security Header X Frame Options
URL	https://www.hackthissite.org
Method	GET

Description

Prevents clickjacking attacks. Header is missing.

Business Impact

A successful clickjacking attack could result in financial losses through unauthorized transactions, compromised user accounts, and erosion of customer trust in your platform's security. Depending on your industry, missing security headers may violate compliance requirements (PCI-DSS, HIPAA, GDPR) and expose your organization to regulatory fines. Additionally, public disclosure of this vulnerability could damage your reputation and provide attackers with a documented entry point for social engineering campaigns.

Remediation

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

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://www.hackthissite.org/

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, HYDRA, IDOR, JWT_SECURITY, KNOCKPY, LDAP_INJECTION, NIKTO, NMAP, NUCLEI, PASSWORD_POLICY, RACE_CONDITION, RATE_LIMIT, RBAC, REVERSE_IP, SECURITY_HEADERS, SQLMAP, SSLYZE, SSRF, SUBFINDER, TEMPLATE_INJECTION, TESTSSL, THEHARVESTER, WEBSOCKET, WFUZZ, WHATWEB, WPSCAN, XSSTRIKE

Test Execution Summary

Tool	Action	Status	Findings	Duration (s)
subfinder	discover_subdomains	SUCCESS	0	1.4
amass	enumerate_subdomains_amass	SUCCESS	0	0.2
knockpy	discover_subdomains_knockpy	FAILED	0	0.0
reverse_ip	discover_reverse_ip_domains	SUCCESS	9	9.9
theharvester	run_theharvester	FAILED	0	6.2
nuclei	run_nuclei	SUCCESS	0	2.8
nikto	run_nikto	SUCCESS	0	1.0

wpscan	run_wpscan	SUCCESS	0	354.3
whatweb	detect_technologies	SUCCESS	8	114.9
sqlmap	run_sqli_scan	SUCCESS	68	612.2
xsstrike	scan_xss	SUCCESS	0	0.8
template_injection	test_template_injection	SUCCESS	0	485.3
ldap_injection	test_ldap_injection	SUCCESS	0	348.1
api_fuzzer	fuzz_api	SUCCESS	0	0.2
wfuzz	fuzz_web_application	SUCCESS	0	11.7
jwt_security	test_jwt_security	SUCCESS	9	0.0
rbac	test_rbac	SUCCESS	3	234.2
idor	test_idor	SUCCESS	9	0.0
brute_force	brute_force_login	SUCCESS	6	52.2
password_policy	test_password_policy	SUCCESS	4	33.0
hydra	run_hydra	SUCCESS	9	79.3
cors	test_cors	SUCCESS	3	37.1
security_headers	test_security_headers	SUCCESS	21	3.8
sslyze	run_ssl_scan	FAILED	0	11.7
testssl	run_testssl	SUCCESS	0	2.0
dns_security	test_dns_security	SUCCESS	15	7.0
clickjacking	test_clickjacking	SUCCESS	12	3.2
csrf	test_csrf	SUCCESS	3	18.8
ssrf	test_ssrf	SUCCESS	18	347.7
file_upload	test_file_upload	SUCCESS	36	36.0
deserialization	test_deserialization	SUCCESS	0	73.9
websocket	test_websocket_security	SUCCESS	0	0.1
rate_limit	test_rate_limiting	SUCCESS	12	28.2
business_logic	test_business_logic	SUCCESS	0	18.0
race_condition	test_race_condition	SUCCESS	2	129.8
dirb	enumerate_directories	SUCCESS	0	0.4
graphql	discover_graphql	SUCCESS	0	0.1

nmap	run_nmap	SUCCESS	18	418.0
cloud_security	test_cloud_security	SUCCESS	90	113.8

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	3
Broken Authentication	2
Sensitive Data Exposure	0
XML External Entities	0
Broken Access Control	1
Security Misconfiguration	6
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.