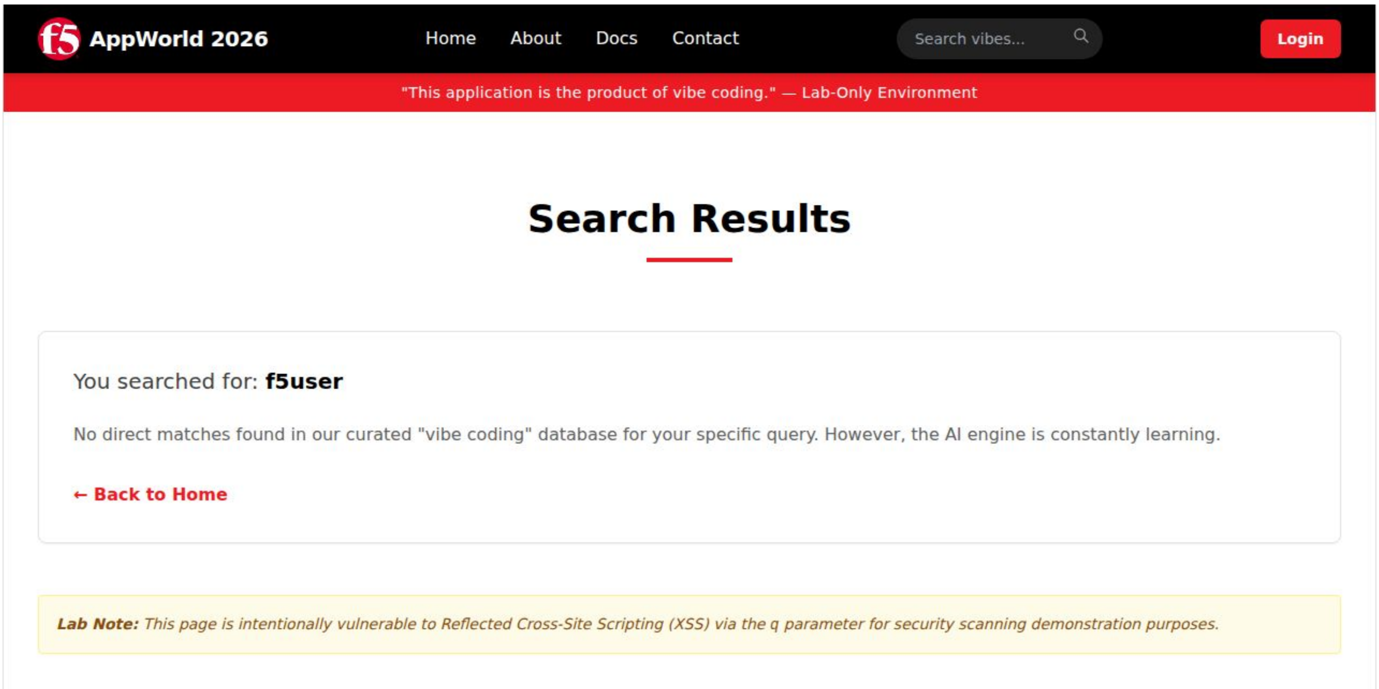
Penetration Test Report

System
f5-ai-generated-app Web Application

Penetration Test Period
February 12, 2026 19:27 PM — 20:16 PM

Scope
https://f5-ai-generated-app.xc.hvf5lab.com/

Conducted By
F5 Distributed Cloud Web App Scanning



Introduction

This document contains the results of the automated penetration test conducted on the f5-ai-generated-app web application.

The penetration testing was performed in the period February 12, 2026 19:27 PM — 20:16 PM (UTC) and scoped to the functionality available on https://f5-ai-generated-app.xc.hvf5lab.com/.

The tests have been performed as a black box test with no access to the source code and in accordance with best practices laid out by the Open Web Application Security Project (OWASP) and the MITRE Corporation's Common Weakness Enumeration. The purpose of the test has been to find, identify, and describe any potential web security vulnerabilities exposed by the web application.

The applied testing methodology follows the OWASP Web Security Testing Guide (https://owasp.org/www-project-web-security-testing-guide/). The test cases that support the results of this report have been conducted to exhaustively cover the OWASP Top 10:2025 (https://owasp.org/www-project-top-ten/) as well as the web-related weaknesses listed by the CWE (https://cwe.mitre.org/) published by the MITRE Corporation.

All vulnerabilites presented in this report have been classified into one of the vulnerabilities listed in the section below. In addition, their severity has been computed according to the Common Vulnerability Scoring System (version 3.0). The CVSS is owned and managed by the Forum of Incident Response and Security Teams, a US-based non-profit organization, whose mission is to help computer security incident response teams. Please refer to FIRST's website for more information on the CVSS (https://www.first.org/cvss/).

The penetration test has been performed by an automated service developed and operated by F5, Inc. For any questions related to this report, please contact F5, Inc.

Contact Details

F5, Inc.
801 5th Ave
Seattle, WA 98104
USA
Email: support@cloud.f5.com
Web: f5.com

Methodology

Best Practice References
Open Web Application Security Project (OWASP) Top 10 (2025) – Web
https://owasp.org/Top10/

Common Weakness Enumeration (CWE) Top 25 (2025)
https://cwe.mitre.org/top25/
Not considered (2011, outdated): https://www.sans.org/top25-software-errors/
Not considered relevant for this web audit: CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, CWE-125: Out-of-bounds Read, CWE-416 Use After Free, CWE-190 Integer Overflow or Wraparound, CWE-787 Out-of-bounds Write, CWE-476 NULL Pointer Dereference.

Automated Test Tools and Packet Capture
Version 3.1.0
Google Chrome
TestSSL
RetireJS
HTTP(S) Request/Response Proxy
Nuclei

Test Method
The web application was automatically examined in Google Chrome while requests were trapped, modified, and repeated with the HTTP(S) Proxy. JavaScript dependency versions were examined with RetireJS and SSL/TLS configuration was scanned with TestSSL.

The web application was methodically examined and the requests to the backend were tested by creating new requests and by intercepting and modifying requests generated by the web app—the resulting responses were carefully examined.

Request parameters were tested for injection and scripting vulnerabilities by changing the parameter values or by injection of malformed data (incl., HTML). Responses were examined for potential vulnerabilities and sensitive information (e.g., stack traces).

The automated penetration test automatically authenticated with the provided test user login and thereby the functionality behind login was included in the penetration test.

Penetration Test Summary

Created	Started	Completed	Duration
Thu, 12 Feb 2026 19:26:12 GMT	Thu, 12 Feb 2026 19:27:42 GMT	Thu, 12 Feb 2026 20:16:39 GMT	0 hours, 48 minutes, 56 seconds

Target Web Application	Address
f5-ai-generated-app	https://f5-ai-generated-app.xc.hvf5lab.com/

Test Profile	Version
Default Profile	3.1.0 (Full Test)

Findings

Severity	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	Total
High	0	0	0	0	2	0	0	0	0	0	2
Medium	0	1	0	1	0	0	0	0	0	0	2
Low	0	4	0	0	0	0	0	1	1	0	6

OWASP Top 10:2025

Category	Tested	Passed
A01:2025 – Broken Access Control	Yes	Yes
A02:2025 – Security Misconfiguration	Yes	No
A03:2025 – Software Supply Chain Failures	Yes	Yes
A04:2025 – Cryptographic Failures	Yes	No
A05:2025 – Injection	Yes	No
A06:2025 – Insecure Design	Yes	Yes
A07:2025 – Authentication Failures	Yes	Yes
A08:2025 – Software or Data Integrity Failures	Yes	Yes
A09:2025 – Security Logging and Alerting Failures	Yes	Yes
A10:2025 – Mishandling of Exceptional Conditions	Yes	Yes

An OWASP Top 10:2025 category has passed if it does not contain any vulnerabilites with a CVSS 3.0 score higher than 4.0 (i.e., no high or medium vulnerabilites). F5, Inc. uses the Common Vulnerability Scoring System (version 3.0) to assess vulnerabilites. The CVSS is published by the Forum of Incident Response and Security Teams, Inc.

Penetration Test Results

This section describes the results of the automated penetration tests of the f5-ai-generated-app web application in relation to the OWASP Top 10:2025.

A01:2025 – Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Results

No vulnerabilities.

A02:2025 – Security Misconfiguration

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Results

VULN-1: Missing Security Headers (Strict-Transport-Security) Medium

CVSS 3.0 Score
4.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

Unique Issue Hash
37e6357ba7d07c0fb41b0f4996ee6a482e9b267357cb083734a2ae074dce1e51

Found
Thu, 05 Feb 2026 17:06:58 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/

N/A

HTTP Method
GET

Accepted
—

Resolved
—

Notes

—

Description

https://f5-ai-generated-app.xc.hvf5lab.com/ does not return the HTTP Response header Strict-Transport-Security

We recommend that Secure Headers are returned by the web-server globally in the HTTP response header.

If not employed globally there is a risk that some specific files may pose a risk for the entire application. A vulnerability may exist in present files (e.g. error pages, custom "out-of-framework" functionality) or in future files and the secure header may help to prevent this.

We found one or more locations where the Secure Header: Strict-Transport-Security was not present, more specifically here: https://f5-ai-generated-app.xc.hvf5lab.com/.
Therefore, we flag the entire hostname as vulnerable since we determined that the header is not employed globally for the entire application.
Naturally, if no vulnerable functionality currently exists in the application the header may seem unnecessary. For example, if the endpoint is guaranteed to only function as CDN with absolutely no interaction or functionality that may pose risk, it may indeed be unnecessary.
However, things change and hosts may get attacked and may be combined in other attack vectors, which is why we recommend the web-server global approach.

If you are confident that host https://f5-ai-generated-app.xc.hvf5lab.com and the provided files and content does not pose a risk now and in the future, you may Reject this vulnerability if you understand and accept the risk.

VULN-2: Missing Security Headers (X-Frame-Options) — Low

CVSS 3.0 Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

Unique Issue Hash

7cb231904bf37e51678389e79a037dee1324ffe860016c7245b2f35d0b08c14f

Found

Thu, 05 Feb 2026 17:06:58 GMT

From URL

https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL

https://f5-ai-generated-app.xc.hvf5lab.com/

N/A

HTTP Method

GET

Accepted

—

Resolved

—

Notes

—

Description

https://f5-ai-generated-app.xc.hvf5lab.com/ does not return the HTTP Response header X-Frame-Options

We recommend that Secure Headers are returned by the web-server globally in the HTTP response header.

If not employed globally there is a risk that some specific files may pose a risk for the entire application. A vulnerability may exist in present files (e.g. error pages, custom "out-of-framework" functionality) or in future files and the secure header may help to prevent this.

We found one or more locations where the Secure Header: X-Frame-Options was not present, more specifically here: https://f5-ai-generated-app.xc.hvf5lab.com/.
Therefore, we flag the entire hostname as vulnerable since we determined that the header is not employed globally for the entire application.
Naturally, if no vulnerable functionality currently exists in the application the header may seem unnecessary. For example, if the endpoint is guaranteed to only function as CDN with absolutely no interaction or functionality that may pose risk, it may indeed be unnecessary.
However, things change and hosts may get attacked and may be combined in other attack vectors, which is why we recommend the web-server global approach.

If you are confident that host https://f5-ai-generated-app.xc.hvf5lab.com and the provided files and content does not pose a risk now and in the future, you may Reject this vulnerability if you understand and accept the risk.

VULN-3: Missing Security Headers (X-Content-Type-Options) — Low

CVSS 3.0 Score
3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

Unique Issue Hash
4e1195b2444dbef2bb7b2aecb3fe836b86ad5a4a61718cdddcf80a1ba421c1e0

Found
Thu, 05 Feb 2026 17:06:59 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/

N/A

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
https://f5-ai-generated-app.xc.hvf5lab.com/ does not return the HTTP Response header X-Content-Type-Options

We recommend that Secure Headers are returned by the web-server globally in the HTTP response header.

If not employed globally there is a risk that some specific files may pose a risk for the entire application. A vulnerability may exist in present files (e.g. error pages, custom "out-of-framework" functionality) or in future files and the secure header may help to prevent this.

We found one or more locations where the Secure Header: X-Content-Type-Options was not present, more specifically here: https://f5-ai-generated-app.xc.hvf5lab.com/.
Therefore, we flag the entire hostname as vulnerable since we determined that the header is not employed globally for the entire application.
Naturally, if no vulnerable functionality currently exists in the application the header may seem unnecessary. For example, if the endpoint is guaranteed to only function as CDN with absolutely no interaction or functionality that may pose risk, it may indeed be unnecessary.
However, things change and hosts may get attacked and may be combined in other attack vectors, which is why we recommend the web-server global approach.

If you are confident that host https://f5-ai-generated-app.xc.hvf5lab.com and the provided files and content does not pose a risk now and in the future, you may Reject this vulnerability if you understand and accept the risk.

VULN-4: Missing Security Headers (Content-Security-Policy) Low

CVSS 3.0 Score
3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

Unique Issue Hash
842fdfe5776d5dad8762c7ba60d573e79a73cbcb617b1e15cdcde8128155b376

Found
Thu, 05 Feb 2026 17:06:59 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/

N/A

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
https://f5-ai-generated-app.xc.hvf5lab.com/ does not return the HTTP Response header Content-Security-Policy

We recommend that Secure Headers are returned by the web-server globally in the HTTP response header.

If not employed globally there is a risk that some specific files may pose a risk for the entire application. A vulnerability may exist in present files (e.g. error pages, custom "out-of-framework" functionality) or in future files and the secure header may help to prevent this.

We found one or more locations where the Secure Header: Content-Security-Policy was not present, more specifically here: https://f5-ai-generated-app.xc.hvf5lab.com/.
Therefore, we flag the entire hostname as vulnerable since we determined that the header is not employed globally for the entire application.
Naturally, if no vulnerable functionality currently exists in the application the header may seem unnecessary. For example, if the endpoint is guaranteed to only function as CDN with absolutely no interaction or functionality that may pose risk, it may indeed be unnecessary.
However, things change and hosts may get attacked and may be combined in other attack vectors, which is why we recommend the web-server global approach.

If you are confident that host https://f5-ai-generated-app.xc.hvf5lab.com and the provided files and content does not pose a risk now and in the future, you may Reject this vulnerability if you understand and accept the risk.

VULN-5: Cookie without Secure Flag (session) — Low

CVSS 3.0 Score
3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

Unique Issue Hash
31f66594ec880f129c7a44f7a1d475bd602cfbc31bab5873c3c40e879b4de750

Found
Thu, 05 Feb 2026 17:18:20 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/login

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/login

Vulnerable Parameter
session

Vulnerable Parameter Value
session

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
The Secure cookie attribute prevents the browser from sending cookies along with unencrypted requests.

The cookie session assigned to the domain f5-ai-generated-app.xc.hvf5lab.com is not maked as Secure.

At the time of the test the cookie had the value eyj1c2vyijoizjv1c2vyin0.ay4qig.bdkjmwop-zlvoui8y52bpknb1xa.

A03:2025 – Software Supply Chain Failures

An application is vulnerable to attack when: i) User-supplied data is not validated, filtered, or sanitized by the application. ii) Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. iii) Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. iv) Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Results

No vulnerabilities.

A04:2025 – Cryptographic Failures

Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

Results

VULN-6: Insecure Transport Layer (DNS Server) — Medium

CVSS 3.0 Score
4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:L)

Unique Issue Hash
53673ced58fc43853cdb2d202560a6dced82608d0e0601d0426e125d64032e9f

Found
Thu, 05 Feb 2026 17:52:31 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/

Vulnerable Parameter
DNS Server

N/A

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
DNSSEC is not configured on the domain hvf5lab.com.

DNSSEC protects applications from accepting forged or manipulated DNS data—such as that created by DNS cache poisoning.

All answers from DNSSEC protected zones are digitally signed and cannot be forged or manipulated.

It is recommended to enable DNSSEC for the domain hvf5lab.com.

A05:2025 – Injection

Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. Unnecessary features are enabled or installed. Default accounts and their passwords are still enabled and unchanged. Error handling reveals stack traces or other overly informative error messages to users. The security settings in the application servers, application frameworks, libraries, databases, etc., are not set to secure values. The server does not send security headers or directives, or they are not set to secure values.

Results

VULN-7: Cross-site Scripting (Reflected) (/search) — High

CVSS 3.0 Score
9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

Unique Issue Hash
87ec6aeabde6974a0c0449468b5f933b7493db26a4e56cb9b23542a164926795

Found
Thu, 12 Feb 2026 19:51:05 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user%27>">hh<img src=a onerror=alert(459554985)>459554985

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user%27%3E%22%3Ehh%3Cimg%20src=a%20onerror=alert(459554985)%3E459554985

Vulnerable Parameter
q

Vulnerable Parameter Value
PERSISTENT

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
The parameter q is vulnerable to Cross-Site Scripting. The input values taken from users are not securely sanitized and escaped. Therefore, it is possible to perform Cross-Site Scripting attacks against users of the web-app.

VULN-8: Cross-site Scripting (Reflected) (/search) High

CVSS 3.0 Score
9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

Unique Issue Hash
6731e63e358be5a57b3d29b326f1e282bf94e43b644e052ea23e34c6f7251c39

Found
Thu, 12 Feb 2026 19:28:32 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=88311852

Vulnerable Parameter
/HTML[1]/BODY[1]/DIV[1]/HEADER[1]/DIV[1]/DIV[1]/DIV[2]/FORM[1]/INPUT[1]

Vulnerable Parameter Value
'>">hh<img src=a onerror=alert(1701812050)>1701812050

HTTP Method
POST

Accepted
—

Resolved
—

Notes
—

Description
The parameter /HTML[1]/BODY[1]/DIV[1]/HEADER[1]/DIV[1]/DIV[1]/DIV[2]/FORM[1]/INPUT[1] is vulnerable to Cross-Site Scripting. The input values taken from users are not securely sanitized and escaped. Therefore, it is possible to perform Cross-Site Scripting attacks against users of the web-app.

A06:2025 – Insecure Design

Software may be vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.

Results

No vulnerabilities.

A07:2025 – Authentication Failures

Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks.

Results

No vulnerabilities.

A08:2025 – Software or Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

Results

VULN-9: Missing Subresource Integrity — Low

CVSS 3.0 Score
2.6 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:L)

Unique Issue Hash
2735fac5b8bbc22a3fe48343b4cb929170a49d5c7a83e55505e8c3e185e124dd

Found
Thu, 05 Feb 2026 17:06:52 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

To URL
https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user

Vulnerable Parameter
Subresource Integrity not implemented

Vulnerable Parameter Value
Full request

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
Subresource Integrity (SRI) is a security feature that enables browsers to verify that resources they fetch (for example, from a CDN or another host) are delivered without unexpected manipulation.

The following JavaScript files were loaded from https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user without the integrity check:

<script src="https://cdn.tailwindcss.com">

A09:2025 – Security Logging and Alerting Failures

This category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected.

Results

VULN-10: Logging and Monitoring — Low

CVSS 3.0 Score
0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N)

Unique Issue Hash
69c7345c5f46a1f8b98c188156bbe2bf49e09a5fb83219bf5407eb719ae85c6b

Found
Thu, 05 Feb 2026 17:52:29 GMT

From URL
https://f5-ai-generated-app.xc.hvf5lab.com

To URL
https://f5-ai-generated-app.xc.hvf5lab.com

N/A

HTTP Method
GET

Accepted
—

Resolved
—

Notes
—

Description
To satisify the logging requirements in this penetration test a HTTP GET request was made with a challenge to https://f5-ai-generated-app.xc.hvf5lab.com:443/was-challenge?token=CHALLENGE on 2026-02-12T19:55:41.0310042Z.

Please examine your logs and find the challenge to demonstrate that you have sufficient logging in place.

To further test if you have alerting in place, please add an alert to trigger when a request is made to /was-challenge.

When you have found the challenge and been alerted, you may mark this finding as Resolved.

A10:2025 – Mishandling of Exceptional Conditions

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

Results

No vulnerabilities.

Vulnerability Overview

ID	Severity	CVSS	Vulnerability	Accepted	Resolved
1	High	9.1	Cross-site Scripting (Reflected) URL: https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user%27%3E%22%3Ehh%3Cimg%20src=a%20onerror=alert(459554985)%3E459554985 Hash: 87ec6aeabde6974a	—	—
2	High	9.1	Cross-site Scripting (Reflected) URL: https://f5-ai-generated-app.xc.hvf5lab.com/search?q=88311852 Hash: 6731e63e358be5a5	—	—
3	Medium	4.3	Missing Security Headers URL: https://f5-ai-generated-app.xc.hvf5lab.com/ Hash: 37e6357ba7d07c0f	—	—
4	Medium	4.0	Insecure Transport Layer URL: https://f5-ai-generated-app.xc.hvf5lab.com/ Hash: 53673ced58fc4385	—	—
5	Low	3.7	Missing Security Headers URL: https://f5-ai-generated-app.xc.hvf5lab.com/ Hash: 7cb231904bf37e51	—	—
6	Low	3.7	Missing Security Headers URL: https://f5-ai-generated-app.xc.hvf5lab.com/ Hash: 4e1195b2444dbef2	—	—
7	Low	3.7	Missing Security Headers URL: https://f5-ai-generated-app.xc.hvf5lab.com/ Hash: 842fdfe5776d5dad	—	—
8	Low	3.7	Cookie without Secure Flag URL: https://f5-ai-generated-app.xc.hvf5lab.com/login Hash: 31f66594ec880f12	—	—
9	Low	2.6	Missing Subresource Integrity URL: https://f5-ai-generated-app.xc.hvf5lab.com/search?q=f5user Hash: 2735fac5b8bbc22a	—	—
10	Low	0.0	Logging and Monitoring URL: https://f5-ai-generated-app.xc.hvf5lab.com Hash: 69c7345c5f46a1f8	—	—

Test Profile Settings

Setting	Value
Name	Default Profile
Test Mode	Full Test
Frequency	On Demand
Browser	Google Chrome
Crawl subdomains?	No
Subdomains to Avoid	—
Paths to Include	—
Paths to Avoid	—
Scan common ports?	No
Ports to Include	—
Ports to Avoid	—
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
Custom Cookies	—
Custom Headers	—
Maximum Number of Requests per Second	—
Test Users	1