Web Application Penetration Testing Report

**22-July-2025**

**Level 1 Report**

# Copyright

The copyright in this work is vested in MCS Pvt. Ltd., and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of MCS Pvt. Ltd. and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of MCS Pvt. Ltd.

**© MCS Pvt. Ltd.**

# Contact Information

**Mr. Gaurav Kumar**

CISA, CIPM, FIP, CIPP/E, ISO 27001

LA, DevOps, MSc, PG Data Science. ( Lead Auditor)

+91 9528637406

[info@xyz.com](mailto:info@xyz.com)

**Corporate Office**

(Address)

UP

HARYANA, India

**Registered Office**

Address

# About Us

UTTAR PRADESH, INDIA

MCS Private Limited is an ISO Certified (ISO 27001:2013) company. MCS aims to provide Auditing; Consulting, Information Risk Management and Managed services tailored as per the market requirements and enhance the satisfaction and confidence index of its existing and potential customers.

MCS has been a CERT-In empaneled IT Security Auditor. It is an acknowledgement of MCS’s technical expertise in conducting Information Security Audits. As a CERT-In empaneled auditor MCS is qualified to conduct security audits of websites, networks & applications. On successfully completing the audit as per CERT-In Guidelines, our team can issue the CERT-In Certification as required by compliance requirements.

From the development of a Security Policy, Security Awareness Training, through to the delivery of complete end-to-end solutions that encompass Perimeter Security, Secure Content Management, Identity and Access Management, Vulnerability Assessment, Risk, Policy and Compliance Management, MCS Private Limited helps organizations understand, monitor and mitigate the risks in their IT infrastructure.

MCS Private Limited has information security experts, compliance professionals and process consultants from different industry verticals with multiple certifications each with experience in handling consulting assignments, audits and training programs.

MCS Consultants has established a reputation for providing practical solutions that are both businesses driven and cost-effective. This has enabled the company to secure the IT Infrastructure of leading Stock Brokers, Government undertakings, Banks, Insurance Companies and Financial Institutions, BPO, KPO, PKI Industry, Data Center, Software Company, Automobile, Healthcare & Life Sciences, Hospitality, Travel, Transportation, Consumer & Retail, Technology, Media & Telecommunication, School, College, Smart City. Security Leadership our experienced team of ethical hackers have identified security vulnerabilities, we have put together a highly qualified team of security researchers with credentials like CISA, CISSP, OSCP, CSOE, CCNP, MCSE+, ISO 27001 LA, ITIL, COBIT, CIPP/E, CIPM, FIS, DISA, CPA, Cyber Law, Data Science, Artificial Intelligence & Machine Learning, DevSecOps, AWS Architect, Azure Architect.

# Table of Contents

* 1. 1.1 Copyright 2
  2. [Contact Information 2](#_bookmark0)

1. [About Us 3](#_bookmark1)
2. [Table of Contents 4](#_bookmark2)
3. Assessment Information 5
   1. Assessment scope summary 5
   2. MCS Pvt. Ltd. Details 5
4. [Engagement Overview 6](#_bookmark3)
5. [Process and Methodology 7](#_bookmark4)
6. [Vulnerability Overview 8](#_bookmark5)
7. [Checklist 9](#_bookmark6)
8. [Test Execution Summary 13](#_bookmark7)
9. [Executive Summary 14](#_bookmark8)
10. Summary vulnerabilities 15
11. [Detailed Findings and Recommendation 16](#_bookmark9)
12. [High-Level Recommendations 26](#_bookmark10)
13. Engagement Overview

**Indian Council of Historical Research** has engaged with **MCS** to conduct a penetration test of their **Web Application**. This report contains all the results of the report as well as all the action items that were included in the penetration test. The purpose of this report is to present the current security level of the external perimeters including gaps, vulnerabilities, and misconfigurations. The findings presented in this report should be fixed to improve the security level of the network systems.

## Service Description

Web application Vulnerability Assessment and Penetration Testing (VAPT) is the process of simulating real-world attacks by using the same techniques as malicious hackers. For a security assessment that goes beyond a simple vulnerability scanner, you need experts in the industry. **MCS** conducts its penetration test by approaching the scope with both a manual and automatic approach.

## Web Application Penetration Test

our application-level penetration testing consists of both unauthenticated and authenticated testing using both automated and manual methods with particular emphasis placed on identifying vulnerabilities associated with the OWASP Top 10 Most Critical Application Vulnerabilities. It is important to note that a penetration test is not just an automated vulnerability scan, and a large portion of web application penetration testing is a manual process with a skilled engineer attempting to identify, exploit, and evaluate the associate risk of security issues.

## Project Objectives

**MCS** consultants conduct all testing manually combined with custom and commercial tools that perform unique attack approaches on the network to make sure we cover the whole system in the test. Our expert knowledge and experience are the value we provide in our services.

# Process and Methodology

MCS has developed a proven Vulnerability Assessment/Penetration Testing Methodology (illustrated below) from best practices including the Open-Source Security Testing Methodology Manual (OSSTMM), the Council for Registered Ethical Security Testers (CREST), the Penetration Testing Execution Standard (PTES), and our 15 plus years of experience. We have also scaled the methodology to account for differing risks and preferred engagement modalities to ensure that we can provide the right testing and assurance at the right cost.

## Reconnaissance



**1**

This process begins with a detailed scanning and enumeration of the network system and infrastructure, and the information related to the system that is exposed on the internet. After this stage, we conduct manual testing of the gathered data to be analyzed further for attack paths.



**2**

## Automated Approach

Once the scope has been fully enumerated, we start to approach the scope manually and with automatic approaches both self- developed and commercial. The goal is to cover most of the network.

## Exploitation And Manual Testing



**3**

At this stage of the assessment, our experts review the gathered attack vectors and try to exploit the vulnerabilities found in a manual safely approach.

## Assessment Report



**4**

Once the engagement has been completed, we start to develop the assessment report which consists of an executive part and a technical part where we present all the findings and recommendations for fix.

## Re-test



**4**

As an additional option to our standard assessment, we offer a full re-test to our clients to check whether the issues has been fixed by the client and if it’s possible to bypass the patches that were implemented. This will then be updated by a new re-test report

# Vulnerability Overview

**MCS** performed a Network Security Assessment for **Indian Council of Historical Research.** on **2024-10-26** to **2024-10-28** This assessment utilized both commercial and proprietary tools for the initial mapping and reconnaissance of the network system as well as custom tools and scripts for unique vulnerabilities. Several attacking tools was used in order to conduct the penetration testing on the network.

## VULNERABILITY RISK DEFINITION AND CRITERIA

The risk rating assigned to each vulnerability are determined by averaging several aspects of the exploit and the environment, including reputation, difficulty and impact.

Critical vulnerabilities pose a serious threat to an organization's security, and should be fixed immediately. They may provide a total compromise of the target environment, or similar critical impacts.



**Critical**

High risk vulnerabilities provide a serious risk to the company environment and should be corrected promptly. These issues can significantly affect the organization's security posture.



**High**

Medium severity vulnerabilities represent a moderate risk to the environment. They may require additional context before remediation but should be remediated after critical and high risks.



**Medium**

Low severity vulnerabilities provide minimal risk to the target environment, and often theoretical in nature. Remediation of low risks is often a lower priority than other security hardening techniques.



**Low**

**Informational**

Informational vulnerabilities have little-or-no impact to the target scope by themselves. They are included however, as they may be a risk when combined with other circumstances or technologies not currently in place. Remediation of informational items is not necessary.

# Checklist

|  |  |  |
| --- | --- | --- |
| **MCS Web Application Security Testing Checklist** | | |
|  | **Objective** | **Test Outcome** |
|  | **Data Validation** |  |
|  | * Test Error page leak * Test for Stored Cross Site * Test for DOM based Cross Site Scripting * Test for Cross Site Flashing * Test for HTML Injection * Test for SQL Injection * Test for LDAP Injection * Test for ORM Injection * Test for XML Injection * Test for XXE Injection * Test for SSI Injection * Test for XPath Injection * Test for XQuery Injection * Test for IMAP/SMTP Injection * Test for Code Injection * Test for Expression Language Injection * Test for Command Injection * Test for Overflow (Stack, Heap and Integer) * Test for incubated vulnerabilities * Test for HTTP Splitting/Smuggling Test for HTTP Verb Tampering * Test for Open Redirection * Test for Local File Inclusion * Test for Remote File Inclusion * Compare client-side and server-side validation rules Test for NoSQL injection * Test for HTTP parameter pollution Test for auto-binding * Test for Mass Assignment * Test for NULL/Invalid Session Cookie | Not Found |

|  |  |  |
| --- | --- | --- |
|  | **Session Management** |  |
|  | * Establish how session management is handled in the application (eg, tokens in cookies, token in URL) Check session tokens for cookie flags (httpOnly and secure) * Check session cookie scope (path and domain) Check session cookie duration (expires and max-age) Check session termination after a maximum lifetime Check session termination after relative timeout Check session termination after logout * Test to see if users can have multiple simultaneous sessions Test session cookies for randomness * Confirm that new session tokens are issued on login, role change and logout * Test for consistent session management across applications with shared session management * Test for session puzzling * Test for CSRF and clickjacking | Not Found |
|  | **Authentication** |  |
|  | * Test for user enumeration Test for authentication bypass * Test for bruteforce protection * Test password quality rules * Test remember me functionality * Test for autocomplete on password forms/input * Test password reset and/or recovery * Test password change process Test CAPTCHA * Test multi factor authentication * Test for logout functionality presence * Test for cache management on HTTP (eg Pragma, Expires, Max-age) Test for default logins * Test for user-accessible authentication history * Test for out-of channel notification of account lockouts and successful password changes * Test for consistent authentication across applications with shared authentication schema / SSO | Not Found |
|  | **Configuration Management** |  |
|  | * Check for commonly used application and administrative URLs Check for old, backup and unreferenced files * Check HTTP methods supported and Cross Site Tracing (XST) * Test file extensions handling * Test for security HTTP headers (e.g. CSP, X-Frame-Options, HSTS) * Test for policies (e.g. Flash, Silverlight, robots) * Test for non-production data in live environment, and vice-versa | Not Found |

|  |  |  |
| --- | --- | --- |
|  | * Check for sensitive data in client-side code (e.g. API keys, credentials) |  |
|  | **Authorization** |  |
|  | * Test for path traversal * Test for bypassing authorization schema * Test for vertical Access control problems (a.k.a. Privilege Escalation) * Test for horizontal Access control problems (between two users at the same privilege level) * Test for missing authorization | Found |
|  | **Business Logic** |  |
|  | * Test for feature misuse * Test for lack of non-repudiation * Test for trust relationships * Test for integrity of data * Test segregation of duties | Not Found |
|  | **Denial of Service** |  |
|  | * Test for anti-automation * Test for account lockout * Test for HTTP protocol DoS * Test for SQL wildcard DoS | Not Found |
|  | **Risky Functionality - File Uploads** |  |
|  | * Test that file size limits, upload frequency and total file counts are defined and are enforced * Test that file contents match the defined file type * Test that all file uploads have Anti-Virus scanning in-place. Test that unsafe filenames are sanitized * Test that uploaded files are not directly accessible within the web root * Test that uploaded files are not served on the same hostname/port * Test that files and other media are integrated with the authentication and authorization schemas | Not Found |
|  | **Risky Functionality - Card Payment** |  |
|  | * Test for known vulnerabilities and configuration issues on Web Server and Web Application * Test for default or guessable password * Test for non-production data in live environment, and vice-versa * Test for Injection vulnerabilities * Test for Buffer Overflows * Test for Insecure Cryptographic Storage | Found |

|  |  |  |
| --- | --- | --- |
|  | * Test for Insufficient Transport Layer Protection * Test for Improper Error Handling * Test for all vulnerabilities with a CVSS v2 score > 4.0 * Test for Authentication and Authorization issues * Test for CSRF |  |
|  | **Cryptography** |  |
|  | * Check if data which should be encrypted is not * Check for wrong algorithms usage depending on context * Check for weak algorithms usage * Check for proper use of salting * Check for randomness functions | Not Found |
|  | **Secure Transmission** |  |
|  | * Check SSL Version, Algorithms, Key length * Check for Digital Certificate Validity (Duration, Signature and CN) * Check credentials only delivered over HTTPS * Check that the login form is delivered over HTTPS * Check session tokens only delivered over HTTPS * Check if HTTP Strict Transport Security (HSTS) in use | Not Found |

# Test Execution Summary

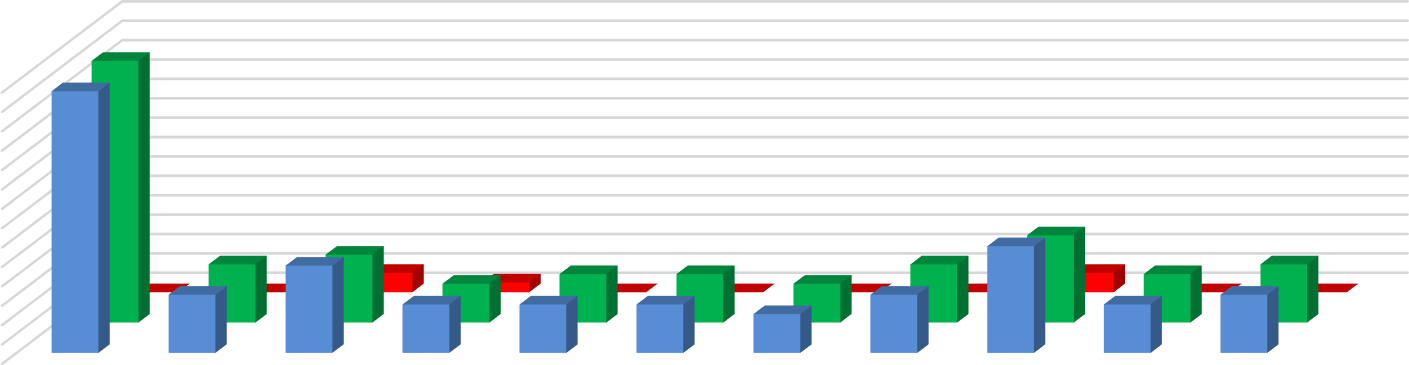


Chart Title

28

26

24

22

20

18

16

14

12

10

8

6

4

2

0

No. Of Failed Cases

No. Of Passed Cases

No. of Test Cases

No. of Test Cases

No. Of Passed Cases

No. Of Failed Cases

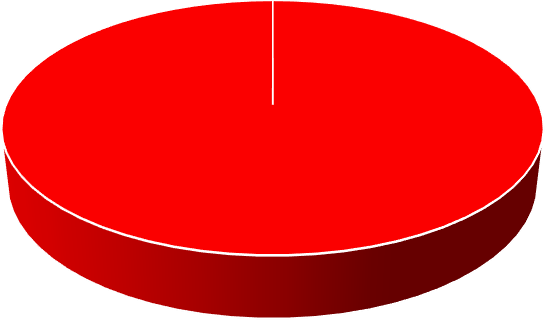
# Executive Summary:

MCS has been engaged by **Indian Council of Historical Research.** to undertake security testing against the [**http://ichr.ac.in/v3**](http://ichr.ac.in/v3)web application. The **Level 1** testing took place over the period from **26/10/2024** to **28/10/2024**. During this period the application was analyzed and assessed using a combination of standard tools and utilities and the knowledge and experience of our technical team. Although at the time of this engagement, the application was not in production, we nonetheless stopped short of undertaking specific tests that would either a) evidently risk the integrity and stability of the systems, or b) actively exploit potential vulnerabilities. Overall, we believe that a reasonable level of security has been attained by the applications that were the target of this test, but due to there being a high and some medium and low risk issues, remedial action needs to be carried out prior to official launch of the product. Testing revealed elements that are well-protected against several well-known vulnerabilities.



Vulnerability by Severity

Critical High Medium Low



Vulnerability Status

Fixed Open

# Summary of Vulnerabilities

Based on the assessment carried out by MCS from **26/10/2024** to **28/10/2024**, the following notable issues have been identified in reference to OWASP standards. This section provides a quick snapshot of the security posture for the Web Application.

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **Vulnerability** | **Severity** | **Level 1 –**  **22/07/2025** |
| **1** | **Potentially Interesting Backup/Cert Files Found** | **High** | **Open** |
| **2** | **X-Content-Type-Options header is not set** | **Medium** | **Open** |
| **3** | **CSP: Failure to Define Directive with No Fallback** | **Medium** | **Open** |
| **4** | **CSP: script-src unsafe-inline** | **Medium** | **Open** |
| **5** | **Cross-Domain Misconfiguration** | **Medium** | **Open** |
| **6** | **Hidden File Found** | **Medium** | **Open** |
| **7** | **Vulnerable JS Library** | **Meduim** | **Open** |
| **8** | **No Server Banner Retrieved** | **Low** | **Open** |
| **9** | **Information Disclosure Suspicious Comments** | **Informational** | **Open** |
| **10** | **Modern Web Application** | **Informational** | **Open** |
| **11** | **Re Examine Cache-Control Directions** | **Informational** | **Open** |
| **12** | **Retrieved from Cache** | **Informational** | **Open** |

# Detailed Findings and Recommendation

h

**12.1 Potentially Interesting Backup/Cert Files Found**

**Description: - The Scan found numerous files identified as Potentially interesting backup/cert file found. (These include**

**files with extensions Ex:- .tar,.lzma,.bz2, .pem, .egg)**

**(along with variation of the hostname Eg:- iaoscgagov.pem, backup.pem. etc)**

**The presence of these files suggests that backup copies of configuration files, certificates, or databases might be publicly accessible**

**Risk :- High**

# 

**Impact:** - This is a critical vulnerability. If these files contain sensitive information (Eg – Private keys,

database credentials, server configurations, or user data), an attacker could download them,

Gain unauthorized access, and potentially compromise the entire system, This could lead to data

breaches , system defacement, or further network penetration.

**Solution: -** Immediate Action: Remove or secure all identified backup and certificate files immediately.

They should not be publicly accessible via the web server

**Tool Used:- nikto -h https://iaos.cga.gov.in**

# 

# 

# Proof of concept 12.1

# 

**12.2 X-Content-Type-Options header is not set**

**Solution: -**  **Configure the web server to send the X-Content-Type-Options: nosniff header for all relevant responses, especially for xakamapl.php. This typically involves server configuration (e.g., Apache, Nginx) or application-level code.**

**Apache: Add Header set X-Content-Type-Options "nosniff" to your configuration.**

**Nginx: Add add\_header X-Content-Type-Options "nosniff"; to your server or location block.**

**Impact URL :-** [**https://iaos.cga.gov.in**](https://iaos.cga.gov.in)

**Tool Used :- Nikto**

**Description:**  The scan identified xakamapl.php and noted that the X-Content-Type-Options header is not set. This header is a security feature that prevents browsers from MIME-sniffing a response away from the declared content-type.

**Relative Risk: Medium**

**Evidence :- Nikto -h https://iaos.cga.gov.in**

**Impact:** Without this header set to nosniff, a browser might interpret a response as a different content type (e.g., an image as an executable script) if the declared content-type is incorrect or missing, potentially leading to Cross-Site Scripting (XSS) attacks or other content-sniffing vulnerabilities. This is particularly relevant if users can upload content to the server.

Proof of Concept 12.2

****

**12.3 CSP: Failure to Define Directive with No Fallback**

**Relative Risk :** **Medium**

**Description:** The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is

the same as allowing anything.

**Impact:** If a Security directive is improperly defined without a fallback mechanism, it can lead to security vulnerabilities

by failing to enforce restrictions when expected

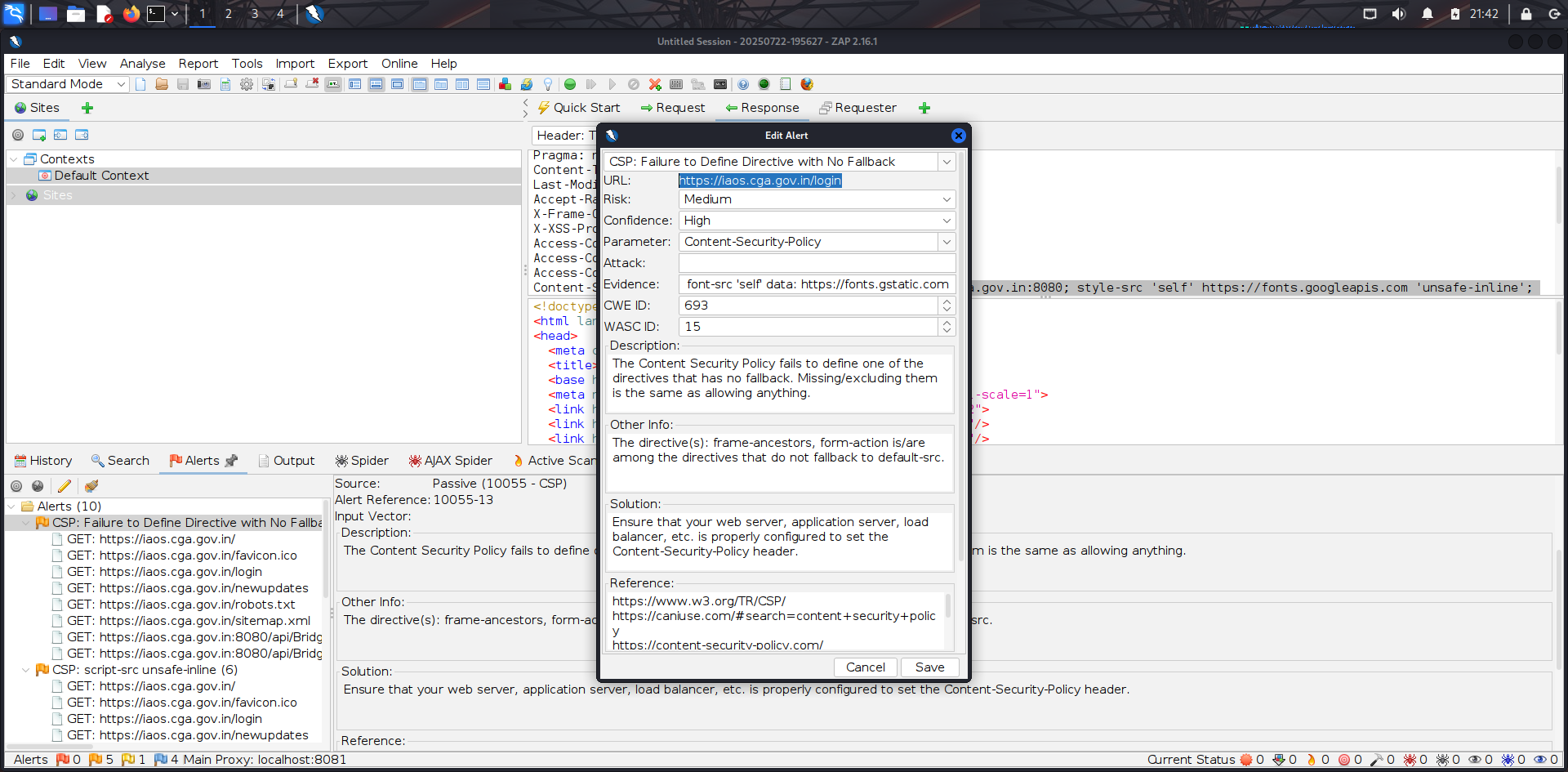
**Recommendation:** Ensure that your web server, application server, load balancer, etc. is properly configured to set the

Content-Security-Policy header.

**Impact URL:-** [**https://iaos.cga.gov.in/login**](https://iaos.cga.gov.in/login)

**Tool Used:** OWASP ZAP

Proof Of Concept 12.3



**Description:-:** Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain

types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

**Affected URL:** <https://164.100.150.68/integration/Login.aspx>

**Tool used** : OWASP ZAP

**Impact:** May contain unpatched vulnerabilities (e.g. DoS, RCE, buffer overflows).

Increases risk of compromise or unauthorized access.

Reduces overall security posture of the system.

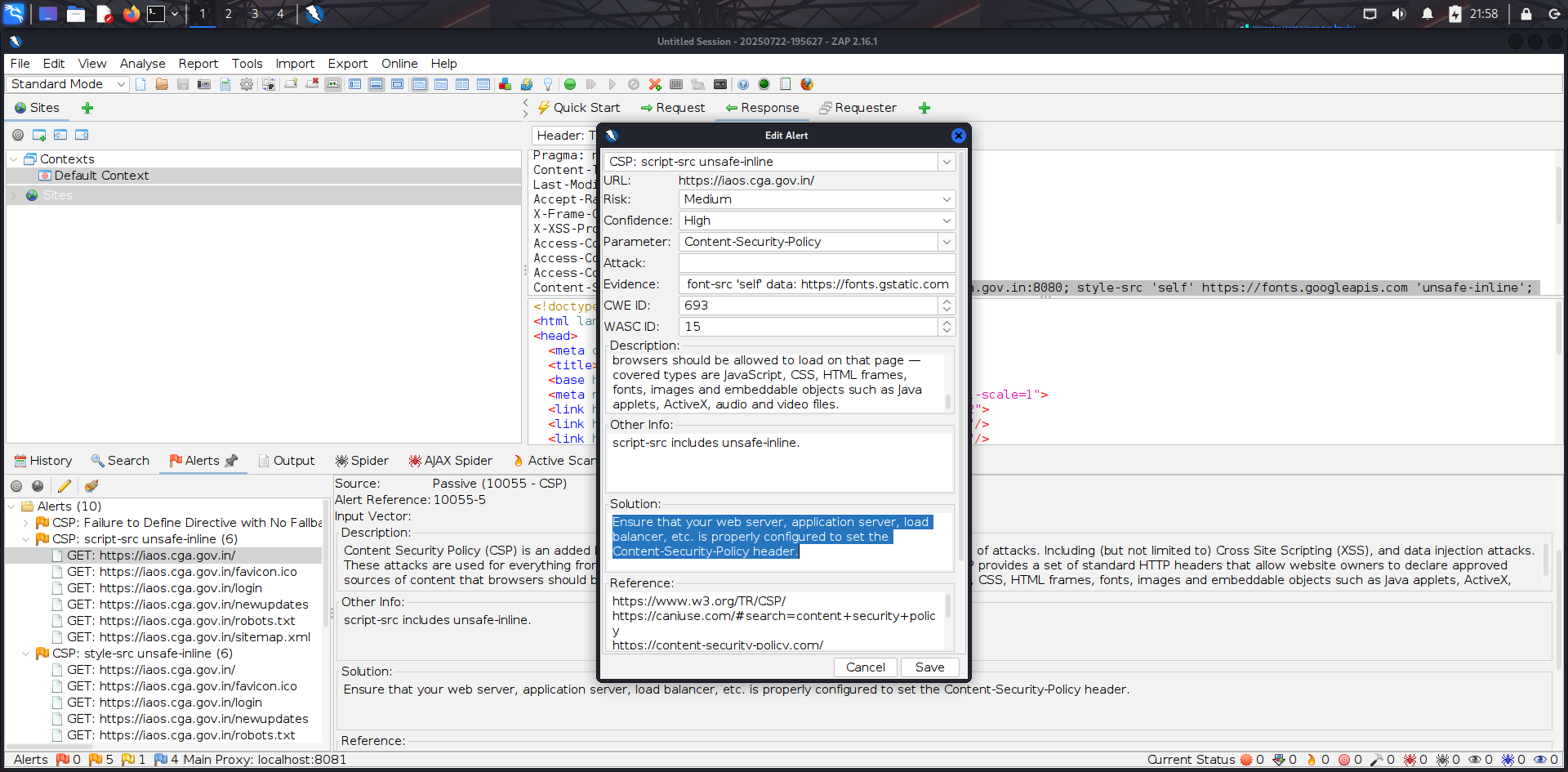
**Solution:-** Ensure that your web server, application server, load balancer, etc. is properly configured to set the

Content-Security-Policy header.

**12.4** **CSP: script-src unsafe-inline**

**Relative Risk: Medium**

**Proof of Concept 12.4**

****

**12.5**  **Cross-Domain Misconfiguration**

**Relative Risk:**  Medium

**Description:** Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS)

misconfiguration on the web server.

**Impact:** Exposes internal APIs to malicious third-party domains . Anyone (even attacker sites) can make authenticated API calls or steal sensitive data. May allow attackers to inject or steal data via cross-window communication, attackers bypass same-origin policy, extract user info or API data

**Recommendation:**

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

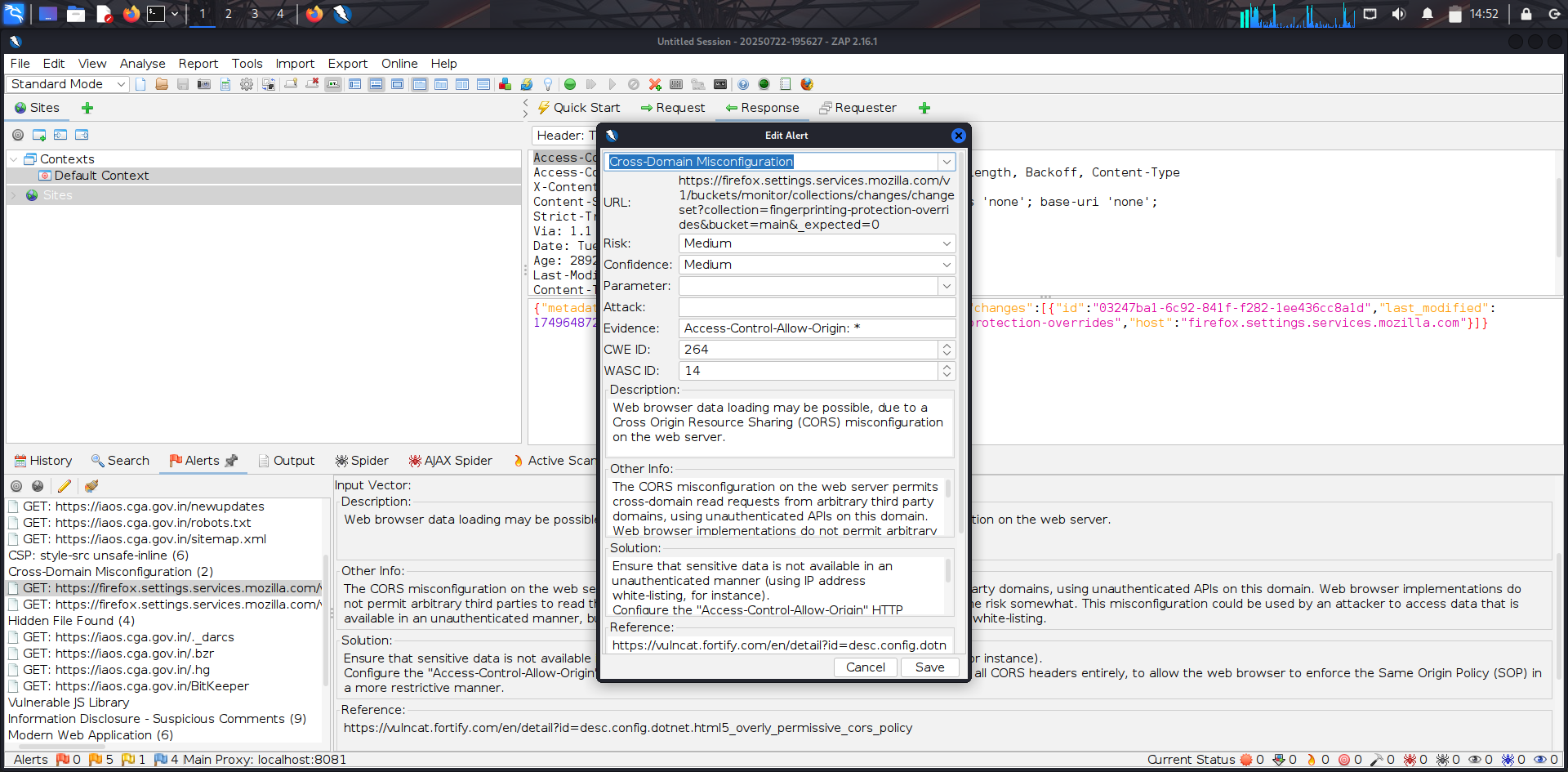
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

**Effect URL: -** [**https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=fingerprinting-protection-overrides&bucket=main&\_expected=0**](https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?collection=fingerprinting-protection-overrides&bucket=main&_expected=0)

**Tool Used: OWASP ZAP**

### OCUMENT

**Proof of Concept 12.5**



**12.6 Hidden File Found**

**Impact: -** Attackers can steal DB credentials, AWS keys, or API secrets and misuse them. They can analyze your code for vulnerabilities (like SQL injection, hardcoded passwords . If old admin panels or backup files are accessible, attackers might log in as admin.

**Recommendation:** Upgrade to the latest version of the affected library

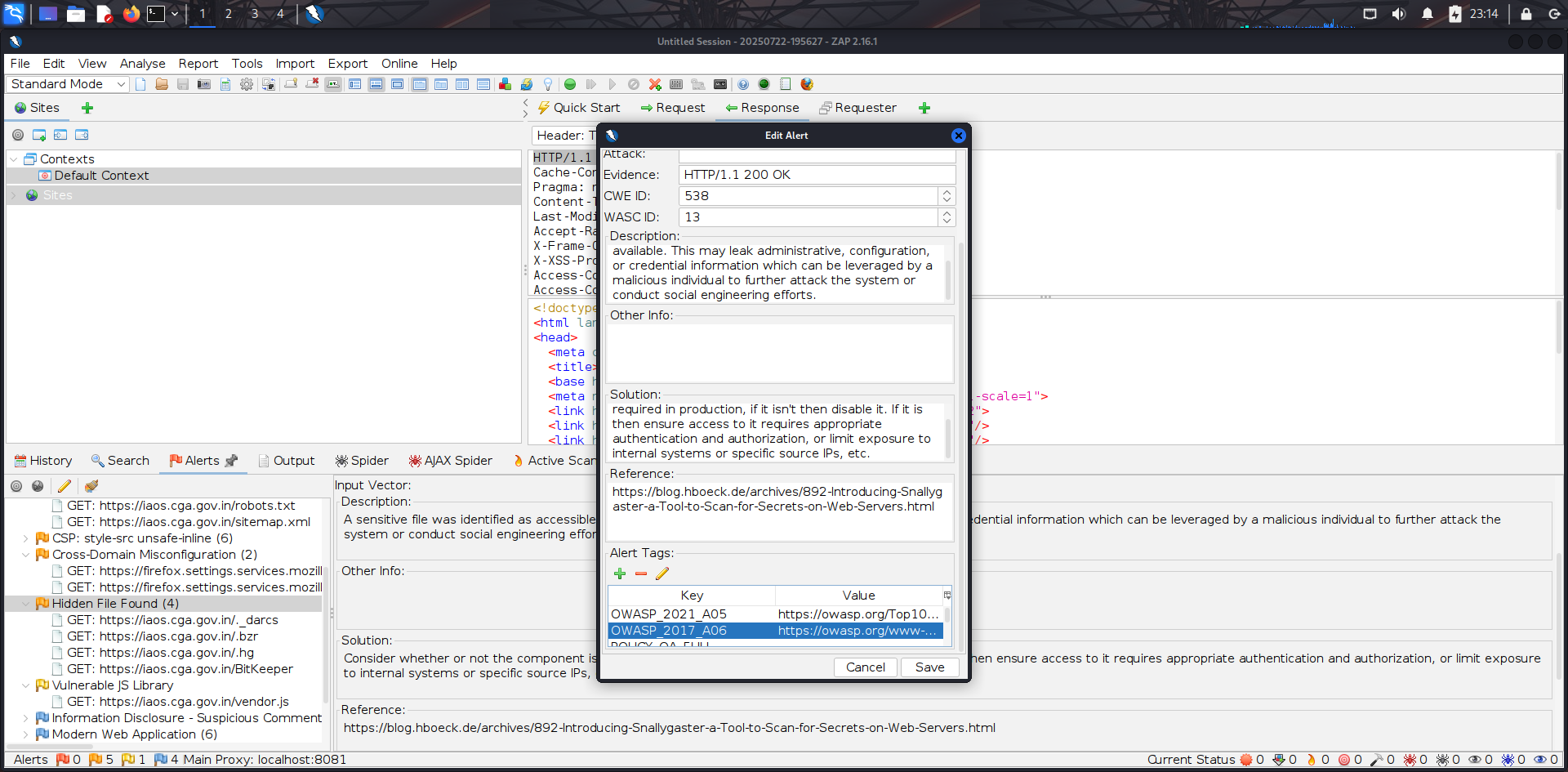
**Effect URL : -** [**https://iaos.cga.gov.in/.hg**](https://iaos.cga.gov.in/.hg)

**Tool Used: Owasp Zap**

**Description:** The identified library appears to be vulnerable.

**Relative Risk: Medium**

**Proof of Concept 12.6**



**12.7 Vulnerable JS Library**

**Relative Risk:-** Medium

**Description: The identified library appears to be vulnerable And bootstrap, version 3.4.1 is vulnerable.**

**Impact:** Attackers can potentially inject malicious scripts (if XSS exists).Opens the door for phishing, session hijacking, or unauthorized actions. Sensitive user data (login credentials in this case) may be compromised. **Solution:** Upgrade to the latest version of the affected library

**Affect URL:** <https://164.100.150.68/integration/js/bootstrap.min.js>

**Tool Used :** OWASP ZAP

**Proof of Concept 12.7**



**12.8 No Server Banner Retrieved**

**Relative Risk:- Low**

**Description:-** The Nikto scan reports "Server: No banner retrieved". This means the web server is not explicitly sending information about its type and version in its HTTP response headers.

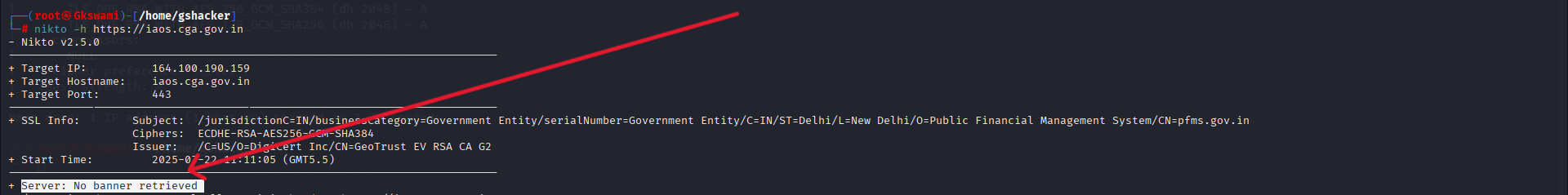
**Impact :-** While not a vulnerability in itself, a missing server banner makes it slightly more difficult for attackers to quickly identify the specific server software and its known vulnerabilities. It's a minor security hardening measure.

**Solution:-** No direct action is needed for this specific message as it indicates a positive security practice (obfuscation). However, ensure that no other server information is being leaked through different channels (e.g., error messages, file paths).

**Tool Used:-**  Nikto

**Effective** [**URL:-**](URL:-)[**https://iaos.cga.gov.in/**](https://iaos.cga.gov.in/)

**Proof OF Concept 12.8**



**12.9 Information Disclosure - Suspicious Comments**

**Relative Risk : Informational**

**Description:** The response appears to contain suspicious comments which may help an attacker.

**Tool used**:- Owasp Zap

**Affect URL:** <https://iaos.cga.gov.in/assets%5Cjs%5Cjquery.min.js>

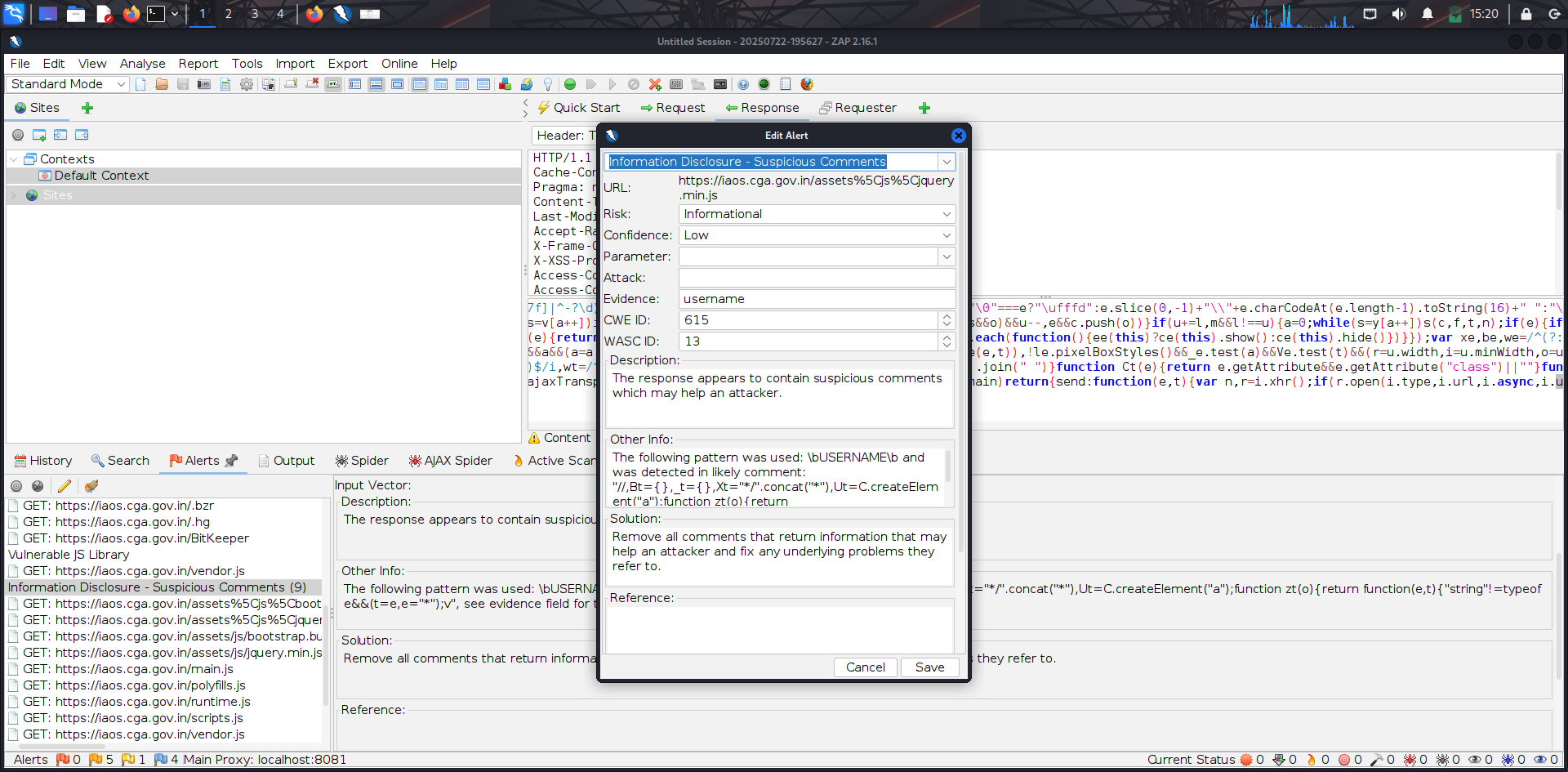
**Evidence From ZAP Scan:** username

**Solution:**  Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

**Impact:** Attackers may find private admin areas

Use exposed keys to interact with third-party services (e.g., Stripe, Firebase)

**Proof of Concept 12.9**



**12.10 Modern Web Application**

**Affect URL:** <https://iaos.cga.gov.in/>

**Tool Used**:- Owasp Zap

**Solution:** This is an informational alert and so no changes are required.

**Impact: -** Attackers could inject and execute malicious scripts on the client-side, potentially compromising user data, session

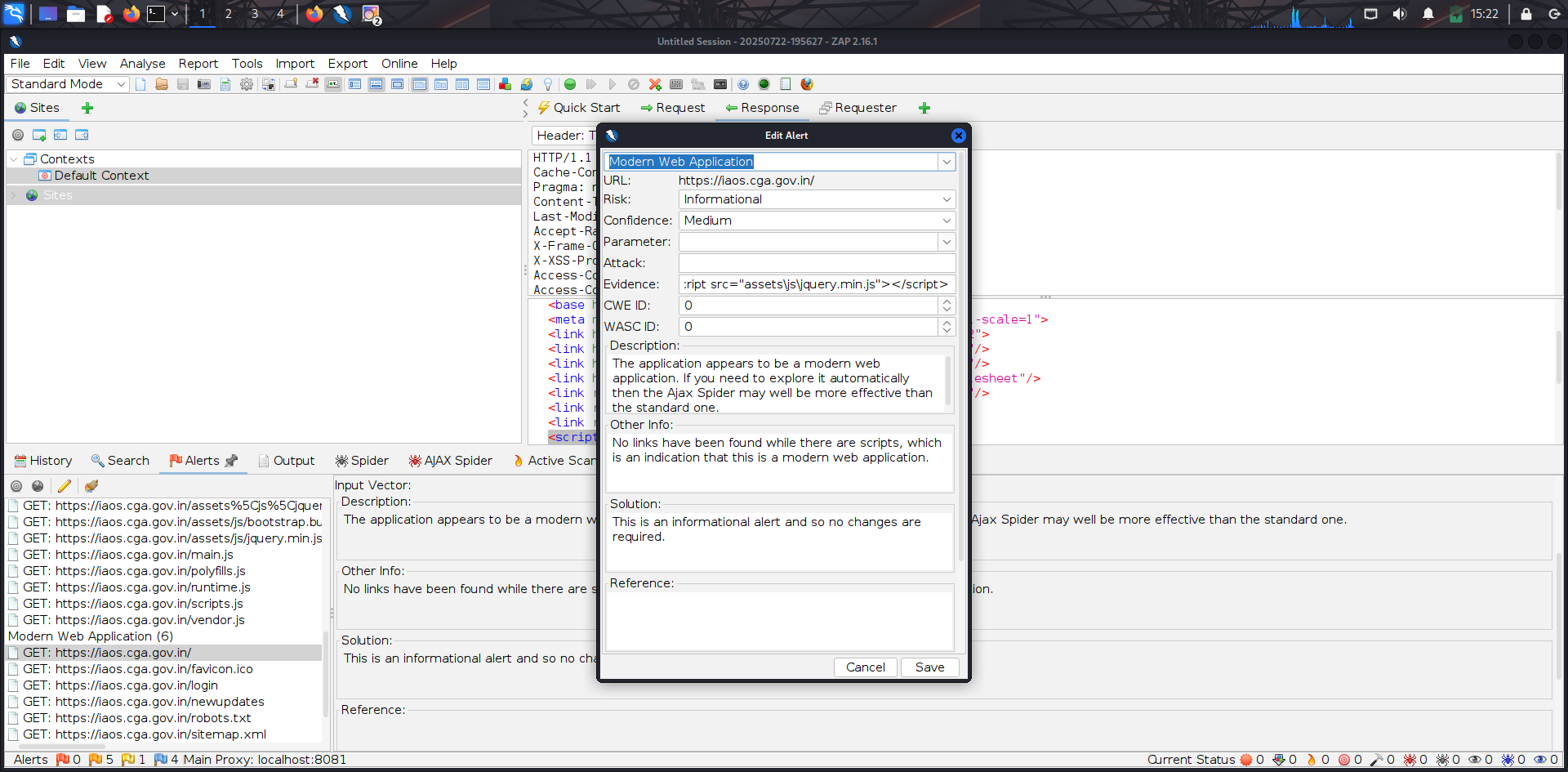
hijacking, defacement, or redirecting users to malicious sites.

**Relative Risk:** Informational

**Description:** The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider

may well be more effective than the standard one.

##### Proof of Concept 12.10

****



CONFIDENTIAL DOCUMENT

12.11 Re-examine Cache-control Directives

###### 

**Relative Risk:- Informational**

**Description:** The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

**Impact:** Improper cache settings can expose sensitive data to unauthorized users via browser or proxy caching.

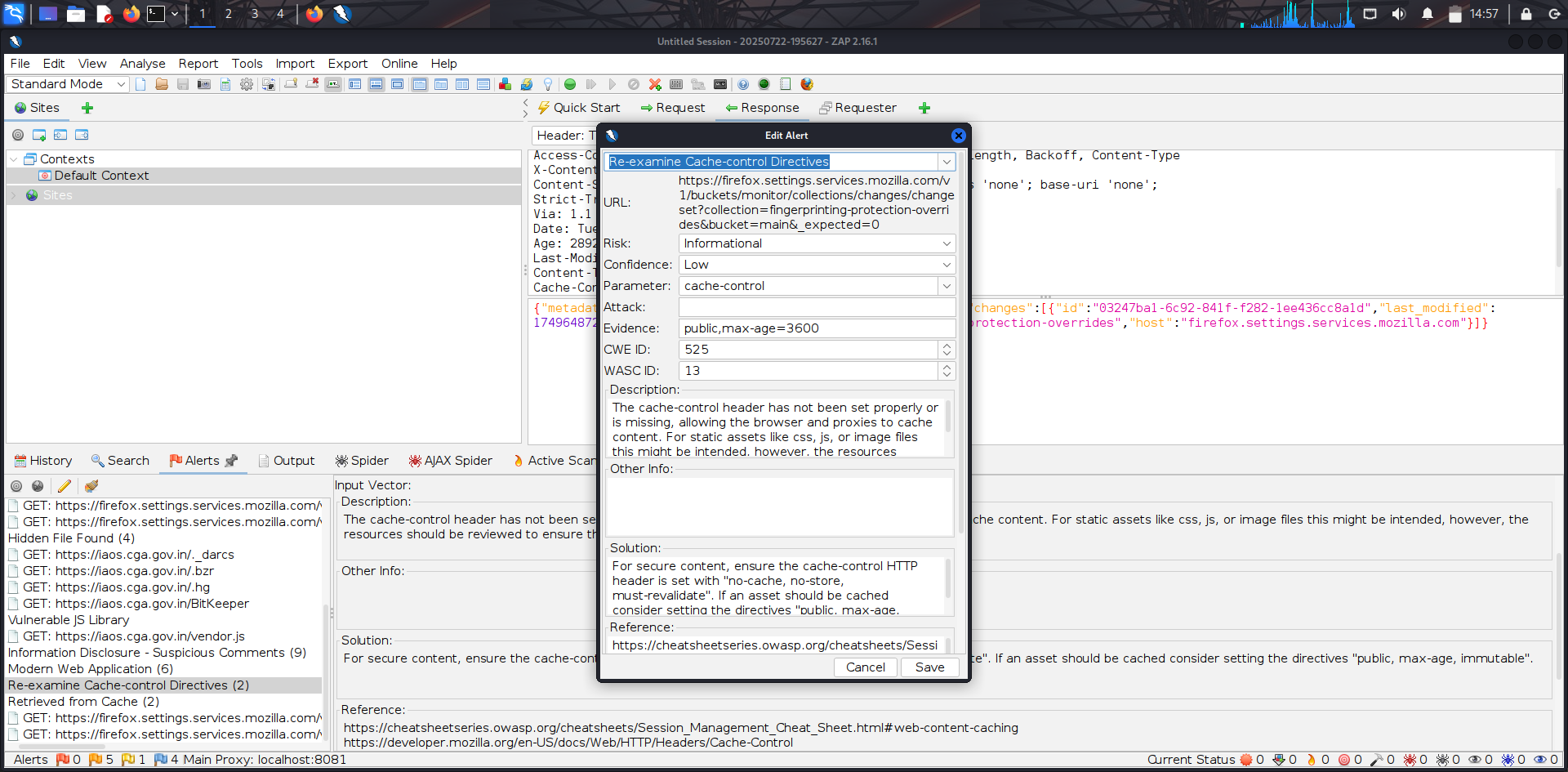
**Solution:** For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must- revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

**Tool Used: OWASP ZAP**

**Affect** [**URl:-**](URl:-) **https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/changeset?** **collection=fingerprinting-protection-overrides&bucket=main&\_expected=0**

**Evidence:** public,max-age=3600

**Proof of Concept 12.11**



**12.12 Retrieved from Cache (2)**

**Relative risk: Informational**

**Description:** The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

**Impact:**

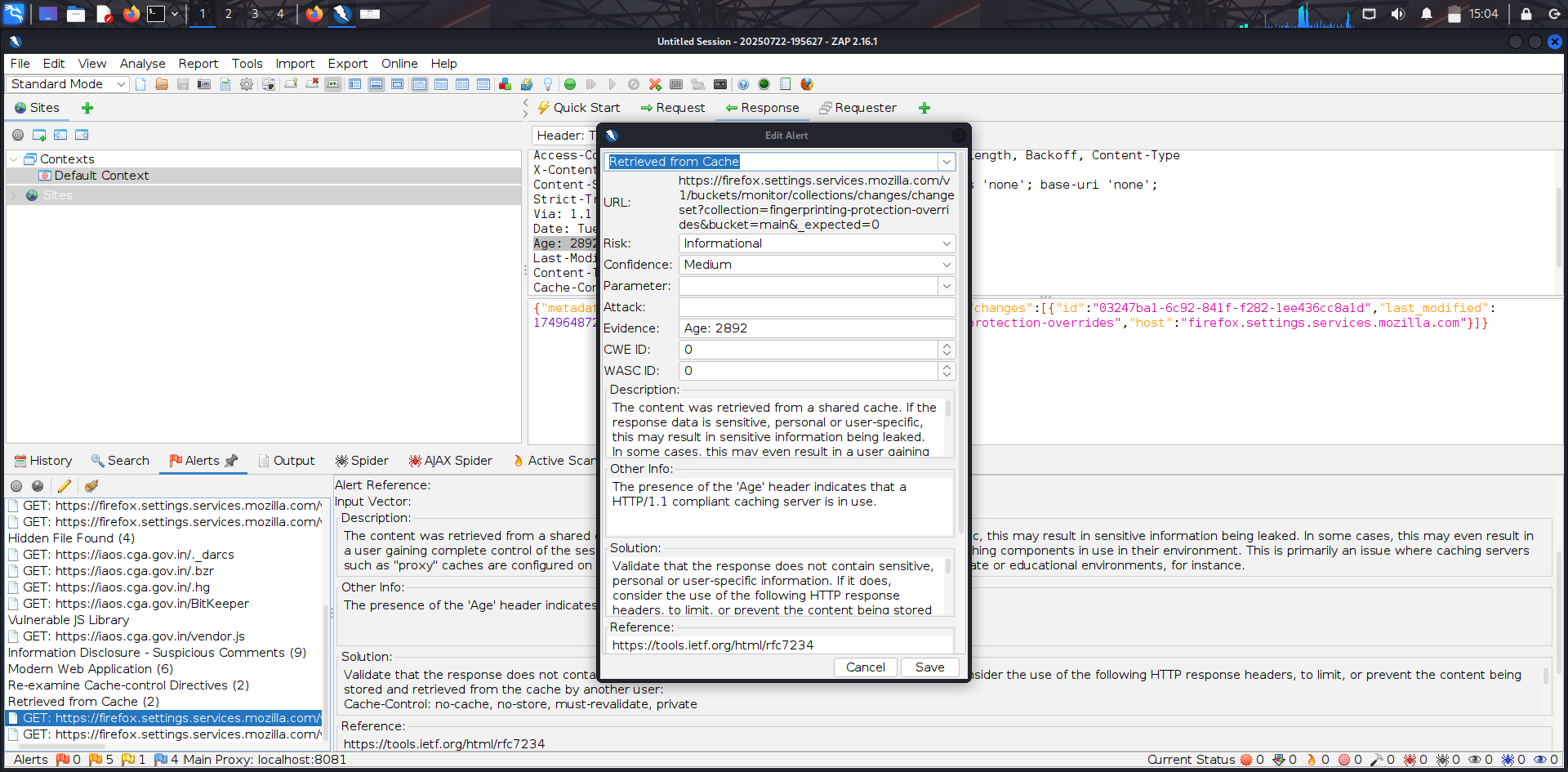
Sensitive data stored in shared cache can be accessed by other users, leading to data leakage or session compromise.

**Solution:** Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user

**Tool Used:** OWASP ZAP

**Evidence: Age: 2892**

**Proof of Concept 12.12**



### AL DOCUMENT

# High-Level Recommendations

###### Taking into consideration all issues that have been discovered, we highly recommend to:

* + - Conduct current vs. future IT/Security program review
    - Conduct Static code analysis for codebase
    - Establish Secure SDLC best practices, assign Security Engineer to a project to monthly review code, conduct SAST & DAST security testing
    - Review Architecture of application
    - Deploy Web Application Firewall solution to detect any malicious manipulations
    - Continuously monitor logs for anomalies to detect abnormal behavior and fraud transactions. Dedicate security operations engineer to this task
    - Implement Patch Management procedures for whole IT infrastructure and endpoints of employees and developers
    - Continuously Patch production and development environments and systems on regular bases with latest releases and security updates
    - Conduct annual Penetration test and quarterly Vulnerability Scanning against internal and external environment
    - Develop and Conduct Security Awareness training for employees and developers
    - Develop Incident Response Plan in case of Data breach or security incidents
    - Analyze risks for key assets and resources
    - Update codebase to conduct verification and sanitization of user input on both, client and server side
    - Use only encrypted channels for communications
    - Do not send any unnecessary data in requests and cookies
    - Improve server and application configuration to meet security best practices