Shaheed Sukhdev College of Business Studies

University of Delhi

Post Graduate Diploma in Cyber Security and Law

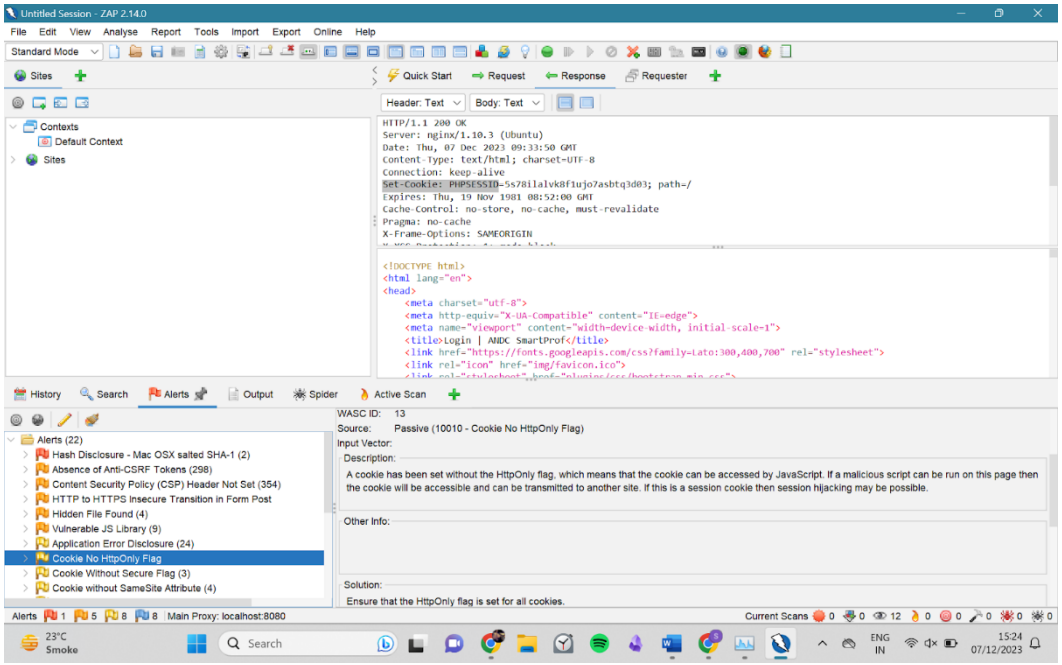
Sakshi Garg • Roll no-23726 • Subject-Web Applications • Semester-1

ZAP Proxy: Vulnerable and Outdated Components

Bug 1- Cookie No Http Only Flag

Description- A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

POC

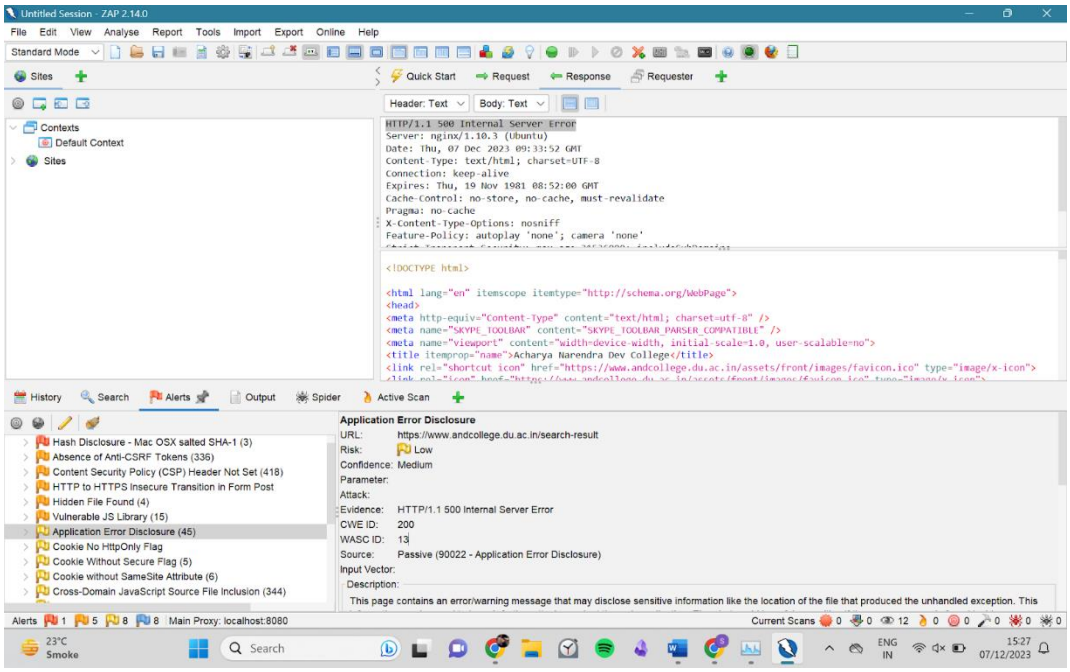


Solution- Ensure that the HttpOnly flag is set for all cookies.

Bug 2- Application Error Disclosure

Description-
This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Response-



Solution-
Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

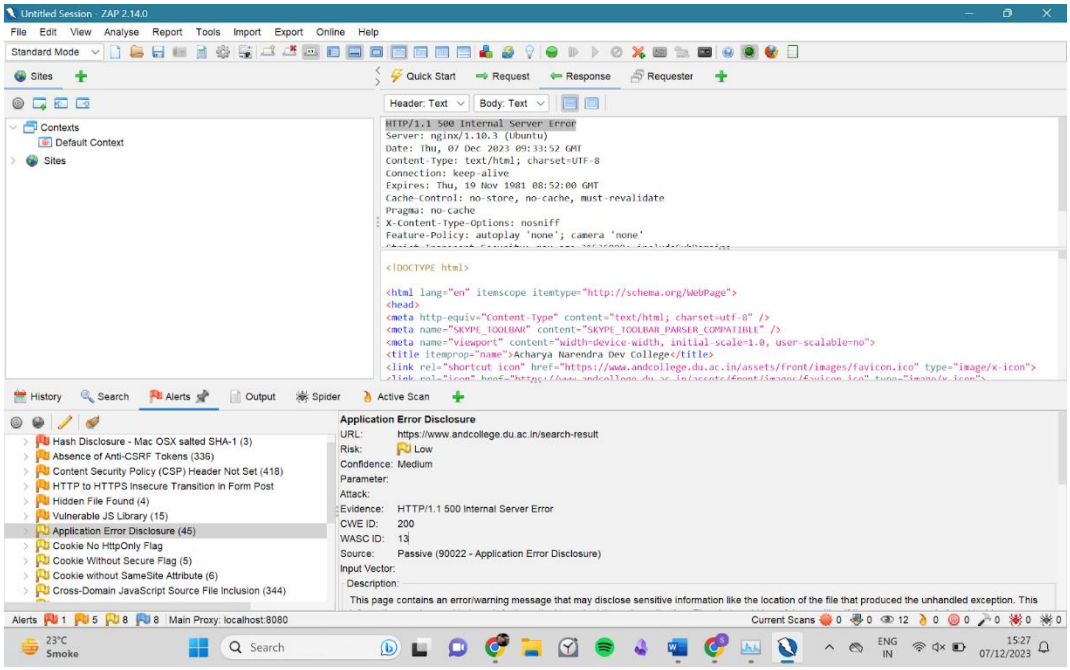
Reference-
https://www.andcollege.du.ac.in/

Bug 3- Vulnerable JS Library

The vulnerable JS library is a security issue that can compromise the security of your web application. To fix this vulnerability, you need to identify the vulnerable JS library, determine the latest version of the library, update the library, test your web application, and keep the library up-to-date

Solution-

- As part of patch management, implement version management for JavaScript
- libraries.
- Remove libraries that are no longer in use to reduce your attack surface.
- Frequently check for patches and upgrade JavaScript libraries to the latest version


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 500 Internal Server Error
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 07 Dec 2023 09:33:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Content-Type-Options: nosniff
Feature-Policy: autoplay 'none'; camera 'none'
<!DOCTYPE html>
<html lang="en" itemscope itemtype="http://schema.org/WebPage">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="SKYPE_TOOLBAR" content="SKYPE_TOOLBAR_PARSER_COMPATIBLE" />
<meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no">
<title itemprop="name">Acharya Narendra Dev College</title>
<link rel="shortcut icon" href="https://www.andcollege.du.ac.in/assets/front/images/favicon.ico" type="image/x-icon">
History
Search
Alerts
Output
Spider
Active Scan
Hash Disclosure - Mac OSX salted SHA-1 (3)
Absence of Anti-CSRF Tokens (336)
Content Security Policy (CSP) Header Not Set (418)
HTTP to HTTPS Insecure Transition in Form Post
Hidden File Found (4)
Vulnerable JS Library (15)
Application Error Disclosure (45)
Cookie No HttpOnly Flag
Cookie Without Secure Flag (5)
Cookie without SameSite Attribute (6)
Cross-Domain JavaScript Source File Inclusion (344)
Application Error Disclosure
URL: https://www.andcollege.du.ac.in/search-result
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: HTTP/1.1 500 Internal Server Error
CWE ID: 200
WASC ID: 13
Source: Passive (90022 - Application Error Disclosure)
Input Vector:
Description:
This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This
Alerts 1 5 8 8 Main Proxy: localhost:8080
Current Scans 0 0 12 0 0 0 0 0
23°C Smoke
Search
ENG IN
15:27 07/12/2023