به نام خدا

فاز دوم پروژه

مهندسی نرم افزار

دکتر فرید فیضی – ترم ۱۴۰۳ دانشگاه گیلان


اعضای گروه :
ثنا منصوری
فرحان باقری
محمد رضا اصفهانی
حسین یداللهی
مهدی نظام دوست

فهرست

مقدمه

در این مرحله، هدف ما ارزیابی امنیت شبکه اجتماعی متن‌باز HumHub است که در گام‌های قبل به عنوان پلتفرم اصلی انتخاب و راه‌اندازی شده است. برای بررسی امنیت این سیستم، از دو ابزار قدرتمند و رایج در حوزه تست نفوذ و تحلیل آسیب‌پذیری‌ها استفاده شد:

- OWASP Zed Attack Proxy (ZAP)
- Acunetix

این ابزارها به ما کمک کردند تا نقاط ضعف امنیتی احتمالی سیستم را شناسایی کنیم، تحلیل کنیم و برنامه‌ای برای رفع آن‌ها طراحی کنیم. انجام این مرحله بخش مهمی از تضمین کیفیت و امنیت نهایی پروژه است.

تحلیل و پیاده‌سازی شبکه اجتماعی متن‌باز + ارزیابی امنیت

۱. راه‌اندازی HumHub
۲. دانلود سورس از GitHub
۳. نصب روی لوکال با استفاده از Apache وPHP
۴. ایجاد کاربران، گروه‌ها و پست‌های آزمایشی
۵. بررسی ماژول‌های مختلف شامل پیام‌رسانی، پروفایل، انجمن‌ها و رویدادها

تحلیل امنیتی پلتفرم انتخاب‌شده

ابزارهای مورد استفاده:

Acunetix و OWASP ZAP برای اسکن آسیب‌پذیری‌ها

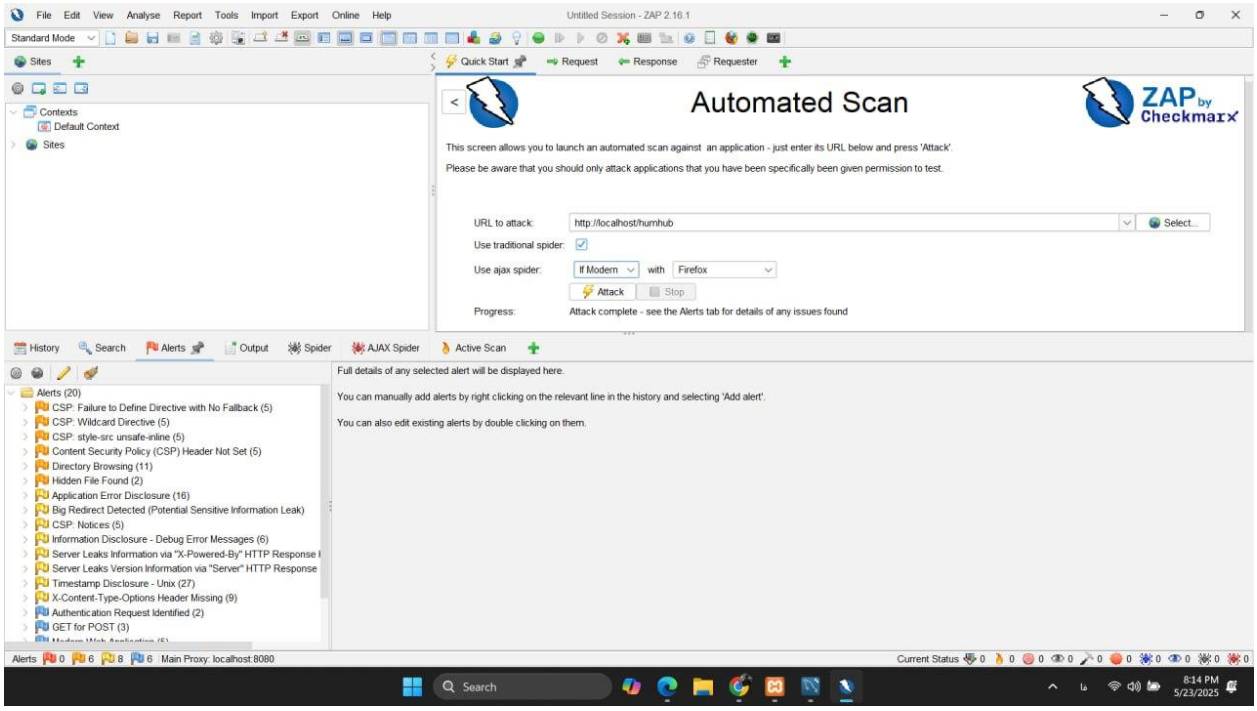
آسیب‌پذیری‌های کشف‌شده

- Missing Content-Security-Policy Header | Medium
- Apache Server-Status Page Exposed | Medium
- Directory Browsing Enabled | Medium

شکل زیر مربوط به همه مشکلات پیدا شده توسط ZAP میباشد.

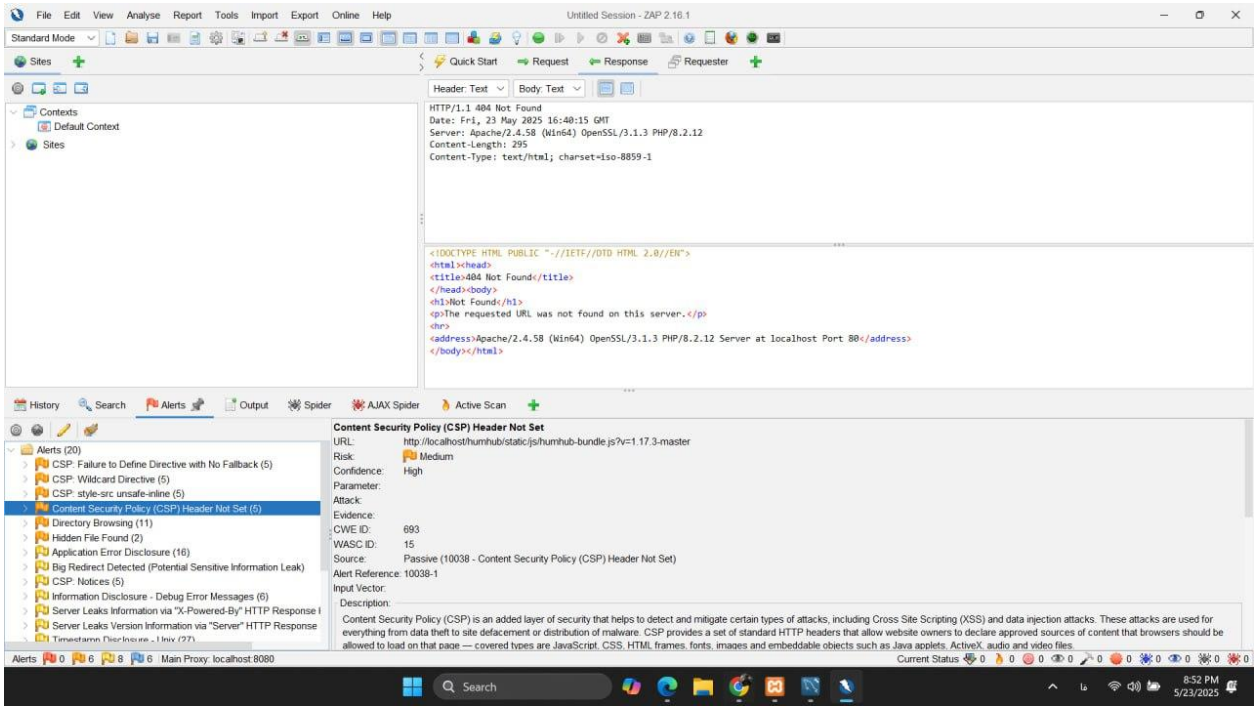
1 . Missing Content-Security-Policy Header

- **شرح :**سرور وب سایت فاقد هدر CSP است. این هدر یکی از ابزارهای مهم برای جلوگیری از حملات XSS و بارگذاری منابع ناخواسته است.
- **ریسک :**متوسط
- **مکان**http://localhost/humhub/static/js/humhub-bundle.js :
- **اقدام پیشنهادی :**افزودن هدر زیر در فایل پیکربندی:Apache



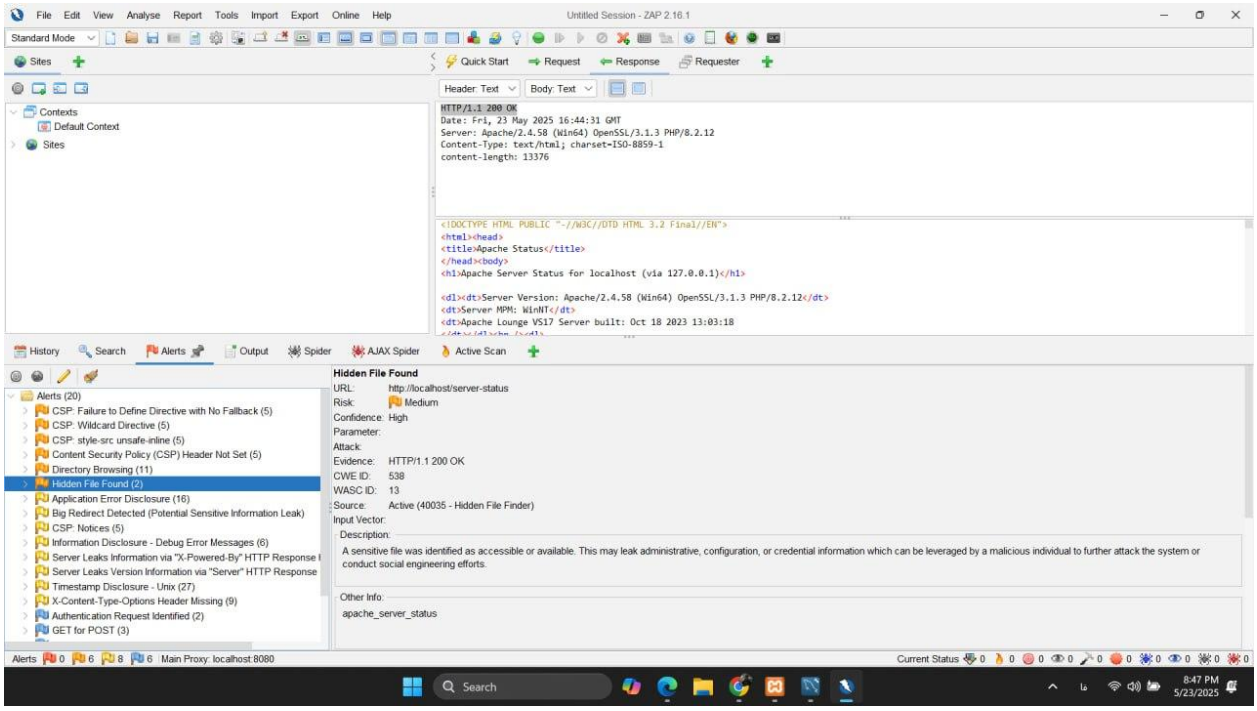
2 . Apache Server Status Page Exposed

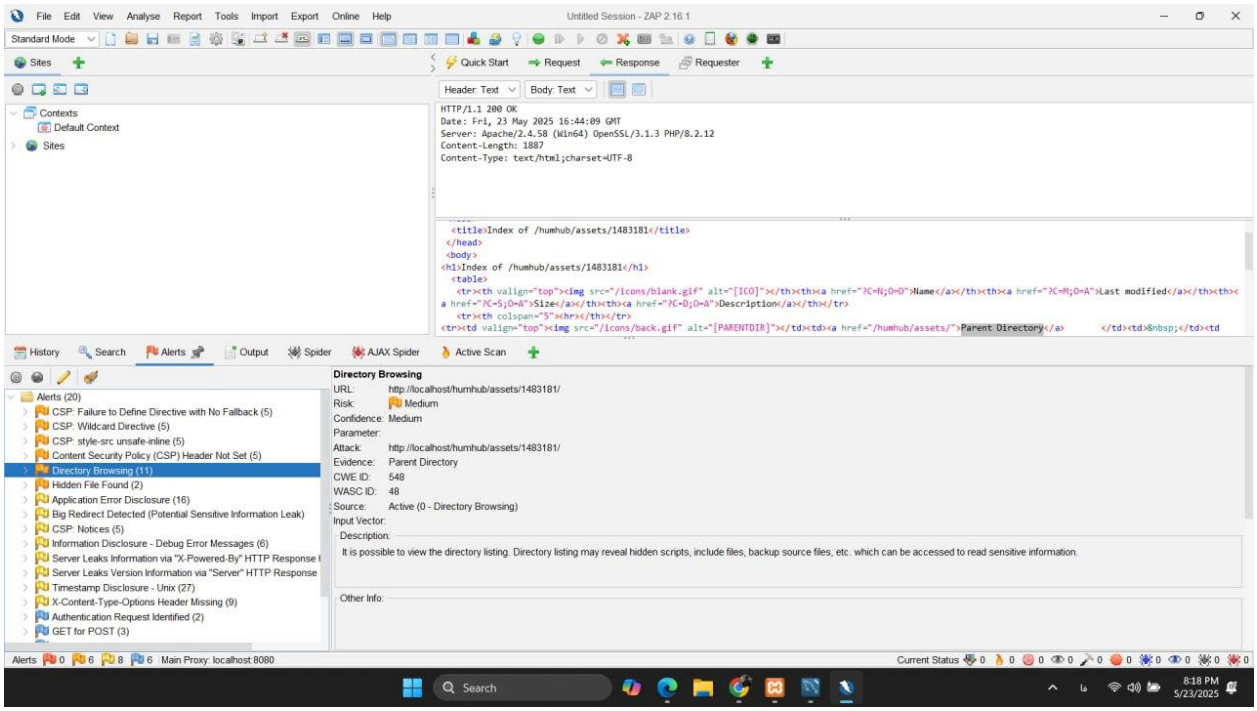
- **شرح :**آدرس server-status/در دسترس عموم است و اطلاعات حساس مانند نسخه سرور، ماژول‌ها و وضعیت پردازش‌ها را نمایش می‌دهد.
- **ریسک :**متوسط
- **مکان**http://localhost/server-status :
- **اقدام پیشنهادی :**محدود کردن دسترسی به IP محلی از طریق پیکربندی زیر در:Apache



3 . Directory Browsing Enabled

- **شرح :**امکان مرور محتویات دایرکتوری /humhub/assets/برای عموم کاربران فراهم است. این مسئله می‌تواند منجر به مشاهده فایل‌های پنهان یا پشتیبان شود.
- **ریسک :**متوسط
- **مکان**/http://localhost/humhub/assets/1483181 :
- **اقدام پیشنهادی :**غیرفعال‌سازی Directory Listing در فایل :htaccess.


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Date: Fri, 23 May 2025 16:44:31 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Type: text/html; charset=ISO-8859-1
content-length: 13376
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html><head>
<title>Apache Status</title>
</head><body>
<h1>Apache Server Status for localhost (via 127.0.0.1)</h1>
<dl><dt>Server Version: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12</dt>
<dt>Server MPM: WinNT</dt>
<dt>Apache Lounge VS17 Server built: Oct 18 2023 13:03:18
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (20)
CSP: Failure to Define Directive with No Fallback (5)
CSP: Wildcard Directive (5)
CSP: style-src unsafe-inline (5)
Content Security Policy (CSP) Header Not Set (5)
Directory Browsing (11)
Hidden File Found (2)
Application Error Disclosure (16)
Big Redirect Detected (Potential Sensitive Information Leak)
CSP: Notices (5)
Information Disclosure - Debug Error Messages (6)
Server Leaks Information via "X-Powered-By" HTTP Response
Server Leaks Version Information via "Server" HTTP Response
Timestamp Disclosure - Unix (27)
X-Content-Type-Options Header Missing (9)
Authentication Request Identified (2)
GET for POST (3)
Hidden File Found
URL: http://localhost/server-status
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
Other Info:
apache_server_status
Alerts 0 6 8 6 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0 0
Search
8:47 PM
5/23/2025


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Date: Fri, 23 May 2025 16:44:09 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 1887
Content-Type: text/html;charset=UTF-8
<title>Index of /humhub/assets/1483181</title>
</head>
<body>
<h1>Index of /humhub/assets/1483181</h1>
<table>
<tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td>Parent Directory</td><td> </td><td
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (20)
CSP: Failure to Define Directive with No Fallback (5)
CSP: Wildcard Directive (5)
CSP: style-src unsafe-inline (5)
Content Security Policy (CSP) Header Not Set (5)
Directory Browsing (11)
Hidden File Found (2)
Application Error Disclosure (16)
Big Redirect Detected (Potential Sensitive Information Leak)
CSP: Notices (5)
Information Disclosure - Debug Error Messages (6)
Server Leaks Information via "X-Powered-By" HTTP Response
Server Leaks Version Information via "Server" HTTP Response
Timestamp Disclosure - Unix (27)
X-Content-Type-Options Header Missing (9)
Authentication Request Identified (2)
GET for POST (3)
Directory Browsing
URL: http://localhost/humhub/assets/1483181/
Risk: Medium
Confidence: Medium
Parameter:
Attack: http://localhost/humhub/assets/1483181/
Evidence: Parent Directory
CWE ID: 548
WASC ID: 48
Source: Active (0 - Directory Browsing)
Input Vector:
Description:
It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
Other Info:
Alerts 0 6 8 6 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0 0
Search
8:18 PM
5/23/2025

ایجادIssues درGitHub

Issue 1: Missing CSP Header

شرح: هدر امنیتی CSP ارسال نمی‌شود

اقدام: افزودن هدر زیر در کانفیگ Apache