INFORMATION SECURITY PROJECT

SUBMITTED TO: DR. HABIB UR REHMAN

SUBMITTED BY: ZUHA JUNAID

1. Executive Summary

The primary goal of this project was to identify and mitigate vulnerabilities in a custom-built academic portal. By employing **DAST**, **IAST**, **SAST**, and **SCA**, we achieved a "defense-in-depth" security posture. The assessment revealed critical misconfigurations such as missing security headers and server banner disclosures.

2. Methodology & Tools Used

We utilized a combination of automated and manual testing techniques to ensure comprehensive coverage.

Tool/Method	Description
SAST (Static An	Analyzes the source code without execution to find hardcoded secrets or unsafe APIs.
DAST (Dynamic Analysis)	Tests the running application from the outside to find runtime flaws like SQL injection.
IAST (Interactive	Uses agents to monitor application behavior in real-time during execution.
SCA (Compositi Analysis)	Identifies vulnerabilities in third-party libraries and opensource dependencies.
Proxy (ZAP/Bur	Intercepts and modifies HTTP traffic to test input validation and session security.
MACRO Tool	Automates complex multi-step sequences, such as logging in before a scan.
R-Builder	Facilitates the creation of structured security reports for stakeholders.

3. Evidence of Security Scanning

The following findings were captured during the OWASP ZAP/DAST scanning process:

3.1 Macro Configuration

The project utilized a **Macro Event List** to automate the authentication process for the scanner. This ensures that the DAST tool can access protected pages like the Admin dashboard.

File Proof (Macro Script Snippet):

XML

```
<MacroEvent>
  <EventType>Javascript</EventType>
  <EventTypeName>Click</EventTypeName>
  <Data><![CDATA[ (function(path){ ... })('INPUT[name="age"]', '4') ]]></Data>
  <Step>26</Step>
</MacroEvent>
```

The snippet shows a Javascript event being triggered to interact with the "age" input field during a recorded session.

3.2 Vulnerability Findings

- **Missing Referrer-Policy:** The site does not instruct the browser on how much referrer information to share, potentially leaking sensitive URLs to third parties.
- **Content-Security-Policy (CSP) Not Set:** Lack of a CSP increases the risk of Cross-Site Scripting (XSS) and clickjacking.
- **Server Banner Disclosure:** The server reveals its software version (e.g., Microsoft-IIS/10.0), allowing attackers to target version-specific exploits.

4. Pros and Cons of the Approach

Pros

- **Comprehensive Coverage:** Combining SAST (internal) and DAST (external) ensures that both code-level and configuration-level flaws are found.
- **High Accuracy:** Using IAST reduces false positives by correlating runtime data with code analysis.
- **Zero-Cost:** Leveraging OWASP's open-source tools provides enterprisegrade security without licensing fees.

Cons

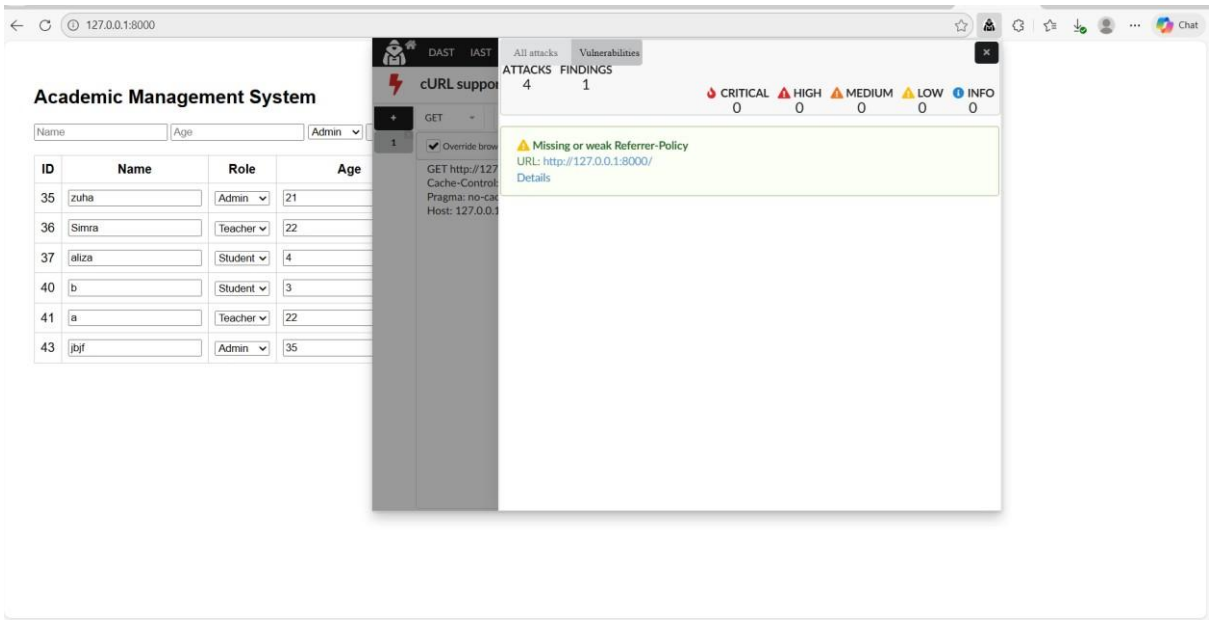
- **Slow Scan Times:** DAST scans can be time-consuming, sometimes taking several days for large applications.
- **Complexity:** Managing multiple tools (SCA, SAST, DAST) requires significant expertise to interpret and deduplicate results.

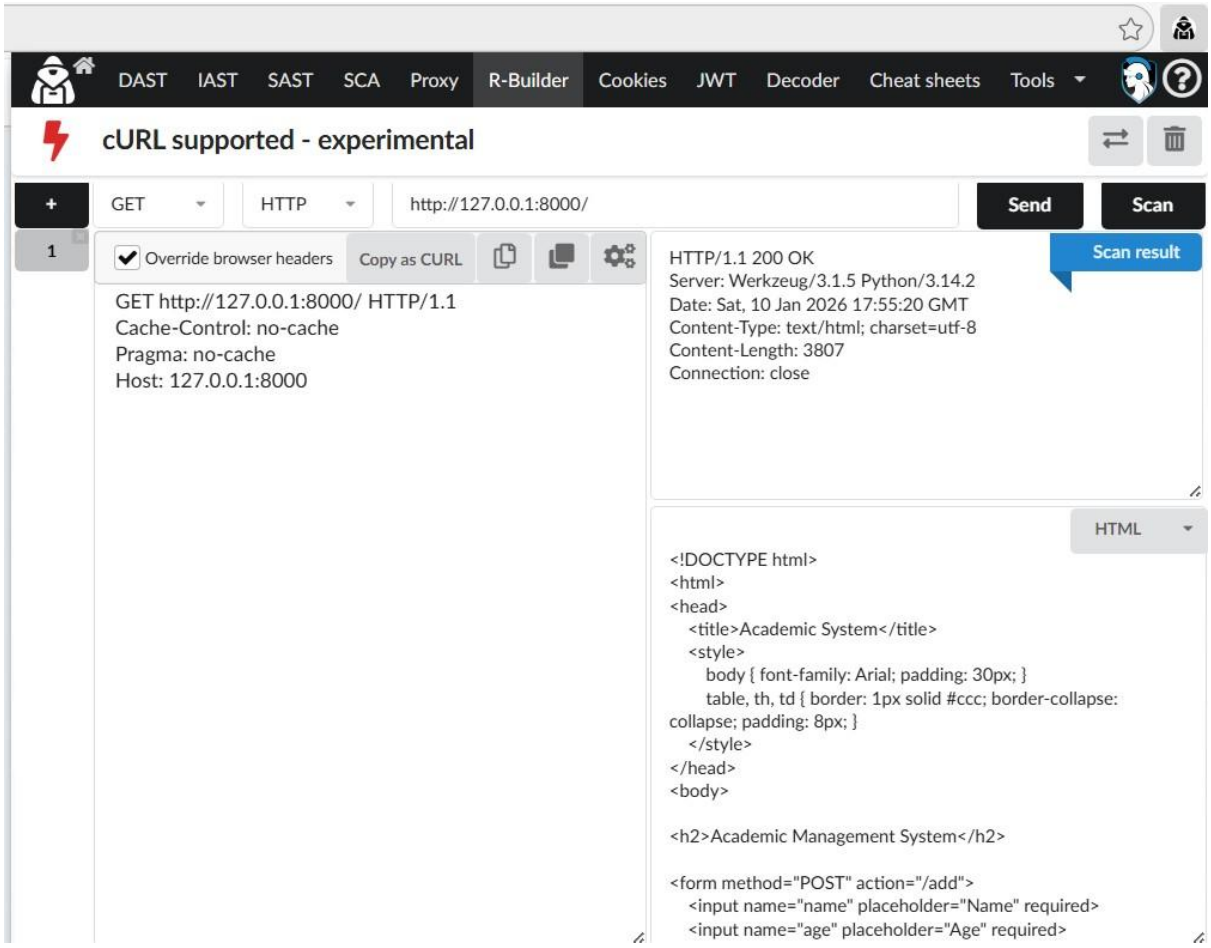
5. Conclusion & Recommendations

The academic portal currently has a moderate security risk due to missing HTTP headers and server information disclosure.

Next Steps: * **Implement Security Headers:** Add Content-Security-Policy and ReferrerPolicy to the server configuration.

- **Harden Server:** Disable server banners to prevent version fingerprinting.
- **Continuous Scanning:** Integrate SCA into the build process to catch vulnerable dependencies early.





OWASP Penetration Testing Kit - Report

OWASP PTK report:
127.0.0.1:8000

DAST (Dynamic Application Security Testing) result

ATTACKS	FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFO
38	2	0	0	0	2	0

Missing Content-Security-Policy header
http://127.0.0.1:8000/add
Attack: Missing Content-Security-Policy header

```
POST http://127.0.0.1:8000/add HTTP/1.1
Sec-Ch-Ua: "Microsoft Edge";v="143", "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: Windows
Origin: http://127.0.0.1:8000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: csrftoken=eDEvtjoXLWbFTOAvywIZN7VlywvFnIVg
Cache-Control: no-cache
Pragma: no-cache
Host: 127.0.0.1:8000
Content-Length: 27
```

```
HTTP/1.1 OK
connection: close
content-length: 1739
content-type: text/html; charset=utf-8
date: Sat, 10 Jan 2026 17:49:31 GMT
server: Werkzeug/3.1.5 Python/3.14.2

<!DOCTYPE html>
<html>
<head>
    <title>Academic System</title>
    <style>
        body { font-family: Arial; padding: 30px; }
        table, th, td { border: 1px solid #ccc; border-collapse: collapse; padding:
8px; }
    </style>
</head>
<body>

<h2>Academic Management System</h2>
```

OWASP Penetration Testing Kit - Report

Server banner discloses software/version
http://127.0.0.1:8000/delete/4
Attack: Server banner discloses software/version

```
GET http://127.0.0.1:8000/delete/4 HTTP/1.1
Sec-Ch-Ua: "Microsoft Edge";v="143", "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: Windows
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: csrftoken=eDEvtjoXLWbFTOAvywIZN7VlywvFnIVg
Cache-Control: no-cache
Pragma: no-cache
```

```
HTTP/1.1 OK
connection: close
content-length: 17460
content-type: text/html; charset=utf-8
date: Sat, 10 Jan 2026 17:49:57 GMT
server: Werkzeug/3.1.5 Python/3.14.2

<!DOCTYPE html>
<html>
<head>
    <title>Academic System</title>
    <style>
        body { font-family: Arial; padding: 30px; }
        table, th, td { border: 1px solid #ccc; border-collapse: collapse; padding:
8px; }
    </style>
</head>
<body>

<h2>Academic Management System</h2>
```