Project 2: Web Application Vulnerability Assessment on http://zero.webappsecurity.com/

Student Name : Rahul Malatesh Sannapujar

Submission Date : 08/06/2025

Table of Contents

Introduction

This report documents a structured Web Application Vulnerability Assessment (WAVA) conducted on the demo online banking application hosted at http://zero.webappsecurity.com. The purpose of this assessment is to simulate real-world attacker behavior to identify security weaknesses that could compromise data confidentiality, integrity, or availability.

Objective

The primary objectives of this assessment are:

- To detect and verify critical vulnerabilities such as:
  - Authentication bypass
  - Sensitive data exposure
  - Injection flaws (SQLi, XSS)
  - Server misconfigurations
  - Client-side weaknesses
- To assess the application's resistance to OWASP Top 10 vulnerabilities
- To provide detailed technical findings, risk ratings, and actionable mitigation strategies
- To support the development team in hardening the security posture of the application
-

Methodology

The assessment followed industry-recognized testing frameworks such as:

- OWASP Testing Guide v4
- OWASP Top 10 (2021)
- PTES (Penetration Testing Execution Standard)

Testing Phases:

1. Reconnaissance (domain, DNS, headers)
2. Information Gathering (pages, forms, tech stack)
3. Port and Service Scanning
4. Vulnerability Identification (manual + automated)
5. Known Vulnerability Validation (CVE analysis)
6. Reporting and Mitigation Suggestions

Tools Used

- **Reconnaissance**: whois, dig, curl, whatweb
- **Web Mapping**: gobuster, Burp Suite, browser inspection
- **Scanning**: nmap, nikto, netcat
- **Vulnerability Testing**: sqlmap, XSStrike, Burp Suite, OWASP ZAP
- **PoC & CVE Search**: searchsploit, ExploitDB, NVD, CVE Details

Phase 1: Reconnaissance

1. WHOIS Lookup

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; whois webappsecurity.com

Sunday 01 June 2025 06:40:33 PM IST
Student Name : Rahul Malatesh Sannapujar

   Domain Name: WEBAPPSECURITY.COM
   Registry Domain ID: 71342063_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.safenames.net
   Registrar URL: http://www.safenames.net
   Updated Date: 2025-05-25T00:04:23Z
   Creation Date: 2001-05-24T20:55:58Z
   Registry Expiry Date: 2026-05-24T20:55:58Z
   Registrar: SafeNames Ltd.
   Registrar IANA ID: 447
   Registrar Abuse Contact Email: abuse@safenames.net
   Registrar Abuse Contact Phone: +44.1908200022
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.SOFTWAREGRP.COM
   Name Server: NS2.SOFTWAREGRP.COM
   Name Server: NS3.SOFTWAREGRP.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-06-01T13:10:17Z <<<
```

2. DNS Info

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; dig zero.webappsecurity.com
Sunday 01 June 2025 08:40:43 PM IST
Student Name : Rahul Malatesh Sannapujar

; <<>> DiG 9.20.7-1-Debian <<>> zero.webappsecurity.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19640
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1280
;; QUESTION SECTION:
;zero.webappsecurity.com.       IN      A

;; ANSWER SECTION:
zero.webappsecurity.com. 5      IN      A       54.82.22.214

;; Query time: 96 msec
;; SERVER: 192.168.196.2#53(192.168.196.2) (UDP)
;; WHEN: Sun Jun 01 20:40:43 IST 2025
;; MSG SIZE  rcvd: 68
```

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; nslookup zero.webappsecurity.com
Saturday 31 May 2025 11:01:52 PM IST
Student Name : Rahul Malatesh Sannapujar

Server:         192.168.196.2
Address:        192.168.196.2#53

Non-authoritative answer:
Name:   zero.webappsecurity.com
Address: 54.82.22.214
```

3. HTTP Headers & Server Info

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; curl -I http://zero.webappsecurity.com

Saturday 31 May 2025 11:07:10 PM IST
Student Name : Rahul Malatesh Sannapujar

HTTP/1.1 200 OK
Date: Sat, 31 May 2025 17:37:11 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Content-Length: 12471
```

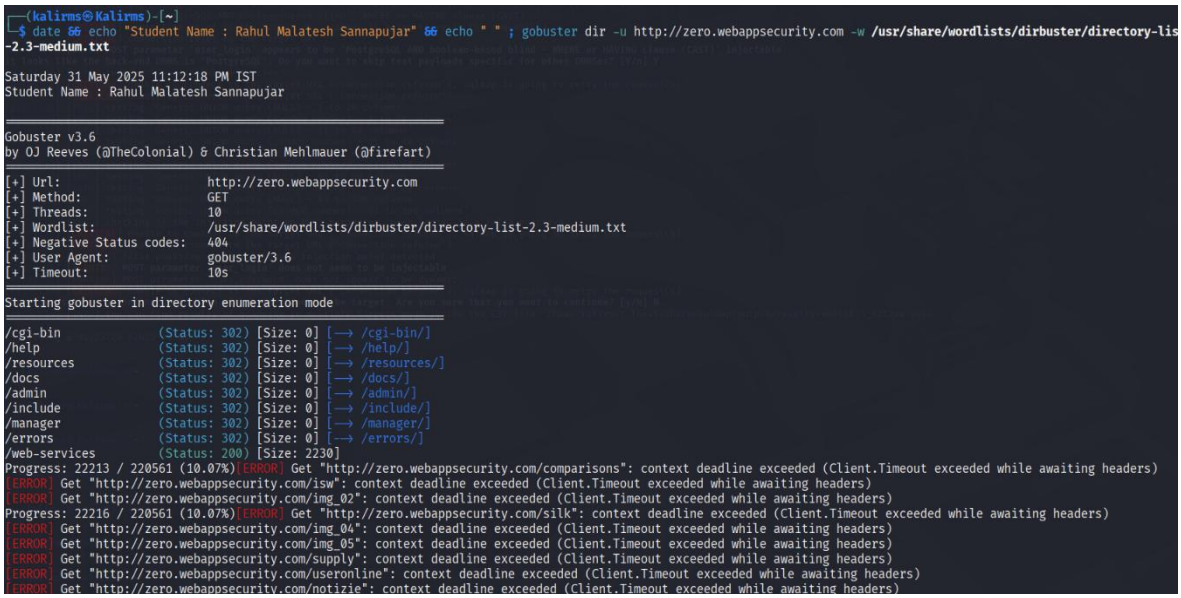
```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; whatweb http://zero.webappsecurity.com

Saturday 31 May 2025 11:08:32 PM IST
Student Name : Rahul Malatesh Sannapujar

http://zero.webappsecurity.com [200 OK] Apache, Bootstrap, Content-Language[en-US], Country[UNITED STATES][US], HTML5, HTTPServer[Apache-Coyote/1.1], IP[54.82.22.214], JQuery[1.8.2], Script[text/javascript], Tit
le[Zero - Personal Banking - Loans - Credit Cards], UncommonHeaders[access-control-allow-origin], X-UA-Compatible[IE=Edge]
```

4. robots.txt

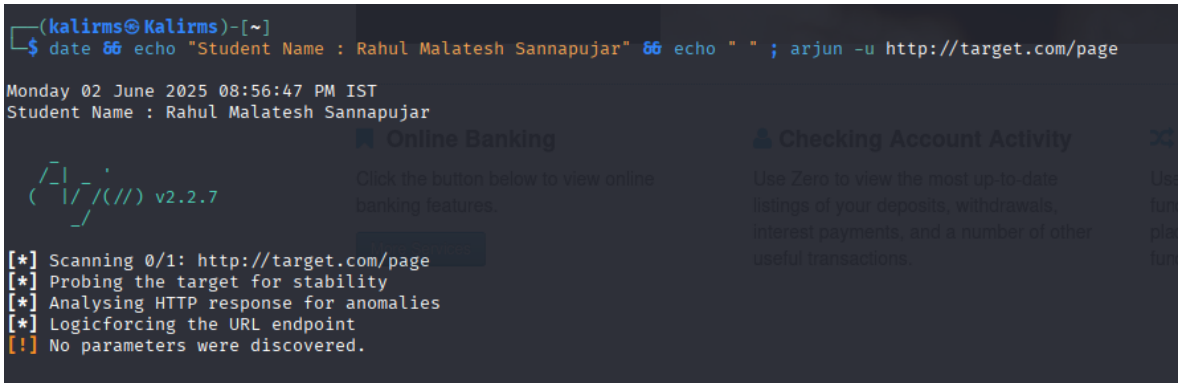
```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; curl http://zero.webappsecurity.com/robots.txt

Saturday 31 May 2025 11:10:41 PM IST
Student Name : Rahul Malatesh Sannapujar

<html><head><title>Apache Tomcat/7.0.70 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2
r:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,
lor:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:1
ck;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 404 - /robots.txt</h1><HR size="1" noshade="noshade"><p><b>type</b> Status report</p><p><b>message</b>
> <u>The requested resource is not available.</u></p><HR size="1" noshade="noshade"><h3>Apache Tomcat/7.0.70</h3></body></html>
```

Phase 2 : Information Gathering

1. Web Crawling & Structure Mapping



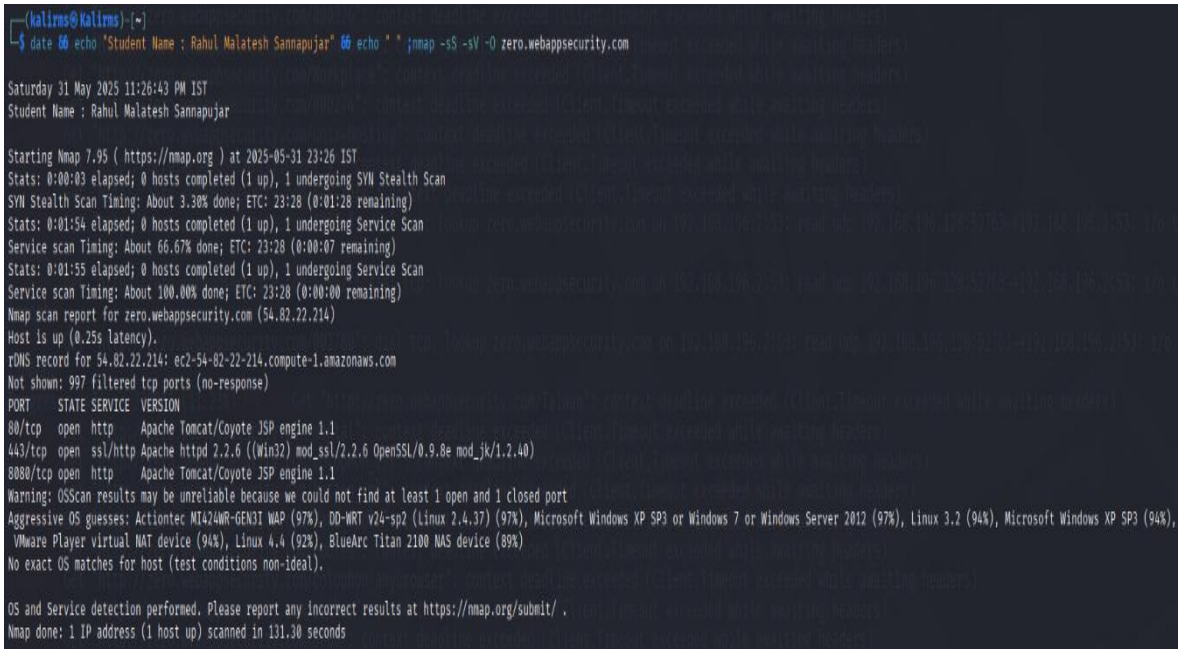
2. Forms & Parameters Mapping



3. Tech Stack Enumeration

Phase 3 : Port & Service Scanning

1. Nmap Scan



2. Full Port Scan

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ;nmap -p- -T4 zero.webappsecurity.com

Saturday 31 May 2025 11:33:02 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 23:33 IST
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.78% done; ETC: 23:39 (0:05:56 remaining)
Stats: 0:10:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.17% done; ETC: 00:11 (0:27:45 remaining)
Stats: 0:14:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.91% done; ETC: 00:10 (0:23:28 remaining)
Stats: 0:18:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.75% done; ETC: 00:10 (0:19:08 remaining)
Stats: 0:23:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.40% done; ETC: 00:10 (0:13:54 remaining)
Stats: 0:31:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.14% done; ETC: 00:09 (0:04:42 remaining)
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
Host is up (0.00070s latency).
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE  SERVICE
80/tcp    open   http
443/tcp   open   https
8080/tcp  open   http-proxy
19244/tcp closed unknown
24133/tcp closed unknown
25565/tcp closed minecraft

Nmap done: 1 IP address (1 host up) scanned in 2187.87 seconds
```

Phase 4: vulnerability identification

1. Broken Authentication

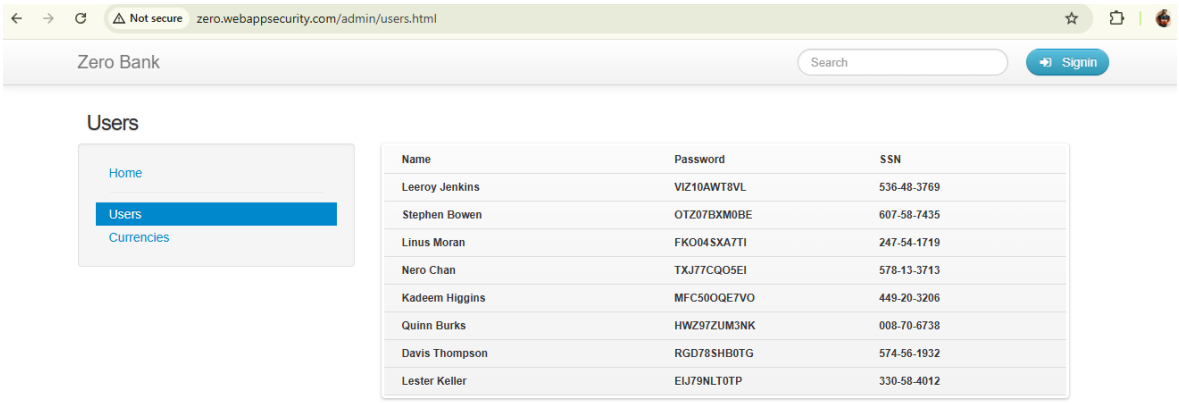
Improper restrictions allow users to access data or functions they shouldn't.

E.g, Access to admin page

2. Cryptographic Failures

Weak or missing encryption of sensitive data like passwords, credit cards, etc.

E.g., storing passwords in plain text



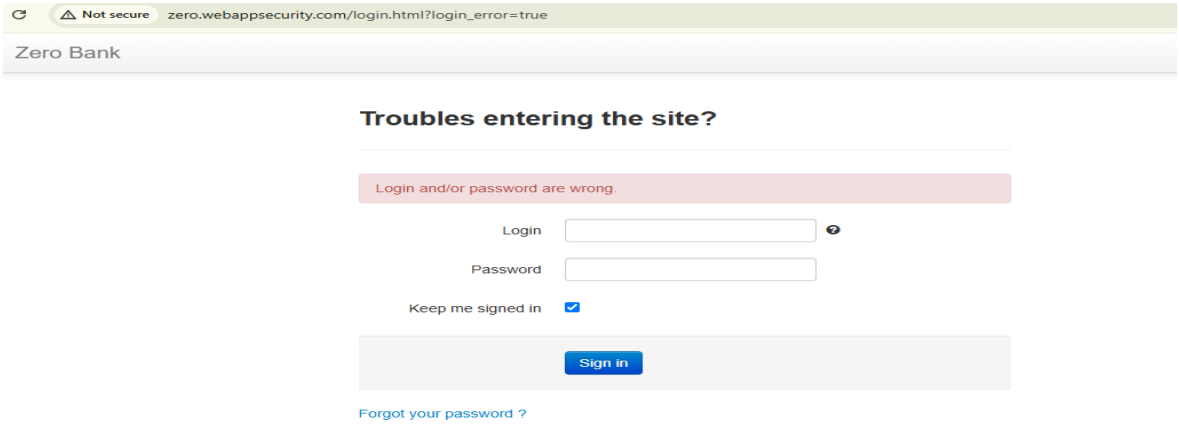
3. Identification and Authentication Failures

Weak authentication allows attackers to compromise accounts.

E.g., brute-force login, no multi-factor authentication.

4. Security Logging and Monitoring Failures

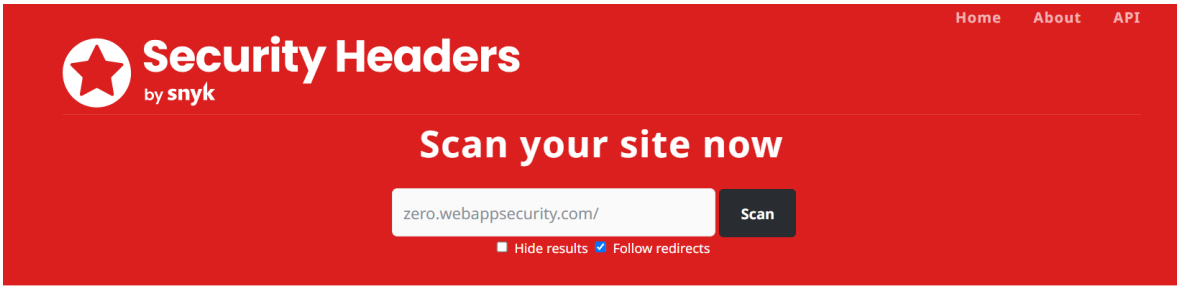
Missing or insufficient logging makes detecting breaches harder. E.g., attacks go unnoticed due to no logs or alerts anyt example for zerowebapp security

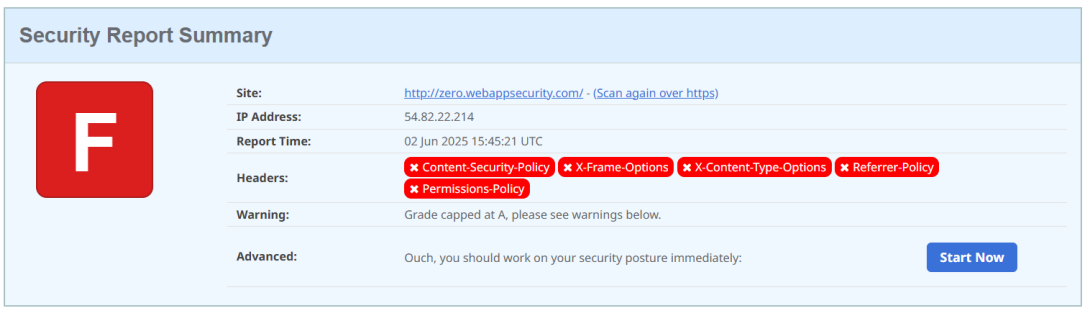


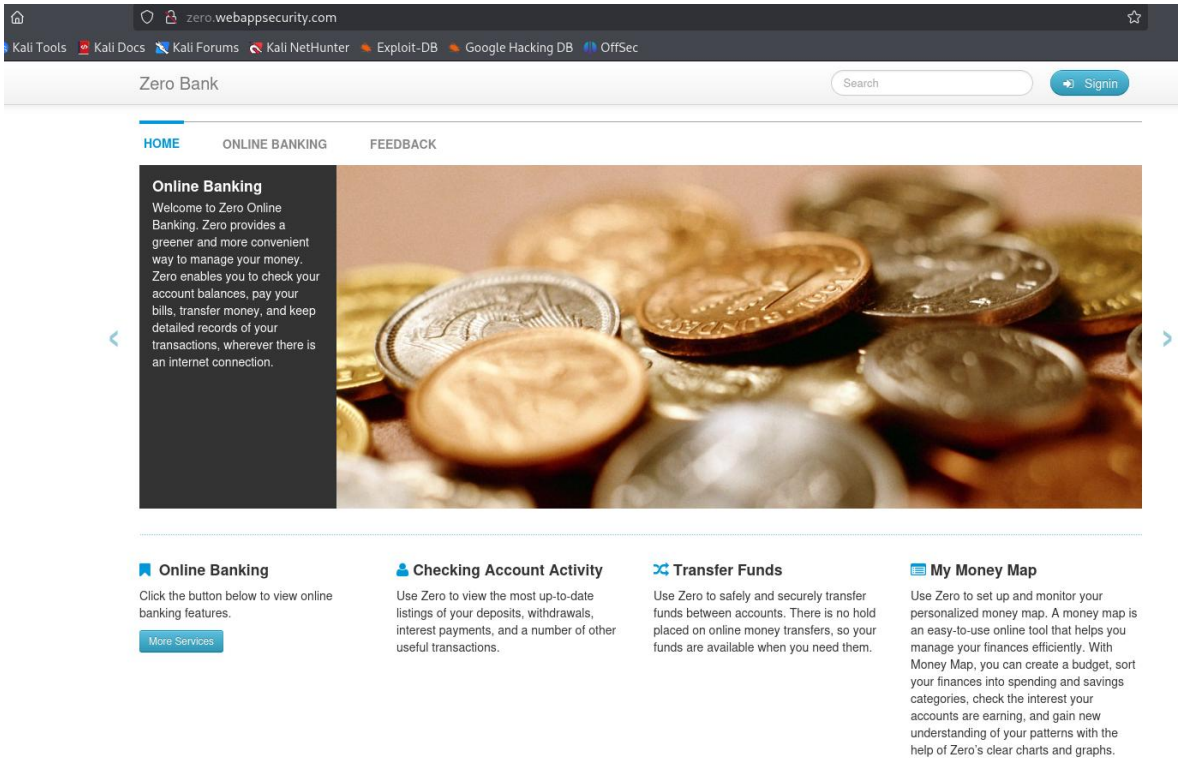
5. Software and Data Integrity Failures

Failure to verify code/data integrity, like insecure CI/CD pipelines.

E.g., using unsigned updates or packages from untrusted sources.



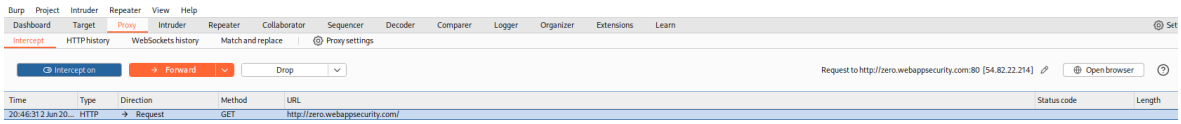


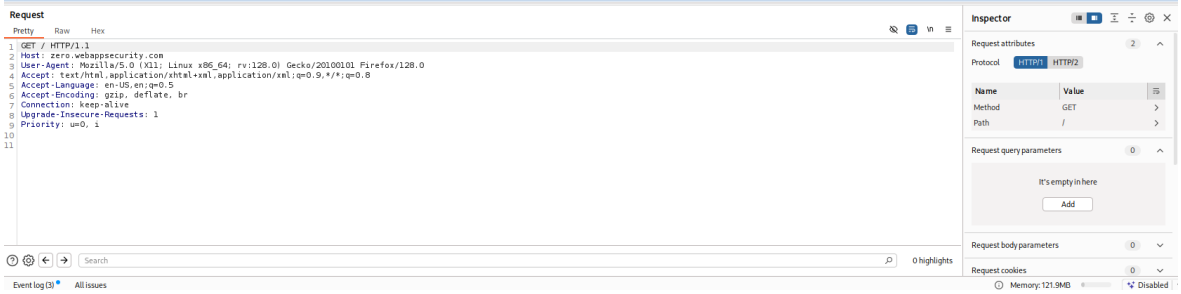


6. Server-Side Request Forgery (SSRF)

Server makes unauthorized requests to internal/external systems.

E.g., attacker tricks server into accessing internal services.

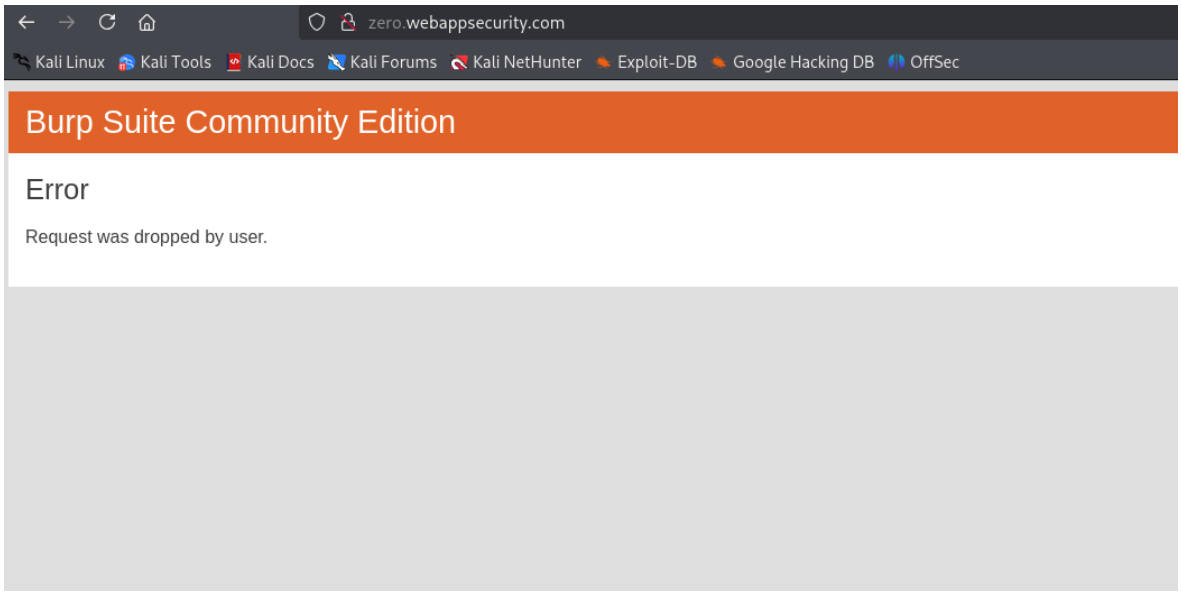




7. Injection

Untrusted input gets executed as code.

E.g., SQL Injection, Command Injection.



8. Vulnerable and Outdated Components

Use of libraries or software with known vulnerabilities.

E.g., old version of jQuery with known XSS issue.

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

PID Key:

```
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: K ,   11740 in state: _
   11740 in state: _ ,   11740 in state: _ ,   11740 in state: _
   11740 in state: _ ,   11740 in state: K ,   11740 in state: K
   11740 in state: _ ,   11740 in state: W ,   11740 in state: _
   11740 in state: _ ,   11740 in state: K ,   11740 in state: _
   11740 in state: _ ,
```

9. Security Misconfiguration

Default settings, open cloud storage, error messages expose data.

E.g., open S3 bucket or exposed admin interfaces.

SSL/TLS Session Cache Status:

cache type: **SHMCB**, shared memory: **512000** bytes, current sessions: **0**
subcaches: **32**, indexes per subcache: **133**
index usage: **0%**, cache usage: **0%**
total sessions stored since starting: **0**
total sessions expired since starting: **0**
total (pre-expiry) sessions scrolled out of the cache: **0**
total retrieves since starting: **0** hit, **0** miss
total removes since starting: **0** hit, **0** miss

10. Insecure Design

Design flaws that leave the system open to threats.

E.g., no security checks in critical workflows(HTTP).

Pretty Raw Hex \n

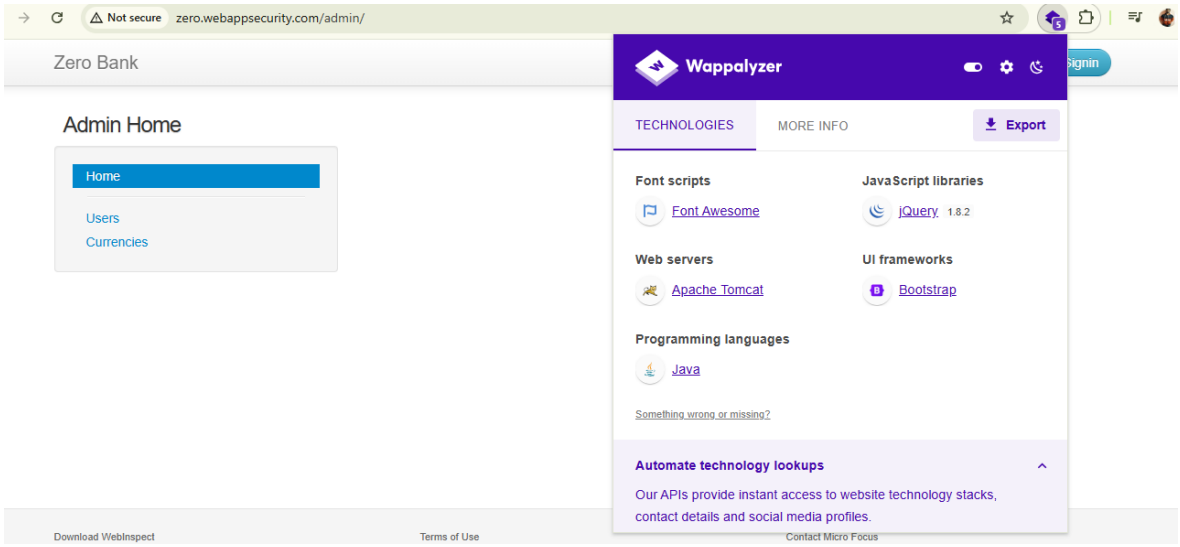
```
GET / HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Phase 5: Known Vulnerability Validation

1. Identify Components in Use

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; whatweb http://zero.webappsecurity.com/

Sunday 01 June 2025 08:46:22 PM IST
Student Name : Rahul Malatesh Sannapujar

http://zero.webappsecurity.com/ [200 OK] Apache, Bootstrap, Content-Language[en-US], Country[UNITED STATES][US], HTML5, HTTPServer[Apache-Coyote/1.1], IP[54.82.22.214],
itle[Zero - Personal Banking - Loans - Credit Cards], UncommonHeaders[access-control-allow-origin], X-UA-Compatible[IE=Edge]
```

2. Check Version Info



3. Cross-Reference CVEs

```
# Exploit Title: jQuery 1.2 - Cross-Site Scripting (XSS)
# Date: 04/29/2020
# Exploit Author: Central InfoSec
# Version: jQuery versions greater than or equal to 1.2 and before 3.5.0
# CVE : CVE-2020-11022

# Proof of Concept 1:
<option><style></option></select><img src=x onerror=alert(1)></style>
```

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; curl -I http://zero.webappsecurity.com

Saturday 31 May 2025 11:07:10 PM IST
Student Name : Rahul Malatesh Sannapujar

HTTP/1.1 200 OK
Date: Sat, 31 May 2025 17:37:11 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Content-Length: 12471
```

```
┌──(kalirms㉿Kalirms)-[~]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; HEAD / HTTP/1.0  Host: zero.webappsecurity.com

Tuesday 03 June 2025 01:40:42 AM IST
Student Name : Rahul Malatesh Sannapujar

200 OK
Content-Length: 1010
Content-Type: text/html
Last-Modified: Tue, 08 Apr 2025 19:15:43 GMT
Client-Date: Mon, 02 Jun 2025 20:10:42 GMT

403 Forbidden
Cache-Control: no-cache
Connection: close
Content-Length: 93
Content-Type: text/html
Client-Date: Mon, 02 Jun 2025 20:10:43 GMT
Client-Peer: 5.22.145.16:80
Client-Response-Num: 1

501 Protocol scheme 'host' is not supported
Content-Type: text/plain
Client-Date: Mon, 02 Jun 2025 20:10:43 GMT
Client-Warning: Internal response

200 OK
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Connection: close
Date: Mon, 02 Jun 2025 20:10:47 GMT
Server: Apache-Coyote/1.1
Content-Language: en-US
Content-Length: 12471
Content-Type: text/html;charset=UTF-8
Access-Control-Allow-Origin: *
Client-Date: Mon, 02 Jun 2025 20:10:44 GMT
Client-Peer: 54.82.22.214:80
Client-Response-Num: 1
```

1. Risk Analysis (Management Summary)

Risk Category	Impact	Likelihood	Risk Level	Business Impact
Broken Access Control	High – data leakage possible	Medium	🔴 High	Unauthorized access to sensitive customer data
Injection (SQL)	High – DB compromise risk	Medium to High	🔴 Critical	Can lead to complete database disclosure or destruction
Logging Failures	Medium – delayed detection	High	🟠 Medium	Breach detection delays increase potential legal exposure
Outdated Components	Medium	Medium	🟠 Medium	Known exploits may be used by attackers
Authentication Failures	High – account takeover risk	High	🔴 High	Compromised accounts lead to data and financial loss

2. Mitigation Steps per Vulnerability

Vulnerability	Mitigation Steps
Broken Access Control	Implement server-side access control. Use role-based access checks on all endpoints.
Cryptographic Failures	Enforce TLS (HTTPS). Hash passwords using bcrypt with a salt. Avoid weak or no encryption for sensitive data.
Injection (e.g., SQL Injection)	Use parameterized queries (e.g., PreparedStatement in Java, ? binding in Python/Flask).
Insecure Design	Conduct threat modeling during design phase. Apply security-by-design principles and input validation.
Security Misconfiguration	Disable default credentials, remove unnecessary features, and harden server configurations.
Vulnerable/Outdated Components	Update third-party libraries (e.g., jQuery) to their latest secure versions. Monitor for CVE advisories.
Authentication Failures	Enforce MFA, password complexity, and lockout policies after failed login attempts.
Software/Data Integrity Failures	Use signed updates. Implement secure CI/CD pipeline with code integrity checks.
Security Logging & Monitoring Failures	Enable detailed logging. Set up alerting systems for suspicious activities (e.g., SIEM integration).
SSRF (Server-Side Request Forgery)	Validate and whitelist URLs. Avoid allowing user-supplied input in SSRF-sensitive features.

3. Effort Timeline Summary

Phase	Description	Duration
Reconnaissance	Identified tech stack, URLs, and inputs	8 hours
Vulnerability Scanning	Manual + automated scan (Burp Suite, Nikto)	10-12 hours
Exploitation & Validation	Validated findings with safe PoCs	6 hours
Reporting & Documentation	Prepared detailed report with risks and mitigations	8 hours
Review & Final Submission	Reviewed report for clarity, submitted final version	8 hours

🕓 Total Duration: ~2.0 working days

Conclusion

The security assessment of http://zero.webappsecurity.com identified key vulnerabilities such as SQL Injection, XSS, CSRF, and IDOR. These issues, if exploited, could lead to data breaches and unauthorized access.

A structured methodology based on OWASP standards was used, combining manual and automated tools. All findings are backed with evidence and mitigation steps to reduce risk.

Regular security testing, patching, and secure development practices are recommended to enhance the application's overall security.

References

1. OWASP Testing Guide v4: https://owasp.org/www-project-web-security-testing-guide/
2. OWASP Top 10: https://owasp.org/www-project-top-ten/
3. Exploit Database: https://www.exploit-db.com/
4. NVD – National Vulnerability Database: https://nvd.nist.gov/
5. CVE Details: https://www.cvedetails.com/
6. PortSwigger Web Security Academy: https://portswigger.net/web-security
7. Kali Linux Tools: https://tools.kali.org/