

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

Scanning and Collaborative Wiki Activity – Zero Bank

FAQ (Frequently Asked Questions)

Q1: What tools were used to scan Zero Bank?

A combination of Kali Linux tools was used, including Nmap for port scanning, for web technology fingerprinting, Nikto for vulnerability scanning, Nmap for port scanning/discovery and WHOIS for hosting and network information. These tools collected in Linux Kali are very commonly used in security assessments and penetration testing to enumerate services and identify potential vulnerabilities.

Q2: What operating system does Zero Bank utilize?

Based on the Nmap OS detection flags (T4-A-v), the server appears to be running a Windows server-based operating system. although the exact distribution details were not detected with 100% accuracy:

(Laštovička et al, 2023).

Operating System	Probability
Windows server 2008 R2 SP1	92%
Microsoft Windows Server 2012 R2	92%
Microsoft Windows Server 2008 R2	89%
Windows 7 SP1	89%
Microsoft Windows 7	85%
Windows Server 2008 R2	85%

Table 1: Nmap OS identification summary

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

In accordance with ethical scanning practices, the full data of the scan will not be shared in this report.

```
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Zero - Personal Banking - Loans - Credit Cards
|_http-server-header: Apache-Coyote/1.1
|_http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS PATCH
|   Potentially risky methods: PUT DELETE TRACE PATCH
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|2012|7 (92%)
OS_CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (92%), Microsoft Windows Server 2012 R2 (92%), Microsoft Windows Server 2008 R2 or Windows 7 SP1 (89%), Microsoft Windows 7 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 261.642 days (since Fri Jun 6 14:04:23 2025)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental

Host script results:
|_clock-skew: 1s
```

Figure 1: Nmap OS identification output in Kali

Q3: What web server software is it running?

Nmap service detection (-sV) identified the web server as Apache Tomcat HTTPD 2.2.6 Server with openSSL 0.9.8e, Tomcat Coyote JSP engine 1.1 and mod_jk 1.2.40. The server banner exposes much information, for instance; Apache-Coyote/1.1' to 'Apache/2.2.6. Apache remains one of the most widely deployed web servers global.

(Laštovička et al, 2023).

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

```
nmap -sV zero.webappsecurity.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 04:52 EST
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
Host is up (0.11s latency).
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache Tomcat/Coyote JSP engine 1.1
443/tcp   open  ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40)
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 22.82 seconds
```

Figure 2: Nmap -sV version detection

Q4: Is it running a CMS?

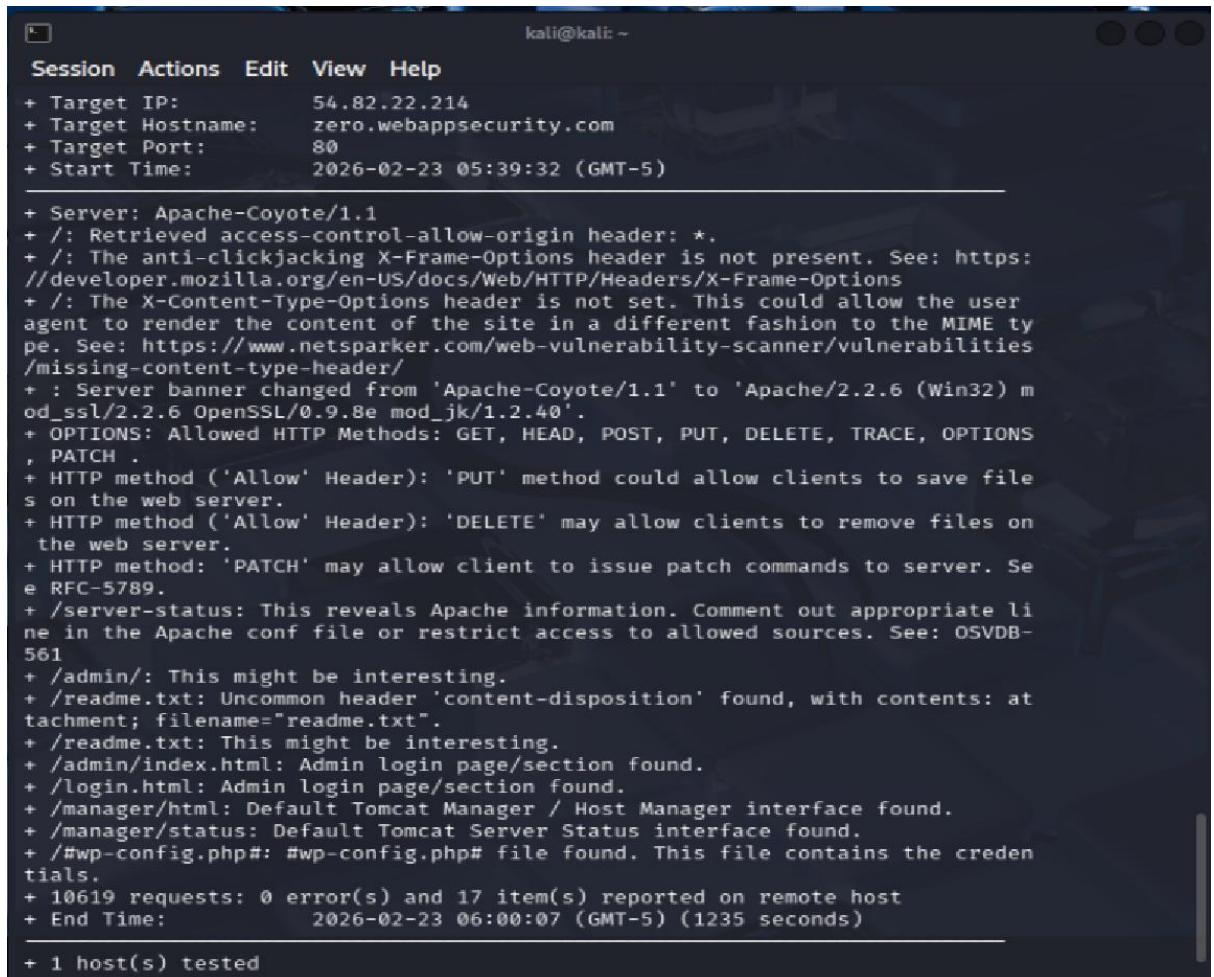
No clear evidence of a CMS such as WordPress or Drupal was detected. What Web did not identify typical CMS fingerprints or any directories or meta generator tags, The application appears to be a java-based web application built with: Apache 2.2.6 (Win32), mod_ssl 2.2.6, OpenSSL 0.9.8e and mod_jk 1.2.40 and run on Windows (32 bit) OS. which is common outdated website architecture.

```
(kali㉿kali)-[~]
$ whatweb zero.webappsecurity.com
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], Title[Zero - Personal Banking - Loans - Credit Cards], UncommonHeaders[access-control-allow-origin], X-UA-Compatible[IE=Edge]
https://zero.webappsecurity.com [200 OK] Apache[2.2.6][Default][mod_jk/1.2.40,mod_ssl/2.2.6], Country[UNITED STATES][US], HTTPServer[Windows (32 bit)][Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40], IP[54.82.22.214], OpenSSL[0.9.8e], UncommonHeaders[access-control-allow-origin]
```

Figure 3: WhatWeb HTTP/HTTPS Details identification

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

Nikto did detect a wp-config.php file which contains credentials and therefore imposes a potential vulnerability. in addition, Nikto found more vulnerabilities.



```
kali㉿kali: ~
Session Actions Edit View Help
+ Target IP: 54.82.22.214
+ Target Hostname: zero.webappsecurity.com
+ Target Port: 80
+ Start Time: 2026-02-23 05:39:32 (GMT-5)
+
+ Server: Apache-Coyote/1.1
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ : Server banner changed from 'Apache-Coyote/1.1' to 'Apache/2.2.6 (Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40'.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method: 'PATCH' may allow client to issue patch commands to server. See RFC-5789.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /admin/: This might be interesting.
+ /readme.txt: Uncommon header 'content-disposition' found, with contents: attachment; filename="readme.txt".
+ /readme.txt: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /login.html: Admin login page/section found.
+ /manager/html: Default Tomcat Manager / Host Manager interface found.
+ /manager/status: Default Tomcat Server Status interface found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 10619 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2026-02-23 06:00:07 (GMT-5) (1235 seconds)
+
+ 1 host(s) tested
```

Figure 4: Nikto’s Zero Bank Scan Results

Nikto Findings Mapping against the MITRA ATT&CK

Finding	CWE	MITRE ATT&CK Mapping
Exposed backup file #wp-config.php#	CWE-200	T1552 – Unsecured Credentials
PUT/DELETE/PATCH	CWE-284	T1210 – Exploitation of Remote Services
Tomcat Manager exposed	CWE-306	T1210 / T1078 – Valid Accounts
Server-status exposed	CWE-200	T1592 – Gather Victim Host Information
Missing security headers	CWE-1021	T1190 – Exploit Public-Facing Application

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

Wildcard CORS	CWE-942	CWE-942 – Permissive Cross-domain Security Policy with Untrusted Domains
Server version disclosure	CWE-200	T1592 – Gather Victim Host Information

(MITRE, 2026a; MITRE; 2026b; MITRE, 2026c; MITRE, 2026d; MITRE, 2026e; MITRE, 2026f; MITRA, 2024)

Q5: What protection mechanisms are in place?

The scans suggest the presence of a mod_jk/1.2.40 which enables Apache to act as a reverse proxy.

(Barnett, no date).

And this is an indication of the existence of such a reverse proxy. AWS Cloud-based CDN was identified which has an indication of a possible Cloud network isolation, Security groups and cloud firewall and likely some network-level filtering, but filtered responses indicate some form of perimeter security. In addition, mod_ssl/2.2.6 and OpenSSL/0.9.8e indicate some level of protection even though quite outdated legacy versions are vulnerable to attacks.

Q6: Where is the site hosted?

WHOIS and traceroute results indicate hosting in the UK. This Public IP address is associated with a hosting provider called: “safenames.net”. Exact data center information was limited due to privacy protection.

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

The screenshot shows a terminal window titled 'kali@kali: ~'. The command \$ whois webappsecurity.com is run, displaying detailed WHOIS information for the domain. The output includes the domain name, registry ID, registrar, creation and expiration dates, name servers (NS1, NS2, NS3), and DNSSEC status. It also provides links to ICANN's Whois Inaccuracy Complaint Form and the last update of the whois database. A notice about the expiration date is present, stating it is the date the registrar's sponsorship of the domain registration in the registry is currently set to expire. A terms of use section from VeriSign Global Registry Services is included, detailing restrictions on automated access and use of the data.

```
(kali㉿kali)-[~]
$ whois webappsecurity.com
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: 2026-02-17T16:09:26Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```

Q7: Are there open ports?

Nmap identified ports 80-tcp, 443-tcp and 8080-tcp, as open. These were expected for a public web application. No unnecessary ports such as 21 (FTP) or 22 (SSH) were externally exposed, which indicates some degree of network hardening.

(Luthfi and Irsan, 2025).

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

Q8: Are there known vulnerabilities?

Nikto identified several potential vulnerabilities on the target, including exposed administrative interfaces, HTTP REST API methods that could allow remote file modification (PUT, DELETE, PATCH), publicly accessible pages such as /readme.txt, some minor findings included missing security headers, such as X-Content-Type-Options and X-Frame-Options, as well as a permissive CORS policy (Access-Control-Allow-Origin: *). A deeper validation against known CVEs, or directly exploitable software flaws analysis, was not conducted.

(Luthfi and Irsan, 2025).

Q9: What versions of software are in use? Are they up to date?

Identified Apache version details were Apache 2.2.6 (Win32), the OS precise validation was limited to few versions of Windows 2012, 2008 and 7, all (32 bit). However, the findings of mod_ssl 2.2.6, OpenSSL 0.9.8e and mod_jk 1.2.40 indicate from the known exploitable vulnerabilities, suggests the system is quite Out-of-Date. Banner enumeration exposes many of the components, which is recommended to obfuscate as a defensive measure.

Results Compilation

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

The combined scanning results indicate that Zero Bank is most probably running on an outdated Windows 32-bit operating system using an outdated Apache HTTP Server. The web Java application appears to rely on a common configuration. Hosting is located in the UK via a commercial hosting provider.

Open ports include 80, 8080 and 443 only, which aligns with expected exposure for a secure web service. No additional unnecessary ports were discovered, reducing the attack surface. Evidence strongly suggests implementation of security controls such as Tomcat/ mod_jk reverse proxy and a possible existence of a firewall filtering or WAF since the service is hosted on Amazon AWS, although this is only an assumption which is based on a common cloud architecture and there is no clear evidence for the existence of a WAF.

Nikto scanning revealed severe vulnerabilities together with some minor configuration weaknesses, due to limitations of time and report, manual validation of any of the findings is Out-of-Scope. Overall, the system demonstrates limited hardening practices including some degree of service exposure, exposed and unfiltered banners information, reverse proxy and probably cloud WAF protection mechanism.

Constructive feedback

Future scans could incorporate manual validation of the findings and SSL/TLS analysis using tools such as SSL-Scan to evaluate certificate strength and protocol versions more in depth. Additionally, passive reconnaissance tools such as Shodan could supplement active scanning results and there is potential for more in-depth

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

scope coverage of non-intrusive scanning activities. Boundaries of scanning activities had to be limited in order to provide structure and avoid excessive details in the report.

Reflection

Some challenges were encountered during scanning. OS fingerprinting returned inconclusive results due to scanning depth limitations. Additionally, service version detection was successful, listing banner information due to missing obfuscation measures.

These challenges were overcome by combining multiple tools and correlating outputs. Instead of relying solely on Nmap, WhatWeb and Nikto results were compared to draw conclusions. Cross-validation improved confidence in the findings.

For the final report, limitations will be clearly stated. some degree of defensive filtering could have effect on scan accuracy, so findings will be described as “best-effort and non-intrusive observations.” Future work could include authenticated scanning, deeper analysis in a controlled lab environment and maybe a more in-depth rules-of engagement that allow more intrusive scope.

(Luthfi and Irsan, 2025).

References

- Barnett, R.,(no date) Apache Web Server 2.2. 0.
- Luthfi, A. and Irsan, M., 2025, October. Identification of Security Vulnerabilities of XYZ Website using Open Web Application Security Project Zed Attack Proxy

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

and Nikto. In 2025 IEEE 9th International Conference on Software Engineering & Computer Systems (ICSECS) (pp. 458-462). IEEE.

- Laštovička, M., Husák, M., Velan, P., Jirsík, T. and Čeleda, P., (2023). Passive operating system fingerprinting revisited: Evaluation and current challenges. Computer Networks, 229, p.109782.
- MITRE (2026a) ATT&CK Technique T1552: Unsecured Credentials. Available at: <https://attack.mitre.org/techniques/T1552/> [Accessed: 24 February 2026].
- MITRE (2026b) ATT&CK Technique T1210: Exploitation of Remote Services. Available at: <https://attack.mitre.org/techniques/T1210/> [Accessed: 24 February 2026].
- MITRE (2026c) ATT&CK Technique T1078: Valid Accounts. Available at: <https://attack.mitre.org/techniques/T1078/> [Accessed: 24 February 2026].
- MITRE (2026d) ATT&CK Technique T1592: Gather Victim Host Information. Available at: <https://attack.mitre.org/techniques/T1592/> [Accessed: 24 February 2026].
- MITRE (2026e) ATT&CK Technique T1190: Exploit Public-Facing Application. Available at: <https://attack.mitre.org/techniques/T1190/> [Accessed: 24 February 2026].
- MITRE (2024) CWE-200: Exposure of Sensitive Information to an Unauthorized Actor. Available at: <https://cwe.mitre.org/data/definitions/200.html> [Accessed: 24 February 2026].
- MITRE (2024) CWE-284: Improper Access Control. Available at: <https://cwe.mitre.org/data/definitions/284.html> [Accessed: 24 February 2026].

Task ‘Scanning and Collaborative Wiki Activity’ Unit 4

- MITRE (2024) CWE-306: Missing Authentication for Critical Function. Available at: <https://cwe.mitre.org/data/definitions/306.html> [Accessed: 24 February 2026].
- MITRE (2024) CWE-1021: Improper Enforcement of HTTP Headers in Web Applications. Available at: <https://cwe.mitre.org/data/definitions/1021.html> [Accessed: 24 February 2026].
- MITRE (2024) CWE-942: Permissive Cross-Origin Resource Sharing (CORS) Policy. Available at: <https://cwe.mitre.org/data/definitions/942.html> [Accessed: 24 February 2026].