

Abdi Osman

Information Management & Technology student at Syracuse University

Case Study 1: Vulnerability Management Lab on Kali Linux

Overview

This project demonstrates how to set up a complete vulnerability management lab using Kali Linux. I deployed OWASP Juice Shop (an intentionally vulnerable web app), scanned it using common security tools, identified weaknesses, and documented mitigation strategies.

Lab Environment

Component | Details

Host OS | Windows 1

Virtualization | VirtualBox running Kali Linux

Web App | OWASP Juice Shop ([Node.js](#))

Tools Used

Tool | Purpose

Nmap | Port scanning, service detection

Nikto | Web server vulnerability scanning

Sqlmap | SQL injection testing

Burp Suite | Manual web vulnerability testing

OWASP ZAP | Automated web security scanner

1. Environment Setup

- Installed Kali Linux on VirtualBox (Windows 11 host).
 - Updated the system packages:

```bash

- sudo apt update && sudo apt upgrade -y

```
[File Actions Edit View Help
-i ncoeg@list711 ~]
$ sudo apt update
[sudo] password for ncoeg:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Hit:2 https://deb.nodesource.com/node_14.x Bullseye
Get:3 https://deb.nodesource.com/node_14.x Bullseye InRelease [11.4 kB]
 From: https://deb.nodesource.com Node.js packages (Bullseye)
 To: /var/lib/apt/lists/_index.list
Warning: https://deb.nodesource.com/node_14.x/lists/bullseye_InRelease: Policy will reject signature within a year, see --audit for details
Fetched 29.4 kB in 2s (25.7 kB/s)
Reading package lists...
Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 1
Download size: 29.4 kB / 25.7 kB available
Space needed: 1.24 kB / 25.7 kB available
Get:1 https://mirrors.jesvincanders.net/kali kali-rolling/main amd64 libwebkitgtk-4.1-0 amd64 [22.3 kB]
Get:2 http://mirrors.jesvincanders.net/kali kali-rolling/main amd64 libjavascriptcoregtk-4.1-0 amd64 2.40.3-1 [6.935 kB]
Fetched 29.4 kB in 2s (24.7 kB/s)
Preparing to unpack .../libwebkitgtk-4.1-0_2.40.3-1_amd64.deb ...
Preparing to unpack .../libjavascriptcoregtk-4.1-0_2.48.1-1_amd64.deb ...
Unpacking libjavascriptcoregtk-4.1-0-amd64 (2.48.1-1) over (2.46.6-1) ...
Setting up libwebkitgtk-4.1-0-amd64 (2.48.1-1) ...
Processing triggers for libc-bin (2.48-9) ...
ncoeg@list711:~]
```

## 2. Installed Security Tools

- sudo apt install nmap nikto zaproxy burpsuite sqlmap git nodejs npm -y

```

File Actions Edit View Help
The following packages were automatically installed and are no longer required:
libdevtools liblts1216a libglapi-mesa libglx-mesa libhyve libmetasploit libmetasploit8 python3-dbusmenu python3-poetry-dynamic-versioning python3-requests-ntlm python3-wheel-whl sphinx-rtfd-theme-common
libhwmon2030002 libhwmon2030007 libhwmon3212 libhwmon3212-stl1b libhwmon8 libhyve libmetasploit python3-nfclient python3-pyinstaller-hooks-contrib python3-setproctitle python3.12-tk strongswan
libdmnl libgeoip3.1.0 libjxl10.10 libpoppler145 libpython3.12t64 python3-sioconsole python3-packaging-whl python3-pyview
Use 'sudo apt autoremove' to remove them.

Upgrading:
libjavascriptcoregtk-4.1-0 libatk-bridge-2.0-0

Not upgrading:
strongswan

Summary:
Upgrading: 2 Installing: 0, Removing: 0, Not Upgrading: 1
Download size: 22.5 MB / 25.7 GB available
Space needed: 7.141 kB / 25.7 GB

Get:1 http://mirrors.jevicandersen.net/kali kali-rolling/main amd64 libatk-bridge2.0-0 amd64 2.48.3-1 [22.5 MB]
Get:2 http://mirrors.jevicandersen.net/kali kali-rolling/main amd64 libjavascriptcoregtk-4.1-0 amd64 2.48.3-1 [6,915 kB]
Fetched 29.4 MB in 1s (23.3 MB/s)
(Reading database ... 455306 files and directories currently installed.)
Preparing to unpack .../libatk-bridge2.0-0_1.0.2-4.0_amd64.deb ...
Unpacking libatk-bridge2.0-0:amd64 (2.48.3-1) ...
Preparing to unpack .../libjavascriptcoregtk-4.1-0_2.48.3-1_amd64.deb ...
Unpacking libjavascriptcoregtk-4.1-0:amd64 (2.48.3-1) ...
Setting up libatk-bridge2.0-0:amd64 (2.48.3-1) ...
Setting up libatk-bridge2.0-0:amd64 (2.48.3-1) ...
Preparing to unpack .../libnmap_0.8.0-1_amd64.deb ...
Unpacking libnmap (0.8.0-1) ...
Setting up libnmap (0.8.0-1) ...

[incog@kali1]:~[-]
└─$ sudo apt --fix-broken install
The following packages were automatically installed and are no longer required:
libdevtools liblts1216a libglapi-mesa libglx-mesa libhyve libmetasploit libmetasploit8 python3-dbusmenu python3-poetry-dynamic-versioning python3-requests-ntlm python3-wheel-whl sphinx-rtfd-theme-common
libhwmon2030002 libhwmon2030007 libhwmon3212 libhwmon3212-stl1b libhwmon8 libhyve libmetasploit python3-nfclient python3-pyinstaller-hooks-contrib python3-setproctitle python3.12-tk strongswan
libdmnl libgeoip3.1.0 libjxl10.10 libpoppler145 libpython3.12t64 python3-sioconsole python3-packaging-whl python3-pyview
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1
[incog@kali1]:~[-]
└─$ sudo dpkg --configure -a
[incog@kali1]:~[-]
└─$ curl https://nikto.nmap.org/nikto --version
nikto 2.1.5 (http://www.sircus.it/nikto/)

[incog@kali1]:~[-]
└─$ curl https://sqlmap.org/burpsuite --version
Burpsuite is already the newest version (7.05edfig-3kali1).

The following packages were automatically installed and are no longer required:
libdevtools liblts1216a libglapi-mesa libglx-mesa libhyve libmetasploit libmetasploit8 python3-dbusmenu python3-poetry-dynamic-versioning python3-requests-ntlm python3-wheel-whl sphinx-rtfd-theme-common
libhwmon2030002 libhwmon2030007 libhwmon3212 libhwmon3212-stl1b libhwmon8 libhyve libmetasploit python3-nfclient python3-pyinstaller-hooks-contrib python3-setproctitle python3.12-tk strongswan
libdmnl libgeoip3.1.0 libjxl10.10 libpoppler145 libpython3.12t64 python3-sioconsole python3-packaging-whl python3-pyview
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1
[incog@kali1]:~[-]

```

## Followed by:

- nmap -V
- nikto -Version
- zap --version
- burpsuite --help
- sqlmap --version

```

File Actions Edit View Help
https://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: no such option: --version
[incog@kali1]:~[-]
└─$ nmap -V
Nmap version 7.95 (https://nmap.org)
Platform: Linux-5.8.0-53-generic-x86_64-Ubuntu-20.04.1 LTS (Ubuntu)
Compiled with: liblts=4.7 openssl=1.1.1.1 libssh2=1.11.1 libcurl=7.68.0 libpcap=1.10.5 libxml=2.9.9 libxmlsec=1.8.10 libgnutls=3.6.14 libgmp=6.2.0 libmpc=3.1.1 libmpfr=4.0.2 libedit=20191231 libssl=1.1.1.1 libnet=1.1.1 libltdl=2.2.10 liblzma=5.2.5 libbz2=1.1.10 libz=1.2.11 libcurl=7.68.0 libxml=2.9.9 libxmlsec=1.8.10 libgnutls=3.6.14 libgmp=6.2.0 libmpc=3.1.1 libmpfr=4.0.2 libedit=20191231 libssl=1.1.1.1 libnet=1.1.1 libltdl=2.2.10 liblzma=5.2.5 libbz2=1.1.10 libz=1.2.11
Available nmap engines: espoll poll select
[incog@kali1]:~[-]
└─$ nikto -Version
Nikto 2.5.0 (http://nikto.org)
[incog@kali1]:~[-]
└─$ curl https://sqlmap.org/burpsuite --version
Could open channel file ./etc/channels.conf
[incog@kali1]:~[-]
└─$ curl https://sqlmap.org
[warning] /usr/bin/burpsuite: No JAVA_CMX set for run_Java, falling back to JAVA_CMD + Java
Usage:
 -help Print this message
 -version Print version details
 -list-all-extensions Print all extensions on startup
 -diagnostics Print diagnostic information
 -use Start Burp in default settings
 -collaborator-server
 Start Burp in Collaborator server mode
 -collaborator-config
 Specify Collaborator server configuration file; defaults to collaborator.config
 -host Set target host
 -project-file Open the specified project file; this will be created as a new project if the file does not exist
 -extension-class-name
 Set extension class name for the specified project
 -config-file Load the specified project configuration file(s); this option may be repeated to load multiple files
 -user-config-file
 Load the specified user configuration file(s); this option may be repeated to load multiple files
 -auto Auto start Burp
 -no-pause-spider-and-scanner Do not pause the Spider and Scanner when opening an existing project
 -disable-auto-update
 Suppress auto update behavior
[incog@kali1]:~[-]
└─$ sqlmap
[incog@kali1]:~[-]
└─$ curl https://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help
[incog@kali1]:~[-]

```

## 3. Deployed OWASP Juice Shop

- git clone <https://github.com/juice-shop/juice-shop.git>
- cd juice-shop
- npm install
- npm start

## 4. Vulnerability Scanning & Results

- Nmap Scan
  - nmap -sV -p- localhost
    - Found open port 3000 running HTTP service.

```

[incog@lx711:~] $ cd juice-shop
[incog@lx711:~/juice-shop]$ git clone https://github.com/juice-shop/juice-shop.git
Cloning into 'juice-shop'...
remote: Enumerating objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0)
Unpacking objects: 100% (10/10), done.
Checking connectivity... done.
[incog@lx711:~/juice-shop]$ cd juice-shop
[incog@lx711:~/juice-shop]$ npm start
> juice-shop@0.0.0 start
> node build/app
info: Detected Node.js version v20.19.2 (OK)
info: Detected CPU x64 (OK)
info: Compiled CPU x64 (OK)
info: Configuration default validated (OK)
info: Configuration environment initialized (OK)
info: Required file server.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file routes.js is present (OK)
info: Required file main.js is present (OK)
info: Required file index.html is present (OK)
info: Required file package.json is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Checking training sets botnefault/trainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
[incog@lx711:~/juice-shop]$ nmap -sV -p- localhost
[incog@lx711:~/juice-shop]$ python3 sqlmap --version
1.9.6.0stable
[incog@lx711:~/juice-shop]$ curl https://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tamper or --dependencies). Use -h for basic and -hh for advanced help
[incog@lx711:~/juice-shop]$ ls
CODE_OF_CONDUCT.md CREDITS.md Dockerfile fts lib logs node_modules REFERENCES.md screenshots SOLUTIONS.md threat-model.json vagrant
CONTRIBUTING.md cypress.config.ts Gruntfile.js lib models package.json routes SECURITY.md tconfig.json views
config crowdin.yaml docker-compose.test.yml frontend LICENSE monitoring README.md rsm server.ts test
config.schema.yaml docker-compose.yml Hall_of_Fame.md
[incog@lx711:~/juice-shop]$
```

## 5. Nikto Web Vulnerability Scan

- nikto -h <http://localhost:3000>
  - Identified missing security headers.
  - Found potentially sensitive .tar, .zip, and .cert backup files.

## 6. SQLMap Injection Testing

- sqlmap -u "http://localhost:3000/?id=1" --batch --risk=3 --level=5
    - Extensively tested multiple injection techniques across:
      - MySQL, PostgreSQL, Oracle, MSSQL, SQLite, Firebird, ClickHouse, SAP MaxDB and more.
    - Ultimately determined:
      - [CRITICAL] all tested parameters do not appear to be injectable

```
[12:44:58] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
[12:44:58] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
[12:44:58] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
[12:44:58] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
[12:44:59] [INFO] testing 'HSQLDB 3 > 1.7.2 AND time-based blind (heavy query - comment)'
[12:44:59] [INFO] testing 'HSQLDB 3 > 1.7.2 AND time-based blind (heavy query - comment)'
[12:44:59] [INFO] testing 'HSQLDB 3 > 1.7.2 AND time-based blind (heavy query - comment)'
[12:44:59] [INFO] testing 'HSQLDB 3 > 1.7.2 AND time-based blind (heavy query - comment)'
[12:44:59] [INFO] testing 'HSQLDB 2 > 2.0 time-based blind (heavy query)'
[12:45:01] [INFO] testing 'HSQLDB 2 > 2.0 OR time-based blind (heavy query)'
[12:45:01] [INFO] testing 'HSQLDB 2 > 2.0 AND time-based blind (heavy query - comment)'
[12:45:01] [INFO] testing 'HSQLDB 2 > 2.0 OR time-based blind (heavy query - comment)'
[12:45:01] [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
[12:45:01] [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
[12:45:01] [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
[12:45:01] [INFO] testing 'ClickHouse AND time-based blind (heavy query)'
[12:45:01] [INFO] testing 'ClickHouse OR time-based blind (heavy query)'
[12:45:01] [INFO] testing 'MySQL > 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[12:45:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (subtraction)'
[12:45:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[12:45:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
[12:45:01] [INFO] testing 'MySQL time-based blind - Parameter replace (iEEt)'
[12:45:01] [INFO] testing 'MySQL time-based blind - Parameter replace (MVAE_SET)'
[12:45:01] [INFO] testing 'MySQL time-based blind - Parameter replace (null place)'
[12:45:01] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
[12:45:01] [INFO] testing 'Oracle time-based blind - Parameter replace (OMBS_LOCK_SLEEP)'
[12:45:01] [INFO] testing 'Oracle time-based blind - Parameter replace (PIPE.RECEIVE_MESSAGE)'
[12:45:01] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'SQLite > 7.0 time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'HSQLDB 3 > 1.7.2 time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'HSQLDB 3 > 1.7.2 time-based blind - ORDER BY clause (heavy query)'
[12:45:01] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[12:45:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[12:45:01] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[12:45:01] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[12:45:01] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
[12:45:01] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (OMBS_LOCK_SLEEP)'
[12:45:01] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (PIPE.RECEIVE_MESSAGE)'
[12:45:01] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[12:45:01] [INFO] testing 'HSQLDB 3 > 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[12:45:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[12:45:01] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[12:45:01] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[12:45:01] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[12:45:09] [WARNING] parameter 'Host' does not seem to be injectable
[12:45:09] [INFO] testing 'MySQL UNION query parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper-space>comment') and/or switch to random-agent'

[*] ending at 12:45:09 / 2025-07-13/
```

## Vulnerability Summary Table

| Vulnerability                     | Tool   | Description                            | Risk   | Recommendation                      |
|-----------------------------------|--------|----------------------------------------|--------|-------------------------------------|
| Open port 3000 externally exposed | Nmap   | Juice Shop HTTP server running on 3000 | Medium | Use firewall to restrict access     |
| Missing X-Content-Type-Options    | Nikto  | HTTP header not set                    | Low    | Add nosniff header in server config |
| Potential sensitive backups found | Nikto  | .tar, .zip, .cert files present        | High   | Remove or secure backups            |
| Outdated JavaScript dependencies  | npm    | Multiple high/critical CVEs on install | High   | Patch or containerize app           |
| SQL injection attempts safe       | sqlmap | No injection vulnerabilities found     | N/A    | Maintain monitoring                 |

## Recommendations & Next Steps

1. Restrict Juice Shop port 3000 to only trusted IPs.
2. Add secure HTTP headers (X-Content-Type-Options, Strict-Transport-Security, etc.).
3. Remove or properly secure backup/archive files on the web server.

4. Keep Node dependencies up to date to reduce known CVEs.
5. Run regular automated scans (Nikto, sqlmap) and periodic manual reviews (Burp Suite, ZAP).

## Conclusion

Through this cybersecurity project, I successfully demonstrated the process of identifying, analyzing, and mitigating vulnerabilities within a deliberately insecure web application. Beginning with setting up a vulnerable environment using tools like OWASP Juice Shop on a Kali Linux virtual machine, I employed industry standard scanning and testing utilities such as OWASP ZAP and Burp Suite to uncover multiple security flaws. These included issues like broken authentication, sensitive data exposure, and improper input validation.

By systematically documenting each vulnerability and replicating exploits, I not only highlighted the risks they posed but also practiced responsible remediation techniques. I implemented secure coding practices and configuration adjustments to close these security gaps, then re-tested the application to verify the effectiveness of the fixes.

This project underscored the critical importance of proactive security testing and continuous vulnerability management in protecting web applications from real world cyber threats. It also helped solidify my hands-on experience with common attack vectors and defensive measures, reinforcing concepts that are vital in the cybersecurity field.

Ultimately, completing this project enhanced both my technical skill set and my understanding of secure software development lifecycles. It also produced a tangible portfolio piece that illustrates my ability to conduct security assessments, document findings, and implement meaningful improvements to all essential capabilities for roles in cybersecurity analysis and consulting.

## Credits

- [OWASP Juice Shop](#)
- Tools: Nmap, Nikto, sqlmap, OWASP ZAP, Burp Suite
- *Chatgpt*, chatgpt.com/. Accessed 13 July 2025.