Security Assessment & VAPT — Comprehensive Report

Project / Lab: Security Assessment (Vulnerability Assessment & Penetration Testing)

Prepared for: Cyart Tech

Prepared by: Arabi Basnet

Date: 2025-11-11

Environment: Kali Linux (attacker), Metasploitable3 (target), VirtualBox

1. Executive Summary

Summarize the engagement in 3–6 sentences:

- Scope: Internal network testing of Metasploitable3 VM (IP: 10.0.2.15), host-only network; web services, SSH, FTP, and custom services tested.
- Approach: Vulnerability scanning (OpenVAS, Nikto), discovery (Nmap), exploitation (Metasploit), and manual verification.
- Key findings: e.g., "3 high CVSS vulnerabilities (outdated Apache/Tomcat, FTP anonymous write), 4 medium, 2 low."
- Risk posture: Overall rating (High / Medium / Low) and recommended next steps: patching, configuration hardening, remove test services.

2. Objectives & Scope

Objective: Evaluate system security using open-source tools, identify and prioritise vulnerabilities, and produce remediation guidance.

Scope: IP ranges, specific VMs/services in-scope (e.g., 192.168.153.129, ports 21,22,80,8080,3306).

Out of scope: Host OS of the attacker machine, destructive attacks on production, social engineering.

3. Methodology (VAPT Phases)

1. **Planning**
    - Define scope and rules of engagement.
    - Tools used list and versions.
    - Example: Dradis CE for reporting .
2. **Discovery**
    - Passive: Banner grabbing, WHOIS (where applicable).
    - Active: nmap -sC -sV -p- -T4 192.168.153.129 and targeted scans (web, ftp).
3. **Vulnerability Scanning**
    - OpenVAS/GVM: full host scan for CVEs and CVSS.
    - Nikto for web server misconfigurations: nikto.
    - OWASP ZAP for web app dynamic scans (if web app present).

4. **Attack / Exploitation**
    - Verify exploitability with Metasploit where safe and permitted.
    - Keep exploitation limited to non-destructive verification (proof-of-concept).
5. **Post-exploitation & Evidence**
    - Capture non-sensitive proof such as service banners, service versions, and proof files.
6. **Reporting**
    - Produce executive-friendly summary and technical appendix with reproduced commands, screenshots, and CVE/CVSS data.

Security Standards & Compliance

Objective: Align with regulations using resources.

In the realm of regulatory compliance and security standards, three significant frameworks stand out: the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and ISO/IEC 27001. Each of these standards plays a crucial role in protecting data, ensuring privacy, and maintaining the integrity of information systems across various industries.

General Data Protection Regulation (GDPR)

The GDPR is a comprehensive data protection regulation enacted by the European Union (EU) to safeguard the personal data of individuals within the EU and the European Economic Area (EEA). Implemented in May 2018, it replaces the 1995 Data Protection Directive and introduces stringent data protection requirements for organizations operating within or interacting with the EU.

Key principles of the GDPR include:

- **Lawfulness, Fairness, and Transparency:** Data processing must be lawful and transparent to the data subject.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes.
- **Data Minimization:** Only data necessary for the intended purpose should be collected.
- **Accuracy:** Personal data must be accurate and kept up to date.
- **Storage Limitation:** Data should not be retained longer than necessary.

- **Integrity and Confidentiality:** Data must be processed securely to protect against unauthorized access or loss.

The GDPR also mandates the appointment of a Data Protection Officer (DPO) for certain organizations, requires data breach notifications within 72 hours, and grants individuals rights such as data access, rectification, erasure, and portability.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a United States legislation enacted in 1996 to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. It applies to healthcare providers, health plans, healthcare clearinghouses, and business associates of these entities.

HIPAA comprises several rules, including:

- **Privacy Rule:** Establishes national standards for the protection of individually identifiable health information.
- **Security Rule:** Sets standards for securing electronic protected health information (ePHI).
- **Breach Notification Rule:** Requires covered entities to notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media of a breach of unsecured PHI.
- **Enforcement Rule:** Provides standards for the enforcement of all the Administrative Simplification Rules.

Compliance with HIPAA involves implementing administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

ISO/IEC 27001

ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.

The standard is based on a risk management process and includes requirements for:

- **Information Security Policies:** Establishing policies and objectives for information security.
- **Risk Assessment and Treatment:** Identifying risks and implementing measures to mitigate them.

- **Leadership and Commitment:** Top management must demonstrate leadership and commitment to the ISMS.
- **Support and Operation:** Providing the necessary resources and ensuring the ISMS is effectively implemented and maintained.
- **Performance Evaluation:** Monitoring and measuring the effectiveness of the ISMS.
- **Improvement:** Continuously improving the ISMS by addressing non-conformities and implementing corrective actions.

ISO/IEC 27001 certification demonstrates an organization's commitment to information security and provides assurance to customers and stakeholders that security best practices are being followed.

(References: Overview of GDPR, HIPAA, and ISO 27001 : Course Cloud Security Fundamentals: Protecting Data in the Cloud | Cursa)

Lab Title: Risk Assessment Basics

Objective:

Prioritize identified vulnerabilities by calculating their severity and categorizing them into risk levels.

Explanation:

1. CVSS Calculator (Common Vulnerability Scoring System):

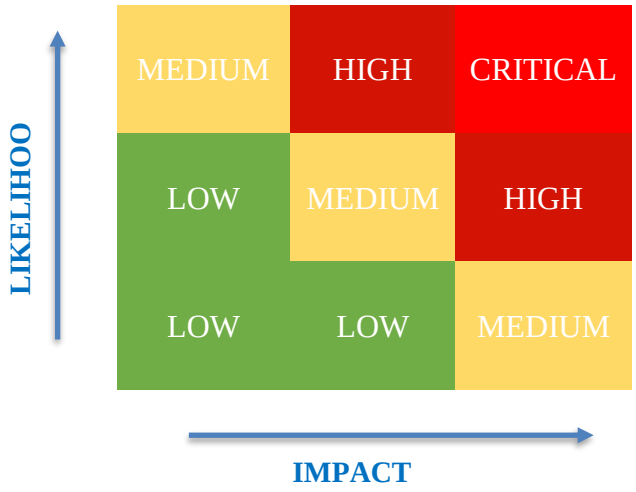
- **Purpose:** The CVSS calculator helps assign a standardized numerical score (from **0.0 to 10.0**) to each vulnerability, indicating how severe it is.
- **Tool:** Use the official **NVD CVSS Calculator** (available at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).
- **Process:**
    1. Identify the vulnerability (for example, from Nmap or Nessus scan results).
    2. Open the CVSS calculator and fill in metrics such as:
        - **Attack Vector (AV)** – Network, Adjacent, Local, or Physical
        - **Attack Complexity (AC)** – Low or High
        - **Privileges Required (PR)** – None, Low, or High
        - **User Interaction (UI)** – Required or None
        - **Confidentiality, Integrity, and Availability Impact (CIA)** – None, Low, or High

3. The calculator generates a **CVSS Base Score**, typically classified as:
    - **0.0–3.9 → Low**
    - **4.0–6.9 → Medium**
    - **7.0–8.9 → High**
    - **9.0–10.0 → Critical**

2. Risk Matrix (Spreadsheet-Based Risk Categorization):

- **Purpose:** Helps visualize and prioritize risks based on their **likelihood** and **impact**.
- **Tool:** Create a matrix in **Google Sheets** or **Microsoft Excel**.
- **Process:**
    1. Define two axes:
        - **Likelihood (Low, Medium, High)**
        - **Impact (Low, Medium, High)**
    2. Assign each vulnerability to a cell in the matrix according to its **CVSS score** or expert judgment.
    3. Use color coding for quick visualization:
        - **Red → High Risk**
        - **Yellow → Medium Risk**
        - **Green → Low Risk**
    4. Document each vulnerability's:
        - Description
        - CVSS Score
        - Risk Level (High/Medium/Low)
        - Recommended Mitigation

Risk Matrix


MEDIUM
HIGH
CRITICAL
LOW
MEDIUM
HIGH
LOW
LOW
MEDIUM
LIKELIHOO
IMPACT

Common Vulnerabilities

Objective: Identify flaws in labs/tools.

1) Network Vulnerabilities — Misconfigurations & Open Ports

What / Why: Unnecessary open ports, weak/default service configs, or exposed admin interfaces let attackers enumerate and exploit services.

How to I detect

- Full TCP port and service scan (fast):
  `nmap -sS -sV -p- --min-rate 500 192.168.153.129 -oA scans/target-allports`
- Quick top-ports + service detection:
  `nmap -sV -p21,22,23,25,80,139,445,3306,8080 192.168.153.129`
- Identify common misconfigurations with NSE scripts:
  `nmap --script vuln,default 192.168.153.129 -oN scans/nse-vuln.txt`

What to look for

- Open/unused ports (e.g., telnet/ftp/samba/mysql exposed).
- Services with banners showing old versions.
- Anonymous FTP writable directories (ftp-anon NSE).
- SMB with guest access or insecure shares.

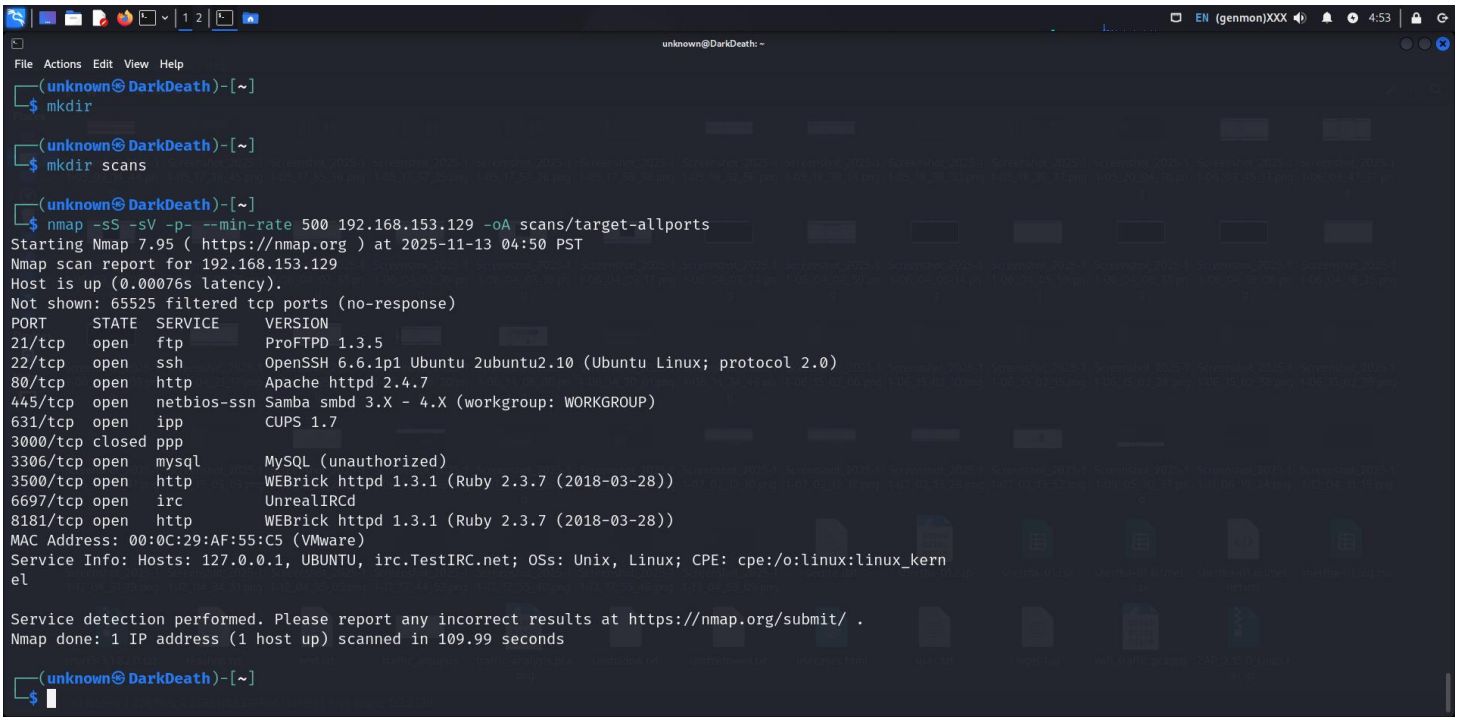
Non-destructive tests

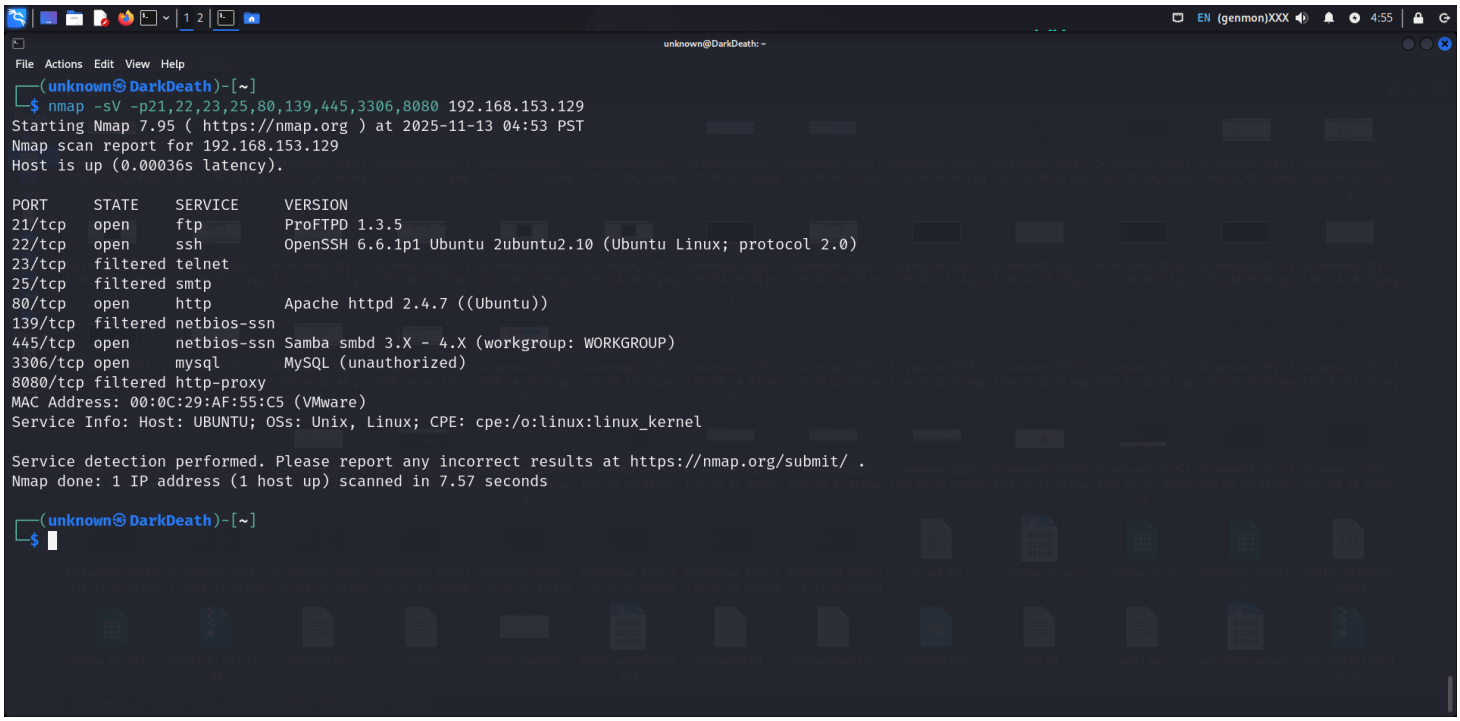
- Check ftp anon: `nmap --script ftp-anon -p21 192.168.153.129`
- Check SMB: `smbclient -L //192.168.153.129 -N (lists shares)`

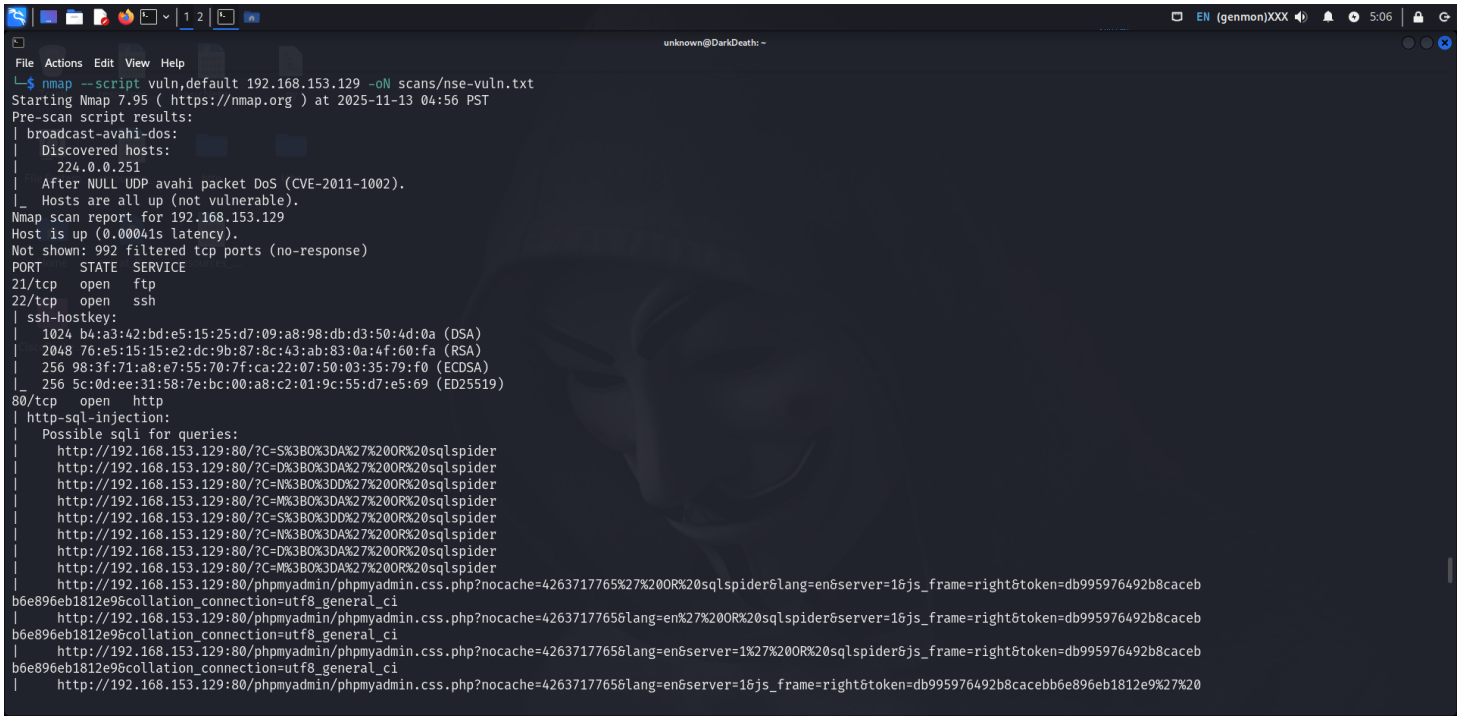
Remediation

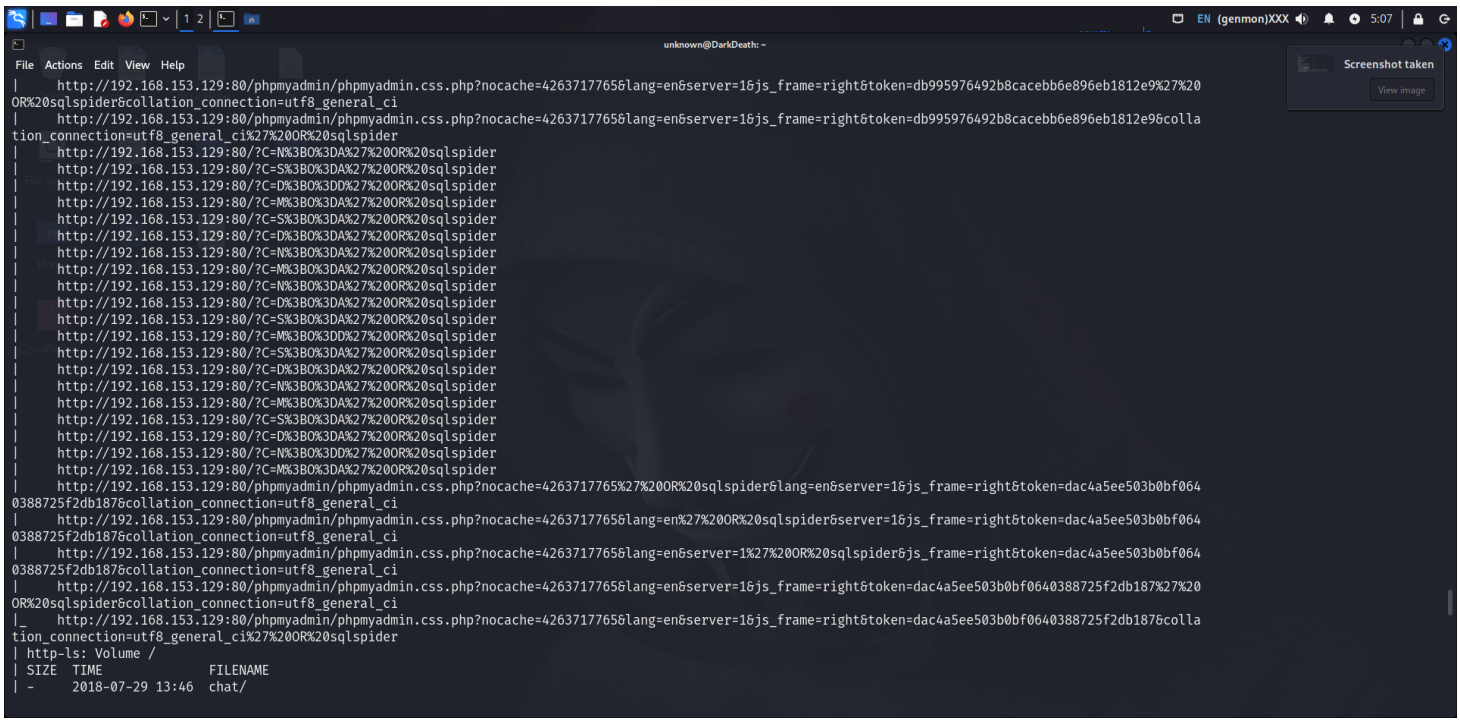
- Close unused ports; disable unnecessary services.
- Apply vendor patches and update packages.
- Restrict admin interfaces to management network or IP ACLs.
- Use firewall rules (iptables/nftables) to limit access.

Appendix

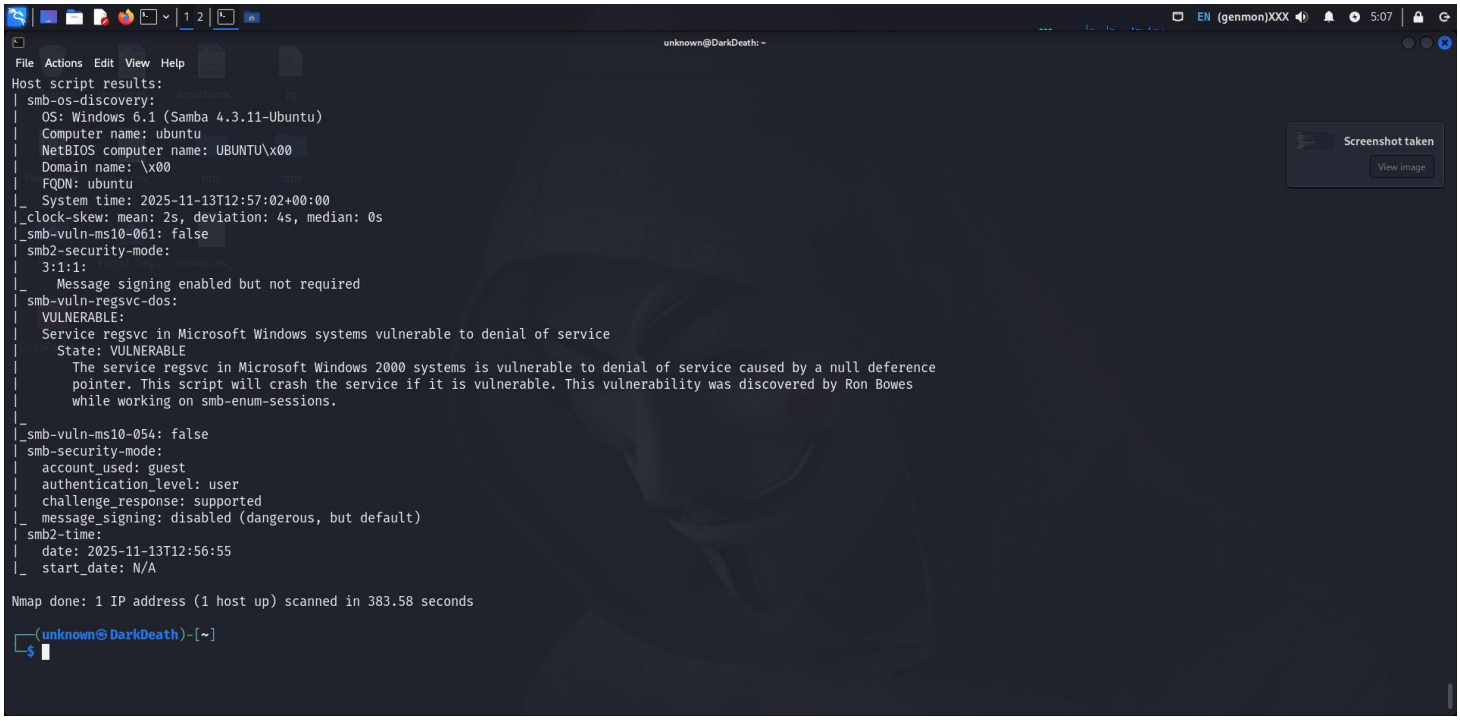

unknown@DarkDeath: ~
File Actions Edit View Help
(unknown㉿DarkDeath)-[~]
$ mkdir
(unknown㉿DarkDeath)-[~]
$ mkdir scans
(unknown㉿DarkDeath)-[~]
$ nmap -sS -sV -p- --min-rate 500 192.168.153.129 -oA scans/target-allports
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 04:50 PST
Nmap scan report for 192.168.153.129
Host is up (0.00076s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
3500/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
6697/tcp open irc UnrealIRCd
8181/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
MAC Address: 00:0C:29:AF:55:C5 (VMware)
Service Info: Hosts: 127.0.0.1, UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kern
el
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.99 seconds
(unknown㉿DarkDeath)-[~]
$


unknown@DarkDeath: ~
File Actions Edit View Help
(unknown㉿DarkDeath)-[~]
$ nmap -sV -p21,22,23,25,80,139,445,3306,8080 192.168.153.129
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 04:53 PST
Nmap scan report for 192.168.153.129
Host is up (0.00036s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
23/tcp filtered telnet
25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
139/tcp filtered netbios-ssn
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open mysql MySQL (unauthorized)
8080/tcp filtered http-proxy
MAC Address: 00:0C:29:AF:55:C5 (VMware)
Service Info: Host: UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
(unknown㉿DarkDeath)-[~]
$


unknown@DarkDeath: ~
File Actions Edit View Help
└─$ nmap --script vuln,default 192.168.153.129 -oN scans/nse-vuln.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 04:56 PST
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.251
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.153.129
Host is up (0.00041s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
| ssh-hostkey:
| 1024 b4:a3:42:bd:e5:15:25:d7:09:a8:98:db:d3:50:4d:0a (DSA)
| 2048 76:e5:15:15:e2:dc:9b:87:8c:43:ab:83:0a:4f:60:fa (RSA)
| 256 98:3f:71:a8:e7:55:70:7f:ca:22:07:50:03:35:79:f0 (ECDSA)
|_ 256 5c:0d:ee:31:58:7e:bc:00:a8:c2:01:9c:55:d7:e5:69 (ED25519)
80/tcp open http
| http-sql-injection:
| Possible sqli for queries:
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DD%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=4263717765%27%20OR%20sqlspider&lang=en&server=1&js_frame=right&token=db995976492b8caceb
b6e896eb1812e9&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en%27%20OR%20sqlspider&server=1&js_frame=right&token=db995976492b8caceb
b6e896eb1812e9&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1%27%20OR%20sqlspider&js_frame=right&token=db995976492b8caceb
b6e896eb1812e9&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1&js_frame=right&token=db995976492b8cacebb6e896eb1812e9%27%20


unknown@DarkDeath: ~
File Actions Edit View Help
Screenshot taken
View image
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1&js_frame=right&token=db995976492b8cacebb6e896eb1812e9%27%20
OR%20sqlspider&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1&js_frame=right&token=db995976492b8cacebb6e896eb1812e9&colla
tion_connection=utf8_general_ci%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DD%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DD%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.153.129:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=4263717765%27%20OR%20sqlspider&lang=en&server=1&js_frame=right&token=dac4a5ee503b0bf064
0388725f2db187&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en%27%20OR%20sqlspider&server=1&js_frame=right&token=dac4a5ee503b0bf064
0388725f2db187&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1%27%20OR%20sqlspider&js_frame=right&token=dac4a5ee503b0bf064
0388725f2db187&collation_connection=utf8_general_ci
| http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1&js_frame=right&token=dac4a5ee503b0bf0640388725f2db187%27%20
OR%20sqlspider&collation_connection=utf8_general_ci
|_ http://192.168.153.129:80/phpmyadmin/phpmyadmin.css.php?nocache=42637177658lang=en&server=1&js_frame=right&token=dac4a5ee503b0bf0640388725f2db187&colla
tion_connection=utf8_general_ci%27%20OR%20sqlspider
| http-ls: Volume /
| SIZE TIME FILENAME
| - 2018-07-29 13:46 chat/


unknown@DarkDeath: ~
File Actions Edit View Help
Disclosure date: 2009-09-17
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http://ha.ckers.org/slowloris/
http-enum:
/: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
/phpmyadmin/: phpMyAdmin
/uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
445/tcp open microsoft-ds
631/tcp open ipp
http-robots.txt: 1 disallowed entry
/
ssl-date: 2025-11-13T12:57:16+00:00; 0s from scanner time.
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and hold
them open as long as possible. It accomplishes this by opening connections to
the target web server and sending a partial request. By doing so, it starves
the http server's resources causing Denial Of Service.
Disclosure date: 2009-09-17
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http://ha.ckers.org/slowloris/
ssl-cert: Subject: commonName=ubuntu
Not valid before: 2018-07-29T13:37:47
Not valid after: 2028-07-26T13:37:47
http-methods:
Potentially risky methods: PUT
http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open mysql
8181/tcp open intermapper
Screenshot taken
View image


unknown@DarkDeath: ~
File Actions Edit View Help
Host script results:
smb-os-discovery:
OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
Computer name: ubuntu
NetBIOS computer name: UBUNTU\x00
Domain name: \x00
FQDN: ubuntu
System time: 2025-11-13T12:57:02+00:00
clock-skew: mean: 2s, deviation: 4s, median: 0s
smb-vuln-ms10-061: false
smb2-security-mode:
3:1:1:
Message signing enabled but not required
smb-vuln-regsvc-dos:
VULNERABLE:
Service regsvc in Microsoft Windows systems vulnerable to denial of service
State: VULNERABLE
The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
while working on smb-enum-sessions.
smb-vuln-ms10-054: false
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)
smb2-time:
date: 2025-11-13T12:56:55
start_date: N/A
Nmap done: 1 IP address (1 host up) scanned in 383.58 seconds
(unknown㉿DarkDeath)-[~]
$
Screenshot taken
View image


unknown@DarkDeath: ~
File Actions Edit View Help
(unknown㉿DarkDeath)-[~]
$ nmap --script ftp-anon -p21 192.168.153.129
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 05:21 PST
Nmap scan report for 192.168.153.129
Host is up (0.00053s latency).
PORT STATE SERVICE
21/tcp open ftp
MAC Address: 00:0C:29:AF:55:C5 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
(unknown㉿DarkDeath)-[~]
$

2) Web Vulnerabilities — SQL Injection (SQLi)

What / Why: Unsanitized inputs allow attackers to inject SQL that the app runs — can exfiltrate, modify, or destroy data.

OWASP Juice Shop as docker

http://192.168.153.135:3000/#/login

How to detect

Try to input `' or 1=1--` as email and . as password

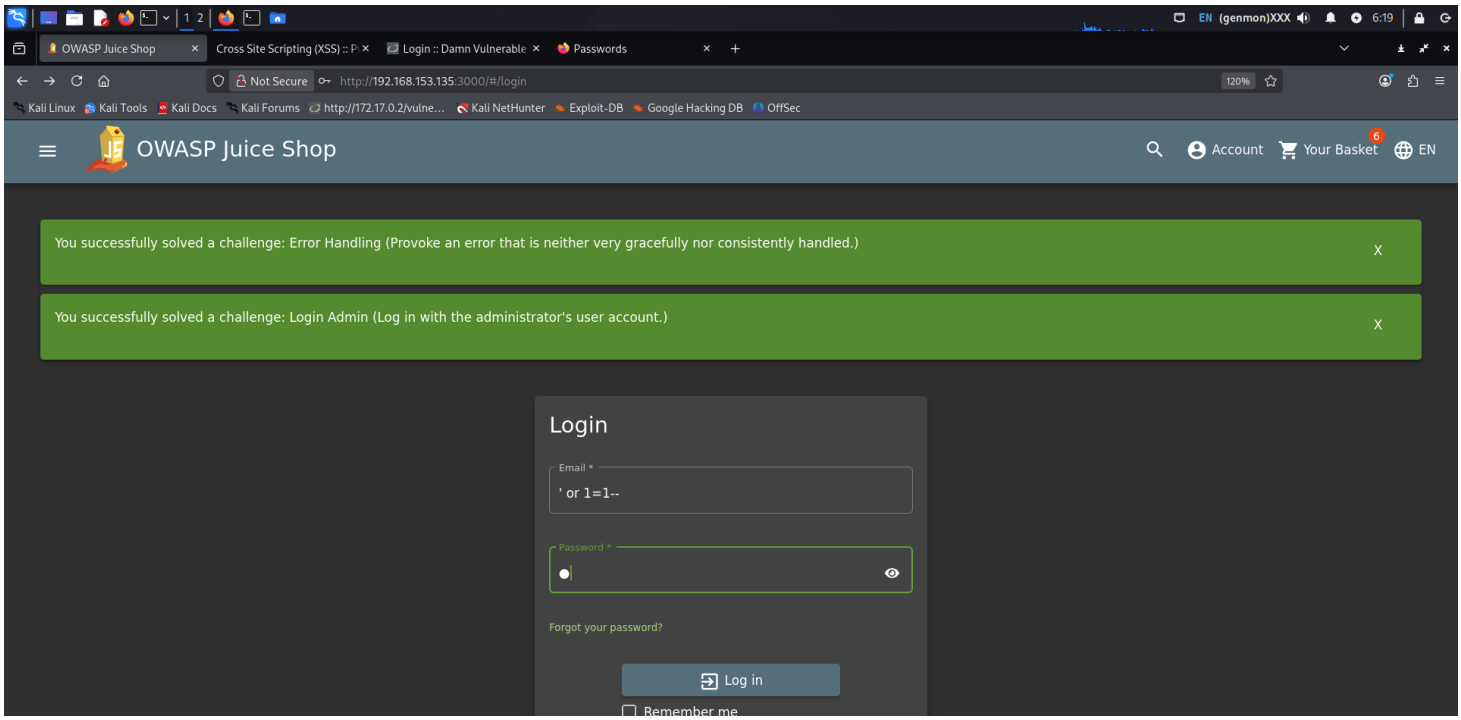
Result:

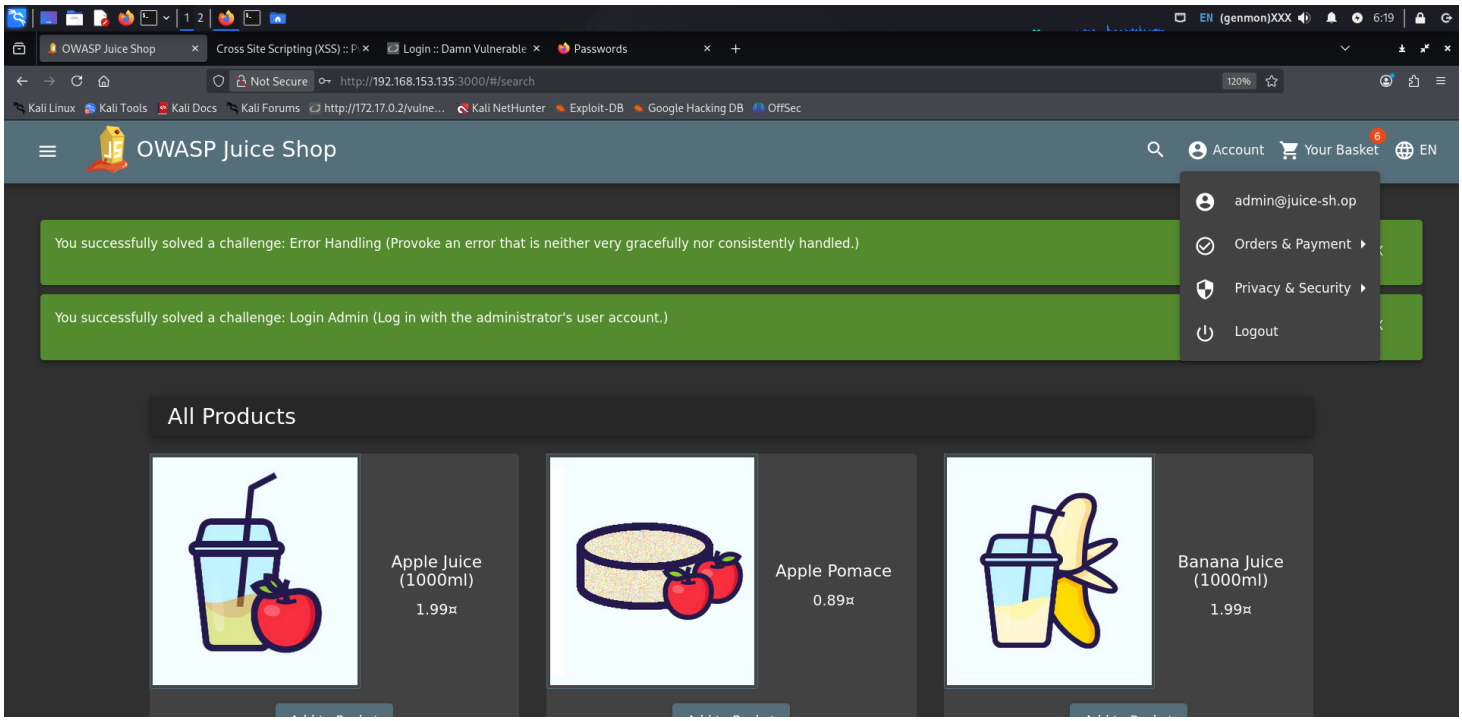
I have successfully entered to the admin user.

Remediation

- Use parameterized queries / prepared statements.
- Enforce least privilege on DB accounts.
- Input validation & output encoding.
- Web Application Firewall (WAF) as an additional layer.

Appendix




OWASP Juice Shop
Cross Site Scripting (XSS) :: P
Login :: Damn Vulnerable
Passwords
Not Secure
http://192.168.153.135:3000/#/search
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤

Web Vulnerabilities — Cross-Site Scripting (XSS)

What / Why: App reflects attacker-provided JavaScript back to other users. Can steal cookies, session tokens, or perform actions.

How to detect

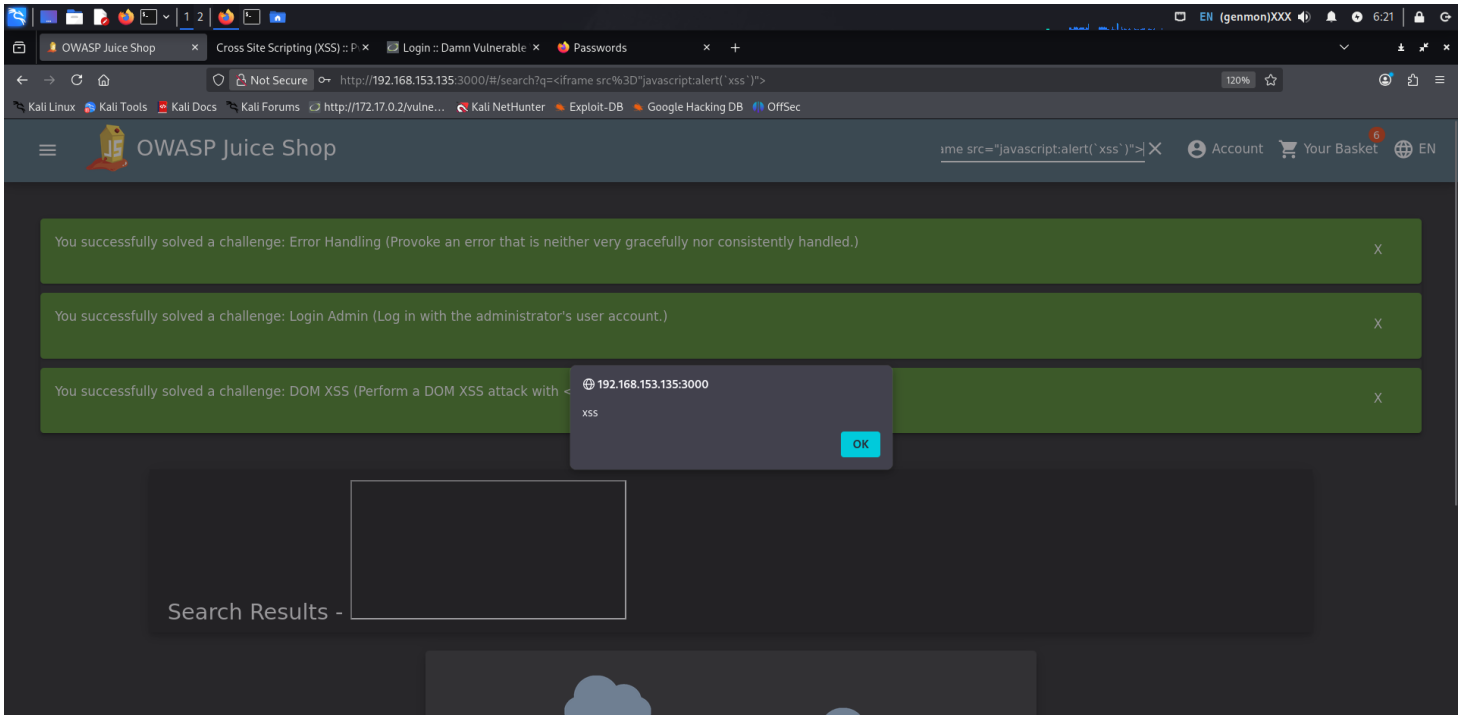
- Manual payloads (reflective XSS quick check):
  Enter `<iframe src="javascript:alert(`xss`)">` into input fields and observe whether the script executes.
- Another one

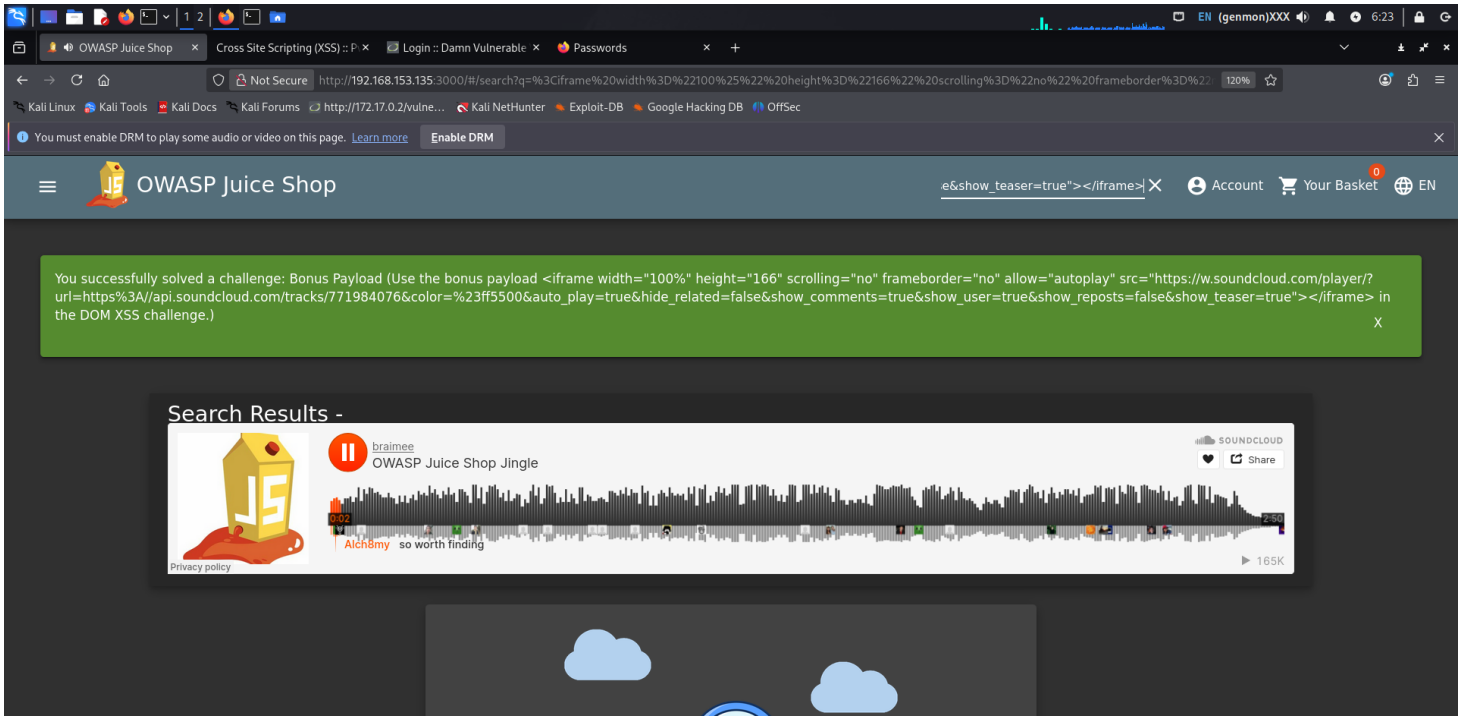
```
<iframe width="100%" height="166" scrolling="no"
frameborder="no" allow="autoplay"
src="https://w.soundcloud.com/player/?url=https%3A//api.s
oundcloud.com/tracks/771984076&color=%23ff5500&auto_play=
true&hide_related=false&show_comments=true&show_user=true
&show_reposts=false&show_teaser=true"></iframe>
```

Remediation

- Escape/encode user output (HTML entity encode).
- Use Content Security Policy (CSP) to reduce impact.
- Validate and sanitize input on server-side (never rely only on client-side).

Appendix




OWASP Juice Shop
Cross Site Scripting (XSS) :: P
Login :: Damn Vulnerable
Passwords
Not Secure
http://192.168.153.135:3000/#/search?q=%3Ciframe%20width%3D%22100%25%22%20height%3D%22166%22%20scrolling%3D%22no%22%20frameborder%3D%22
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
You must enable DRM to play some audio or video on this page.
Learn more
Enable DRM
OWASP Juice Shop
e&show_teaser=true"></iframe>
Account
Your Basket
EN
You successfully solved a challenge: Bonus Payload (Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe> in the DOM XSS challenge.)
Search Results -
braimee
OWASP Juice Shop Jingle
SOUNDCLOUD
Share
0:02
2:50
Alch8my
so worth finding
Privacy policy
165K

6. Documentation Fundamentals

Objective:

- Learn how to create professional and structured reports for security assessments using available tools.

Explanation:

Documentation is a critical part of security testing. It ensures that all findings are clearly recorded, organized, and communicated to stakeholders or clients. Well-documented reports improve clarity, reduce errors, and help in remediation planning.

Tools:

1. Dradis CE (Community Edition)
    - Purpose: Collaborative reporting and evidence management for penetration tests.
    - Key Features:
        - Team collaboration on findings.
        - Centralized storage for screenshots, logs, and notes.
        - Built-in report templates for PDF, Word, or HTML outputs.
    - Learning Tip: Start with free templates from GitHub or the Dradis CE documentation to create sample reports.
2. CherryTree
    - Purpose: Hierarchical note-taking tool for technical findings.
    - Key Features:
        - Organize notes with headings, sub-headings, and tables.
        - Attach screenshots, code snippets, or evidence.
        - Export notes in various formats for reporting.
3. Other Standard Tools:
    - Microsoft Word, LibreOffice Writer, or Markdown editors can also be used for creating structured reports.
    - Templates for pentest reports are widely available online.