# MRSEC

# NBN Corp

## Security Assessment Findings Report

**Business Confidential**

**Date:** May 11th, 2024
**Project:** NBN-001
**Version:** 1.0

## Confidentiality Statement

This document is the exclusive property of NBN Corp and MRSEC.
This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both NBN Corp and MRSEC.
NBN Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

## Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.
Time-limited engagements do not allow for a full evaluation of all security controls. MRSEC prioritized the assessment to identify the weakest security controls an attacker would exploit. MRSEC recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## Contact Information

| Name | Title | Contact Information |
|---|---|---|
| Bill Gibson | CISO, NBN Corp | bgibson@nbncorp.com |
| Mayank Ramnani | Lead Pentester, MRSEC | hi@mayankramnani.com |

# Executive Summary

NBN Corp, the preeminent media conglomerate globally, faces substantial security vulnerabilities throughout its network infrastructure. Our penetration test uncovered critical issues within both server and client systems, presenting severe risks to data confidentiality, integrity, and availability. These vulnerabilities, if left unaddressed, could result in data breaches, service disruptions, and reputational harm, underscoring the urgent need for comprehensive remediation measures.

The assessment revealed systemic weaknesses in NBN Corp's security posture, including inadequate access controls, insecure authentication mechanisms, and susceptibility to various exploitation techniques such as SQL injection, Local File Inclusion, and buffer overflows. With data privacy concerns mounting and regulatory scrutiny intensifying, NBN Corp must prioritize remediation efforts to fortify its defenses and safeguard against potential cyber threats. By addressing these vulnerabilities proactively, NBN Corp can enhance resilience, foster customer trust, and uphold its position as a leader in the media industry.

**Client Security Rating:** High Risk

# Introduction

The penetration test conducted for NBN Corp was aimed at evaluating the resilience of its network infrastructure against potential cyber threats and identifying vulnerabilities that could compromise the confidentiality, integrity, and availability of critical assets. With the overarching goal of enhancing NBN Corp's security posture, the test encompassed a comprehensive assessment of both server and client systems, utilizing a combination of automated tools and manual techniques to simulate real-world attack scenarios. By emulating the tactics, techniques, and procedures (TTPs) commonly employed by malicious actors, the test sought to provide actionable insights into the organization's security strengths and weaknesses.

Prior to commencing the penetration test, clear rules of engagement were established to delineate the scope, objectives, and constraints of the assessment. These rules outlined the permissible actions, targets, and testing methodologies, while also specifying points of contact (POCs), timelines, and reporting mechanisms.
The scope of the test encompassed two machine images within NBN Corp's network: the `nbnserver` and `nbnclient`, each representing critical components of the organization's infrastructure. The timeline for the assessment was structured to accommodate thorough testing without causing disruptions to ongoing operations, ensuring minimal impact on business continuity.

Throughout the assessment, several major flaws were unearthed within NBN Corp's network infrastructure, highlighting systemic vulnerabilities that pose significant risks to data security and operational resilience. Immediate actions and fixes were identified to address these flaws, including **patching known vulnerabilities, implementing secure authentication mechanisms, and fortifying access controls.** The overall security rating assigned to the client reflects the severity of these vulnerabilities and underscores the urgent need for remediation efforts to mitigate risks effectively. By prioritizing cybersecurity initiatives and implementing proactive measures, NBN Corp can enhance its security posture, bolster defenses, and safeguard against emerging threats.

### Scope

| Owner | Machine Name | Interfaces |
|---|---|---|
| NBN Corp | nbnserver | eth0: 10.10.0.66<br>eth1: 172.16.1.1 |
| NBN Corp | nbnclient | eth0: 172.16.1.2 |

### Scope Exclusions

Per client request, MRSEC did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by NBN Corp.

### Client Allowances

NBN Corp provided MRSEC the following allowances:

- Network access to `172.168.1.1` and `172.168.1.2` machines

## Methodology

### Overview

From May 1st, 2024 to May 11th, 2024, NBN Corp engaged MRSEC to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test.

All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

### Assessment Components

External Penetration Test: An external penetration test emulates the role of an attacker from outside the network. An engineer will scan the network to identify potential host vulnerabilities and perform

common and advanced external network attacks, along with web application testing on found applications.
The engineer will seek to gain access to hosts through lateral movement, compromise user and root accounts, and exfiltrate sensitive data.

To provide management with an indication as to the significance of the risk involved and the priority with which the same needs to be addressed, all risks have been rated per the classifications given below:

CVSS v3.0 Ratings*

| Severity | Base Score Range |
|---|---|
| None | 0.0 |
| Low | 0.1 – 3.9 |
| Medium | 4.0 – 6.9 |
| High | 7.0 – 8.9 |
| Critical | 9.0 – 10.0 |

*Vulnerability Severity Ratings provided by the National Vulnerability Database (nvd.nist.gov)

The methodology consisted of several high-level steps, each tailored to assess specific aspects of security posture and risk exposure.

**1. Pre-Assessment Preparation:**
- Prior to initiating the test, thorough reconnaissance was conducted to gather information about NBN Corp's system and services.
- Tools such as Nmap were utilized to identify open ports, active services, and potential entry points into the machines.

**2. Web Application Testing:**
- Manual inspection and testing of web applications were conducted to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and directory traversal.
- Tools such as Burp Suite and OWASP ZAP were utilized to intercept and analyze HTTP requests, identify input validation flaws, and assess session management mechanisms.
- Automated tools such as sqlmap were also used to exfiltrate data out of sql injection flaws.

**3. Binary Analysis:**
- Reverse engineering and analysis of binary executables were performed to identify vulnerabilities such as buffer overflows.

- Tools such as Ghidra and Binary Ninja were used to disassemble and analyze binary code, identify potential security flaws, and assess the impact of exploitation.

**4. Risk Assessment and Scoring:**

- Vulnerabilities were categorized based on severity, impact, and exploitability to prioritize remediation efforts.
- A risk matrix was used to assign risk scores to identified vulnerabilities, considering factors such as likelihood of exploitation, potential impact on confidentiality, integrity, and availability, and ease of remediation.

**5. Reporting:**

- Findings were documented in this comprehensive report, detailing identified vulnerabilities, exploitation techniques, and recommended remediation measures.
- Each vulnerability was assigned a risk rating, ranging from low to critical, based on its severity and potential impact on the organization's security posture.

By following this methodology, the penetration test provided valuable insights into NBN Corp's security vulnerabilities, enabling the organization to prioritize remediation efforts and strengthen its defenses against cyber threats.

---

# Findings

1. **FTP Misconfiguration**

   **Discovery**: Identified during initial reconnaissance using Nmap.
   **Exploitation**: An anonymous login allowed access to the home directory of the `gibson` user, exposing sensitive data including Flag3
   **Tools/Methodology**: Nmap for network reconnaissance, manual testing for anonymous login. (See Appendix A1)
   **Importance**: Misconfigured FTP servers can expose sensitive data and provide unauthorized access to system resources.
   **Risk:** High
   **Recommendation**: Disable anonymous login and enforce strong authentication mechanisms such as username/password authentication or SSH/SFTP.

2. **Misconfigured Access Controls for Staging Web Server**

**Discovery**: Found through port recon using Nmap.
**Exploitation:** Broken access controls on staging server led to leakage of backend code (see Appendix A3). Employee login is possible with any username and password.
**Tools/Methodology**: Nmap, Manual testing. (See Appendix A1)
**Importance**: Inadequate access controls can facilitate unauthorized access to sensitive information and compromise application security.
**Risk:** Medium
**Recommendation**: Implement proper access controls to restrict access to the public from staging or development resources.

### 3. Misconfigured Production Web Server

**Discovery**: Found through manual testing.
**Exploitation:** Public access to open directories and php configuration leads to customer data leaks (See Appendix A2, A4)
**Tools/Methodology**: Manual testing.
**Importance**: Inadequate access controls can facilitate unauthorized access to sensitive information and compromise application security.
**Risk:** Medium
**Recommendation**: Implement proper access controls to restrict access to the sensitive resources.

### 4. Local File Inclusion

**Discovery**: Manual testing after printing of customer.list file
**Exploitation**: Exploiting LFI allowed dumping of any file on the server that the www-data user has access to, including `/etc/passwd` file (See Appendix A7). This can also cause remote code execution when paired with Arbitrary File Writes (Finding 5).
**Tools/Methodology**: Manual testing using browser and Burp Suite.
**Importance**: LFI leads to unauthorized file access to the webserver which can leak important data about the application, or cause remote code execution.
**Risk:** High
**Recommendation**: Sanitize user supplied input to make sure directory traversal is not possible.

### 5. Arbitrary File Writes

**Discovery**: Manual testing of web application
**Exploitation**: Exploiting this allowed writing arbitrary data into the `/var/www/html/data/customer.list` file on the server. This can cause remote code execution when paired with Local File Inclusion (Finding 4).
**Tools/Methodology**: Manual testing of the web application - subscribe functionality.
**Importance**: When combined with LFI, can lead to remote code execution. See data at bottom of Appendix A2 for an example.
**Risk**: Medium
**Recommendation**: Sanitize user supplied input before storing it in the file.

## 6. SQL Injection

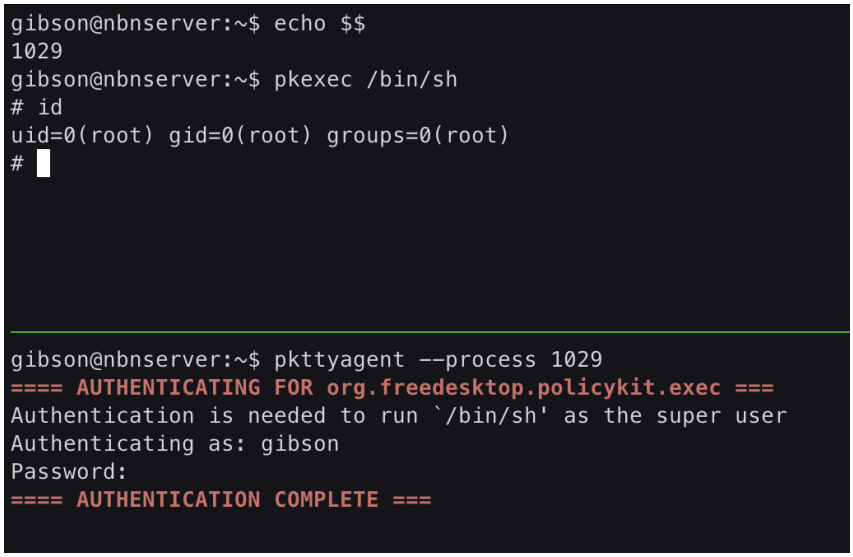
**Discovery**: SQL query errors seen during manual testing of the web application.
**Exploitation**: Exploiting the SQL injection vulnerability allowed dumping of the database, including the users table containing passwords.
**Tools/Methodology**: Manual testing using error log for identifying injection points. SQLMap for dumping databases.
**Importance**: SQL injection can lead to unauthorized access to sensitive data and compromise of user accounts. See Appendix A8.
**Risk**: Critical
**Recommendation**: Implement parameterized queries or use ORM frameworks to prevent SQL injection attacks. Hide error messages like below from users.


## 7. Insecure Password Handling

**Discovery**: Detected during analysis of backend server code.
**Exploitation**: Passwords using MD5 hashing were easily cracked, hashes were obtained from db dump, provided unauthorized access to accounts. See Appendix A8.
**Tools/Methodology**: Manual code review and JohnTheRipper.
**Importance**: Insecure password storage mechanisms facilitate unauthorized access to user accounts.
**Risk:** Low

**Recommendation**: Upgrade to stronger hashing algorithms such as SHA256 or bcrypt for secure password storage.

## 8. Privilege Escalation: Server




**Discovery**: Identified by looking for binaries with suid bit set.

**Exploitation**: Exploiting `pkexec` and the fact that gibson user was present in sudo group allowed gaining of root privileges.

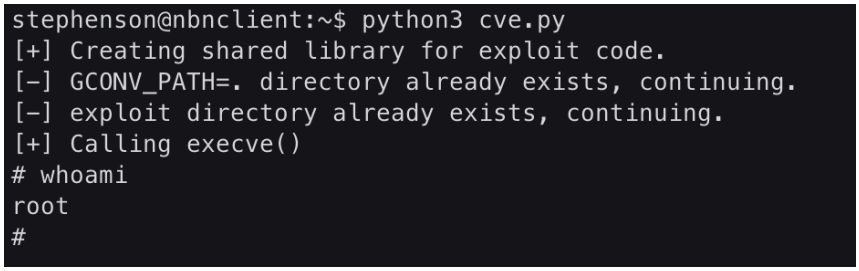
**Tools/Methodology**: Manual Testing + Process Followed

**Importance**: Privilege escalation misconfigurations allow attackers to gain elevated privileges and execute unauthorized commands.

**Risk:** Critical

**Recommendation**: Remove suid bit from `pkexec` and other binaries where it is not essential. Remove unprivileged users from the sudo group.

## 9. Privilege Escalation: Client




**Discovery**: Running `linpeas.sh` gave results about possible vulnerabilities.

**Exploitation**: Exploiting the `CVE-2021-4034` vulnerability allowed privilege escalation to gain root access.

**Tools/Methodology**: linpeas.sh and Manual Testing
**Importance**: Privilege escalation vulnerabilities can enable attackers to gain elevated privileges and execute unauthorized commands.
**Risk:** Critical
**Recommendation**: Apply patches provided by the vendor and limit user privileges to mitigate the risk of privilege escalation attacks.

## 10. Insufficient Protection of Server SSH Private Keys

**Discovery**: Detected during post exploitation and analysis of server configurations.
**Exploitation**: Unprotected SSH private keys could be used for unauthorized access to other services like Github and lateral movement within the network.
**Tools/Methodology**: Manual inspection of server config and files.
**Importance**: Unprotected private keys pose a significant risk for unauthorized access and compromise of sensitive data.
**Risk**: Low
**Recommendation**: Encrypt SSH private keys using passphrases and restrict access to authorized users only. If ssh private keys have passphrases, their header will be different than this.

```
root@nbnserver:~/.ssh# head ~/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAnZuESp+mU6uvOPqdmn7lKJTinylK2aUgdPSWtc9hRiq/9QGy
MGLav53Jp95gZEBVKZk2rgwn6wNJDs+Gno+xJTiox+BOG/r/Ns2qH1TlZZl2zVdu
VQ9Ig/3Obpy93hYB5/Sh9FbvKiO62A8uUH1I1CmfXQPvvm1ICYEYbYEdq24zh5Ny
0hudGdZwtrQr6giCplgAC7E7XCpg8UnHdda3quajHxIGvVzt4GzATPobjIEDNPeg
1bocYsspfxwcA2WECSsm8UeqWspebkmG6bJQ8NkUD78QuEMKzTyCQy2Bz9kR6ov8
GDKiUx1RacnyKwS7GPdaobRAanAXGQyEd7l5vQIDAQABAoIBAQCUIUKpUHvnUAmU
```

## 11. Buffer Overflow in Client Binary - nbn and nbn.backup

**Discovery**: Identified during binary analysis using Ghidra.
**Exploitation**: Buffer overflow vulnerability in the client binary allowed for denial of service attacks and potential remote exploitation. Binary is running over the network as root, which allows for root access to attackers when compromised. See Appendix A5.
**Tools/Methodology**: Binary Ninja for binary analysis, manual testing for crafting exploit payloads. See Appendix A9.
**Importance**: Buffer overflow vulnerabilities can lead to arbitrary code execution and compromise of system integrity.
**Risk**: High

**Recommendation**: Implement bounds checking and input validation to prevent buffer overflow vulnerabilities. Use memory-safe languages to mitigate this risk.
Use lower privileged user accounts to run applications on the network.

## 12. Insufficient Access Controls on Server and Client

**Discovery**: Detected during analysis of configurations.
**Exploitation**: Enabled root login and SSH password authentication, posing risks of unauthorized access and privilege escalation from binary compromise or password leakage.
**Tools/Methodology**: Manual inspection of client configurations.
**Importance**: Inadequate access controls can facilitate unauthorized access to sensitive systems and compromise security.
**Risk**: Low
**Recommendation**: Disable root login and enforce strong authentication mechanisms such as public key authentication to mitigate the risk of unauthorized access.

## 13. Insecure Organizational Password Policies

**Discovery**: Detected after obtaining initial passwords
**Exploitation**: Use of weak passwords allowed easily cracking passwords for both login and root access. Password reuse allowed easy access to new services. See Appendix A6.
**Tools/Methodology**: Manual testing.
**Importance**: Password policies are essential in organizations for enhancing security, ensuring compliance with regulatory standards, mitigating risks associated with unauthorized access, raising user awareness about password hygiene, and enforcing best practices in password management.
**Risk:** Low
**Recommendation**: Force employees to use strong and unique passwords for each service.

## Conclusion

The penetration test conducted on NBN Corp's network infrastructure aimed to assess its resilience against potential cyber threats and identify vulnerabilities that could compromise data security and operational integrity. Through a systematic evaluation of the server and client system, numerous critical issues were uncovered, highlighting systemic weaknesses that require immediate attention and remediation.

The test revealed a multitude of vulnerabilities across the network, ranging from misconfigurations and access control issues to severe exploitation risks such as SQL injection and privilege escalation. These findings underscore the importance of robust security measures to mitigate risks effectively and safeguard critical assets from unauthorized access and exploitation.

Immediate fixes are imperative to address the identified vulnerabilities and strengthen NBN Corp's security posture. Recommendations include disabling anonymous login on the FTP server, implementing proper access controls on staging and production web servers, and upgrading password hashing algorithms and policies to enhance user account security. Additionally, patching known vulnerabilities, limiting user privileges, and encrypting SSH private keys are crucial steps to mitigate the risk of unauthorized access and privilege escalation.

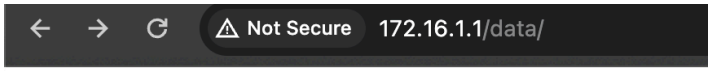
In summary, the penetration test identified significant security gaps within NBN Corp's network infrastructure, emphasizing the need for proactive measures to fortify defenses, mitigate risks, and uphold data confidentiality, integrity, and availability. By prioritizing remediation efforts and implementing recommended fixes, NBN Corp can enhance its security posture, mitigate potential threats, and safeguard against emerging cyber risks.

# APPENDIX A - Ports, Passwords, Configuration

1. Open Ports: **nbnserver**

| Port | Service | Version | Comment |
|---|---|---|---|
| 80 | HTTP | Apache httpd 2.4.29 | Production webserver |
| 8001 | HTTP | Apache httpd 2.4.29 | Likely staging webserver |
| 443 | SSH | OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 | Allows password login |
| 3306 | MySQL | mysqld 10.1.38-MariaDB-0ubuntu0.18.04.1 | MySQL Database Server |
| 65534 | FTP | vsFTPd 3.0.3 | Allows anonymous login, access to **/home/gibson** |

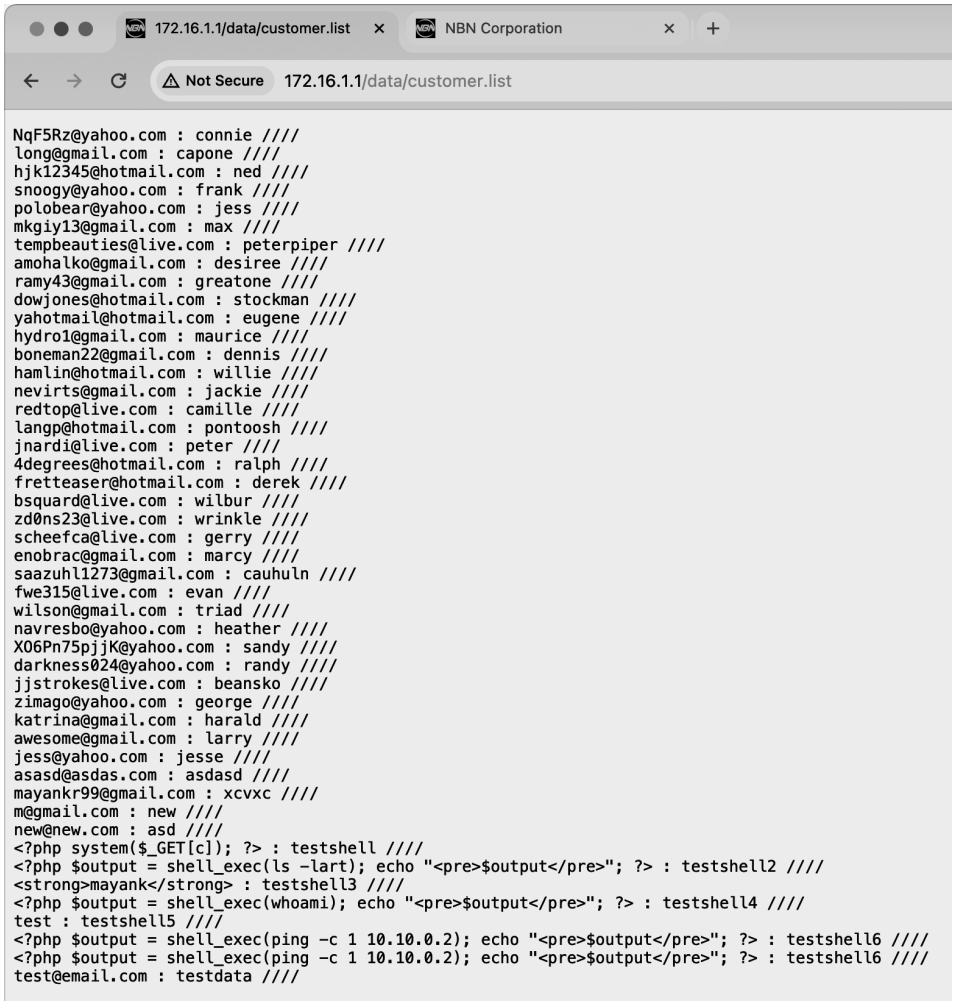
2. Data Leak in Web Server in Open directory: http://172.16.1.1/data/




# Index of /data

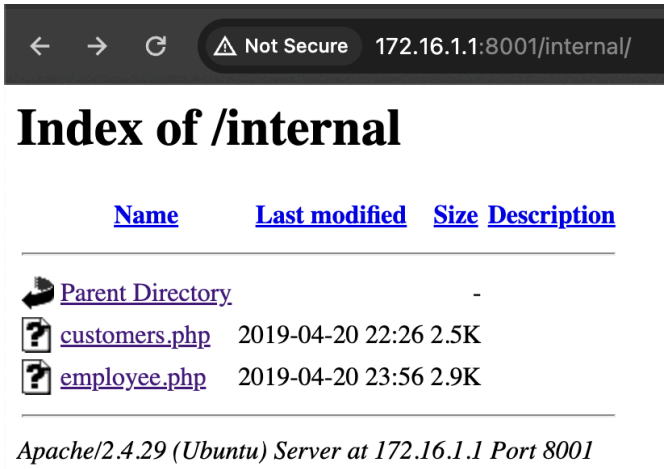
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| CEO_gibson.jpg | 2017-05-11 18:35 | 56K | |
| customer.list | 2024-05-09 00:59 | 1.8K | |
| customerservice.jpg | 2019-04-20 23:49 | 238K | |
| flag1 | 2020-01-14 17:25 | 1.3K | |
| flag4.jpg | 2019-04-20 23:49 | 70K | |
| newtech.jpg | 2019-04-20 23:49 | 180K | |
| ourCEO.jpg | 2019-04-20 23:49 | 201K | |
| servicetechs.jpg | 2019-04-20 23:49 | 171K | |
| stephenson.jpg | 2014-08-30 22:13 | 37K | |

*Apache/2.4.29 (Ubuntu) Server at 172.16.1.1 Port 80*

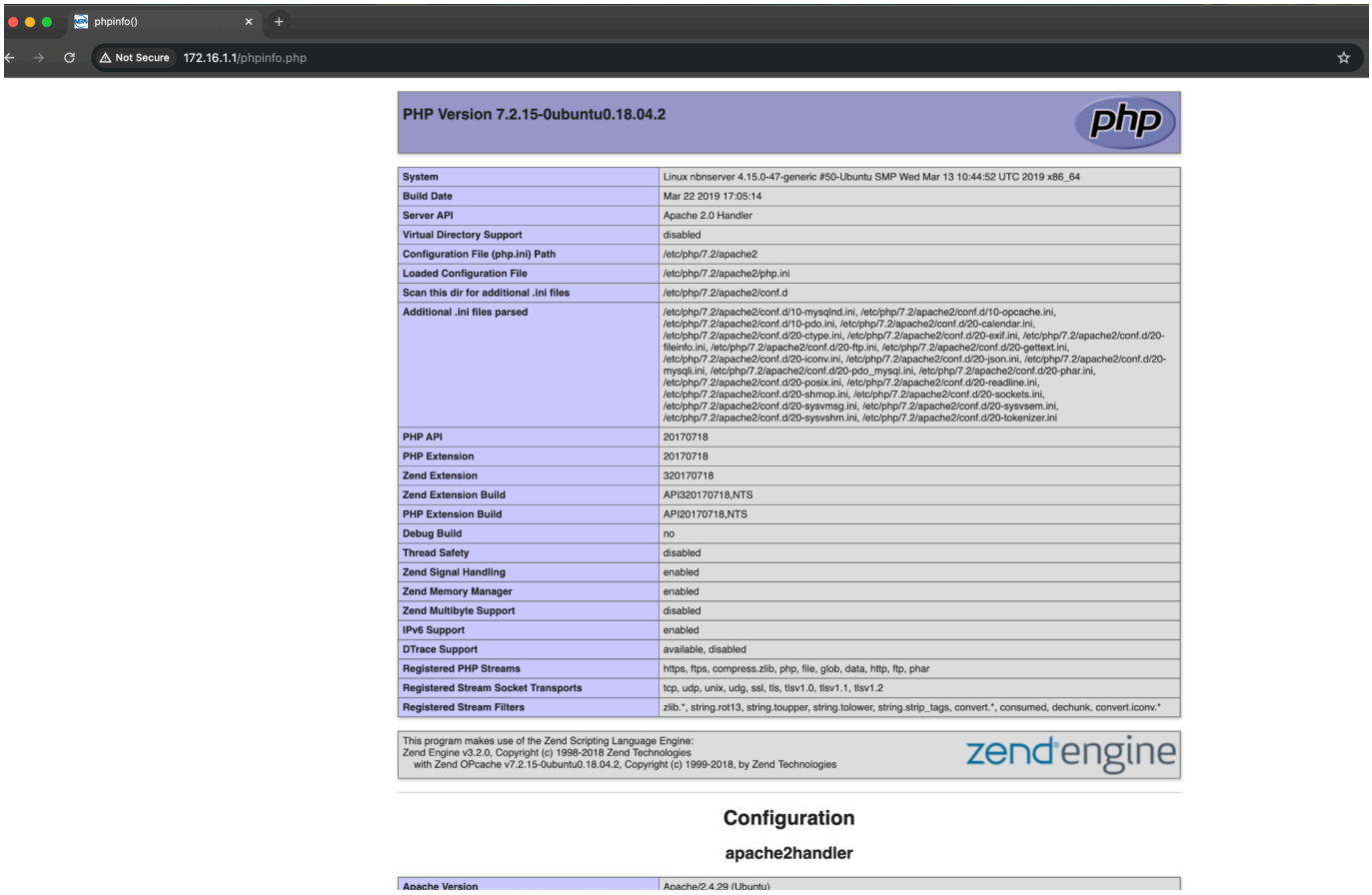



3. Internal Server Code Leak in Staging Server (Port 8081)

   Open directory - http://172.16.1.1:8001/internal/



4. PHP Configuration visible by anyone




5. Notable Open Ports - **nbnclient**

| Port | Service | Version | Comment |
|---|---|---|---|
| 6573 | HTTP | /home/stephenson/nbn | Custom binary for customer management portal |
| 22 | SSH | OpenSSH_7.5p1 Ubuntu-10ubuntu0.1 | Allows password login |

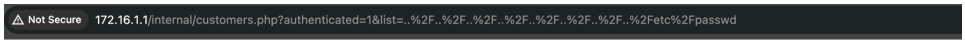
Also other ports open regarding dovecot (mail server), postfix (mail server) and fortune (unix game).

6. Revealed Passwords:

| Username | Password | Source | Service(s) | Comment |
|---|---|---|---|---|
| gibson | digital | SQL Database | Webserver Login, SSH to | Cracked using publicly |

| | | | | |
|---|---|---|---|---|
| | | Dump | server machine | available MD5 databases |
| stephenson | pizzadeliver | SQL Database Dump | Webserver Login, SSH to client machine | Cracked using publicly available MD5 databases |
| root | 1986angeles | /etc/shadow | Server SSH Login | Cracked using JohnTheRipper |
| root | $pacebubble | /etc/shadow | Client SSH Login | Cracked using JohnTheRipper |

7. Dump `/etc/passwd` using LFI




FOR INTERNAL USE ONLY

flag2{down_a_rabbithole}
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin gibson:x:1000:1000:gibson:/home/gibson:/bin/bash
ftp:x:111:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin mysql:x:112:115:MySQL Server,,,:/nonexistent:/bin/false

8. SQLMap Database Dump:

| Hash | Type | Result |
|---|---|---|
| e0e1d64fdac4188f087c4d44060de65e | md5 | digital |
| 942cbb4499d6a60b156f39fcbaacf0ae | md5 | pizzadeliver |

9. Binary exploitation crash register offsets:
   - eip = 118
   - ebx = 110
   - ebp = 114
   - esp point to 122

# Appendix B - Sensitive Data Exposure

1. **Data**: FLAG1{CYBERFELLOWS_GOODLUCK}
   **Details**: Open directory on the nbnserver leading to sensitive file leak.
   **Prevention**: Disallow public access to /data directory or remove the sensitive file.


2. **Data**: `flag2{down_a_rabbithole}`
   **Details**: On logging in as the `stephenson` user, all customer data is visible.
   Even without logging in, cookie 'authenticated=1' can be set in the browser, and on going to http://172.16.1.1/internal/employee.php page, future customer list can be clicked to see the sensitive data.
   **Prevention**: Remove sensitive data from logged in users. Have stricter verification checks about access rather than just setting a cookie.
   http://172.16.1.1/internal/customers.php?list=..%2Fdata%2Fcustomer.list

**Future Customers**

FOR INTERNAL USE ONLY

flag2{down_a_rabbithole}

3. **Data**: `flag3{brilliantly_lit_boulevard}`

   **Details**: In the home directory of `gibson` user, file flag3 present and accessible by any user. FTP is enabled which allows anyone access to this directory.

   **Prevention**: Disallow access to unprivileged users by disallowing ftp anonymous login. Or encrypt the sensitive file in the server.

```
root@nbnserver:/home/gibson# ls -l flag3
-rw-rw-rw- 1 root root 46037 Apr  3  2020 flag3
root@nbnserver:/home/gibson# strings flag3 | grep flag3
The goggles throw a light, smoky haze across his eyes and reflect a distorted wide-angle view of a flag3
{brilliantly_lit_boulevard} that stretches off into an infinite blackness. This boulevard does not reall
y exist, it is a computer-rendered view of an imaginary place.
```

4. **Data**: `flag4{youre_going_places}`

   **Details**: Sensitive data hidden within an xml tag in an image. This is an insufficient way to hide sensitive information.

   **Prevention**: Encrypt the sensitive data with a secure encryption algorithm to store it.

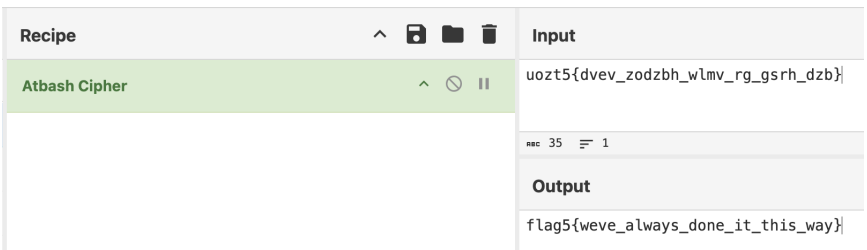
```
root@nbnserver:/var/www/html/data# ls -l flag4.jpg
-r-------- 1 root root 71770 Apr 20  2019 flag4.jpg
root@nbnserver:/var/www/html/data# strings flag4.jpg | grep flag4
<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rd
f:Description flag4="flag4{youre_going_places}" xmlns:MicrosoftPhoto="http://ns.microsoft.com/photo/1.0/
"/></rdf:RDF></x:xmpmeta>
root@nbnserver:/var/www/html/data#
```

5. **Data**: `flag5{weve_always_done_it_this_way}`

   **Details**: On logging in as root to the server, there's mention of a **...** directory in the `lookingforsomething` file. The ... directory contains a lot of ASCII text files, most of which contain garbade data. Sensitive data is found on looking through it programmatically.

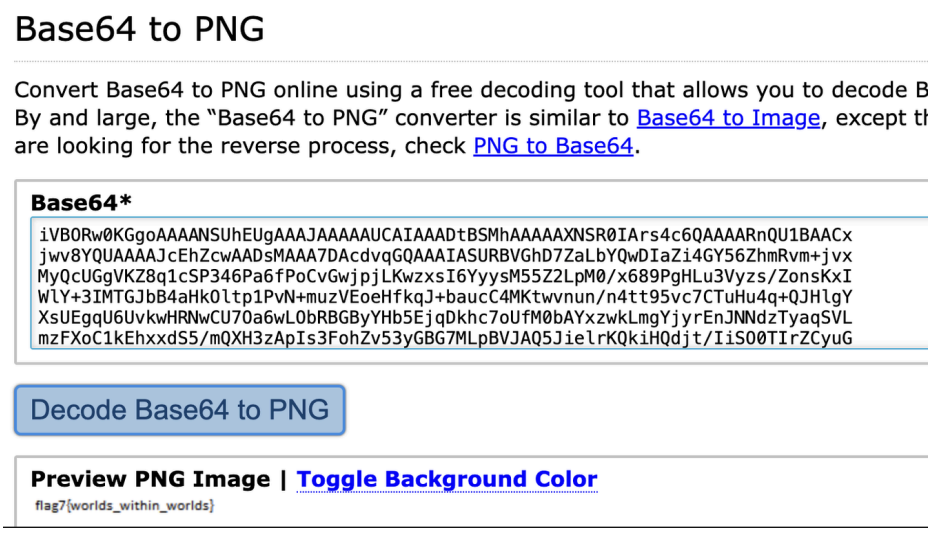
   **Prevention**: Avoid hiding data in between garbage data. Obfuscation is easy to break, encryption is difficult.

```
root@nbnserver:~/.../\# pwd
/root/.../\
root@nbnserver:~/.../\# grep -rv "NOTAFLAG" .
./512:uozt5{dvev_zodzbh_wlmv_rg_gsrh_dzb}
root@nbnserver:~/.../\#
```

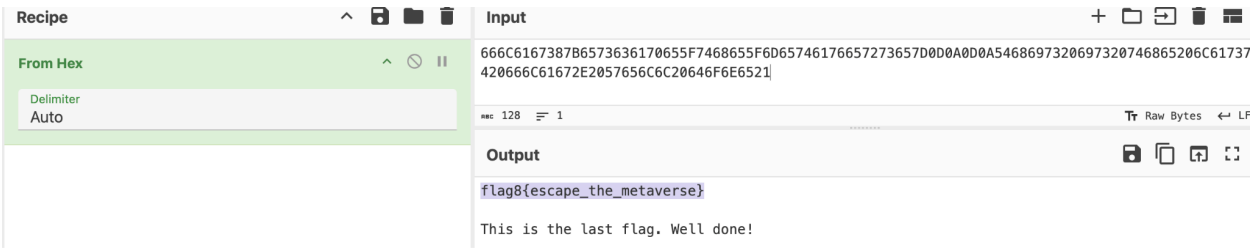


6. **Data:** `flag6{listen}`
   **Details**: On the client machine, in running processes, found a hex encoded string. On decoding it from hex to ascii, found sensitive data.
   **Prevention**: If sensitive data is required to be kept in running processes, have it be encrypted.

7. **Data**: `flag7{worlds_within_worlds}`
   **Details**: On logging in as the `stephenson` user on the client machine, a base64 encoded file found with the name of flag7. On decoding it from base64, IHDR and sRGB strings are seen, which are typically present in png images.
   Found sensitive data on decoding it from base64 to png.
   **Prevention**: Avoid keeping images with sensitive data in any format in the home directory of the user unencrypted.




8. Data: `flag8{escape_the_metaverse}`
   Details: On logging in as the root user in client machine, flag8.txt file found which contains hex encoded sensitive data.
   Prevention: Encrypt sensitive data.




END