PENTEST REPORT

nFuse website

Made by Bert Moelans

Table of contents

Introduction

My name is Bert Moelans, a student of Thomas More Geel. I am a Cybersecurity trainee from nFuse and was asked to do a PenTest of their website in a sandbox environment. A sandbox environment is a locked environment, a place where only I can connect to.

nFuse gave me 2 URL's to investigate. The first one is their site with basic vulnerabilities and with the second URL, it's more difficult to find vulnerabilities. The second site is also used as a mitigated environment for the found vulnerabilities of the first site.

Research question

What is the effect of PenTesting unknown web applications in a sandbox environment?

I will perform a PenTest or a Penetration Test on the two web applications given to me. So, I will test the security of these web applications, starting with the first one. This is the most important and time-consuming website. A lot of tools can help me in my search for vulnerabilities. Therefore, I will list them all further in this document.

After the information gathering and hacking phases, I will make a mitigation plan. Mitigating is finding solutions for vulnerabilities and fixing the things that cause them. The mitigation plan will be given to nFuse. They will mitigate the first web application. After that, it's my job to check, if these vulnerabilities still exist. Important to know is that I don't know anything about these web applications, besides the URL links given to me.

Disclosure policy

Confidentiality statement

All client's Personal Identifiable Information (PII) – which includes any data that can be used to identify a person. Examples are social security numbers, mailing or email addresses, phone numbers, … Any other information of a private or sensitive nature is considered confidential. Confidential Information should not be read or discussed by any employee unless on his or her specific job requirements.

Examples of inappropriate disclosures include:

- Employees discussing or revealing PII or other Confidential Information to friends or family members
- Employees discussing or revealing PII or other Confidential Information to other employees without a legitimate need to know
- The disclosure of a patient's presence in the office, hospital, or another medical facility, which may reveal the nature of the illness, without the patient's consent, to any unauthorized party without a legitimate need to know

Employee confidentiality agreement

I hereby acknowledge that I understand that PHI and Confidential Information and data to which I have knowledge and access in the course of my employment with nFuse is to be kept confidential, and this confidentiality is a condition of my employment.

This information shall not be disclosed to anyone under any circumstances, except to the extent necessary to fulfil my job requirements. I understand that my duty to maintain confidentiality continues even after I am no longer employed. Further, upon termination with nFuse, I shall return to the company all confidential information.

Disclaimer

Please read this disclaimer carefully before reading this document operated by Bert Moelans. The content displayed on this document is the intellectual property of the business nFuse. You may not reuse, republish, or reprint such content without my written consent. All information posted is merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this document? You do so at your own risk. While the information in this document has been verified to the best of my abilities, I cannot guarantee that there are no mistakes or errors. I reserve the right to change this policy at any given time, of which you will be promptly updated.

(TemplateLab, n.d.)

Contact information

bertmoelans@hotmail.com

https://bertmoelans.github.io/Mijn_Portfolio/

Assessment

Overview

There is a recurring process used in this Penetration Test. First, there's an analysis of the site. This is searching for vulnerabilities on the site in any way possible. After that follows exploiting these vulnerabilities. That means that there will be tried to hack the site. Then, there is the mitigation phase where these vulnerabilities are fixed and solutions are found. The last phase is proving that the vulnerabilities are gone and the site is protected against them. So, to summarize there will always be an analysis, then an exploit, after that a mitigation and finally validating the mitigation with proving.

Components

External penetration test

These kinds of penetration tests focus on the assets of the company which are visible on the internet. This includes the website of the company, email and DNS servers, … The goal is to gain access and secret data from the company.

Black box penetration test

These tests are made for penetration testers that know very little of the environment they are going to hack. This way a tester really takes the role of a malicious hacker and tries to expose as many vulnerabilities in the network. These threats are exploitable from outside the network.

(Poston, 2020)

Severity levels

Security levels are defined for each vulnerability to assess the danger or impact it could have. In the following table, you will see a summary of these levels with the matching CVSS v3.0 score and definition. CVSS stands for Common Vulnerability Scoring System and is used for scoring the severity of vulnerabilities.

Severity level	CVSS v3.0 score	Definition
Critical	9.0 – 10.0	A direct danger to your property (systems, servers, databases, networks) and should be mitigated immediately. The exploitation can be performed by someone with little knowledge of hacking.
High	7.0 – 8.9	A significant danger to your property and can be exploited by someone with some advanced skills. Should be mitigated shortly after the detection.
Moderate	4.0 – 6.9	These vulnerabilities should be checked within a recurring timeframe. The exploitation can be performed by someone with advanced and special skills. Social engineering might be necessary to exploit.

Low	0.1 – 3.9	There is no direct danger of exploitation because there is a small chance of data compromise. Should be mitigated when you find the time.
Informational	0.0	Purely informational, just to inform the client. No direct threat or danger.

Risk factors

The risk factors used in this penetration test are based on the CVSS scoring system. I will use an online CVSS v3.1 calculator to score the vulnerabilities I found. The CVSS score is determined by the combination of three elements namely the base score, the temporal score and the environmental score. Although you only need the base score to create a CVSS score but also using the other two elements gives us a more accurate score.

(Segal, 2020)

Base score

This element represents the different characters of the vulnerabilities. These characters are time and environment independent and consist of three subscores namely exploitability, impact and scope.

Exploitability subscore

Exploitability subscore is defined by metrics that define how easy it is to exploit the vulnerability.

- Attack vector
  - how easily the vulnerability can be used
- Attack complexity
  - the higher this is how easier it is to exploit
- Privileges required
  - how many privileges are required to exploit
- User interaction
  - how much the actions of a user impact the exploit

Impact subscore

The impact subscore defines how disastrous the outcome of an exploit can be.

- Confidentiality
  - how much confidential data is lost
- Integrity
  - how truthful is the data and what's the impact if exposed
- Availability
  - how available is the affected component

Scope subscore

Each system is protected while defining a security scope. When attackers can find a vulnerability outside that scope, we define the scope subscore. This could increase the severity of the vulnerability significantly.

Temporal score

The temporal score is based on the usage of known exploit techniques, patches and updates.

- Exploit code maturity
  - The existence and availability to exploit the vulnerability
- Remediation level
  - How available the level of remediation is to correct the vulnerability
- Report confidence
  - How accurate the vulnerability report is

Environmental score

The environmental score is defined on the impact of a vulnerability to your own company. Maybe a threat isn’t really dangerous for you company, because you already mitigated something like that in the past. It’s also possible that you know your security is well established around the threat thus it can’t impact your company that much. This means that it’s part of the risk appetite of your organisation. Risk appetite is the amount of risk an organisation is prepared to accept.

Executive summary

Synopsis

This is the executive summary which is just a short overview of my Penetration Test. The executive summary must be understandable for everyone, also for people without an IT background. If you want to see the more detailed documentation, you can take a look at the technical summary.

My findings

First of all, it was possible to make a **topology** based on best practices and a tool called nmap. With nmap all open ports and versions used could be seen. This gives a good idea of how the infrastructure looks like.

Second, there are a lot of **outdated versions** found. These versions are from the Divi theme (v4.8.2), PHP software (v7.2.34) and ninja forms plug-in (v3.3.21.3).

Third, there was a vulnerability found in your **SSL certificate**. A Beast attack is possible on your SSL connection. This was found with the TestSSL tool which tests your SSL connection and finds vulnerabilities for this.

Recommendations

The first thing you need to do is **update all your outdated versions** on the WordPress site. You can do this by going to the WordPress dashboard.

Next, you should **disable the directory listing**. This would allow a hacker to see all directories you have on your site.

Then it's important to have **no versions** mentioned in the source code of the site or anywhere else.

Update your SSL certificate and **check your open ports**. If you're not using a port, just shut it down or block it immediately. This way a hacker has no chance of entering your network via this port.

Another thing I haven't mentioned is that your employees need to be security-aware. You can do this by giving **security awareness training**. In these training, your employees will learn how not to click on links in emails and have strong passwords.

Technical summary

Target

There were two URL's given which needed to be investigated. They are running in a sandbox environment and are a copy of the nFuse site filled with vulnerabilities. A sandbox environment is an isolated environment and mainly used for testing purposes. In this environment nothing wrong can be done. The original site can't be affected. This gives the opportunity to do whatever it takes to find the weaknesses in these web applications.

- First URL - https://wp1.nfuse.cloud/
- Second URL - https://wp2.nfuse.cloud/

Methodology

In the Pentest journey, five phases are going through.

- Phase 1
  - Analysis and fingerprinting of the given set-up
  - Detection and findings guide
- Phase 2
  - Further investigation found vulnerabilities
  - Making use of these weaknesses by execution of exploits
- Phase 3
  - Set up a mitigation plan based on previous findings
  - Server hardening (Network and OS level)
  - Application hardening (how to mitigate fingerprinting)
    - Application
    - Database
- Phase 4
  - Execution of mitigation plan
- Phase 5
  - Analysis of patched environment

Overview findings

Resume

In the first phase, the objective is to gather as much information as possible. Finding vulnerabilities is, of course, the main goal, but information gathering is the first step. In this phase, there will also be a list of the best tools that can be used for fingerprinting or information gathering and for exploiting.

Target information overview:

- IP Address: 54.195.170.225
- WordPress site 5.6.2 “Simone”
- Username nfuse_root exists
- Plugins
    - Ninja forum
    - WP Post ratings
    - Mu-plugins
    - Autoptimize
- Theme: Divi 4.8.2
- Plesk toolkit
- AWS hosting
- Php version 7.2.34
- Akeeba Backup 7.5.3
- Akeeba Kickstart 7.0.3

Overview tools

Phase 1 - Information gathering	**Phase 2 - Exploiting and hacking**
Nslookup	Metasploit
Traceroute	Postman
Nmap	Burp suite intruder
Metasploit	Hydra
Dirbuster	John the ripper toolkit
Enum4linux	Owasp Zap
WPscan	Akeeba Extract Wizard
Dnsenum	crunch
Burp suite	SeToolkit
SQLmap	SSLyze
	shellshock
	TestSSL

Overview ports

Nmap

TCP port & service	22 – SSH	
	80 – HTTP	
	111 – rpcbind	
	3306 – MySQL	
	8080 – HTTP-proxy	
	443 – HTTPS	
UDP port & service	67 - dhcps	
	68 - dhcpc	
	111 – rpcbind	
	161 – snmp	
	162 – snmptrap	
	520 – route	
	4500 nat-t-ike	
Version & port	OpenSSH 7.4 (protocol 2.0)	22 SSH
	nginx 1.18.0	80/tcp HTTP
	2-4 (RPC #100000)	111/tcp rpcbind
	nginx 1.18.0	443/tcp SSL/HTTP
	MariaDB (unauthorized)	3306/tcp MySQL
	Apache httpd 2.4.46	8080/tcp HTTP

Zenmap

UDP Port & services		
136 – 17302	**17754 – 34215**	**35438 – 55587**
136 – profile	17754 – zep	35438
443 – https	17836	39213 – sygatefw
686 – hcp-wismar	18255	44334
959	18987	45928
996 – vsinet	19283 – keysrvr	47915
1042 – afrog	20449	49166
1050 – cma	20525	49205
1064 – jstel	21663	49226
2049 – nfs	24511	49503
3283 – netassistant	24594	40099
5093 – sentinel-lm	26407	54114
7000 – asf3-fileserver	28465	54321 – bo2k
16779	32528	55587
17091	32818	
17302	34125	

Overview vulnerabilities

An attack vector is a method that a hacker uses to exploit a vulnerability and gain access to a server, in this case, the nFuse webserver. These are possible attack vectors for each given vulnerability.

Vulnerability	**Attack vector**
PhpMyAdmin login page	Brute force attack with hacking tools or social engineering
WordPress login page	Brute force attack with Hydra or Burp intruder
Ninja forum plugin	Cross-site scripting (XSS) with Postman
Divi theme 4.8.2 (outdated)	Php file upload with Postman
Php version 7.2.34 (outdated)	Multiple exploits (Cookie forging, DOS with IMAP, …) with the Metasploit tool
Ninja forums plugin	CSRF and XSS attacks
Akeeba Backup/Kickstart pages	Restore the site back up on my SQL Database
Rpcbind port 111	Amplification/reflection attack with Postman
XSS found with Zap	Active scan to attack the site with XSS and Zap tool
Directory browsing	Dirbuster can see all folders and files on the site
Ports visible with nmap	SSH, MySQL and HTTP-proxy were key in setting up the topology
Versions visible with nmap	Apache, Nginx, OpenSSH versions are visible and are useful when searching for vulnerabilities
Sygate firewall	Buffer overflow with public exploit
wp-signup.php file	Somehow enable the registration on the site
XML-RPC	DDOS and brute-force attacks
WPscan username	I found nfuse_root username with WPscan
SQL injection	SQL injection with SQLmap
X-frame-options header not set	Clickjacking attacks with iframes
Yellow flag alerts	6 alerts from the Owasp Zap tool
No anti-CSRF tokens	Cross-site request forgery attack (XSS)
Source code	The version of WordPress, Divi theme, plugin wp-postratings, … are all visible in the source code of the website (CTRL + U)

Risk assessment

In this assessment, every important vulnerability will be discussed and given a severity risk score. There will also be talked about mitigating these vulnerabilities so that these won't be a threat anymore.

Severity level	Informational	Low	Moderate	High	Critical
CVSS v3.0 score	0.0	0.1 – 3.9	4.0 – 6.9	7.0 – 8.9	9.0 -10.0

Critical severity level

Social engineering

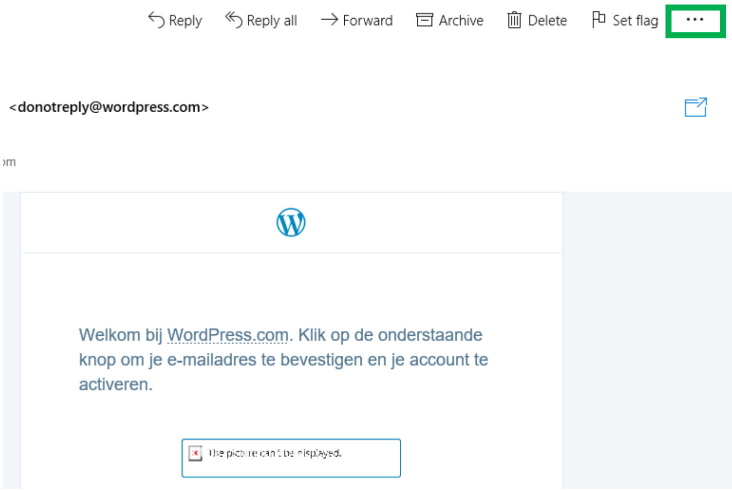
Explanation

A fake site is made which is an exact copy of the nFuse website. Then a phishing link is sent by mail that includes a link to this site. When the end-user clicks on that link and logs in on the fake site, all credentials used will be displayed.

SeToolkit or SET is used, which stands for the Social Engineering Toolkit. This is a built-in and open-source framework on a Kali virtual machine for penetration testing designed for social engineering attacks. It is created by David Kennedy, the founder of the company TrustedSec. SET has multiple attack vectors and a credential harvester. Something nice is that after de credentials are given, the site will redirect to the real site.

Tutorial

First, an email template is needed for phpMyAdmin or WordPress. After some searching, I only managed to get a WordPress email when trying to make an account.



<donotreply@wordpress.com>

Welkom bij WordPress.com. Klik op de onderstaande knop om je e-mailadres te bevestigen en je account te activeren.

The picture can't be displayed.

Figure 1 – WordPress registration mail

Click on the three bullets on the top right corner and save the file on your computer. Next, open it using Notepad. There you can see all the HTML code used for this email. The next step is to modify this coded text and lay out for your needs. The email headers are removed in this code file (top of the page).

Ubuntu server

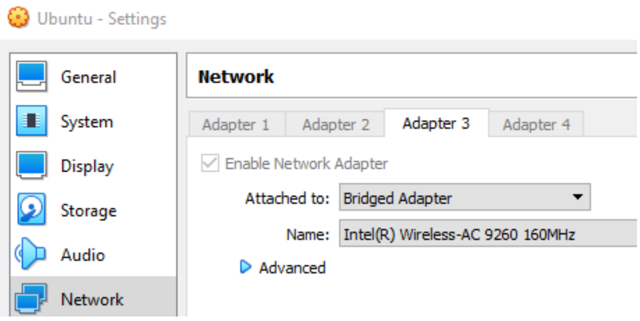
An up-to-date Ubuntu server is used to set up the fake copy of the PhpMyAdmin interface webpage.

Command's used to set up the fake site:

```
sudo setoolkit
Choose 1 -> 2 -> 3 -> 2
Now enter your global IP address
Paste in the following site https://wp1.nfuse.cloud/phpMyAdmin/
```

Now this will only work on the local machine, but the link of the fake site needs to be used across the internet.

Virtual box machine settings → network settings → Bridged adapter



☑ Enable Network Adapter

Attached to: Bridged Adapter

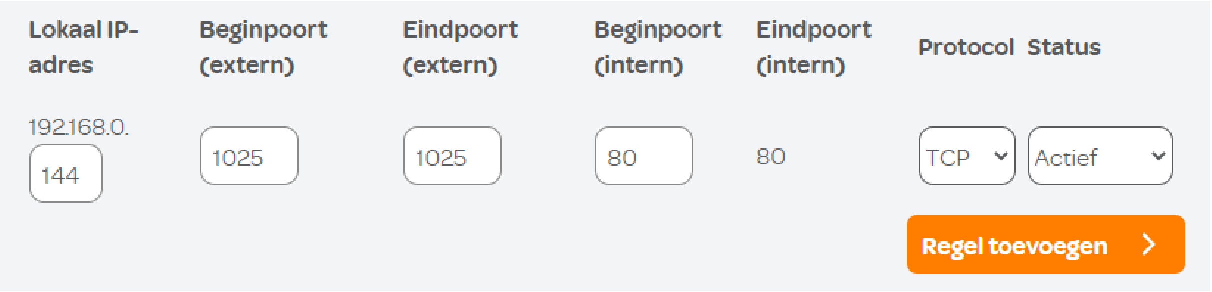
Name: Intel(R) Wireless-AC 9260 160MHz

Figure 2 – VirtualBox settings

There you can see the local IP.

ifconfig

Use this local IP to forward it to the router you use. This is a Telenet example.



Lokaal IP-adres	Beginpoort (extern)	Eindpoort (extern)	Beginpoort (intern)	Eindpoort (intern)	Protocol	Status
192.168.0.144	1025	1025	80	80	TCP	Actief

Figure 3 – Own provider settings

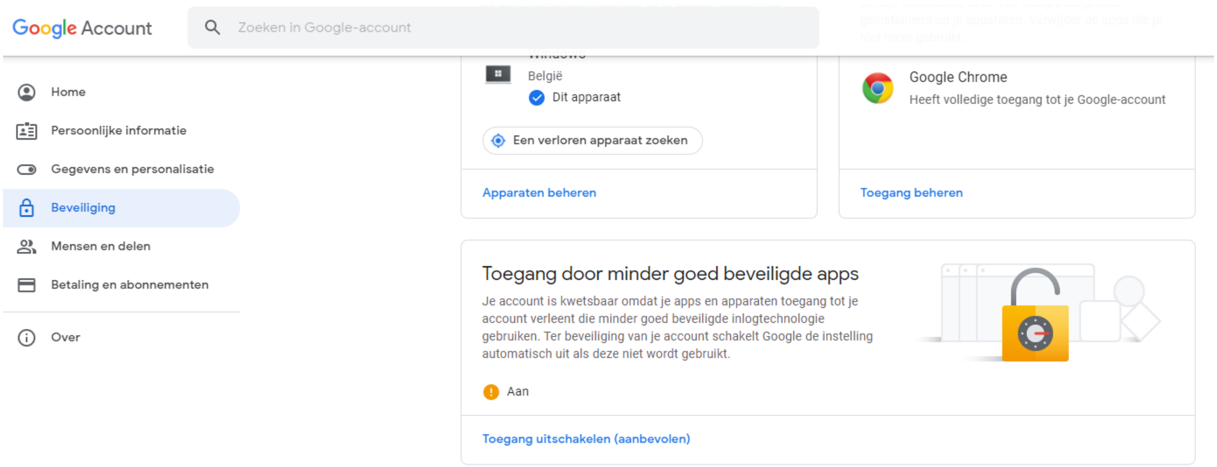
Also important to use a >= 1024 port externally, otherwise it wouldn't work.

Now use your global IP address as a URL and define the port used, in my case 1025.

http://<your-global-ip-adres>:1025/

You can find your global IP address by searching in Google "What's my IP".

You have to turn on the option to let less secure apps be used for your sending mail.



Heeft volledige toegang tot je Google-account

Toegang door minder goed beveiligde apps

Je account is kwetsbaar omdat je apps en apparaten toegang tot je account verleent die minder goed beveiligde inlogtechnologie gebruiken. Ter beveiliging van je account schakelt Google de instelling automatisch uit als deze niet wordt gebruikt.

Aan

Figure 4 - Google chrome settings

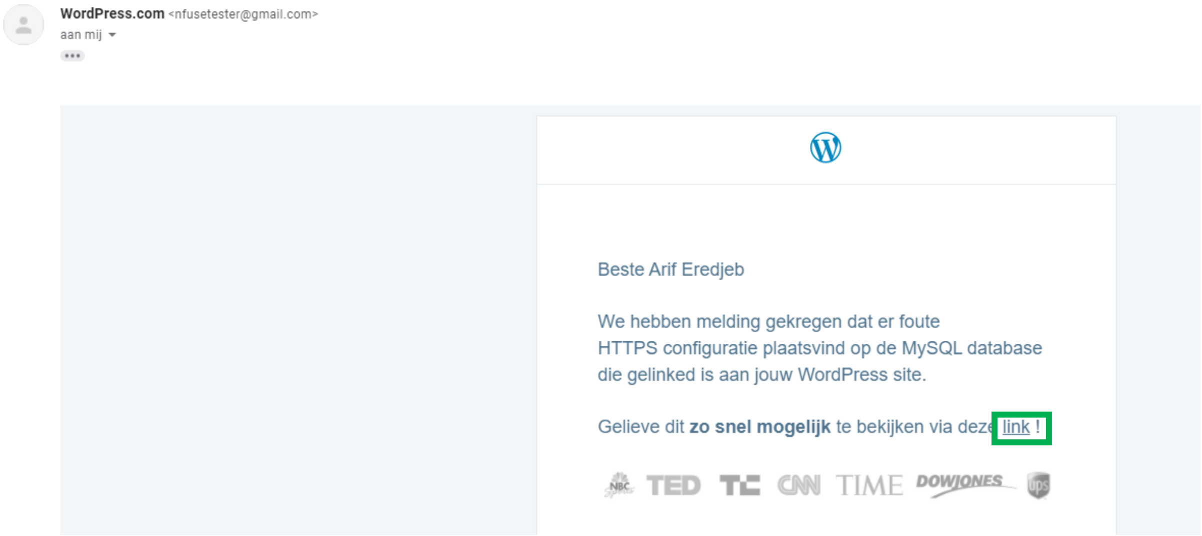
<u>Kali server</u>

An up-to-date Kali Linux server is used to send the mail with HTML code to the end-user, containing the link to my fake site.

Command’s used to send mail:

```
sudo setoolkit
Choose 1 -> 5 -> 1
Type in the receiver mail address
Choose 1
Type in the sending Gmail address
Type in the from name (WordPress.com)
Now give the password of the sending mail address
Email subject -> HTTPS misconfiguration for example
Now choose “h” for HTML code implementation I found earlier
Paste in the HTML code and type END to end the email body and send the email.
```

This is what the mail looks like.



WordPress.com <nfusetester@gmail.com>
aan mij

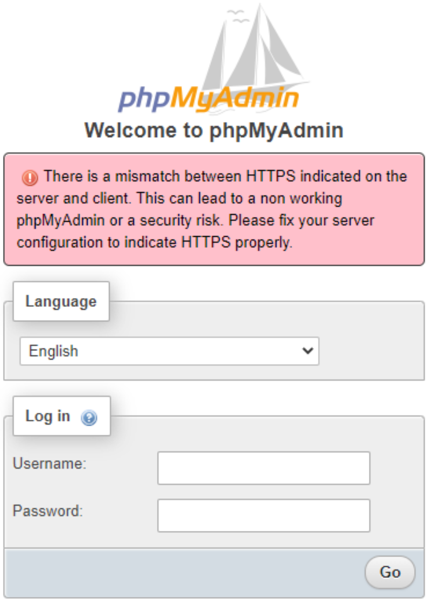
Beste Arif Eredjeb

We hebben melding gekregen dat er foute HTTPS configuratie plaatsvind op de MySQL database die gelinked is aan jouw WordPress site.

Gelieve dit **zo snel mogelijk** te bekijken via deze link !

Figure 5 – Phishing email

When the end-user clicks on the link, they will be redirected to my fake site which looks like this.



Welcome to phpMyAdmin

There is a mismatch between HTTPS indicated on the server and client. This can lead to a non working phpMyAdmin or a security risk. Please fix your server configuration to indicate HTTPS properly.

Language

English

Log in

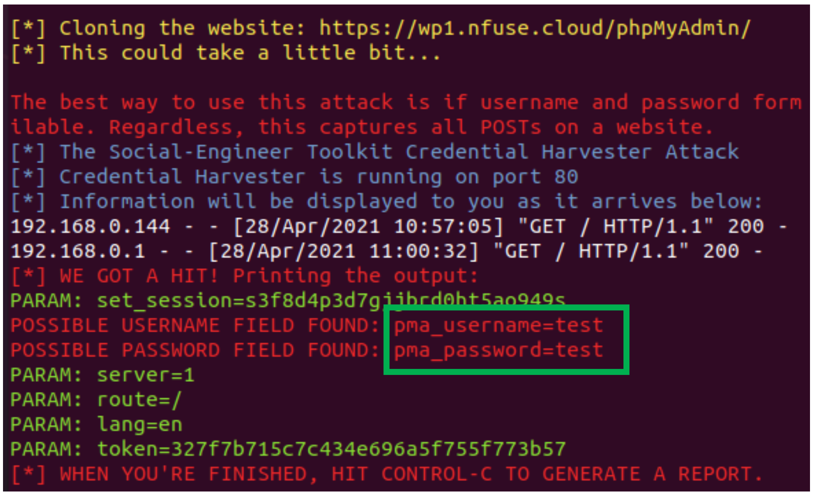
Username:

Password:

Figure 6 – PhpMyAdmin fake webpage

The HTTPS error is generated because the Ubuntu server and SeToolkit use port 80 to launch the fake site. That is why the HTTPS misconfiguration error is used to setting up the mail body.

When someone logs into this interface, the credentials are displayed on the Ubuntu terminal.

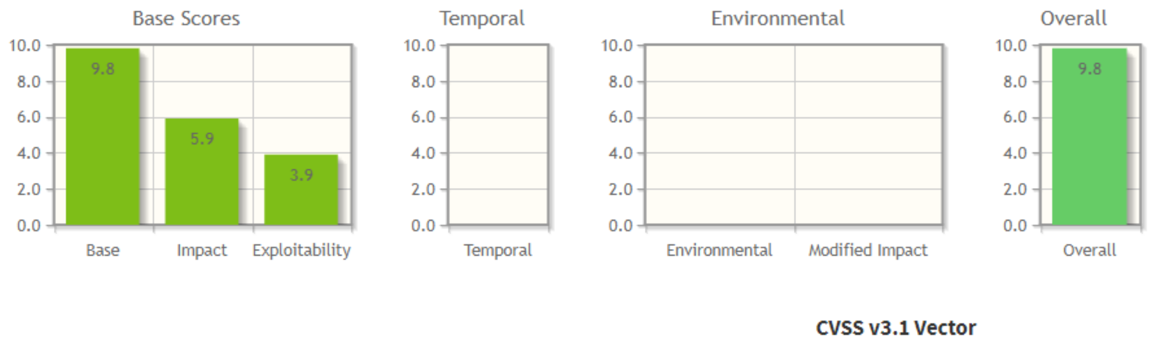


```
[*] Cloning the website: https://wp1.nfuse.cloud/phpMyAdmin/
[*] This could take a little bit...

The best way to use this attack is if username and password form
ilable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.144 - - [28/Apr/2021 10:57:05] "GET / HTTP/1.1" 200 -
192.168.0.1 - - [28/Apr/2021 11:00:32] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: set_session=s3f8d4p3d7gjjbrd0ht5ao949s
POSSIBLE USERNAME FIELD FOUND: pma_username=test
POSSIBLE PASSWORD FIELD FOUND: pma_password=test
PARAM: server=1
PARAM: route=/
PARAM: lang=en
PARAM: token=327f7b715c7c434e696a5f755f773b57
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 7 – Output of SeToolkit on Ubuntu server

Severity score

If this works it could be a disaster to your server so the score is 9.8 and **critical**.



CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

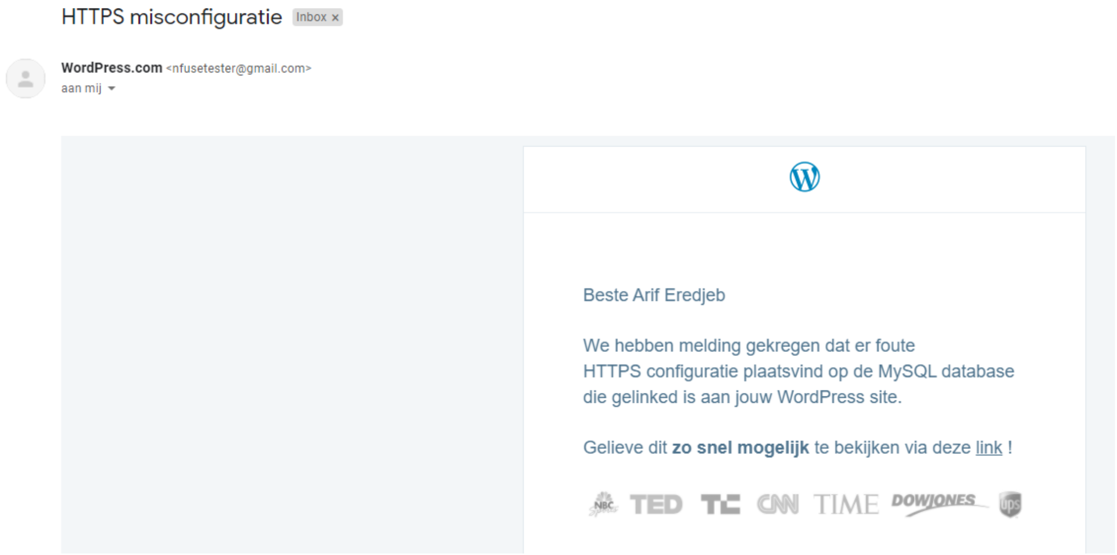
Figure 8 – Graphs of NIST CVSS 3.1 severity calculator

Mitigation

There is not a whole lot you can do to prevent phishing attacks like this phishing email. However, there are ways to recognize it and preventing to be a victim of it. As a company, you should invest in **security awareness training**. This way the employees are protected against possible phishing attacks because they would know what it looks like or how it works. A phishing attack can't only be executed via email, but also by a phone call or a text message.

Some other tips and tricks to not fall in the hands of phishers are never click on links in your email. Always go to the site in question and log in there. Also don't rely on the green lock icon in the address bar of the webpage. That certainly doesn't mean you can only go to websites where HTTP is used in the URL. HTTP at the front of a URL means the connection isn't secure, so always go to sites with HTTPS.

How to verify the phishing mail is false



HTTPS misconfiguratie

WordPress.com <nfusetester@gmail.com>
aan mij

Beste Arif Eredjeb

We hebben melding gekregen dat er foute HTTPS configuratie plaatsvind op de MySQL database die gelinked is aan jouw WordPress site.

Gelieve dit **zo snel mogelijk** te bekijken via deze link !

Figure 9 – Phishing email

First of all, WordPress wouldn't send any emails about misconfiguration. This is because AWS is the hosting service used. The sending email address is also not a WordPress official email address.

In the mail, there are three words in bold text implicating that you have to click urgently on the link. Phishing attackers try to let you click on links in a hurry. Then you wouldn't be able to stand still and think about your actions.

Outdated versions

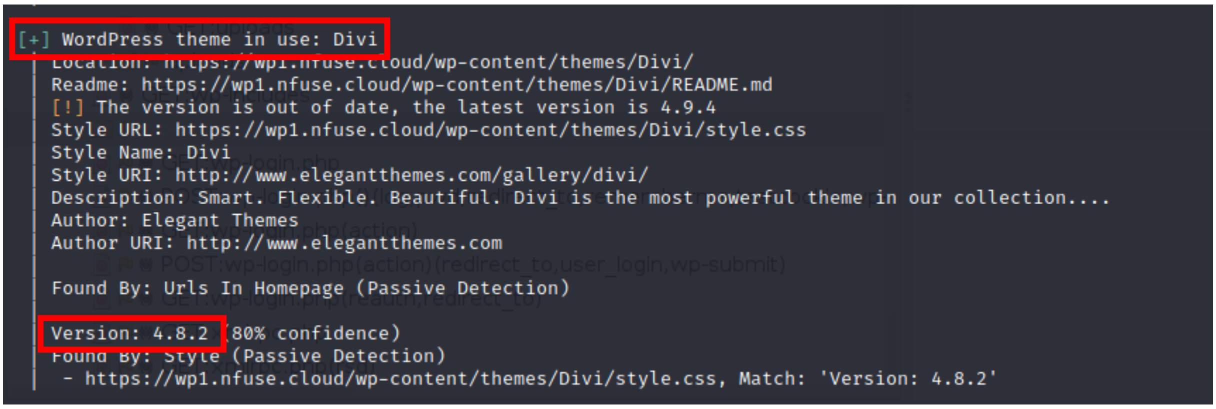
Explanation

Three outdated versions were found attached to the WordPress site.

- Divi theme 4.8.2
- Php 7.2.34
- Ninja forms 3.3.21.3

The Divi theme version is found with the wpscan tool. This scanning tool is specially designed to scan WordPress sites. It was found using the following command.

```
wpscan --url https://wp1.nfuse.cloud/ --enumerate u
```

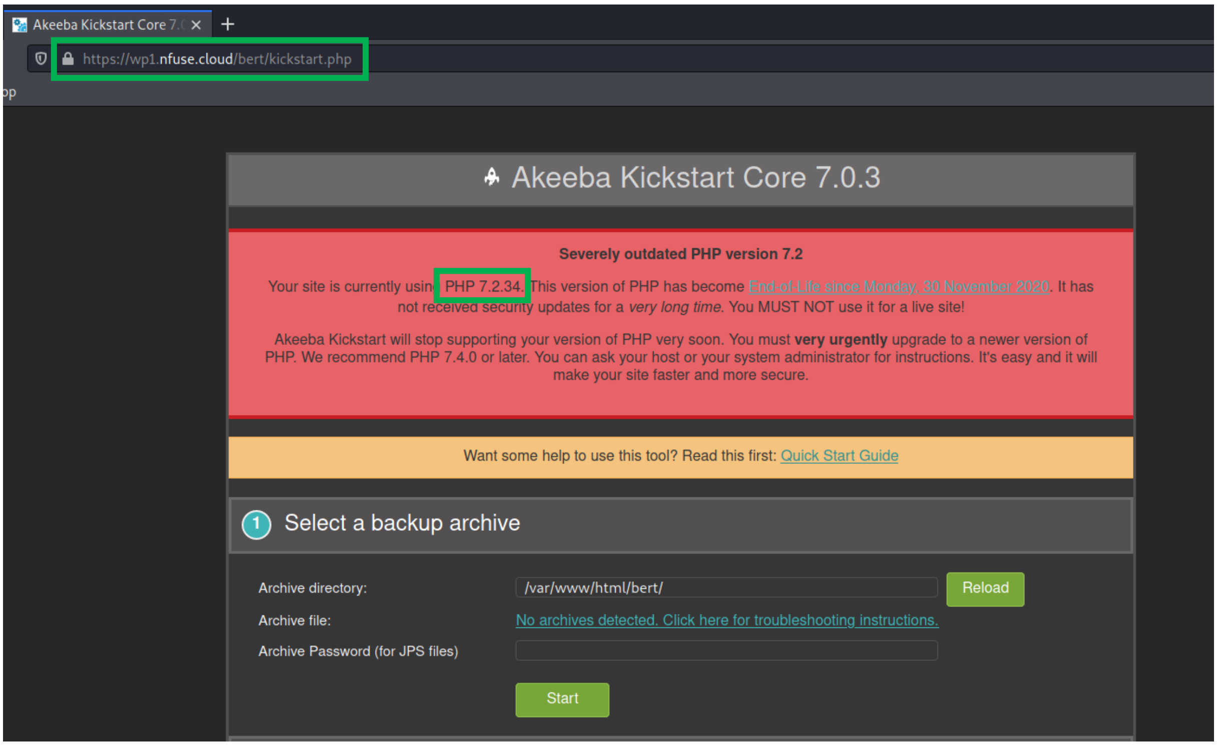


```
[+] WordPress theme in use: Divi
 | Location: https://wp1.nfuse.cloud/wp-content/themes/Divi/
 | Readme: https://wp1.nfuse.cloud/wp-content/themes/Divi/README.md
 | [!] The version is out of date, the latest version is 4.9.4
 | Style URL: https://wp1.nfuse.cloud/wp-content/themes/Divi/style.css
 | Style Name: Divi
 | Style URI: http://www.elegantthemes.com/gallery/divi/
 | Description: Smart. Flexible. Beautiful. Divi is the most powerful theme in our collection....
 | Author: Elegant Themes
 | Author URI: http://www.elegantthemes.com
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 4.8.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://wp1.nfuse.cloud/wp-content/themes/Divi/style.css, Match: 'Version: 4.8.2'
```

Figure 10 – Output of WPScan tool

There were 2 ways to find out the php version. The first is opening the “bert” folder found with the Dirbuster tool. The second is going to the info.php file also found with Dirbuster.

https://wp1.nfuse.cloud/bert/kickstart.php



Akeeba Kickstart Core 7.0.3

Severely outdated PHP version 7.2

Your site is currently using PHP 7.2.34. This version of PHP has become End of Life since Monday, 30 November 2020. It has not received security updates for a *very long time*. You MUST NOT use it for a live site!

Akeeba Kickstart will stop supporting your version of PHP very soon. You must **very urgently** upgrade to a newer version of PHP. We recommend PHP 7.4.0 or later. You can ask your host or your system administrator for instructions. It's easy and it will make your site faster and more secure.

Want some help to use this tool? Read this first: Quick Start Guide

1 Select a backup archive

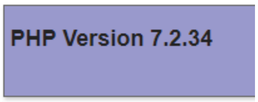
Archive directory: /var/www/html/bert/

Archive file: No archives detected. Click here for troubleshooting instructions.

Archive Password (for JPS files)

Figure 11 – Screenshot of kickstart webpage found in “Bert” folder

https://wp1.nfuse.cloud/info.php

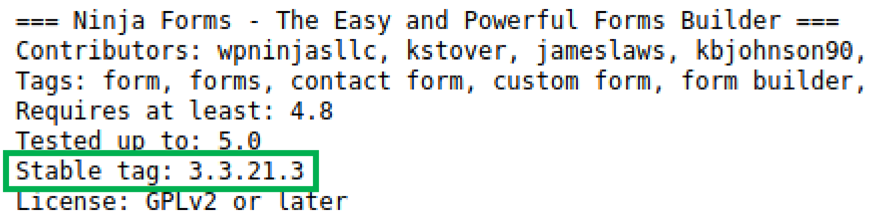


PHP Version 7.2.34

Figure 12 – Screenshot of PHP info page

There was tried to type readme.txt behind the URL that redirects to the ninja-forms map. This was a lucky guess with great success.

https://wp1.nfuse.cloud/wp-content/plugins/ninja-forms/readme.txt



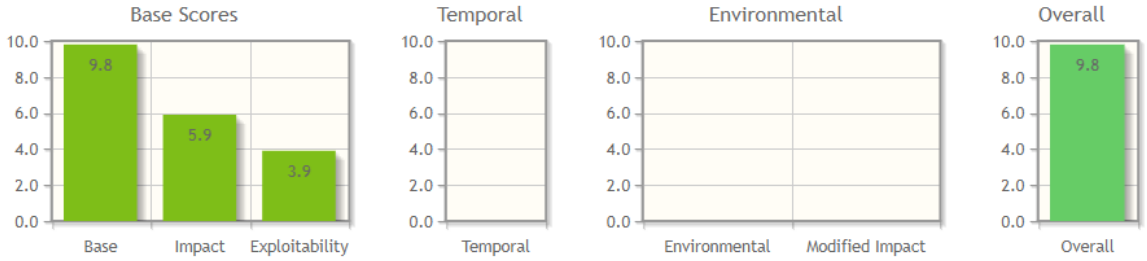
```
=== Ninja Forms - The Easy and Powerful Forms Builder ===
Contributors: wpninjasllc, kstover, jameslaws, kbjohnson90,
Tags: form, forms, contact form, custom form, form builder,
Requires at least: 4.8
Tested up to: 5.0
Stable tag: 3.3.21.3
License: GPLv2 or later
```

Figure 13 – Screenshot of ninja-forms readme.txt file

Version 3.3.21.3 of ninja forms was found. On the cybersecurity-help.cz site the version 3.3.21.3 was found to be vulnerable to cross-site request forgery.

Severity score

Because this could have lots of different vulnerabilities according to which version it has, this vulnerability has to be put in the **critical** severity level category with a 9.8 score.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Figure 14 – Graphs of NIST CVSS 3.1 severity calculator

Mitigation

Depending on the outdated version, it can have vulnerabilities according to the version. Updating is the first thing anyone would do to mitigate their system. It is fairly easy and quick to execute. You can look at the hands-on mitigation a little further in this document. The Divi theme and WordPress version were found by simply looking at the source code and searching for the word "generator."

High severity level

None.

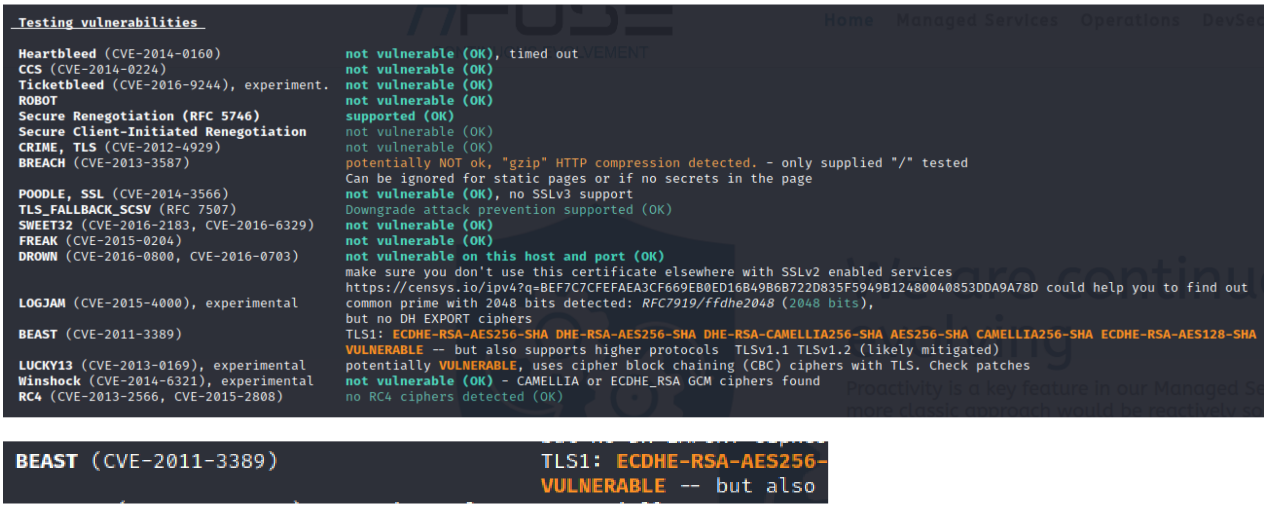
Moderate severity level

SSL certificate

Explanation

My mentor gave me a hint that the SSL certificate of the site has some vulnerabilities. This is a secure socket layer for data protection while transporting data (by encrypting the data). Your SSL certificate ensures an HTTP**S** connection with your site. The following tools are all tools to gather information about the SSL certificate and connection of the site. They can also track possible vulnerabilities, let's see what there's find out.

Your website is vulnerable to the BEAST attack. This was discovered with a tool called TestSSL. This tool tests your SSL connection. You're also potentially vulnerable for the lucky13 attack.



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), timed out
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
                                           Can be ignored for static pages or if no secrets in the page
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention supported (OK)
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://censys.io/ipv4?q=BEF7C7CFEFAEA3CF669EB0ED16B49B6B722D835F5949B12480040853DDA9A78D could help you to find out
 LOGJAM (CVE-2015-4000), experimental      common prime with 2048 bits detected: RFC7919/ffdhe2048 (2048 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     TLS1: ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA AES256-SHA CAMELLIA256-SHA ECDHE-RSA-AES128-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.1 TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - CAMELLIA or ECDHE_RSA GCM ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

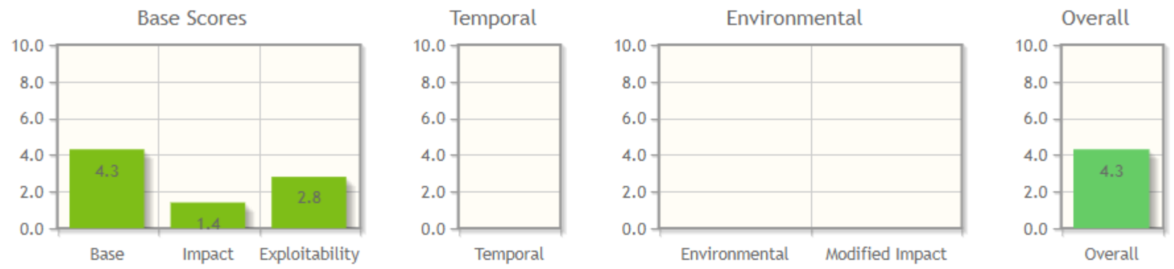
```
BEAST (CVE-2011-3389)                   TLS1: ECDHE-RSA-AES256-
                                        VULNERABLE -- but also
```

Figure 15 and 16 – Screenshots of output TestSSL tool

Beast stands for Browser Exploit Against SSL/TLS. This is a man-in-the-middle attack that allows a hacker to uncover information from an encrypted SSL/TLS 1.0 session.

Severity score

According to the cvedetails website, this vulnerability has a 4.3 severity score and therefore moderate.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Figure 17 - Graphs of NIST CVSS 3.1 severity calculator

Mitigation

You can mitigate this by only allowing TLS 1.3 because this will fix the TLS 1.0 vulnerability. TLS 1.3 is the latest version, so it's highly recommended for your website. Another way of doing this is using another SSL certificate. You are using "Let's encrypt", which's a free certificate. A difference between free and paid SSL certificates is that paid certificates more validation checks are done on the clients who access the site.

Low severity level

None.

Informational severity level

Topology

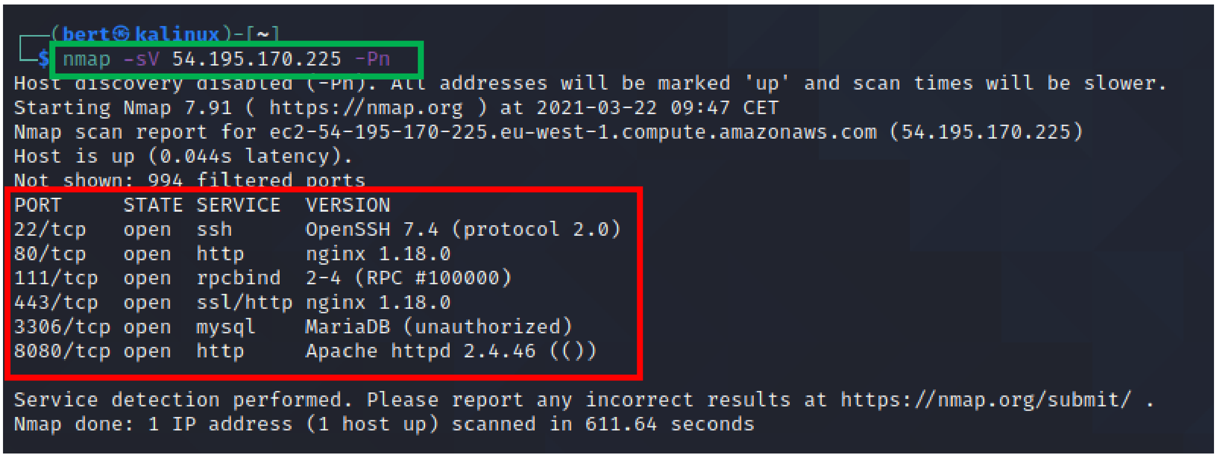
Explanation

A topology was made where the site is running on. The topology is based on logical thinking and best practices. Two tools were very helpful in setting up this topology, named nmap and Dirbuster. With the nmap tool, a lot of these components/servers were found because it scans on the network side. Dirbuster scans on the web application side and generates a list of all directories and files found on the site.

The following nmap command is the best command used with this tool because it had the most detailed output. The -sV searches for versions on the server. As you can see below, there are multiple ports and versions found.

(BORGES, 2021)

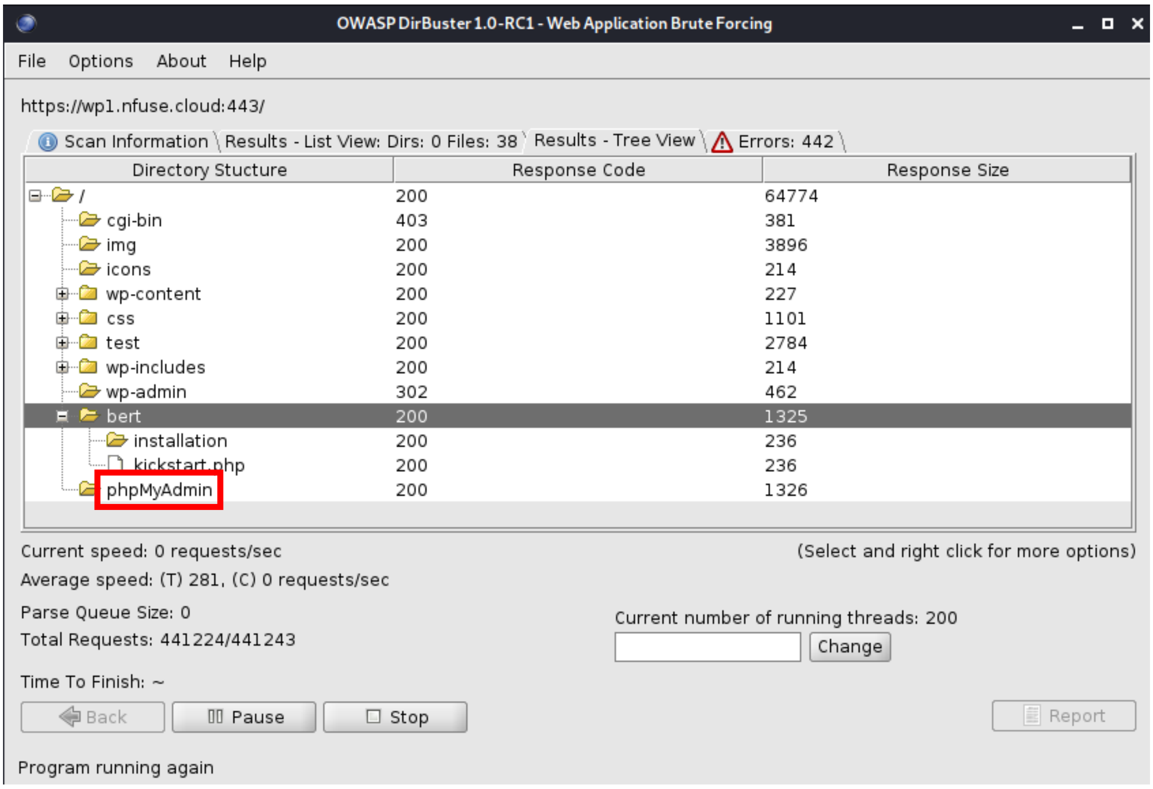
```
nmap -sV 54.195.170.225 -Pn
```



```
┌──(bert㉿kalinux)-[~]
└─$ nmap -sV 54.195.170.225 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-22 09:47 CET
Nmap scan report for ec2-54-195-170-225.eu-west-1.compute.amazonaws.com (54.195.170.225)
Host is up (0.044s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http     nginx 1.18.0
111/tcp  open  rpcbind  2-4 (RPC #100000)
443/tcp  open  ssl/http nginx 1.18.0
3306/tcp open  mysql    MariaDB (unauthorized)
8080/tcp open  http     Apache httpd 2.4.46 (())

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 611.64 seconds
```

Figure 18 – Output of nmap command containing versions

Dirbuster stands for directory buster. This is a Java application that brute forces directories and files on a web application server. Below you can see the output of this tool and showing the phpMyAdmin map which redirects to a phpMyAdmin login page.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 38
Results - Tree View
Errors: 442
Change
Back
Pause
Stop
Report

https://wp1.nfuse.cloud:443/

Directory Stucture	Response Code	Response Size
/	200	64774
cgi-bin	403	381
img	200	3896
icons	200	214
wp-content	200	227
css	200	1101
test	200	2784
wp-includes	200	214
wp-admin	302	462
bert	200	1325
installation	200	236
kickstart.php	200	236
phpMyAdmin	200	1326

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 281, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 441224/441243

Current number of running threads: 200

Time To Finish: ~

Program running again

Figure 19 – Output of Dirbuster tool with an overview of directories and files

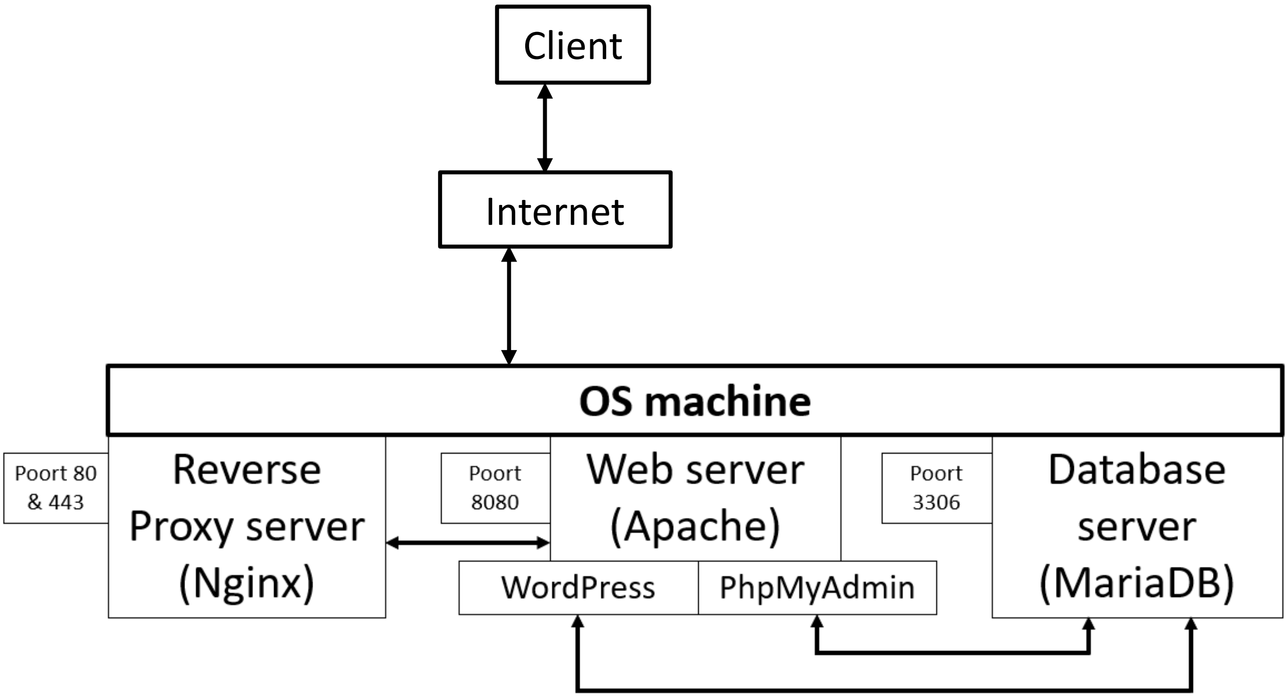
It was early discovered that the site is using WordPress. You can just find it in the source code of the site. To know what version of WordPress the site is using you can go to the source code and search for the word “generator.” Newer themes would disable this tag, but this site doesn’t.

WordPress 5.6.2 “Simone”

```
<meta name="generator" content="WordPress 5.6.2"
```

Visualisation WordPress site

WordPress is an open-source CMS (= Content management system) based on PHP and MySQL. CMS is computer software or an application that uses a database. In this case, a MySQL database to manage all of its content for example updating your site or website structure.

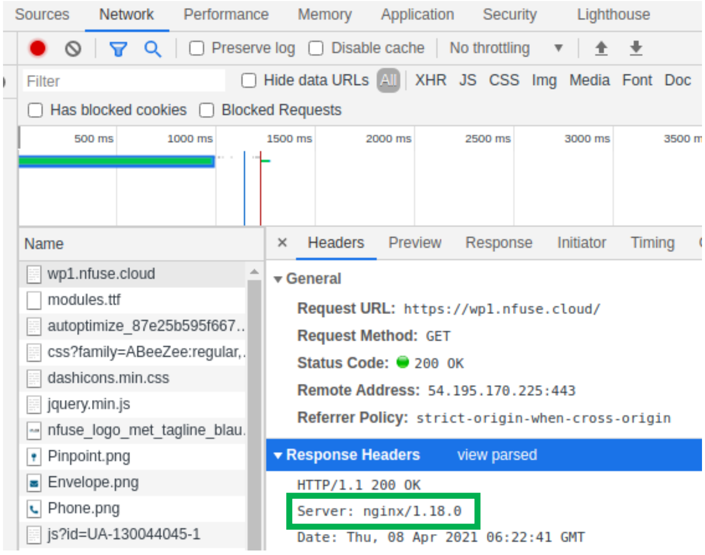


Explanation components

Reverse proxy server

It's known there's a webserver proxy, because of intense scanning with the nmap tool. After some research, it was found that a reverse proxy uses SSL encryption. This can be the link to the HTTPS protocol which uses port 443. A characteristic of a reverse proxy is that it collects requests on the origin server's behalf. It also passes on these requests to the internet and clients. All requests coming from clients will first pass the reverse proxy, after that the webserver with the WordPress site. So the main difference between a forward proxy and a reverse proxy is that a reverse proxy is used by servers and a forward proxy by clients.

It can be verified that the reverse proxy server is an nginx server because this can be found in the response headers of the DevTools kit in a google chrome browser. The fact that a site uses ports 80 and 443 with the HTTP or HTTPS protocol matches the findings with the nmap tool. It's also known that a client connecting to a site always first connects to the reverse proxy server because this is a server that stands between the client and the webserver.



wp1.nfuse.cloud
modules.ttf
autoptimize_87e25b595f667..
css?family=ABeeZee:regular,.
dashicons.min.css
jquery.min.js
nfuse_logo_met_tagline_blau.
Pinpoint.png
Envelope.png
Phone.png
js?id=UA-130044045-1

▾ General

Request URL: `https://wp1.nfuse.cloud/`
Request Method: `GET`
Status Code: ● `200 OK`
Remote Address: `54.195.170.225:443`
Referrer Policy: `strict-origin-when-cross-origin`

▾ **Response Headers** view parsed

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Thu, 08 Apr 2021 06:22:41 GMT
```

Figure 20 – Screenshot of Google chrome DevTools Network tab

(A, 2018)

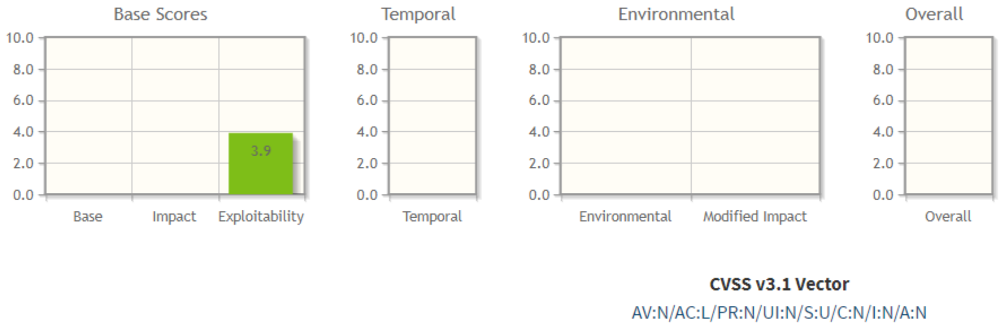
Webserver and database

When you want to install WordPress you will have three requirements. You will need a webserver (Apache), a database (MariaDB), and PHP support (to talk to your database).

With nmap a port 8080 was found running Apache. The ports 443 and 80 are used by the reverse proxy server with Nginx. Thus the port 8080 will be used by the webserver with Apache. Also found was a 3306 port which indicates a MySQL connection with MariaDB. Lastly, this database needs to be managed and is done by PhpMyAdmin. The phpMyAdmin interface was found with the Dirbuster tool scanning for folders on the site. It's also known that it's a WordPress site because it is found in the source file of the site.

Severity score

The severity score for this vulnerability is 0.0 and **informational**.



CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Figure 21 - Graphs of NIST CVSS 3.1 severity calculator

Mitigation

So, it is possible to set up a network infrastructure topology of the nFuse website. Nmap showed all open ports and services running, so deserves most of the credit. Although it's important to know that you can't be 100 % certain of this topology. On the other hand, you can be 99% sure that this is what the infrastructure would look like according to best practices and logic.

How to defend against nmap

The best defence begins with a good **offence**. As an administrator of a site, it's important that you scan proactively and according to these scans close or block ports. You can scan with tools like nmap to know what attackers might see. When you don't use a port anymore, immediately close or block it.

You can block tools like nmap with well-configured **firewalls**. The most critical rule here is to deny by default. First, you have to block everything and then allow only the essential traffic.

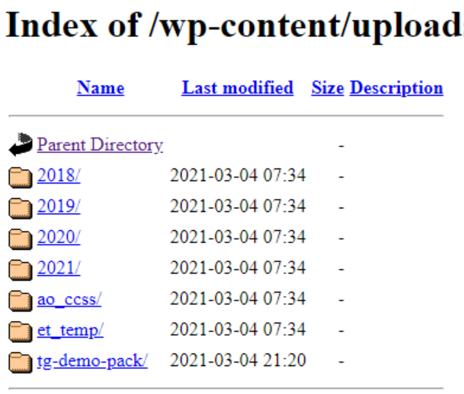
Another defence against nmap is to use **scan detecting** tools like PortSentry or Scanlogd. With these tools, you can see when your system is scanned by someone. These scans are most of the time harmless but there are a lot of attackers out there trying to scan systems for vulnerabilities. You can also use an **intrusion detection system** like Snort to have a good overview of all possible threats to your systems.

Directory listing

Explanation

The phpMyAdmin and WordPress login page were found using the Dirbuster tool. This is a tool that scans a site for directories and files. That's why it is important to **disable directory browsing** in WordPress. This way the hacker can't access readme.txt files or see other directories containing valuable info.

You can find an example image below. The URL is https://wp1.nfuse.cloud/wp-content/uploads/.



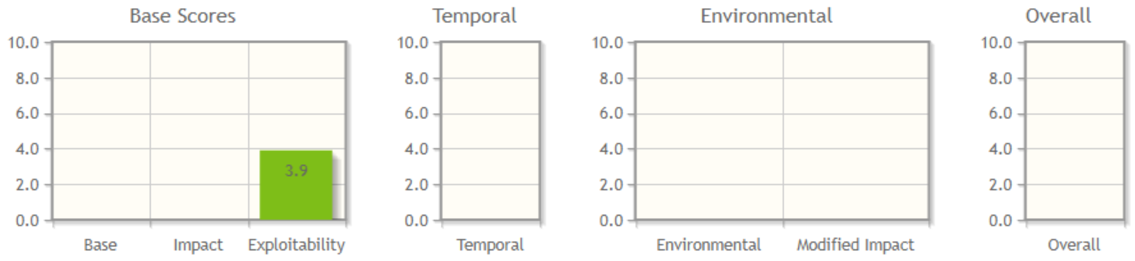
Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2018/	2021-03-04 07:34	-	
2019/	2021-03-04 07:34	-	
2020/	2021-03-04 07:34	-	
2021/	2021-03-04 07:34	-	
ao_ccss/	2021-03-04 07:34	-	
et_temp/	2021-03-04 07:34	-	
tg-demo-pack/	2021-03-04 21:20	-	

Figure 22 - Screenshot of the uploads directory listing in the wp-content directory

Severity score

The severity score for this vulnerability is 0.0 and **informational**.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Figure 23 - Graphs of NIST CVSS 3.1 severity calculator

Mitigation

A way to mitigate this is if you’re using Apache is by accessing the .htaccess file and adding the following code

```
Options -Indexes
```

Because of this, the site won’t show the index, or directory and files listing, of the WordPress website.

Doing this won’t stop Dirbuster from finding some directories. Therefore you can also configure a **WAF**. This stands for a Web application firewall. With this firewall, you can configure to block an IP address that sends a large number of GET requests to the server in a short period.

Hand’s on mitigation

Step 1 – Updates

1. Update your outdated software.
2. Go to the WordPress dashboard located with the URL https://wp1.nfuse.cloud/wp-admin.
3. On the left, you will see a tab “Updates”. Check for updates and update all of them.
4. Now on your OS machine, you can update the outdated PHP version.

Step 2 – Disable directory listing

It’s strongly advised to disable directory listing. The way you can do this depends on which software you use. For example, with Apache, you can update the .htaccess file in the root directory of your site.

https://wp1.nfuse.cloud/.htaccess

Open it and go to the end of the file. There you can insert the following code: Options -Indexes

Step 3 – No versions

WordPress version, themes and plugins

Remove the WordPress version from the source code.

You can do this manually by appending the following code to the functions.php file in the /wp-contents/themes directory.

The following code was found on the getastra website in an article named “[Plugin+Manual method] How to Hide WordPress Version Number in Your Website?”

```
remove_action(‘wp_head’, ‘wp_generator’)
function remove_version_info() {
return '';
}
add_filter('the_generator', 'remove_version_info');
```

Another way of showing no versions is using plugins. it’s recommended to use “Hide My WP Ghost” because it’s a very good plugin for this. It has lots of free security features and over 70000 active installations. It has brute force protection and there are also login email alerts available as a feature. The rating is 4.5 stars on the official WordPress site.

(wordpress, n.d.)

- Go to your /wp-admin directory and access the WordPress dashboard.
- Click on plugins on the left sidebar. Search for “Hide My WP Ghost” and click “install now”.
- You also need to activate it before it is enabled on your site. There should be a new element on the left sidebar of your page directed to this plugin.
- Let’s go to Permalinks on the left and access the Admin settings. Enable the two buttons hiding the wp-admin and the new admin path. Of course, you can also define a new wp-admin path.
- Now we’ll go to the login settings and hide the wp-login.php and login path. Change the path.
- Now go to the plugin settings and hide the plugin names and hide all plugins. Change the path.
- Next, go to the theme settings and hide the theme names and hide the IDs. Change the path.
- In the hide/show options it’s important to enable “Hide versions and WordPress tags”. This will remove the versions I found of WordPress and the Divi theme in the source code.

Apache and Nginx

To manually hide the Apache version in requests made to the website, you can turn off the “server signature”. The file where this is specified depends on what system you are using.

For Debian or Ubuntu systems it’s in the /etc/apache2/apache2.conf file.

For RHEL or CentOS systems it’s in the /etc/httpd/conf/httpd.conf file.

There you need to add or modify the code to the following:

```
ServerSignature Off
```

To manually hide the Nginx version you can go to the file /etc/nginx/nginx.conf and also add or modify the following code (under # http options and ##):

```
server_tokens off;
```

Step 4 – Update SSL certificate

Disable TLS 1.0 and only allow the TLS 1.3 version. You can also look for a paid SSL certificate which will give you more security and validation checks.

Step 5 – Check open ports

Check the following ports if you’re using them or not. If you’re not using them it’s best practice to close them or only make them available for certain IP addresses you know. You can do this with IP whitelisting. This is a list of IP addresses that you can trust and are only permitted to use for example ssh to your site. So, check the following ports.

- Port 22 for SSH
- Port 111 for rpcbind
- Port 3306 for MySQL
- Port 8080 for HTTP-proxy

Step 6 – Be security-aware

Plan some security awareness training for your employees regularly. There are a few important topics that need to be discussed during this training. These topics are email scams, malware, password security, safe internet habits, social engineering, clean desk policy, and the BYOD policy which stands for bring-your-own-device.

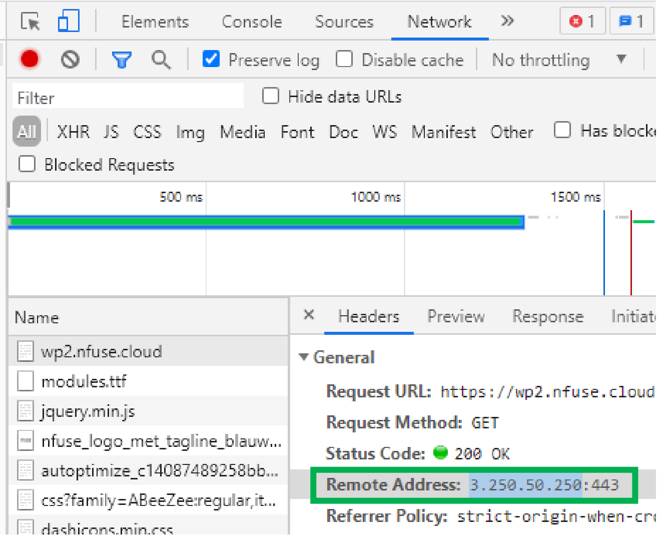
Analysis of patched environment

This phase is all about testing the found vulnerabilities on the second site. The nFuse site 2 is essentially the patched version of site 1. It also has vulnerabilities but these are much harder to find. So now, there will be checked if the previously found vulnerabilities are patched on site 2.

3.250.50.250 is the IP address of site 2.

This was found by using the dev toolkit on the Google Chrome browser (CTRL + shift + i) in the Network tab.

https://wp2.nfuse.cloud/



wp2.nfuse.cloud
modules.ttf
jquery.min.js
nfuse_logo_met_tagline_blauw...
autoptimize_c14087489258bb...
css?family=ABeeZee:regular,it...
dashicons.min.css

General

Request URL: https://wp2.nfuse.cloud
Request Method: GET
Status Code: ● 200 OK
Remote Address: 3.250.50.250:443
Referrer Policy: strict-origin-when-cr

Figure 24 – Screen of Google chrome DevTools Network tab

Topology

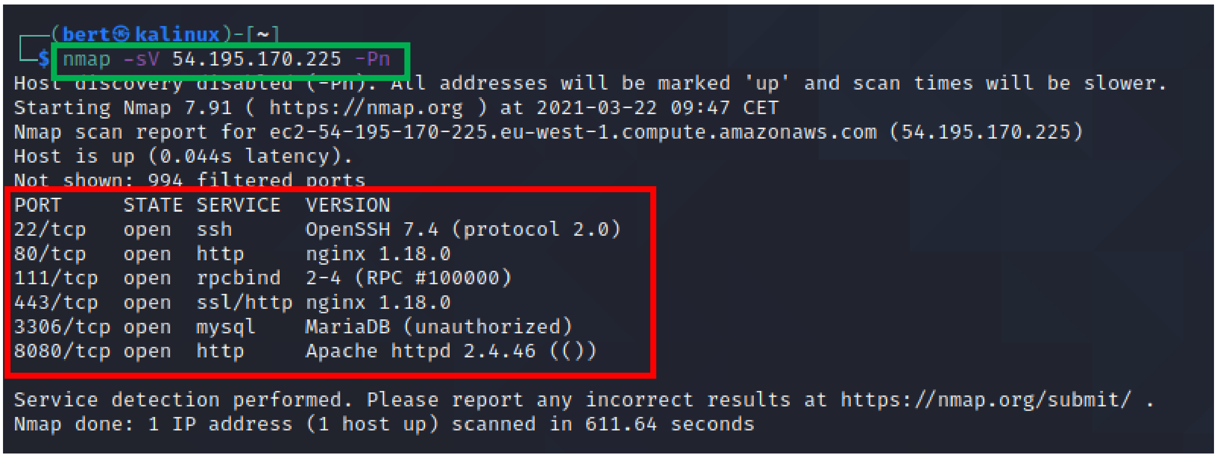
The two most important tools used by setting up the topology of the site were nmap and Dirbuster. These tools are put to the test, to know if they also work on wp2 (the second site).

Nmap

The following command gave the most insight on all open ports and their versions.

```
nmap -sV 3.250.50.250 -Pn
```

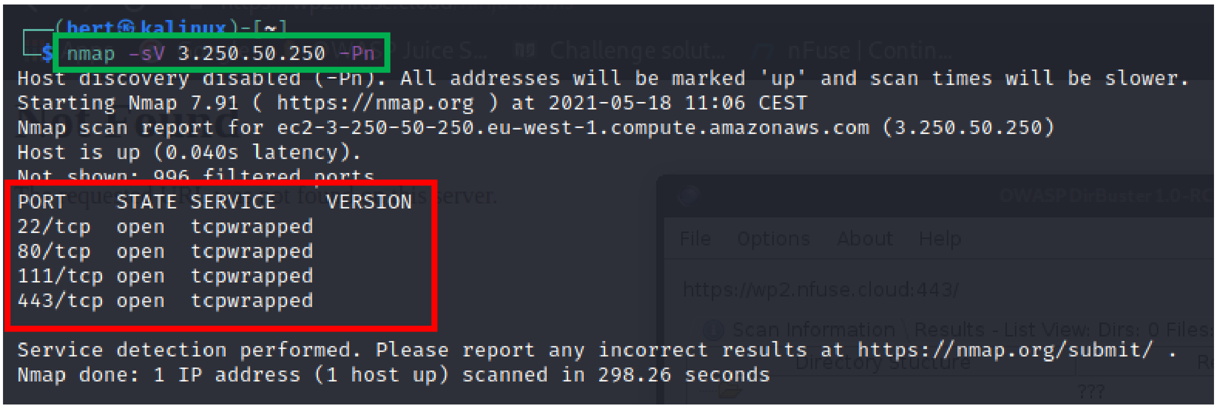
Site 1:



```
┌──(bert㉿kalinux)-[~]
└─$ nmap -sV 54.195.170.225 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-22 09:47 CET
Nmap scan report for ec2-54-195-170-225.eu-west-1.compute.amazonaws.com (54.195.170.225)
Host is up (0.044s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http     nginx 1.18.0
111/tcp  open  rpcbind  2-4 (RPC #100000)
443/tcp  open  ssl/http nginx 1.18.0
3306/tcp open  mysql    MariaDB (unauthorized)
8080/tcp open  http     Apache httpd 2.4.46 (())

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 611.64 seconds
```

Figure 25 – Output of nmap command containing versions

Site 2:



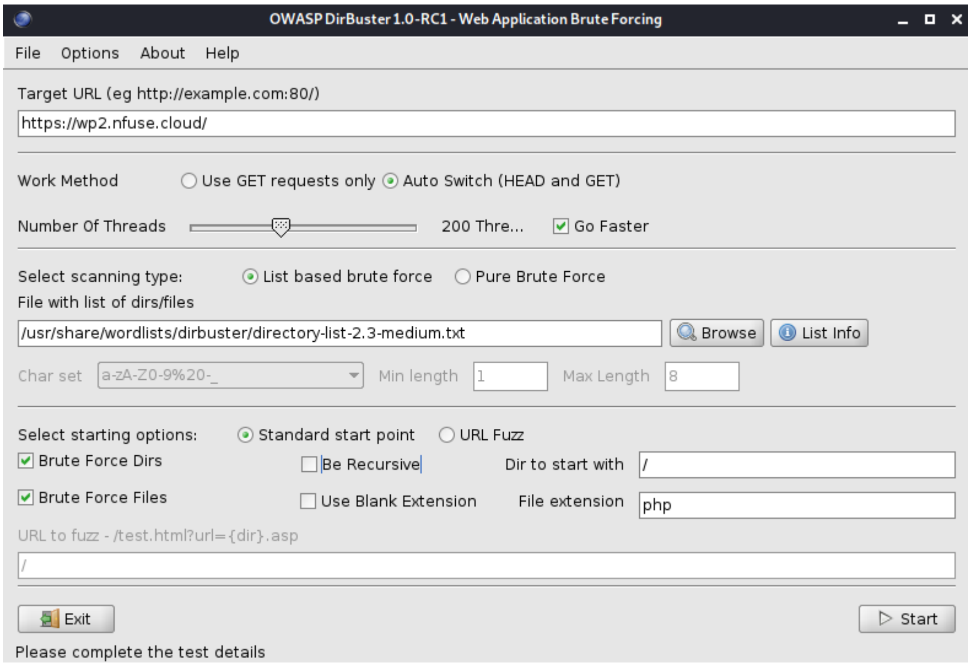
```
┌──(bert㉿kalinux)-[~]
└─$ nmap -sV 3.250.50.250 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 11:06 CEST
Nmap scan report for ec2-3-250-50-250.eu-west-1.compute.amazonaws.com (3.250.50.250)
Host is up (0.040s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
80/tcp  open  tcpwrapped
111/tcp open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 298.26 seconds
```

Figure 26 – Output of nmap command containing no versions

There are no more versions. Also, the MySQL port 3306 and the HTTP-proxy port 8080 aren't there anymore.

Dirbuster

Let’s first scan for PHP files and being non-recursive to only see the top directories and files.



Target URL (eg http://example.com:80/)

https://wp2.nfuse.cloud/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs □ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

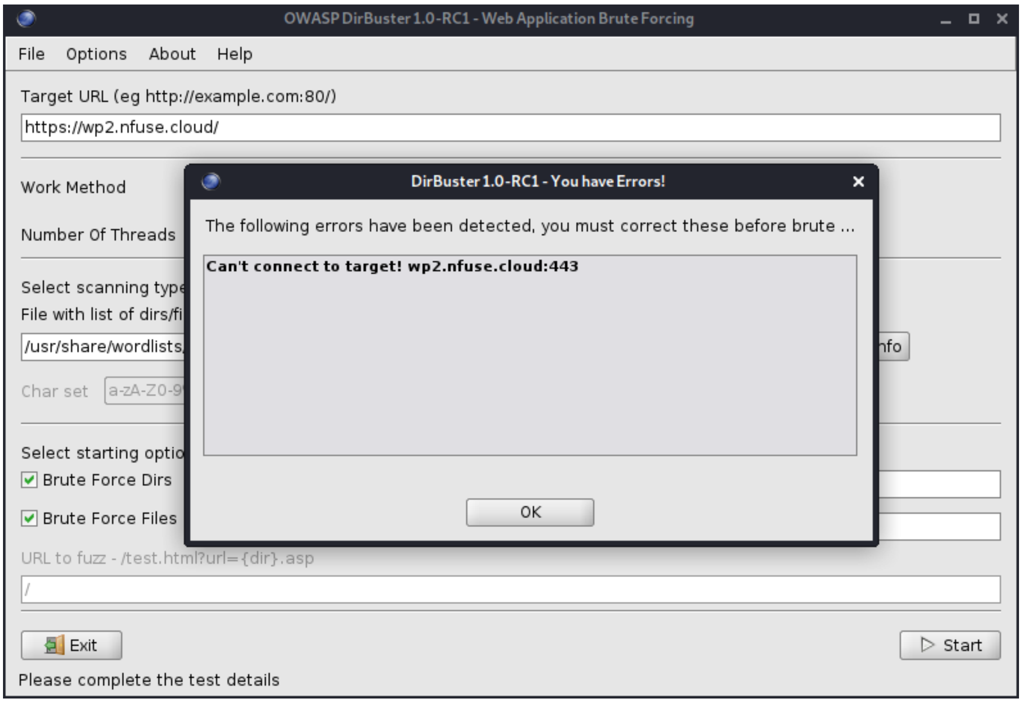
URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details

Figure 27 – Screenshot of Dirbuster settings before scanning

This gives an error saying that it can’t connect to the website. The reason for this could be that a firewall is blocking these requests that are sent with brute force. The firewall can detect a large load of these requests and then block these.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
DirBuster 1.0-RC1 - You have Errors!
OK
Exit
Start

Target URL (eg http://example.com:80/)

https://wp2.nfuse.cloud/

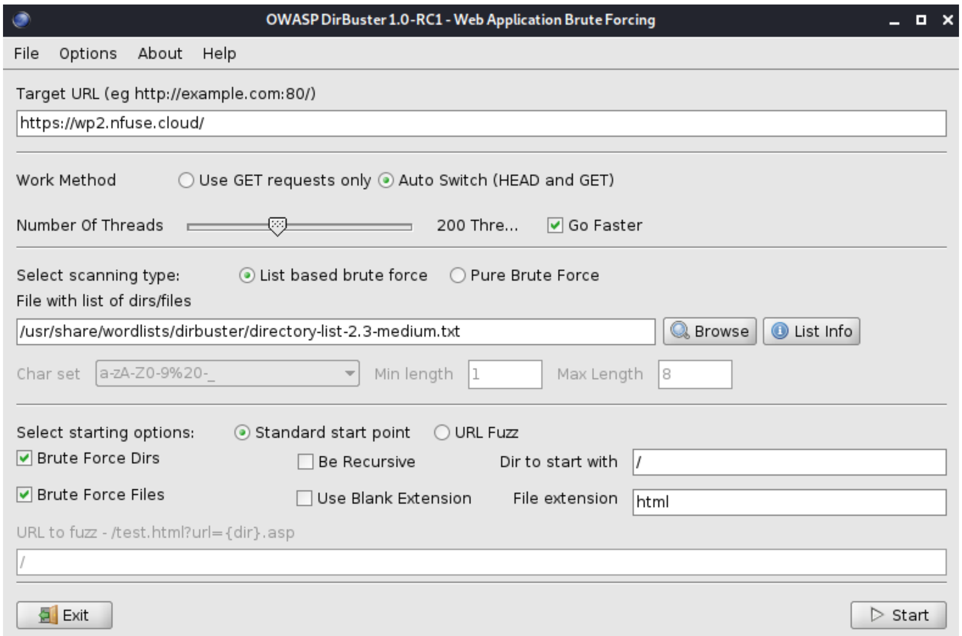
The following errors have been detected, you must correct these before brute ...

```
Can't connect to target! wp2.nfuse.cloud:443
```

Please complete the test details

Figure 28 – Screenshot of Dirbuster error

Now let's scan for HTML files.



Target URL (eg http://example.com:80/)
https://wp2.nfuse.cloud/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

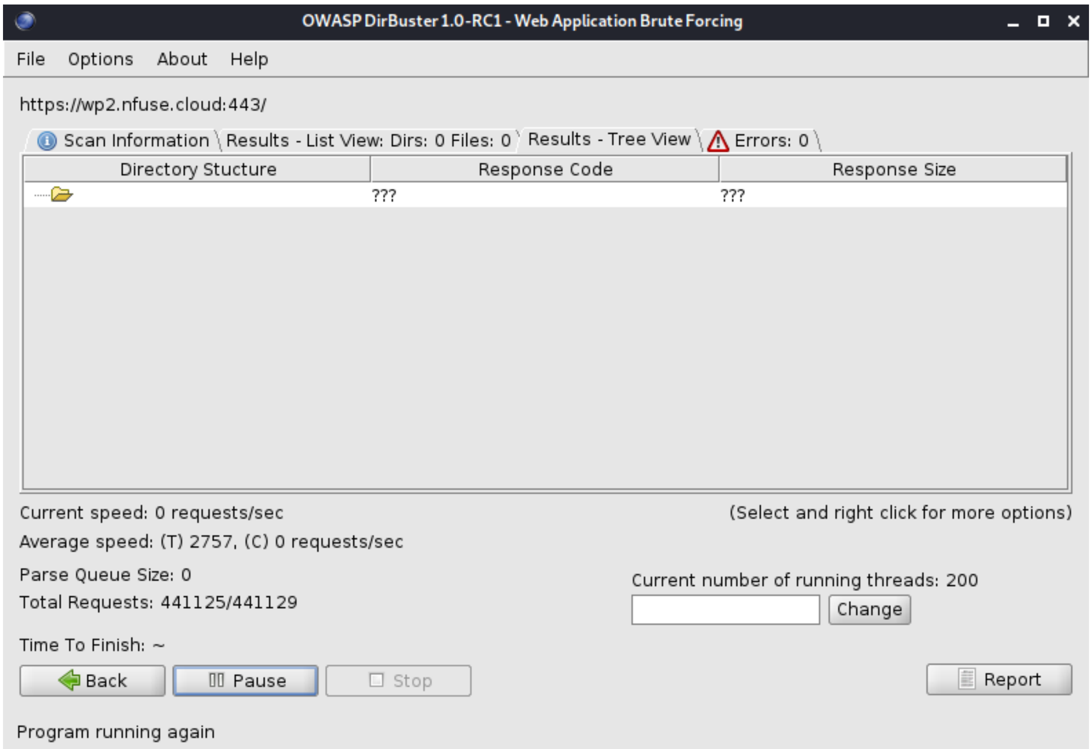
Select scanning type: ● List based brute force ○ Pure Brute Force
File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz
☑ Brute Force Dirs ☐ Be Recursive Dir to start with /
☑ Brute Force Files ☐ Use Blank Extension File extension html
URL to fuzz - /test.html?url={dir}.asp
/

Figure 29 – Screenshot of Dirbuster settings before scanning

This also can't detect any directories or files as you can see below.


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 0 Files: 0
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

https://wp2.nfuse.cloud:443/

Directory Stucture	Response Code	Response Size
	???	???

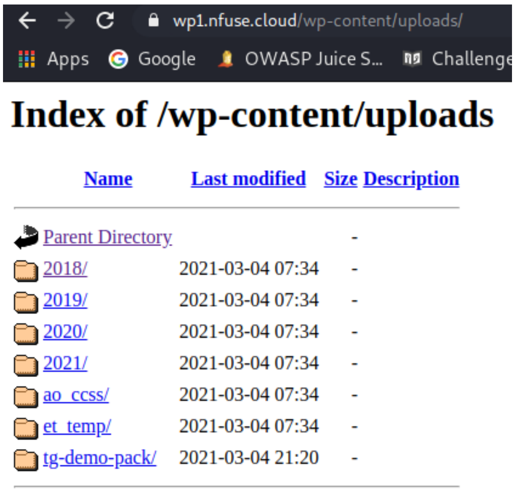
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 2757, (C) 0 requests/sec
Parse Queue Size: 0
Current number of running threads: 200
Total Requests: 441125/441129
Time To Finish: ~
Program running again

Figure 30 – Screenshot of Dirbuster with no directory tree

Directory listing

Previously, when the URL https://wp2.nfuse.cloud/wp-content/uploads/ was visited, a directory listing could be seen of all directories containing files on the server.

First site:

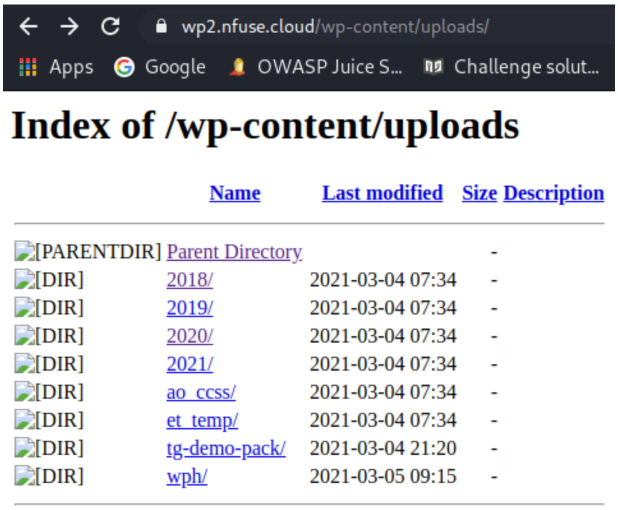


Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2018/	2021-03-04 07:34	-	
2019/	2021-03-04 07:34	-	
2020/	2021-03-04 07:34	-	
2021/	2021-03-04 07:34	-	
ao_ccss/	2021-03-04 07:34	-	
et_temp/	2021-03-04 07:34	-	
tg-demo-pack/	2021-03-04 21:20	-	

Figure 31 - Screenshot of the uploads directory listing in the wp-content directory

Second site:



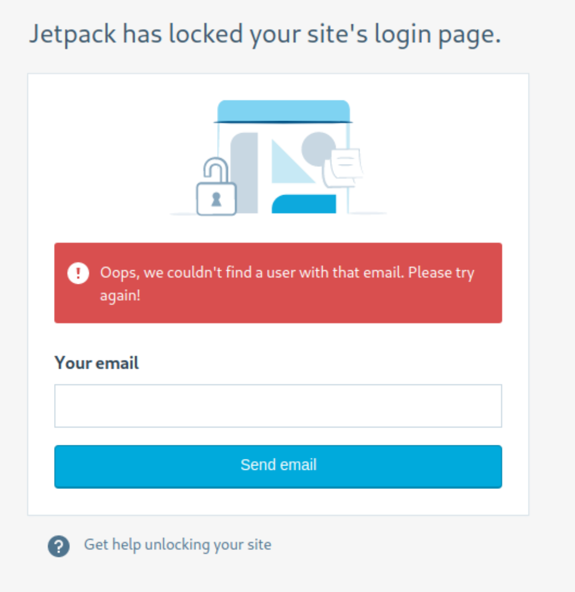
Index of /wp-content/uploads

	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
[DIR]	2018/	2021-03-04 07:34	-	
[DIR]	2019/	2021-03-04 07:34	-	
[DIR]	2020/	2021-03-04 07:34	-	
[DIR]	2021/	2021-03-04 07:34	-	
[DIR]	ao_ccss/	2021-03-04 07:34	-	
[DIR]	et_temp/	2021-03-04 07:34	-	
[DIR]	tg-demo-pack/	2021-03-04 21:20	-	
[DIR]	wph/	2021-03-05 09:15	-	

Figure 32 - Screenshot of the uploads directory listing in the wp-content directory

Now, there's a clear difference in presenting the directories but it's still possible to open files in these directories. The biggest difference is that you can't get an overview of Dirbuster anymore. So, it's much harder to find these directories and files.

The wp-admin login page is locked.



Jetpack has locked your site's login page.

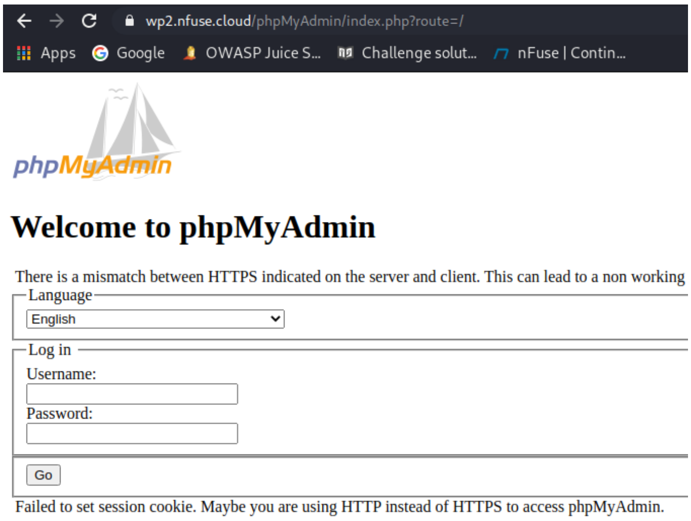
Oops, we couldn't find a user with that email. Please try again!

Your email

Get help unlocking your site

Figure 33 – Screenshot of wp-admin webpage with error

The PhpMyAdmin login page is operational, but there's an HTTPS mismatch and a very different layout.



Welcome to phpMyAdmin

There is a mismatch between HTTPS indicated on the server and client. This can lead to a non working

Language: English

Log in

Username:

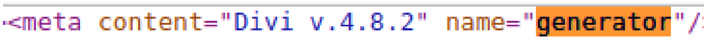
Password:

Failed to set session cookie. Maybe you are using HTTP instead of HTTPS to access phpMyAdmin.

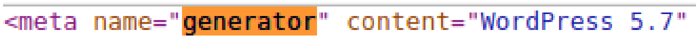
Figure 34 – Screenshot of PhpMyAdmin webpage

Versions

When searched for the word “generator” in the source code the WordPress version 5.7 and the Divi theme v.4.8.2 still can be found. These are more updated versions than the first nFuse site. So, WordPress is up-to-date, but the Divi theme is **outdated** and can still be updated to version 4.9.4.



```
<meta content="Divi v.4.8.2" name="generator"/
```

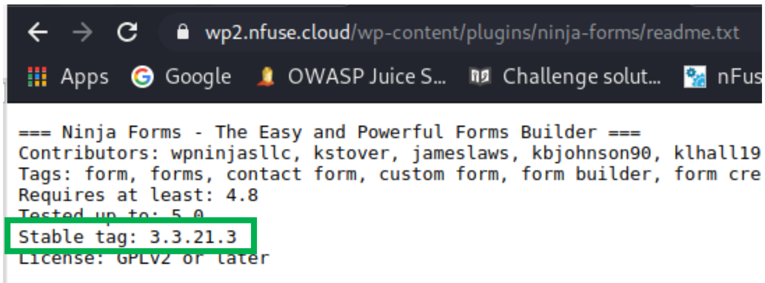


```
<meta name="generator" content="WordPress 5.7"
```

Figure 35 and 36 – Screenshot of source code of the nFuse website

https://wp2.nfuse.cloud/wp-content/plugins/ninja-forms/readme.txt

This URL still presents a readme.txt file that contains the current version of Ninja forms plug-in being 3.3.21.3. This is still an **outdated version** because the newest version is 3.4.24.1.



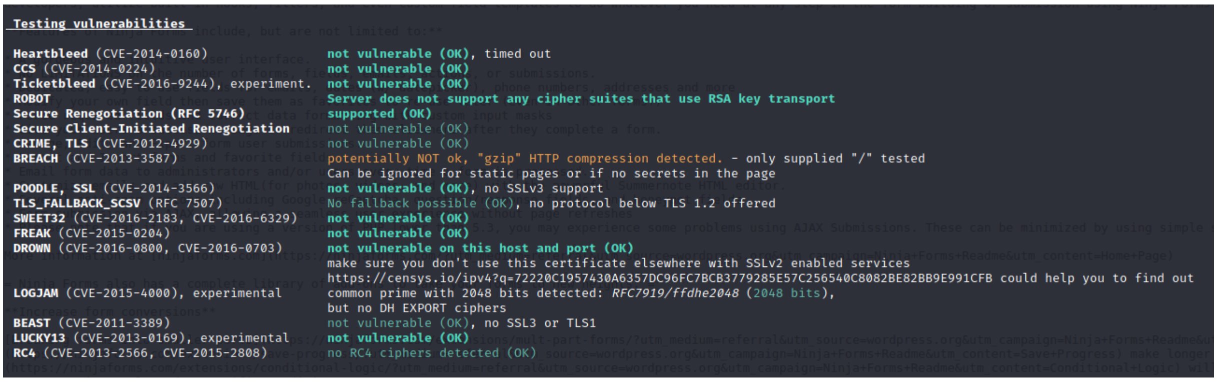
```
=== Ninja Forms - The Easy and Powerful Forms Builder ===
Contributors: wpninjasllc, kstover, jameslaws, kbjohnson90, klhall19
Tags: form, forms, contact form, custom form, form builder, form cre
Requires at least: 4.8
Tested up to: 5.0
Stable tag: 3.3.21.3
License: GPLv2 or later
```

Figure 37 – Screenshot of ninja-forms readme.txt file

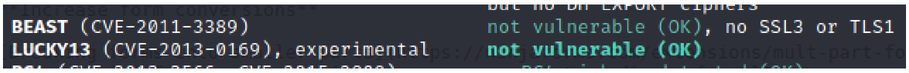
SSL certificate

On the nFuse site 1, there was a Beast and Lucky13 vulnerability found. On the second site, these vulnerabilities aren’t there.

```
sudo testssl.sh 3.250.50.250
```



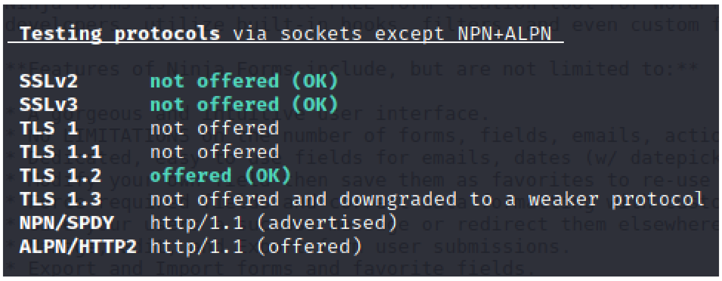
```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), timed out
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     Server does not support any cipher suites that use RSA key transport
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
                                           Can be ignored for static pages or if no secrets in the page
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://censys.io/ipv4?q=72220C1957430A6357DC96FC7BCB3779285E57C256540C8082BE82BB9E991CFB could help you to find out
 LOGJAM (CVE-2015-4000), experimental      common prime with 2048 bits detected: RFC7919/ffdhe2048 (2048 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```



```
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     not vulnerable (OK)
```

Figure 38 and 39 – Screenshots of output TestSSL tool

Something important to notice is that there isn't a TLS 1 or TLS 1.1 version anymore. TLS 1.2 is more secure and will patch these vulnerabilities.



```
 Testing protocols via sockets except NPN+ALPN 

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   http/1.1 (advertised)
 ALPN/HTTP2 http/1.1 (offered)
```

Figure 40 – Screenshot of output TestSSL tool

Conclusion

Security rating

The highest security rating is 9.8 which is critical. It's very important to check all of these vulnerabilities and mitigate them. In this document the most obvious and straightforward vulnerabilities are discussed, so please check the "overview vulnerabilities" to take a look at all vulnerabilities that were found. In the other document "PenTest_nFuse_journey" you can see how all of these are found in chronological order.

To conclude, you have problems to mitigate in your infrastructure and some are easy to fix. If you can mitigate all the found vulnerabilities, you will have a strong environment and website.

Strengths

Using a reverse proxy is your absolute strength, this ensures a secure HTTPS connection. This way it was not easy for me as a hacker to hijack or capture data being sent to your website. After the patch, the Dirbuster tool couldn't find any directories and nmap wasn't able to find as many ports with versions. This is a very good step in the right direction.

Weaknesses

The biggest weakness is having vulnerabilities. As long as you don't fix these, you will have a weak and vulnerable website/server that can be hacked by hackers. Even after the patch of the first site, there were outdated versions. Please update the Divi theme and Ninja-forms plugin.

Bibliography

A, J. (2018). *How To Configure Nginx as a Web Server and Reverse Proxy for Apache on One Ubuntu 18.04 Server*. Retrieved from digitalocean: https://www.digitalocean.com/community/tutorials/how-to-configure-nginx-as-a-web-server-and-reverse-proxy-for-apache-on-one-ubuntu-18-04-server

Abela, R. (2021). *Statistics highlight the biggest source of WordPress vulnerabilities*. Retrieved from wpwhitesecurity: https://www.wpwhitesecurity.com/statistics-highlight-main-source-wordpress-vulnerabilities/

akeeba. (n.d.). *Include data to the backup*. Retrieved from akeeba: https://www.akeeba.com/documentation/akeeba-backup-documentation/include-data-to-archive.html#:~:text=By%20default%2C%20Akeeba%20Backup%20automatically,site's%20root%20for%20increased%20security

alertlogic. (n.d.). *WordPress (CMS) Ninja Forms File Upload Vulnerability*. Retrieved from alertlogic: https://support.alertlogic.com/hc/en-us/articles/115004991226-WordPress-CMS-Ninja-Forms-File-Upload-Vulnerability

Assmann, B. (2020). *HTTP Keep-Alive, Pipelining, Multiplexing and Connection Pooling*. Retrieved from haproxy: https://www.haproxy.com/blog/http-keep-alive-pipelining-multiplexing-and-connection-pooling/

avinetworks. (n.d.). *Reverse Proxy Server*. Retrieved from avinetworks: https://avinetworks.com/glossary/reverse-proxy-server/

Banach, Z. (2020). *How the BEAST Attack Works*. Retrieved from netsparker: https://www.netsparker.com/blog/web-security/how-the-beast-attack-works/

Banach, Z. (2020). *How the BEAST Attack Works*. Retrieved from netsparker: https://www.netsparker.com/blog/web-security/how-the-beast-attack-works/

Banu, S. (2020). *12 WordPress Security Issues (Vulnerabilities) & Tips To Fix Them*. Retrieved from malcare: https://www.malcare.com/blog/wordpress-security-issues/

beyondsecurity. (n.d.). *Finding and Fixing Vulnerabilities in Remote Portmapper Forwards NFS Requests , a High Risk Vulnerability*. Retrieved from beyondsecurity: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-remote-portmapper-forwards-nsf-requests.html

BORGES, E. (2021). *Top 16 Nmap Commands to Scan Remote Hosts - Tutorial Guide*. Retrieved from securitytrails: https://securitytrails.com/blog/nmap-commands

Chamberland, C. (2021). *One Million Sites Affected: Four Severe Vulnerabilities Patched in Ninja Forms*. Retrieved from wordfence: https://www.wordfence.com/blog/2021/02/one-million-sites-affected-four-severe-vulnerabilities-patched-in-ninja-forms/

Chamberland, C. (2021). *One Million Sites Affected: Four Severe Vulnerabilities Patched in Ninja Forms*. Retrieved from wordfence: https://www.wordfence.com/blog/2021/02/one-million-sites-affected-four-severe-vulnerabilities-patched-in-ninja-forms/

cloudflare. (n.d.). *DNS Amplification Attack*. Retrieved from cloudflare: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

CMS. (n.d.). *CMS*. Retrieved from atinternet: https://www.atinternet.com/en/glossary/cms/#:~:text=CMS%20stands%20for%20content%20management,and%2For%20your%20website%20structure

computerhope. (2021). *Linux traceroute command*. Retrieved from computerhope: https://www.computerhope.com/unix/utracero.htm

Corporation, S. (n.d.). *Top 5 SSL Attack Vectors*. Retrieved from muycomputerpro: https://www.muycomputerpro.com/wp-content/uploads/2016/12/symantec-top-five-ssl-uk.pdf

CurlS. (2019). *How to Bypass filtered portmapper port 111 (CTF)*. Retrieved from medium: https://medium.com/@sebnemK/how-to-bypass-filtered-portmapper-port-111-27cee52416bc

cvedetails. (n.d.). *Ninja Forms : Security Vulnerabilities*. Retrieved from cvedetails: https://www.cvedetails.com/vulnerability-list/vendor_id-15289/product_id-31215/Ninjaforms-Ninja-Forms.html

cvedetails. (n.d.). *Vulnerability Details : CVE-2010-2305 (1 public exploit)*. Retrieved from cvedetails: https://www.cvedetails.com/cve/CVE-2010-2305/

cvedetails. (n.d.). *Vulnerability Details : CVE-2014-6271*. Retrieved from cvedetails: https://www.cvedetails.com/cve/CVE-2014-6271/

cvedetails. (n.d.). *Vulnerability Details : CVE-2014-7228 (1 Metasploit modules)*. Retrieved from cvedetails: https://www.cvedetails.com/cve/CVE-2014-7228/

cybersecurity-help. (2020). *Cross-site request forgery in Ninja Forms Contact Form – The Drag and Drop Form Builder for WordPress plugin*. Retrieved from cybersecurity-help: https://www.cybersecurity-help.cz/vdb/SB2020043017

DRD_. (2018). *Exploit Shellshock on a Web Server Using Metasploit*. Retrieved from wonderhowto: https://null-byte.wonderhowto.com/how-to/exploit-shellshock-web-server-using-metasploit-0186084/

Essentials, A. (n.d.). *Penetration Testing*. Retrieved from imperva: https://www.imperva.com/learn/application-security/penetration-testing/#:~:text=A%20penetration%20test%2C%20also%20known,web%20application%20firewall%20(WAF)

exploit-db. (2021). *WordPress Plugin Ninja Forms 3.3.17 - Cross-Site Scripting*. Retrieved from exploit-db: https://www.exploit-db.com/exploits/45880

exploit-db. (n.d.). *WordPress Core 2.0 - 'wp-register.php' Multiple Cross-Site Scripting Vulnerabilities*. Retrieved from exploit-db: https://www.exploit-db.com/exploits/30602

Feoktistov, I. (n.d.). *Guide to Web Application Penetration Testing*. Retrieved from relevant.software: https://relevant.software/blog/penetration-testing-for-web-applications/

first. (n.d.). *Common Vulnerability Scoring System version 3.1: Specification Document*. Retrieved from first: https://www.first.org/cvss/examples

Gall, R. (2020). *High Severity Vulnerability Patched in Ninja Forms*. Retrieved from wordfence: https://www.wordfence.com/blog/2020/04/high-severity-vulnerability-patched-in-ninja-forms/

Gall, R. (2020). *High Severity Vulnerability Patched in Ninja Forms*. Retrieved from wordfence: https://www.wordfence.com/blog/2020/04/high-severity-vulnerability-patched-in-ninja-forms/

Glauser, R. (2018). *The Top 7 Vulnerabilities of the Decade*. Retrieved from vulcan: https://vulcan.io/blog/top-7-vulnerabilities/

Glauser, R. (2018). *The Top 7 Vulnerabilities of the Decade*. Retrieved from vulcan: https://vulcan.io/blog/top-7-vulnerabilities/

guru99. (2021). *40 Best Penetration Testing (Pen Test) Vapt Tools in 2021*. Retrieved from guru99: https://www.guru99.com/top-5-penetration-testing-tools.html

HackerOne. (n.d.). *Pentest Reporting and Best Practices*. Retrieved from youtube: https://www.youtube.com/watch?v=6QIrXgPGJhM

hackertarget. (2009). *Nmap Cheat Sheet*. Retrieved from hackertarget: https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

hacktricks. (n.d.). *111/TCP/UDP - Pentesting Portmapper*. Retrieved from hacktricks: https://book.hacktricks.xyz/pentesting/pentesting-rpcbind

Heckel, P. C. (2013). *How To: Use mitmproxy to read and modify HTTPS traffic*. Retrieved from heckel: https://blog.heckel.io/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/#:~:text=Mitmproxy%20is%20an%20open%20source,%2Dmiddle%20attack%20(MITM)

hidemywp. (n.d.). *What Hide My WP Ghost can do for you?* Retrieved from hidemywp: https://hidemywp.co/security-features/

HollyGraceful. (2015). *Bypass RPC Portmapper Filtering*. Retrieved from gracefulsecurity: https://gracefulsecurity.com/bypass-rpc-portmapper-filtering/

hrushikeshk. (2018). *Enumeration tools*. Retrieved from hkh4cks: https://hkh4cks.com/blog/2018/01/22/common-enumeration-tools/

Imam, F. (2020). *Top 10 security awareness training topics for your employees [updated 2020]*. Retrieved from infosecinstitute: https://resources.infosecinstitute.com/topic/top-10-security-awareness-training-topics-for-your-employees/

kali. (n.d.). *SSLyze Package Description*. Retrieved from kali: https://tools.kali.org/information-gathering/sslyze

Keshri, A. (2020). *[Plugin+Manual method] How to Hide WordPress Version Number in Your Website?* Retrieved from getastra: https://www.getastra.com/blog/cms/wordpress-security/how-to-hide-wordpress-version-number/

Kili, A. (2017). *How to Hide Apache Version Number and Other Sensitive Info*. Retrieved from tecmint: https://www.tecmint.com/hide-apache-web-server-version-information/

kinsta. (2021). *How to Check Your WordPress Version (4 Methods)*. Retrieved from kinsta: https://kinsta.com/knowledgebase/check-wordpress-version/

Kody. (2020). *Use Ettercap to Intercept Passwords with ARP Spoofing*. Retrieved from wonderhowto: https://null-byte.wonderhowto.com/how-to/use-ettercap-intercept-passwords-with-arp-spoofing-0191191/

Lewis, P. (2018). *WordPress: Best Practices on AWS*. Retrieved from amazon: https://aws.amazon.com/blogs/architecture/wordpress-best-practices-on-aws/

Lowrie, D. (2020). *HOW TO CREATE A PENETRATION TEST REPORT*. Retrieved from itpro: https://blog.itpro.tv/how-to-create-a-penetration-test-report/

MadHatter. (2018). *Crunch: using -d 1, -d 1% options with first two chars DD*. Retrieved from superuser: https://superuser.com/questions/1321206/crunch-using-d-1-d-1-options-with-first-two-chars-dd

Maurya, H. (2021). *How to install Zenmap Nmap GUI on Ubuntu 20.04 LTS*. Retrieved from how2shout: https://www.how2shout.com/linux/install-zenmap-nmap-gui-on-ubuntu-20-04-lts-linux/

McCollin, R. (2021). *A Complete Guide on xmlrpc.php in WordPress (What It Is, Security Risks, How to Disable It)*. Retrieved from kinsta: https://kinsta.com/blog/xmlrpc-php/

Nasser, H. (2020). *DNS Reflection Attack Explained*. Retrieved from youtube: https://www.youtube.com/watch?v=S6hZcxM3Sz4

NetworkChuck. (2020). *how Hackers SNiFF (capture) network traffic // MiTM attack*. Retrieved from youtube: https://www.youtube.com/watch?v=-rSqbgI7oZM

nist. (n.d.). *CVE-2018-10846 Detail*. Retrieved from nist: https://nvd.nist.gov/vuln/detail/CVE-2018-10846

nist. (n.d.). *CVE-2018-19935 Detail*. Retrieved from nist: https://nvd.nist.gov/vuln/detail/CVE-2018-19935

nist. (n.d.). *Vulnerability Metrics*. Retrieved from nist: https://nvd.nist.gov/vuln-metrics/cvss

nmap. (n.d.). *Chapter 11. Defenses Against Nmap*. Retrieved from nmap: https://nmap.org/book/defenses.html

offensive-security. (n.d.). *INTRODUCTION TO METASPLOIT*. Retrieved from offensive-security: https://www.offensive-security.com/metasploit-unleashed/introduction/

One, H. (2017). *I Used Phishing To Get My Colleagues' Passwords. This Is What I Did.* Retrieved from medium: https://medium.com/hike-one-digital-product-design/how-i-used-phishing-to-get-my-colleagues-passwords-this-is-how-i-did-it-73b9215689f1

pentasecurity. (2016). *Reflection Attacks and Amplification Attacks*. Retrieved from pentasecurity: https://www.pentasecurity.com/blog/reflection-attacks-amplification-attacks/

portswigger. (n.d.). *Using Burp Intruder*. Retrieved from portswigger: https://portswigger.net/burp/documentation/desktop/tools/intruder/using

Poston, H. (2020). *What are Black Box, Grey Box, and White Box Penetration Testing? [Updated 2020]*. Retrieved from infosecinstitute: https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/#:~:text=A%20black%2Dbox%20penetration%20test,systems%20within%20the%20target%20network

RAMADHAN, B. F. (2017). *Crack Web Based Login Page With Hydra in Kali Linux*. Retrieved from linuxhint: https://linuxhint.com/crack-web-based-login-page-with-hydra-in-kali-linux/

rapid7. (2018). *Portmapper Amplification Scanner*. Retrieved from rapid7: https://www.rapid7.com/db/modules/auxiliary/scanner/portmap/portmap_amp/

rapid7. (n.d.). *PHP Vulnerability: CVE-2020-7070*. Retrieved from rapid7: https://www.rapid7.com/db/vulnerabilities/php-cve-2020-7070/

rapid7. (n.d.). *WordPress Ninja Forms Unauthenticated File Upload*. Retrieved from rapid7: https://www.rapid7.com/db/modules/exploit/multi/http/wp_ninja_forms_unauthenticated_file_upload/

Ravoof, S. (2021). *Zo zet je een reverse proxy op (stap-voor-stap voor Nginx en Apache)*. Retrieved from kinsta: https://kinsta.com/nl/blog/reverse-proxy/

Ravoof, S. (2021). *Zo zet je een reverse proxy op (stap-voor-stap voor Nginx en Apache)*. Retrieved from kinsta: https://kinsta.com/nl/blog/reverse-proxy/

Ray, J. (n.d.). *How to Hide or Remove WordPress Version Number*. Retrieved from wpmyweb: https://www.wpmyweb.com/how-to/remove-wordpress-version.html#:~:text=function%20remove_wordpress_version()%20%7B%20return%20'',from%20the%20header%20and%20RSS

S, G. (2018). *Fast and Complete SSL Scanner to Find Mis-configurations affecting TLS/SSL Severs-A Detailed Analysis*. Retrieved from gbhackers: https://gbhackers.com/fast-and-complete-ssl-scanner-to-find-mis-configurations-affecting-tlsssl-severs-a-detailed-analysis/

Segal, E. (2020, 05). *Understanding Vulnerability Scoring: CVSS Explained*. Retrieved from securityboulevard: https://securityboulevard.com/2020/05/understanding-vulnerability-scoring-cvss-explained/#:~:text=CVSS%20is%20a%20set%20of,the%20most%20critical%20vulnerability%20level.

Shacklett, M. E. (2021). *attack vector* . Retrieved from techtarget: https://searchsecurity.techtarget.com/definition/attack-vector

softwaretestinghelp. (2021). *OWASP ZAP Tutorial: Comprehensive Review Of OWASP ZAP Tool*. Retrieved from softwaretestinghelp: https://www.softwaretestinghelp.com/owasp-zap-tutorial/

Staff, E. (2014). *How to Disable Directory Browsing in WordPress*. Retrieved from wpbeginner: https://www.wpbeginner.com/wp-tutorials/disable-directory-browsing-wordpress/

Teeman, B. (n.d.). *Restoring a Site on Any Server*. Retrieved from akeeba: https://www.akeeba.com/videos/1212-akeeba-backup/1618-abtc04-restore-site-new-server.html

TemplateLab. (n.d.). *24 Simple Confidentiality Statement & Agreement Templates*. Retrieved from TemplateLab: https://templatelab.com/confidentiality-statements/

Threats, A. (n.d.). *Clickjacking*. Retrieved from imperva: https://www.imperva.com/learn/application-security/clickjacking/#:~:text=Clickjacking%20is%20an%20attack%20that,money%2C%20or%20purchase%20products%20online

w3. (n.d.). *Persistent Connections*. Retrieved from w3: https://www.w3.org/Protocols/rfc2616/rfc2616-sec8.html

w3schools. (n.d.). *SQL Injection*. Retrieved from w3schools: https://www.w3schools.com/sql/sql_injection.asp

wchen-r7. (2016). *wp_ninja_forms_unauthenticated_file_upload cannot find the nonce when the ninja form version is not vulnerable #7022*. Retrieved from github: https://github.com/rapid7/metasploit-framework/issues/7022

WebsitePolicies. (2021). *Sample Disclaimer Template and Examples*. Retrieved from WebsitePolicies: https://www.websitepolicies.com/blog/sample-disclaimer-template

Whittle, M. (2020). *Ethical Hacking (Part 9): DNS Hijacking & Credential Harvesting*. Retrieved from gitconnected: https://levelup.gitconnected.com/ethical-hacking-part-9-dns-hijacking-credential-harvesting-db57302e5131

wikipedia. (2017). *Portmap*. Retrieved from wikipedia: https://en.wikipedia.org/wiki/Portmap#:~:text=portmap%20or%20just%20portmap%2C%20or,that%20version%20of%20that%20program

Wilson, B. (2021). *How to Tell Which WordPress Plugins a Website Uses*. Retrieved from winningwp: https://winningwp.com/how-to-tell-which-plugins-a-website-uses/

Wong, D. (2017). *BEAST: An Explanation of the CBC Attack on TLS*. Retrieved from youtube: https://www.youtube.com/watch?v=-_8-2pDFvmg

wordpress. (n.d.). *Hide My WP Ghost – Security Plugin*. Retrieved from wordpress: https://nl.wordpress.org/plugins/hide-my-wp/

wppluginchecker. (n.d.). *WordPress Plugin Checker*. Retrieved from wppluginchecker: http://wppluginchecker.earthpeople.se/?wordpress-site=https%3A%2F%2Fwp1.nfuse.cloud%2F

WRIGHT, K. (2020). *5 Common WordPress Security Issues*. Retrieved from ithemes: https://ithemes.com/wordpress-security-issues/

WRIGHT, K. (2021). *5 Common WordPress Security Issues*. Retrieved from wpwhitesecurity: https://www.wpwhitesecurity.com/statistics-highlight-main-source-wordpress-vulnerabilities/

youngzsoft. (n.d.). *A brief introduction to most popular proxy server software*. Retrieved from youngzsoft: https://www.youngzsoft.net/ccproxy/proxy-server-softwares.htm

Zayzay, R. (2018). *Install WordPress on Ubuntu 16.04 LTS with Apache2, MariaDB and PHP 7.1 Support*. Retrieved from websiteforstudents: https://websiteforstudents.com/install-wordpress-on-ubuntu-16-04-lts-with-apache2-mariadb-and-php-7-1-support/