**Afbeelding met tekst, Lettertype, geel, Graphics

Automatisch gegenereerde beschrijving16/05/2024 Fontys Hogescholen ben.vanderlinden@student.fontys.nl**

**Afbeelding met tekst, Lettertype, geel, Graphics

Automatisch gegenereerde beschrijving**

**Penetratietest rapport  
Hogeschool Fontys – Onderwijsstichting Triade**13 t/m 15 mei 2024

**Uitvoerders**

Andrew Fleetwood-Bird

Ben van der Linden

Bogdan Nikolov

Khaled Ali

Reuel Dooren

Roan Kessels

Contents

[1. Inleiding 2](#_Toc167359841)

[2. Key finds 3](#_Toc167359842)

1. [2.1 LOW SEVERITY 3](#_Toc167359843)
2. [2.2 MEDIUM SEVERITY 4](#_Toc167359844)
3. [2.3 Risk matrix 6](#_Toc167359845)

[3. Phishing campagne 7](#_Toc167359846)

[4. Appendix 8](#_Toc167359847)

1. [4.1 Tooling 8](#_Toc167359848)
2. [4.2 Ons team 9](#_Toc167359849)

## 1. Inleiding

Dit rapport presenteert de bevindingen en analyse van een penetratietest uitgevoerd op Onderwijsstichting Triade. De doelstelling van deze penetratietest was om de veiligheidsmaatregelen van het IT-infrastructuurnetwerk, applicaties en systemen van Triade te evalueren en kwetsbaarheden te identificeren die kunnen worden misbruikt door kwaadwillende “hackers”. Het onderzoek werd uitgevoerd door Andrew, Ben, Bogdan, Khaled, Reuel en Roan, gedurende de periode 13 t/m 15 mei 2024.

De penetratietest omvatte een grondige analyse van zowel externe als interne systemen, met een focus op het identificeren van zwakke plekken in de beveiligingsinfrastructuur. Methoden zoals vulnerability scanning, manuele kwetsbaarheidsanalyse, penetratietests en social engineering werden toegepast om de algehele veiligheid van het netwerk en de applicaties te beoordelen.

Dit rapport bevat een samenvatting van de ontdekte kwetsbaarheden, gerangschikt op basis van hun ernst, samen met aanbevelingen voor het verhelpen van de geïdentificeerde zwakke punten. Het doel van deze bevindingen is om Triade te voorzien van inzichten die kunnen helpen bij het verbeteren van de algehele beveiliging en het versterken van de verdediging tegen potentiële cyberdreigingen.

We danken Triade voor de fijne samenwerking tijdens deze penetratietest. We hopen dat dit rapport een waardevolle bijdrage zal leveren aan het versterken van de beveiligingsmaatregelen.

## 2. Key finds

### 2.1 LOW SEVERITY

#### 2.1.1 Denial of Service via XML-RPC (DDoS)

Een DDoS-aanval via XML-RPC (Remote Procedure Call) maakt gebruik van een protocol dat door veel content managementsystemen (CMS) zoals WordPress wordt ondersteund. Het XML-RPC-protocol biedt functies voor communicatie met de CMS, zoals het plaatsen van berichten en uitvoeren van andere handelingen op afstand.

Hoe een DDoS-aanval via XML-RPC werkt:

**Misbruik van de** system.multicall **functie:** Dit is een van de meest misbruikte functies binnen XML-RPC. Het stelt aanvallers in staat om meerdere commando's in één enkele HTTP-verzoek te bundelen. Hierdoor kunnen aanvallers een groot aantal verzoeken in een zeer korte tijd versturen, wat de server kan overbelasten.

**Amplification Attacks:** Aanvallers kunnen de XML-RPC-interface gebruiken om een groot aantal verzoeken naar een doelwit te sturen, wat resulteert in een DDoS-aanval. Deze methode wordt vaak gebruikt om de server te overspoelen met verkeer, waardoor deze traag wordt of zelfs crasht.

**Ontwijken van Cloudflare via WordPress Pingbacks**

**Context:** Cloudflare is een populaire webbeveiligings- en prestatieoplossing die websites beschermt tegen verschillende soorten aanvallen door als een tussenpersoon tussen de gebruiker en de webserver te fungeren. Soms willen aanvallers echter de originele IP-adressen van servers achter Cloudflare ontdekken om aanvallen direct op de server uit te voeren, zonder tussenkomst van Cloudflare.

**Pingbacks in WordPress:** Pingbacks zijn een WordPress-functie die gebruikt wordt om blogs op de hoogte te stellen wanneer andere blogs naar hun inhoud linken. Dit werkt door middel van XML-RPC verzoeken die tussen WordPress-sites worden verzonden.

**Proof of Concept**

1. Controleer XML-RPC

Bevestig dat **xmlrpc.php** toegankelijk is op de doelwebsite

Bijvoorbeeld: <https://stichtingtriade.nl/xmlrpc.php>

In dit voorbeeld kun je zien dat Cloudflare een error gooit laten we Cloudflare omzeilen.

1. Stuur het Pingback-verzoek

Gebruik een tool zoals Burp suite om een XML-RPC-pingback-verzoek te sturen:

A screenshot of a computer program

Description automatically generated

Vang het request naar **/xmlrpc.php** op via de burp proxy en verander het naar een post request en voeg de code toe die in de screenshot te zien is.

Verander attackersite naar een webserver waar je de response op wil ontvangen.

1. Inspecteer de Verzoeken

Controleer de logs van attackersite.com om het inkomende verzoek van de doelserver te zien en noteer het IP-adres.

#### 2.1.2 Publieke Wordpress RESTAPI

#### Gevolgen van een Publieke WordPress REST API

**Gevoeligheid voor Data Lekken**:

De standaardinstellingen van de WordPress REST API kunnen gevoelige informatie onthullen, zoals gebruikersnamen, post metadata, en custom endpoints. Dit kan worden misbruikt door aanvallers.

**Brute Force Aanvallen**:

Publieke toegang tot de REST API kan brute force aanvallen op inlogpagina’s en endpoints bevorderen. Aanvallers kunnen proberen inloggegevens te raden of misbruik maken van de API voor andere kwaadaardige activiteiten.

**Overbelasting van de Server**:

Een ongecontroleerde REST API kan leiden tot een hoge belasting van de server als gevolg van een groot aantal verzoeken, wat de prestaties van je website kan verminderen.

**Exploits via Kwetsbaarheden**:

Onvoldoende beveiligde API's kunnen kwetsbaar zijn voor exploits zoals SQL-injectie, XSS-aanvallen en andere vormen van kwaadwillige activiteiten.

Verbeteringen voor de Veiligheid van de REST API

**Authenticatie en Autorisatie**:

Zorg ervoor dat alleen geautoriseerde gebruikers toegang hebben tot gevoelige endpoints door gebruik te maken van authenticatiemechanismen zoals OAuth, JWT (JSON Web Tokens), of API-sleutels.

**Beperk API-toegang**:

Gebruik plugins zoals "Disable REST API" om de toegang tot de REST API te beperken voor niet-ingelogde gebruikers. Hiermee kun je de API volledig uitschakelen voor anonieme gebruikers of toegang alleen toestaan voor bepaalde gebruikersrollen.

**Whitelisting van IP-adressen**:

Beperk de toegang tot de API door alleen specifieke IP-adressen toe te staan. Dit kan helpen om de API te beschermen tegen ongeautoriseerde toegang.

**Gebruik van Caching**:

Implementeer caching voor API-verzoeken om de belasting op de server te verminderen. Plugins zoals "WP REST Cache" kunnen hierbij helpen.

**Rate Limiting**:

Beperk het aantal verzoeken dat een gebruiker of een IP-adres binnen een bepaalde tijdsperiode kan doen. Dit voorkomt misbruik van de API en beschermt tegen brute force-aanvallen.

**Monitoren van API-verkeer**:

Houd het verkeer van de REST API in de gaten om verdachte activiteiten snel te detecteren. Gebruik logging- en monitoringtools om een overzicht te krijgen van wie de API gebruikt en hoe vaak.

**Regelmatige Updates en Patching**:

Zorg ervoor dat je WordPress-installatie, thema’s, en plugins altijd up-to-date zijn om beveiligingslekken te dichten die misbruikt kunnen worden via de API.

**SIDE NOTE**

Dit is een hele simpele fix, er zijn genoeg plugins die dit automatisch regelen met thema’s daarom is dit een low severity. Een goede wordpress plugin hiervoor installeren zal deze kwetsbaarheid meteen oplossen.

**Proof of Concept**

Voorbeeld: <https://stichtingtriade.nl/wp-json/wp/v2>

A screenshot of a computer

Description automatically generated

### 2.2 MEDIUM SEVERITY

#### 2.2.1 Weinig tot geen brute force protectie.

**Wat is een Brute-Force Aanval?** Een brute-force aanval is een poging van een aanvaller om toegang te krijgen tot een systeem door herhaaldelijk verschillende combinaties van gebruikersnamen en wachtwoorden te proberen totdat de juiste combinatie is gevonden. Dit kan worden gedaan met behulp van geautomatiseerde tools die duizenden tot miljoenen inlogpogingen per seconde kunnen uitvoeren.

**Preventie van Brute-Force Aanvallen op WordPress:**

1. **Sterke Wachtwoorden en Unieke Gebruikersnamen:**

* Gebruik complexe en lange wachtwoorden die moeilijk te raden zijn.
* Vermijd het gebruik van standaardgebruikersnamen zoals "admin".

1. **Loginpogingen Beperken:**

* Installeer een plugin zoals "Limit Login Attempts Reloaded" die het aantal inlogpogingen per IP-adres beperkt. Na een bepaald aantal mislukte pogingen wordt het IP-adres tijdelijk geblokkeerd.

1. **Tweefactorauthenticatie (2FA):**

* Voeg een extra beveiligingslaag toe door tweefactorauthenticatie in te schakelen. Dit vereist naast het wachtwoord ook een tweede verificatiemethode, zoals een SMS-code of een authenticatie-app.

1. **CAPTCHA Implementeren:**

* Gebruik CAPTCHA's op het inlogscherm om te verifiëren dat de inlogpogingen door mensen en niet door geautomatiseerde bots worden uitgevoerd.

1. **Beveiligingsplugins:**

* Installeer beveiligingsplugins zoals "Wordfence Security" of "iThemes Security" die uitgebreide bescherming bieden tegen brute-force aanvallen en andere beveiligingsrisico's.

1. **Verberg Login URL:**

* Verander de standaard login-URL van **/wp-admin** of **/wp-login.php** naar iets minder voorspelbaars met behulp van plugins zoals "WPS Hide Login".

Door deze maatregelen te implementeren, kan je de kans op een succesvolle brute-force aanval op je WordPress-website aanzienlijk verminderen en de algehele beveiliging verbeteren.

#### 2.2.2 Username enumeratie Wordpress

**Wat is Username Enumeratie?**

Username enumeratie is een techniek waarbij een aanvaller probeert geldige gebruikersnamen van een website te achterhalen. Dit kan worden gedaan door verschillende methoden, zoals het gebruik van de WordPress REST API, auteur archiefpagina's, of foutmeldingen bij het inloggen. Zodra een aanvaller geldige gebruikersnamen heeft verzameld, kunnen deze worden gebruikt voor verdere aanvallen, zoals brute-force aanvallen.

**Preventie van Username Enumeratie op WordPress:**

1. **Beperk Toegang tot de REST API:**

* Stel de REST API zo in dat deze alleen toegankelijk is voor geauthenticeerde gebruikers, of gebruik een plugin zoals "Disable REST API" om ongeautoriseerde toegang te blokkeren.

**Proof Of Concept:**

<https://bsdedriesprong.nl/wp-json/wp/v2>

End-points zoals **/user** en **/pages** kunnen heel interessant zijn voor aanvallers.

/users geeft namelijk de users van de WordPress website weer en /pages kan ip’s van de server lekken.

A screenshot of a computer

Description automatically generated

1. **Verberg Gebruikersnamen in URL's:**

* Verberg de gebruikersnamen die in de URL van auteur archiefpagina's worden weergegeven. Dit kan worden gedaan met behulp van plugins zoals "Edit Author Slug".

**Proof Of Concept:**

<http://bsdedriesprong.nl/?author=1>  
Als je op deze link klikt zie je dat de URL in de zoekbalk veranderd naar de gebruikersnaam die ID 1 heeft.

A screenshot of a computer

Description automatically generated

1. **Gebruik Plugins voor Extra Beveiliging:**

* Installeer beveiligingsplugins zoals "WP Hide & Security Enhancer" of "iThemes Security" die specifieke instellingen bieden om username enumeratie te voorkomen.

1. **Aanpassen van Foutmeldingen bij Inloggen:**

* A screenshot of a computer

  Description automatically generatedA screenshot of a computer

  Description automatically generatedZorg ervoor dat foutmeldingen bij mislukte inlogpogingen niet onthullen of de gebruikersnaam correct was. Dit kan worden aangepast door code aan je **functions.php** toe te voegen of door een beveiligingsplugin te gebruiken.

1. **Verberg Auteur Archieven:**

* Schakel auteur archiefpagina's uit als ze niet nodig zijn, of beperk de toegang ertoe. Dit kan via de instellingen van je thema of door een beveiligingsplugin.

1. **Gebruik van Custom Login URL:**

* Verander de standaard login-URL om het voor aanvallers moeilijker te maken om toegangspunten voor username enumeratie te vinden. Dit kan worden gedaan met plugins zoals "WPS Hide Login".

### 2.3 Risk matrix

|  |  |
| --- | --- |
| **Notities over WordPress login** | |
| Ontbrekende Multifactor-Authenticatie | Risico notitie |
| Ontbrekende CAPTCHA Verificatie | Risico notitie |
| Geen limiet op aantal inlogpogingen | Risico notitie |
| Default WordPress login URL  **/wp-login.php** | Risico notitie |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kwetsbaarheid** | **Waarschijnlijkheid** | **Impact** | **Risico** | **Aanbeveling** |
| 3.1.1 Denial of Service (DDoS) | Laag | Laag | Matig | Schakel XML-RPC uit als dit niet nodig is. Gebruik anders een plugin om het aantal verzoeken naar dit eindpunt te beperken. |
| 3.1.2 WP-Json is Publiek | Matig | Matig | Matig | Installeer een plugin die toegang tot de REST API verbiedt |
| 3.2.1 WordPress Username Enumeratie | Medium | Medium | Medium | Implementeer maatregelen om username enumeratie te voorkomen, zoals het wijzigen van responsberichten voor ongeldige inlogpogingen en het beperken van de toegang tot auteur archieven. |
| 3.2.2 Wordpress Login Bruteforce | Medium | Medium | Medium | Implementeer beveiligingsmaatregelen zoals het beperken van het aantal inlogpogingen, CAPTCHA's en tweefactorauthenticatie (2FA) om brute force-aanvallen te voorkomen. |

## 3. Phishing campagne

A screenshot of a computer screen

Description automatically generated

A screenshot of a dashboard

Description automatically generated

Zoals je kan zijn zijn er 10 mensen geweest die hebben geklikt op de email. Gelukkig heeft niemand zijn of haar wachtwoord en email ingegeven.

Op links klikken kan soms net zo slecht zijn, deze test was alleen om te kijken of mensen hun gegevens in zouden vullen. Een kwaadaardige aanvaller zou ook de link kunnen infecteren met malware wat meteen uitgevoerd wordt als er op de link geklikt wordt. Klik dus nooit op links die er vreemd uitzien of van een onbekende afzender komt.

## 4. Appendix

### 4.1 Tooling

De “main” tools die we gebruikt hebben tijdens deze penetratietest.

#### Burp Suite

**Burp Suite** is een platform voor het testen van webapplicatiebeveiliging. Het biedt een reeks tools, zoals een proxyserver, scanner, en intruder, die kunnen worden gebruikt voor het identificeren en exploiteren van beveiligingslekken.

#### Burp Proxy

**Burp Proxy** is een onderdeel van Burp Suite. Het werkt als een man-in-the-middle proxy, waarmee testers HTTP/S-verzoeken tussen de client (meestal een browser) en de server kunnen onderscheppen, inspecteren en aanpassen. Dit is handig voor het analyseren en manipuleren van webverkeer tijdens penetratietests.

#### Nmap

**Nmap (Network Mapper)** is een gratis en open-source netwerk-scanner. Het wordt gebruikt voor netwerkontdekking en beveiligingsaudits. Nmap kan hosts en diensten op een computernetwerk identificeren door verschillende soorten scans, zoals TCP, SYN, en UDP, uit te voeren.

#### SQLMap

**SQLMap** is een open-source penetratietesttool die geautomatiseerd SQL-injectie aanvallen uitvoert. Het ondersteunt een breed scala aan databases en kan gebruikt worden om database-informatie te extraheren, gegevens te dumpen en soms zelfs een shell te verkrijgen.

#### WPScan

**WPScan** is een beveiligingsscanner specifiek voor WordPress-sites. Het detecteert kwetsbaarheden in geïnstalleerde thema's, plugins, en de WordPress-core zelf. WPScan maakt gebruik van een uitgebreide database van bekende kwetsbaarheden.

#### Gophish

**Gophish** is een open-source phishing toolkit. Het wordt gebruikt om phishing campagnes te plannen, uit te voeren en te beheren. Gophish biedt een gebruikersvriendelijke interface voor het creëren van phishing e-mails en het volgen van de resultaten van de campagne.

#### Evil-Nginx

**Evil-Nginx** is een omgekeerde proxytool waarmee aanvallers inloggegevens en sessiecookies kunnen stelen door middel van phishing-aanvallen. Het werkt door het onderscheppen en manipuleren van verkeer tussen de gebruiker en een legitieme website, zonder dat de gebruiker zich hiervan bewust is.

#### Hydra

**Hydra** is een snelle en flexibele wachtwoord-cracker. Het ondersteunt een breed scala aan protocollen en diensten, waaronder HTTP, FTP, SMTP, en meer. Hydra probeert brute-force aanvallen uit te voeren door verschillende combinaties van gebruikersnamen en wachtwoorden te testen.

#### CrackMapExec

**CrackMapExec (CME)** is een tool voor post-exploitatie en kwetsbaarheidsonderzoek. Het is specifiek gericht op grote Windows-netwerken en Active Directory. CME kan wachtwoorden testen, gebruikersgegevens ophalen, en verschillende netwerkacties uitvoeren met behulp van verzamelde inloggegevens.

### 4.2 Ons team

**Andrew Fleetwood-Bird:**

Ik ben een student aan Fontys ICT binnen de richting infrastructuur. Ik ben geïnteresseerd in IT-infrastructuur en cybersecurity. Mijn meeste kennis is op het gebied van infrastructuur en verder heb ik ook kennis in blue team-tactieken, Op het gebied van Redteaming wil ik me verbeteren.

**Ben van der Linden:**

[LinkedIn](https://www.linkedin.com/in/ben-van-der-linden-36a4a4193/)

Student cybersecurity met een passie voor cybersecurity en het beveiligen van digitale landschappen, Voornamelijk pentester/bugbounty-hunter maar ook veel interesse op het gebied van Redteaming. Op moment werkend naar zijn eerste officiële certificering genaamd OSCP.

**Bogdan Nikolov:**

Bogdan Nikolov, ook bekend als bnn, is een ambitieuze cybersec engineer. Momenteel is hij Junior Software Engineer bij een bedrijf dat op de Top 100 Forbes Cloud-lijst staat. Hij is ook leider van een CTF-team dat deelneemt aan verschillende internationale CTF-evenementen zoals HTB Cyber Apocalypse, TrojanCTF, etc. Zijn belangrijkste expertise ligt in het creëren van schaalbare en veilige software voor automatisering. Een van zijn interesses is reverse engineering.

**Khaled Ali:**

[LinkedIn](https://www.linkedin.com/in/khaled-ali-1aa472266/)

Komt uit infrastructure, mijn kennis en passie ligt daar ook waar ik graag bezig ben met het bouwen van netwerken en werken met cloud platformen zoals AWS en Azure. Momenteel doe ik de cybersecurity profiel als vierde semester student bij Fontys.

**Reuel Dooren:**

Reuel van Dooren, een student aan de Technische Hogeschool Eindhoven en is een actief lid van een CTF-team dat mee heeft gedaan aan het nationale evenement de CTC. Met ervaring in netwerken, transmissie en cryptografie uit zijn tijd in het leger, brengt Reuel praktische expertise mee. Hij is gefocust op het verdiepen van zijn kennis over cybersecurity binnen de militaire context, terwijl hij bijdraagt aan de activiteiten van het team in cyberverdedigingsuitdagingen.

**Roan Kessels:**

Roan Kessels is een tweedejaars student bij Fontys ICT in Eindhoven. Komende uit het Software Development profiel, waar hij ervaring heeft opgedaan in de full-stack implementatie van veilige webapplicaties. Hij studeert dit semester Cybersecurity, met een focus of Defensieve Cybersecurity.