

**LAPORAN PRAKTIKUM  
ETHICAL HACKING MODUL 2**



Disusun oleh :

**Nama : Iki Adfi Nur Mohamad**

**NRP : 5027221033**

**Kelas : Ethical Hacking A**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER  
KOTA SURABAYA  
2024**

## Assesment Overview

Pada Sabtu, 4 Mei 2024 sampai dengan Rabu, 8 Mei 2024 pukul 23.59, saya melakukan testing untuk menemukan kerentanan pada perusahaan FortifyTech. Pada testing yang saya lakukan ditemukan vulnerability Anonymous FTP users engaging in unauthorized activities CVE-1999-0497 pada IP 10.15.42.36 dan CVE-2023-4596 WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution pada IP 10.15.42.7 . Terdapat fase testing yang saya lakukan antara lain:

## Planning

Saya merencanakan IP mana yang akan di tes berdasarkan soal praktikum, dan metode scanning apa yang dipilih untuk menemukan vulnerability nya berdasarkan modul 2 Ethical Hacking.

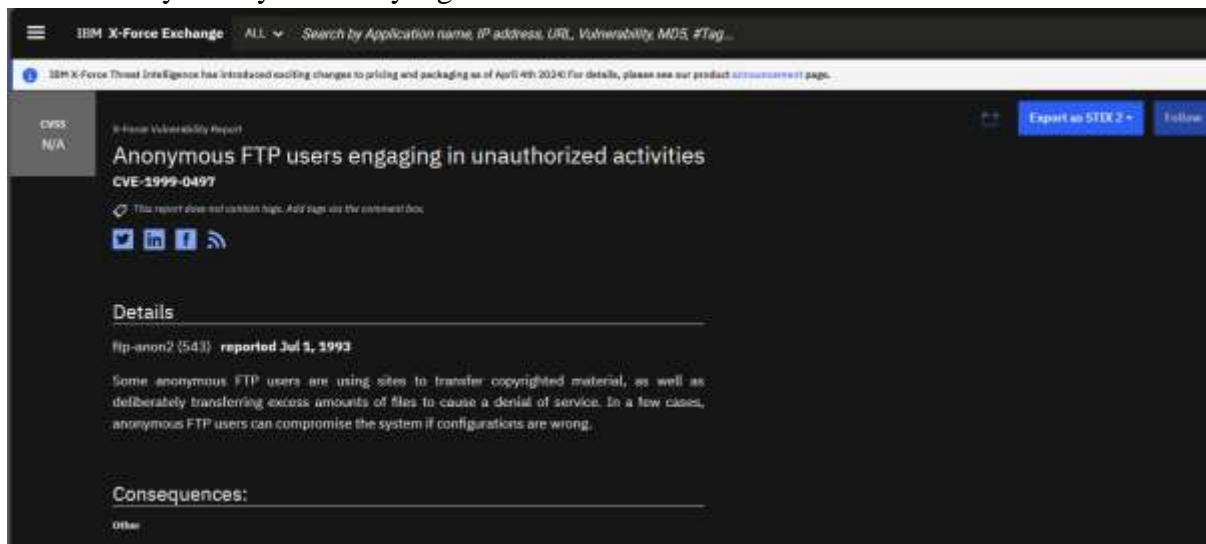
## Scanning

Saya melakukan scanning menggunakan metode nmap, gobuster, feroxbuster, wp, dan nuclei

## Analysing

Saya melakukan analisis setiap vulnerability pada sumber-sumber lain di internet. Seperti memahami setiap vulnerability dari IP 10.15.42.36 dan 10.15.42.7.

Vulnerability Anonymis FTP yang ditemukan dari IP 10.15.42.36



The screenshot displays a vulnerability report on the IBM X-Force Exchange platform. The report title is "Anonymous FTP users engaging in unauthorized activities" with the CVE identifier "CVE-1999-0497". It includes a note that the report does not contain tips and a link to add tips. The "Details" section states that the vulnerability was reported on July 1, 1993, by "ftp-anon2 (543)". The description explains that some anonymous FTP users use sites to transfer copyrighted material or cause a denial of service. The "Consequences" section is partially visible at the bottom.

IBM X-Force Exchange

Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...

IBM X-Force Threat Intelligence has introduced exciting changes to pricing and packaging as of April 4th 2024! For details, please see our product [announcement](#) page.

CVSS: N/A

9-Force Vulnerability Report

Anonymous FTP users engaging in unauthorized activities

CVE-1999-0497

This report does not contain tips. Add tips via the comment box.

Details

ftp-anon2 (543) reported Jul 1, 1993

Some anonymous FTP users are using sites to transfer copyrighted material, as well as deliberately transferring excess amounts of files to cause a denial of service. In a few cases, anonymous FTP users can compromise the system if configurations are wrong.

Consequences:

Other

Selanjutnya adalah vulnerability dari versi forminator yang sudah out to date, sehingga vulnerabilitynya kemungkinan rentan

The screenshot shows the Exploit Database interface for the exploit titled "WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution". The header bar is dark blue with the "EXPLOIT DATABASE" logo on the left and navigation icons on the right. The main content area has a light gray background. At the top, the title is displayed in a large, bold font. Below the title, there are several metadata fields arranged in a grid. The "EDB-ID:" field shows "13664". The "CVE:" field shows "N/A". The "Author:" field shows "MEHMET KALINCI". The "Type:" field shows "WEBSITE". The "Platform:" field shows "PHP". The "Date:" field shows "2025-07-29". Below these fields, there are three buttons: "EDB Verified: ✖", "Exploit: 1 / 1", and "Vulnerable App:". Below the buttons, there is a large text area containing the exploit details. The text starts with "# Exploit Title: WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution" and continues with "# Date: 2025-07-29", "# Exploit Author: Mehmet Kalinci", "# Vendor Homepage: https://github.com/project-forminator/forminator", "# Software Link: https://wordpress.org/plugins/forminator/", "# Version: 1.24.6", and "# Tested on: PHP - MySQL - Apache2 - Windows 10". Below this, there is a section titled "HTTP Request and vulnerable parameter:" followed by a detailed HTTP request. The request is a POST to "/wp-admin/admin-ajax.php" with a "Host: localhost" and "Content-Length: 4756". The "sec-ch-ua:" field is set to "Google Chrome". The "Accept:" field is set to "\*/\*". The "Content-Type:" field is set to "multipart/form-data". The "boundary:" field is set to "-----WebKitFormBoundaryTepN8ug6jmm". The "X-Requested-With:" field is set to "XMLHttpRequest". The "sec-ch-ua-mobile:" field is set to "0".

WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution

EDB-ID: 13664 CVE: N/A Author: MEHMET KALINCI Type: WEBSITE Platform: PHP Date: 2025-07-29

EDB Verified: ✖ Exploit: 1 / 1 Vulnerable App:

# Exploit Title: WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution  
# Date: 2025-07-29  
# Exploit Author: Mehmet Kalinci  
# Vendor Homepage: https://github.com/project-forminator/forminator  
# Software Link: https://wordpress.org/plugins/forminator/  
# Version: 1.24.6  
# Tested on: PHP - MySQL - Apache2 - Windows 10

HTTP Request and vulnerable parameter:

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost
Content-Length: 4756
sec-ch-ua: Google Chrome
Accept: */*
Content-Type: multipart/form-data;
boundary: -----WebKitFormBoundaryTepN8ug6jmm
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: 0
```

Reporting – Saya melakukan pembuatan laporan untuk menjelaskan kelemahan 2 IP tersebut

## Assessment Components

Saya melakukan testing vulnerability terhadap IP yang sudah disediakan pada praktikum kali ini, yaitu 10.15.42.36 dan 10.15.42.7 menggunakan VPN ITS atau tersambung dalam jaringan ITS.

## Scope

Assessment	Details
Vulnerability Test	10.15.42.36
	10.15.42.7

## Executive Summary

Pada testing yang saya lakukan ditemukan vulnerability Anonymous FTP users engaging in unauthorized activities CVE-1999-0497 pada IP 10.15.42.36 dan CVE-2023-4596 WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution pada IP 10.15.42.7

## Testing Summary

### A. IP 10.15.42.36

Hasil pemindaian menunjukkan bahwa host dengan alamat IP 10.15.42.36 menjalankan layanan SSH pada port 22. Analisis menemukan bahwa host menggunakan algoritma autentikasi SSH yang rentan terhadap serangan brute force melalui password. Selain itu, algoritma HMAC-SHA1 yang digunakan untuk integritas pesan juga rentan terhadap serangan. Celah keamanan CVE-2023-48795, dikenal sebagai "Terrapin", ditemukan pada host ini, meningkatkan potensi kerentanan dan risiko keamanan. Namun "Terrapin" ternyata tidak seefektif itu. Informasi lebih lanjut menunjukkan bahwa host menggunakan perangkat lunak OpenSSH versi 8.21 di atas sistem operasi Ubuntu. Metode autentikasi yang didukung adalah kunci publik dan kata sandi, yang menunjukkan adanya potensi untuk serangan autentikasi. Selain layanan SSH, layanan FTP juga aktif pada host ini dengan kemungkinan akses anonim yang memungkinkan, menambahkan potensi kerentanan dan potensi masuk yang lebih luas. Dalam keseluruhan, hasil pemindaian ini menyoroti kebutuhan mendesak untuk langkah-langkah perbaikan keamanan yang efektif untuk mengurangi risiko eksploitasi dan akses tidak sah ke host tersebut.

```
(root@ikiadfi)-[/home/keyfee]
$ cat scanbynuclei-ip36.txt
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.36:22
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 ["publickey","password"]
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21
```

Hasil pemindaian menunjukkan adanya kerentanan terkait aktivitas pengguna FTP anonim yang pada host dengan alamat IP 10.15.42.36. Kerentanan ini, yang diidentifikasi sebagai CVE-1999-0497, terkait dengan penggunaan FTP anonim yang dapat dieksploitasi untuk melakukan aktivitas yang tidak diizinkan. Dalam IP ini, FTP dengan akses anonim yang memungkinkan dapat memberikan peluang bagi

penyerang untuk melakukan berbagai jenis serangan, seperti pencurian data atau pengunggahan file berbahaya. Vulnerability ini meningkatkan risiko keamanan secara keseluruhan, terutama ketika digabungkan dengan kerentanan lain yang ditemukan pada layanan SSH, seperti algoritma autentikasi yang rentan dan celah keamanan CVE-2023-48795 yang telah diidentifikasi sebelumnya.

#### B. IP 10.15.42.7

Hasil scanning menunjukkan bahwa pada alamat IP 10.15.42.7 dihosting pada server Apache versi 2.4.59 dengan PHP versi 8.2.18. Situs ini tampaknya menggunakan WordPress versi 6.5.2. Namun, beberapa header keamanan tampaknya hilang, termasuk permissions-policy, x-frame-options, dan x-content-type-options. Hal ini bisa menjadi masalah keamanan. Selain itu, situs ini tampaknya memiliki konten pasif campuran, yang berarti beberapa sumber daya dimuat melalui HTTP meskipun situs itu sendiri mungkin dimuat melalui HTTPS. Hal ini dapat membuat situs tersebut rentan terhadap serangan man-in-the-middle. Web ini juga tampaknya memiliki beberapa endpoint yang mungkin rentan, termasuk halaman login WordPress, file readme.html, dan file robots.txt. Selain itu, tampaknya ada beberapa pengguna yang dapat diidentifikasi, termasuk pengguna dengan nama 'admin'.

Pada sisi SSH, metode autentikasi termasuk publickey dan password, dan server tampaknya menjalankan OpenSSH versi 8.21 pada Ubuntu. Ada juga indikasi bahwa server ini mungkin rentan terhadap serangan Terrapin (CVE-2023-48795). Namun ketika dicek, ternyata terrapin bukan merupakan kelemahan terkuatnya.

```

root@kali:~# cat scanby nuclei-ip7.txt
[adventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.6.2"]
[tech-detect:php] [http] [info] http://10.15.42.7
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7
[mixed-passive-content:img] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exterior.webp", "http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-building.webp", "http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-srv] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?v=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[ooob-header-based-interaction:dns] [http] [info] http://10.15.42.7
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wp-license-file] [http] [info] http://10.15.42.7/License.txt
[wp-user-enum:username] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]

```

Hasil scanning menunjukkan bahwa situs web yang dihosting pada alamat IP 10.15.42.7 menggunakan plugin WordPress Forminator versi 1.24.6. Versi ini tampaknya rentan terhadap eksekusi perintah jarak jauh yang tidak diautentikasi. Eksploitasi ini memanfaatkan celah keamanan dalam penanganan file unggahan oleh plugin. Secara khusus, parameter `postdata-1-post-image` dan fungsi `$image_field_name` dalam kode sumber plugin tampaknya rentan. Seorang penyerang dapat mengunggah file dengan ekstensi yang valid (dalam hal ini, file PHP). Dalam contoh payload yang diberikan, file `mehmet.php` berisi kode PHP yang memungkinkan eksekusi perintah jarak jauh melalui parameter GET function dan cmd.

```

# Exploit Title: WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution
# Date: 2023-01-26
# Exploit Author: @hacker_420x
# Vendor Homepage: https://www.wondershare.com/wordpress/forminator-plugin/
# Software Link: https://wordpress.org/plugins/forminator/
# Version: 1.24.6
# Tested on: PHP - Apache - Windows 11

HTTP Request and vulnerable parameter:
-----
POST /?forminator/wp-admin/index.php HTTP/1.1
Host: localhost
Content-Length: 2750
User-Agent: Mozilla/5.0 (Windows NT 10.0; ARMv8) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.339 Safari/537.36
Accept: */*
Content-Type: multipart/form-data;
boundary=----AMKX1Fomboundary7eaf74a9a63c9a
X-Requested-With: XMLHttpRequest
Accept-Charset: utf-8
Cookie: wp-settings-t=5e3d80794383;
wordpress_test_cookie=WP2COOKIES324hck; wp_lang_pr_18
Connection: close

```

Jika berhasil, eksploitasi ini dapat memungkinkan penyerang untuk menjalankan perintah sembarang pada server yang menjalankan WordPress dengan plugin Forminator versi 1.24.6 ini. Ini bisa berpotensi merusak, karena penyerang dapat memperoleh kontrol penuh atas server. Eksploitasi ini hanya mungkin jika penyerang dapat mengunggah file ke server (misalnya, melalui formulir unggahan file yang tidak aman atau jika penyerang sudah memiliki akses ke akun pengguna dengan hak unggah file). Selain itu, server harus dikonfigurasi untuk memungkinkan eksekusi file PHP yang diunggah, yang bukanlah praktik standar pada banyak hosting web bersama.

## Technical Finding

1. Pertama saya melakukan scanning menggunakan nmap aggressive pada IP 10.15.42.36 . Kemudian ditemukan hasil berikut ini:

```
—(root@ikiadfi)~[/home/keyfee]
❯ cat nmaplogaggressive1.log
# Nmap 7.94SVN scan initiated Tue May  7 20:25:47 2024 as: nmap -A -oN nmaplogaggressive1.log 10.15.42.36
Nmap scan report for 10.15.42.36
Host is up (0.0000s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: PASV IP 172.18.0.3 is not the same as 10.15.42.36
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c0:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:B6:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: Login Page
|_ http-server-header: Apache/2.4.38 (Debian)
Aggressive OS guesses: Linux 4.15 - 5.0 (93%), Linux 5.3 - 5.4 (93%), Linux 2.6.32 (92%), Linux 5.0 - 5.5 (92%), Linu
x 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (91%), Linux 5.0 (90%), Linux 5.0 - 5.4
(90%), Adtran 424RG FTTH gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT      ADDRESS
0  0.35 ms  ikiadfi.sshome.net (172.30.32.1)
1  7.12 ms  10.33.0.1
2  ... 7
3  7.62 ms  10.15.42.36

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May  7 20:26:07 2024 -- 1 IP address (1 host up) scanned in 20.14 seconds
```



2. Hal yang sama, saya lakukan pada IP 10.15.42.7 . Kemudian ditemukan hasil berikut ini:

```
(root@ikiadfi)~[/home/keyfee]
# cat nmaplogaggressive2.log
# Nmap 7.94SVN scan initiated Tue May  7 20:26:36 2024 as: nmap -A -oN nmaplogaggressive2.log 10.15.42.7
Nmap scan report for 10.15.42.7
Host is up (0.036s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:0f:0b:4a:8b:7a:42 (RSA)
|   256 08:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_  256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:17 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-generator: WordPress 6.5.2
|_ http-title: Hello World
|_ http-server-header: Apache/2.4.59 (Debian)
Aggressive OS guesses: Linux 4.15 - 5.8 (93%), Linux 5.3 - 5.4 (93%), Linux 2.6.32 (92%), Linux 5.0 - 5.5 (92%), Linu
x 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (91%), Linux 5.0 (90%), Linux 5.0 - 5.4
(90%), Adtran 424RC FTTH gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   0.34 ms   ikiadfi.mshome.net (172.30.32.1)
2   85.79 ms  10.33.0.1
3   ... 7
8   85.84 ms  10.15.42.7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May  7 20:26:59 2024 -- 1 IP address (1 host up) scanned in 22.80 seconds
```

3. Saya melakukan scanning menggunakan Gobuster pada IP 10.15.42.36 . Kemudian ditemukan hasil berikut ini:

```
(root@ikiadfi)~[/home/keyfee]
# cat gobuster-output-a.log
/. (Status: 200) [Size: 603]
/.htaccess-dev (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htaccess-local (Status: 403) [Size: 278]
/.htaccess-marco (Status: 403) [Size: 278]
/.htaccess.bak (Status: 403) [Size: 278]
/.htaccess.inc (Status: 403) [Size: 278]
/.htaccess.old (Status: 403) [Size: 278]
/.htaccess.sample (Status: 403) [Size: 278]
/.htaccess.bak1 (Status: 403) [Size: 278]
/.htaccess.orig (Status: 403) [Size: 278]
/.htaccess/ (Status: 403) [Size: 278]
/.htaccess.save (Status: 403) [Size: 278]
/.htaccessOLD2 (Status: 403) [Size: 278]
/.htm (Status: 403) [Size: 278]
/.htaccessBAK (Status: 403) [Size: 278]
/.htaccess.txt (Status: 403) [Size: 278]
/.htaccessOLD (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/.htpasswd-old (Status: 403) [Size: 278]
/.htpasswd.bak (Status: 403) [Size: 278]
/.htpasswd.inc (Status: 403) [Size: 278]
/.htpasswd/ (Status: 403) [Size: 278]
/.httr-oauth (Status: 403) [Size: 278]
/.icons/ (Status: 403) [Size: 278]
./index.php (Status: 200) [Size: 603]
```



4. Hal yang sama, saya lakukan pada IP 10.15.42.7 . Kemudian ditemukan hasil berikut ini:

```
(root@ikindf1) ~/home/keyfee
# cat gobuster-output-b.log
/A3eN2e//google.com (Status: 400) [Size: 302]
/ (Status: 301) [Size: 0] [-> http://10.15.42.7/]
/.htaccess (Status: 403) [Size: 275]
/.htaccess-dev (Status: 403) [Size: 275]
/.htaccess-local (Status: 403) [Size: 275]
/.htaccess-marco (Status: 403) [Size: 275]
/.htaccess.bak (Status: 403) [Size: 275]
/.htaccess.bak1 (Status: 403) [Size: 275]
/.htaccess.inc (Status: 403) [Size: 275]
/.htaccess.old (Status: 403) [Size: 275]
/.htaccess.orig (Status: 403) [Size: 275]
/.htaccess.sample (Status: 403) [Size: 275]
/.htaccess.save (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.htaccess/ (Status: 403) [Size: 275]
/.htaccessOLD2 (Status: 403) [Size: 275]
/.htaccessOLD (Status: 403) [Size: 275]
/.htaccessBAK (Status: 403) [Size: 275]
/.htal (Status: 403) [Size: 275]
/.htpasswd-old (Status: 403) [Size: 275]
/.htpasswd.inc (Status: 403) [Size: 275]
/.htpasswd.bak (Status: 403) [Size: 275]
/.httr-auth (Status: 403) [Size: 275]
/.htpasswd/ (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/e (Status: 301) [Size: 0] [-> http://10.15.42.7/e/]
/E/ (Status: 300) [Size: 86944]
/P/ (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/Post (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/admin/ (Status: 302) [Size: 0] [-> http://10.15.42.7/wp-admin/]
/atom (Status: 301) [Size: 0] [-> http://10.15.42.7/feed/atom/]
/atom/ (Status: 301) [Size: 0] [-> http://10.15.42.7/feed/atom/]
/dashboard (Status: 302) [Size: 0] [-> http://10.15.42.7/wp-admin/]
/dashboard/ (Status: 302) [Size: 0] [-> http://10.15.42.7/wp-admin/]
/embed (Status: 301) [Size: 0] [-> http://10.15.42.7/embed/]
/embed/ (Status: 300) [Size: 86944]
/favicon.ico (Status: 302) [Size: 0] [-> http://10.15.42.7/wp-includes/images/e/logo-bliss-white-6p.png]
/feed (Status: 301) [Size: 0] [-> http://10.15.42.7/feed/]
/feed/ (Status: 300) [Size: 7230]
/h (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/hello-world/]
/h/ (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/hello-world/]
/ha/ (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/hello-world/]
/hello (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/hello-world/]
/icons/ (Status: 403) [Size: 275]
/index.php (Status: 301) [Size: 0] [-> http://10.15.42.7/]
/license.txt (Status: 300) [Size: 19915]
/login/ (Status: 302) [Size: 0] [-> http://10.15.42.7/wp-login.php]
/p (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/p/ (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/page1 (Status: 301) [Size: 0] [-> http://10.15.42.7/]
/post (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/post/ (Status: 301) [Size: 0] [-> http://10.15.42.7/2020/02/04/post-feedback/]
/rdf (Status: 301) [Size: 0] [-> http://10.15.42.7/feed/rdf/]
/readme.html (Status: 300) [Size: 7401]
```

5. Metode lainnya saya mencoba menggunakan feroxbuster pada IP 10.15.42.36, namun tidak dapat tersambung/ terkoneksi, sehingga tidak dapat dilakukan scanning.

```
(root@ikindf1) ~/home/keyfee
# feroxbuster -u http://10.15.42.36 -x pdf -x js,html -x php txt json docx

FERROX OXIDE
by Ben "epi" Risher ver: 2.10.3

Target Url      http://10.15.42.36
Threads        50
Wordlist        /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes
Timeout (secs)  7
User-Agent      feroxbuster/2.10.3
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
Extensions     [pdf, js, html, php, txt, json, docx]
HTTP methods    [GET]
Recursion Depth 4

Press [ENTER] to use the Scan Management Menu

Could not connect to http://10.15.42.36, skipping...
=> error sending request for url [http://10.15.42.36/]: error trying to connect: tcp connect error: Connection refused (os error 111) [RHOST: Could not connect to any target provided]
```

6. Dengan metode yang sama, saya menggunakan feroxbuster pada IP 10.15.42.7 dan ditemukan hasil seperti berikut ini

```
(root@ihiafi) ~/home/keyfee
# feroxbuster -u http://10.15.42.7 -x pdf -x js,html -x php txt json docx

FERROXIDE
by Ben "epi" Risher ver: 2.10.3

Target Url      http://10.15.42.7
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent      feroxbuster/2.10.3
Config File     /etc/feroxbuster/ferox-config.toml
Extract Links   true
Extensions     [pdf, js, html, php, txt, json, docx]
HTTP methods    [GET]
Recursion Depth 4

Press [ENTER] to use the Scan Management Menu"

400 GET 11 1w 1c http://10.15.42.7/wp-admin/admin-ajax.php
302 GET 01 0w 0c http://10.15.42.7/wp-admin/ => http://10.15.42.7/wp-login.php?redirect_to=
http://10.15.42.7/wp-admin/?2F10.15.42.7%2Fwp-admin%2Ffireauth=1
403 GET 91 28w 275c Auto-filtering found 404-like response and created new filter; toggle off
with --dont-filter
404 GET 3791 1947w 56870c Auto-filtering found 404-like response and created new filter; toggle off
with --dont-filter
301 GET 91 28w 313c http://10.15.42.7/wp-content => http://10.15.42.7/wp-content/
301 GET 91 28w 314c http://10.15.42.7/wp-includes => http://10.15.42.7/wp-includes/
302 GET 01 0w 6c http://10.15.42.7/admin => http://10.15.42.7/wp-admin/
301 GET 91 28w 311c http://10.15.42.7/wp-admin => http://10.15.42.7/wp-admin/
301 GET 01 0w 0c http://10.15.42.7/feed => http://10.15.42.7/feed/
302 GET 01 0w 0c http://10.15.42.7/login => http://10.15.42.7/wp-login.php
309 GET 11 26w 3380c http://10.15.42.7/wp-includes/blocks/navigation/view.min.js
308 GET 21 829w 35849c http://10.15.42.7/wp-includes/js/dist/interactivity.min.js
308 GET 11 183w 16484c http://10.15.42.7/wp-includes/blocks/navigation/style.min.css
308 GET 11 139w 7849c http://10.15.42.7/wp-includes/blocks/image/style.min.css
405 GET 11 6w 42c http://10.15.42.7/xmlrpc.php
404 GET 01 0w 0c http://10.15.42.7/wp-includes/blocks/
309 GET 5161 2974w 228732c http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows
.webp
300 GET 2621 1514w 128008c http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist
-and-building.webp
404 GET 01 0w 8c http://10.15.42.7/node
404 GET 01 0w 0c http://10.15.42.7/images
404 GET 01 0w 0c http://10.15.42.7/themes
404 GET 01 0w 8c http://10.15.42.7/sites
404 GET 01 0w 0c http://10.15.42.7/misc
404 GET 01 0w 0c http://10.15.42.7/img
404 GET 01 0w 8c http://10.15.42.7/dyn
404 GET 01 0w 0c http://10.15.42.7/password
404 GET 01 0w 0c http://10.15.42.7/tag
```

7. Saya juga menggunakan metode scanning menggunakan nuclei untuk IP 10.15.42.36 ditemukan hasil seperti berikut:

```
(root@ihiafi) ~/home/keyfee
# cat scanbynuclei-ip36.txt
[ssh-password-auth] [javascript] [info] 10.15.42.36:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.36:22
[CVE-2023-48795] [javascript] [medium] 10.15.42.36:22 ["Vulnerable to Terrapin"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.36:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[ssh-auth-methods] [javascript] [info] 10.15.42.36:22 [{"publickey","password"}]
[ftp-anonymous-login] [tcp] [medium] 10.15.42.36:21
```

8. Berikut hasil scanning menggunakan nuclei pada IP 10.15.42.7

```
(root@ikiadfi)~/home/keyfee
# cat scanbynuclei-ip7.txt
[addeventlistener-detect] [http] [info] http://10.15.42.7
[apache-detect] [http] [info] http://10.15.42.7 ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7 ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7 ["WordPress 6.5.2"]
[tech-detect:php] [http] [info] http://10.15.42.7
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7
[mixed-passive-content:img] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exterior.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-crl] [http] [info] http://10.15.42.7 ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7 ["6.5.2"]
[msf-detect:apachegeneric] [http] [info] http://10.15.42.7
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wp-user-enum:username] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["publickey","password"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulnerable to Terrapin"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-shal-hmac-algo] [javascript] [info] 10.15.42.7:22
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
```

9. Selanjutnya pasa scanning WP di IP 10.15.42.36 tidak dapat dilakukan, kemungkinan web down atau factor lainnya

```
(root@ikiadfi)~/home/keyfee
# wpscan --url http://10.15.42.36

      _____
     /  _  _  _  \
    /  /  _  _  \
   /  /  _  _  \
  /  /  _  _  \
 /  /  _  _  \
/  /  _  _  \

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_ @ethicalhack3r @erman_lr @firefart

Scan Aborted: The url supplied 'http://10.15.42.36/' seems to be down (Couldn't connect to server)
```

10. Terakhir adalah hasil scan WP untuk IP 10.15.42.7

```
(root@ikiadfi) ~ [~/home/keyfee]
$ cat scanbywp-ip7.txt

-----
  W P S C A N
-----

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

-----

[*] URL: http://10.15.42.7/ [10.15.42.7]
[*] Started: Tue May 7 23:31:45 2024

Interesting Finding(s):

[*] Headers
| Interesting Entries:
| - Server: Apache/2.4.59 (Debian)
| - X-Powered-By: PHP/8.2.18
| Found By: Headers (Passive Detection)
| Confidence: 100%

[*] robots.txt found: http://10.15.42.7/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[*] XML-RPC seems to be enabled: http://10.15.42.7/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[*] WordPress readme found: http://10.15.42.7/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[*] The external WP-Cron seems to be enabled: http://10.15.42.7/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
```

11. Terakhir saya melakukan analisis setiap vulnerability pada sumber-sumber lain di internet. Seperti memahami setiap vulnerability dari IP 10.15.42.36 dan 10.15.42.7.

Vulnerability Anonymis FTP yang ditemukan dari IP 10.15.42.36

IBM X-Force Exchange

ALL

Search by Application name, IP address, URL, Vulnerability, MO5, #Tag...

IBM X-Force Threat Intelligence has introduced exciting changes to pricing and packaging as of April 4th 2024! For details, please see our product [announcement](#) page.

CVE:  
N/A

X-Force Vulnerability Report

Anonymous FTP users engaging in unauthorized activities

CVE-1999-0497

This report does not contain tips. Add tips via the comment box.

Details

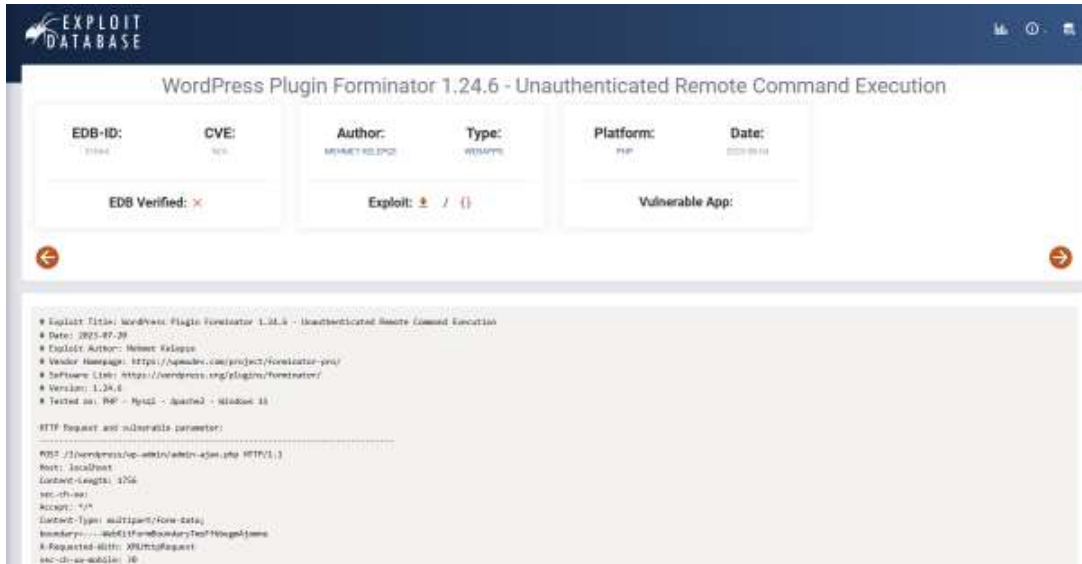
ftp-anon2 (543) reported Jul 1, 1993

Some anonymous FTP users are using sites to transfer copyrighted material, as well as deliberately transferring excess amounts of files to cause a denial of service. In a few cases, anonymous FTP users can compromise the system if configurations are wrong.

Consequences:

Other

Selanjutnya adalah vulnerability dari versi forminator yang sudah out to date



The screenshot shows the Exploit Database interface for the vulnerability "WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution". The header includes the Exploit Database logo and navigation icons. The main content area displays the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
11884	N/A	0x00000000	WordPress	PHP	2025-07-20
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App:	

Below the details, there is a section for the exploit script, which includes the following information:

```
# Exploit Title: WordPress Plugin Forminator 1.24.6 - Unauthenticated Remote Command Execution
# Date: 2025-07-20
# Exploit Author: 0x00000000
# Vendor Homepage: https://wondercms.com/project/forminator-pro/
# Software Link: https://wordpress.org/plugins/forminator/
# Version: 1.24.6
# Tested on: PHP - MySQL - Apache2 - Windows 10

HTTP Request and vulnerable parameter:

POST /?forminator-pro-admin-ajax.php HTTP/1.1
Host: localhost
Content-Length: 1756
User-Agent: curl
Content-Type: multipart/form-data;
boundary=...
X-Requested-With: XMLHttpRequest
Content-Type: 10
```

## Additional Scans and Reports

Pada link Github saya sudah saya masukkan additional file berupa .log dan .txt versi lengkap scanning yang saya lakukan pada IP 10.15.42.36 dan 10.15.42.7