NMAP

10.15.42.7

```
# Nmap 7.94SVN scan initiated Tue May  7 01:14:54 2024 as: nmap -p- -sV -sC -T4 -oN
/home/user/Desktop/log-7.log 10.15.42.7
Nmap scan report for 10.15.42.7
Host is up (0.086s latency).
Not shown: 65533 filtered tcp ports (no-response)
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:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|   256 00:9c: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:a9:37 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Hello World
|_http-server-header: Apache/2.4.59 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 6.5.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue May  7 01:19:57 2024 -- 1 IP address (1 host up) scanned in 302.50
seconds
```

10.15.42.36

```
# Nmap 7.94SVN scan initiated Tue May  7 01:15:40 2024 as: nmap -Pn -p- -sV -sC -T4
-oN /home/user/Desktop/log-36.log 10.15.42.36
Nmap scan report for 10.15.42.36
Host is up (0.070s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RSA)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDSA)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Login Page
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Tue May  7 01:30:33 2024 -- 1 IP address (1 host up) scanned in 892.97
seconds
```

DirListing 10.15.42.7

gobuster dir -u 10.15.42.7 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -o /home/user/Desktop/dirlog-7.log

then

sed '/Size: 0/d' ./dirlog-7.log > edit-dirlog-7.log

```
/wp-content          [36m (Status: 301)[0m [Size: 313][34m [-->
http://10.15.42.7/wp-content/][0m
/wp-admin            [36m (Status: 301)[0m [Size: 311][34m [-->
http://10.15.42.7/wp-admin/][0m
```

WPScan 10.15.42.7

wpscan --url http://10.15.42.7

```
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         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 01:51:29 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

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</generator>
 |  - http://10.15.42.7/comments/feed/,
<generator>https://wordpress.org/?v=6.5.2</generator>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to
any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'
```

Nuclei Scan

nuclei -u http://10.15.42.7 -o nuclei7.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:x-permitted-cross-domain-policies] [http] [info]
http://10.15.42.7
[http-missing-security-headers:clear-site-data] [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-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:permissions-policy] [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:referrer-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:content-security-policy] [http] [info] http://10.15.42.7
[http-missing-security-headers:x-frame-options] [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.we
bp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-build
ing.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-sri] [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"]
[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"]
[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-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wp-user-enum:usernames] [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-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1
Ubuntu-4ubuntu0.5"]
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
```

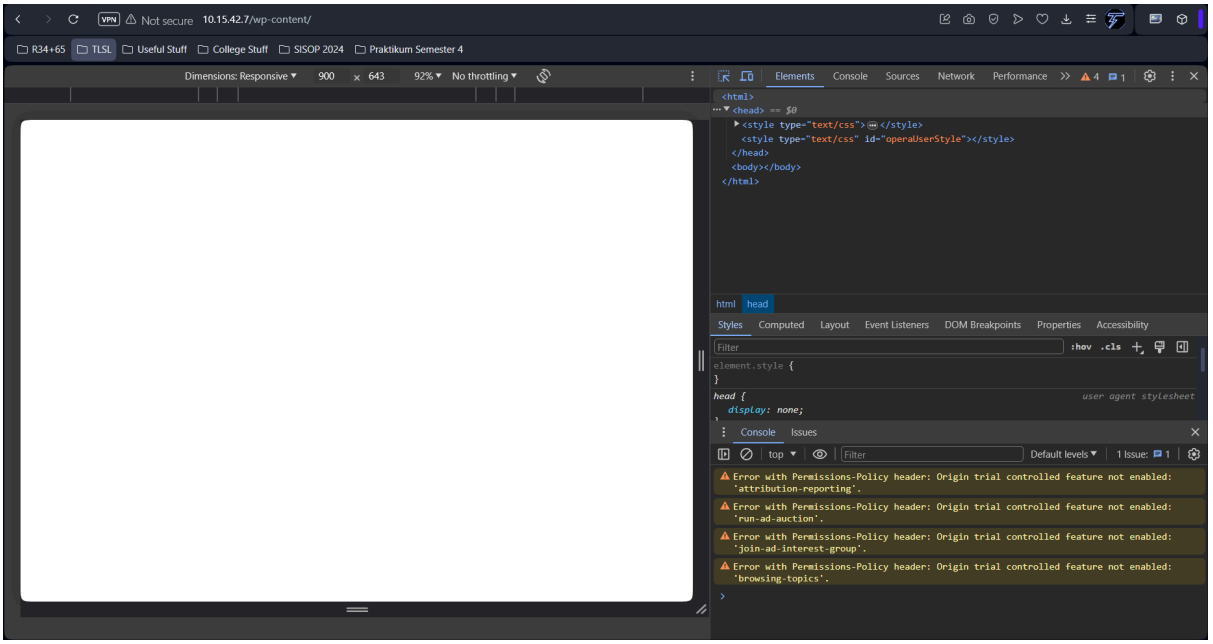
nuclei -u 10.15.42.36:8888 -o nuclei36.txt

```
[apache-detect] [http] [info] http://10.15.42.36:8888 ["Apache/2.4.38 (Debian)"]
[php-detect] [http] [info] http://10.15.42.36:8888 ["7.2.34"]
```

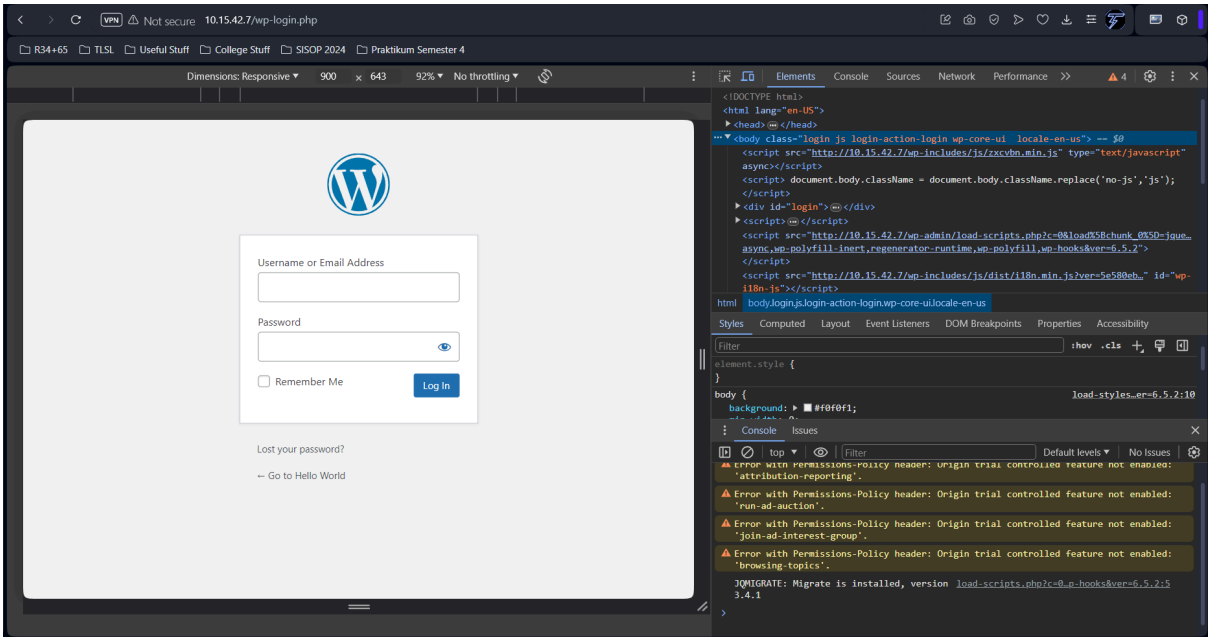
[tech-detect:php] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-resource-policy] [http] [info]
http://10.15.42.36:8888
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info]
http://10.15.42.36:8888
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info]
http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-opener-policy] [http] [info]
http://10.15.42.36:8888
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.36:8888
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888

Doc

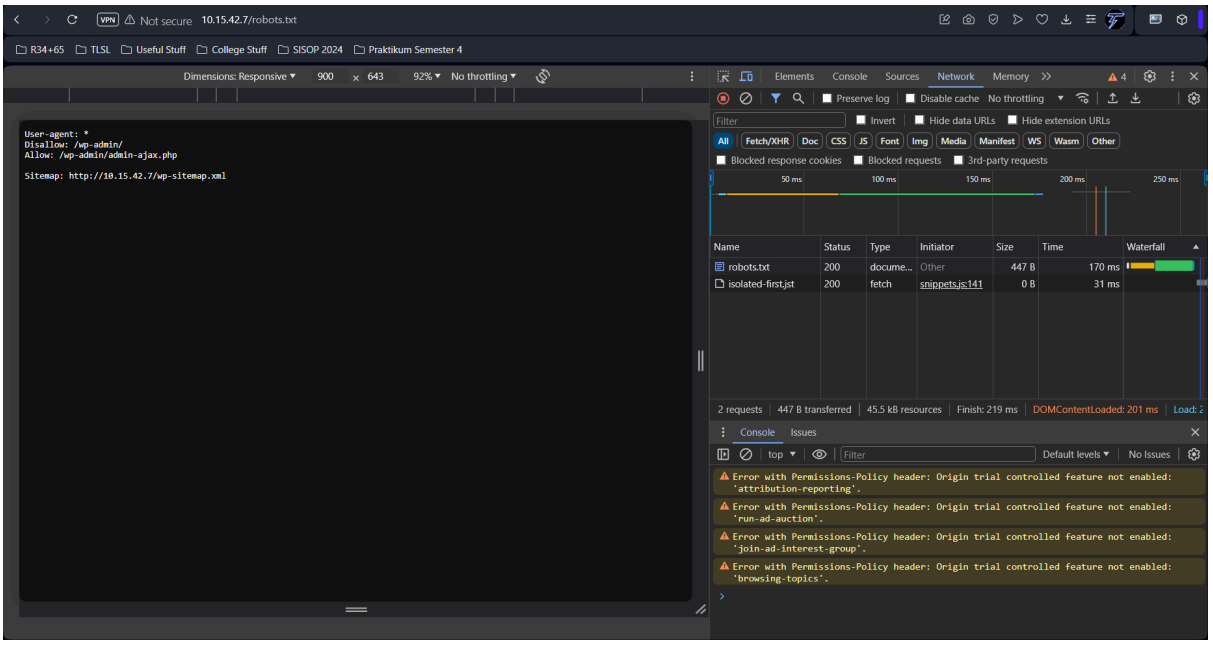
http://10.15.42.7/wp-content/



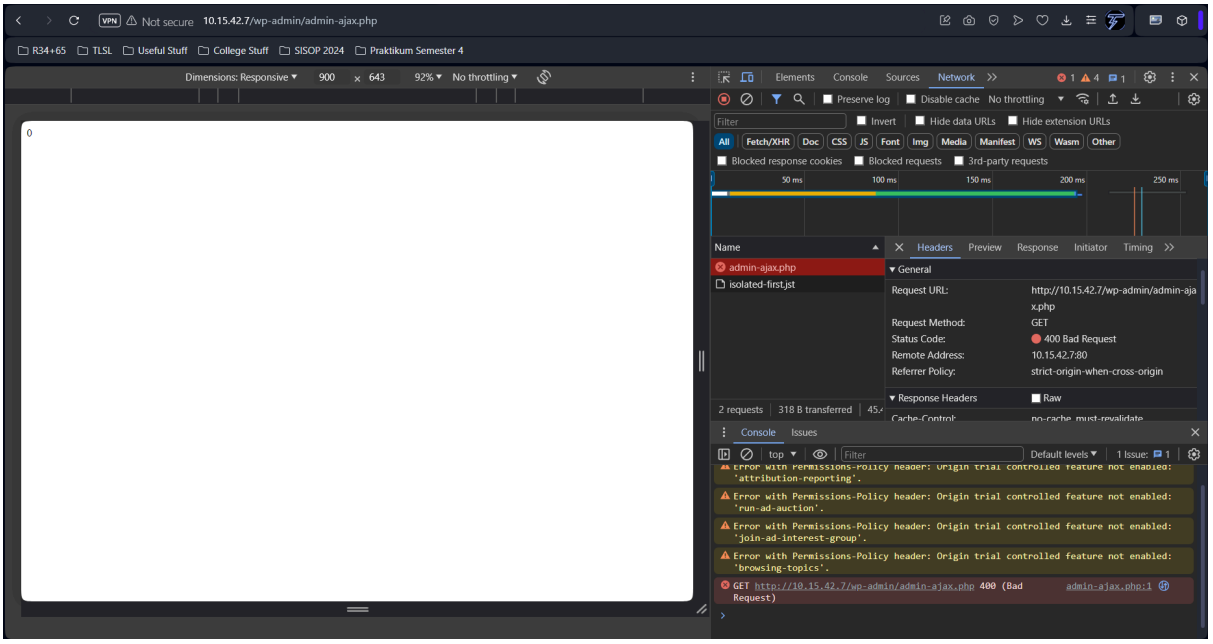
http://10.15.42.7/wp-login.php?redirect_to=http%3A%2F%2F10.15.42.7%2Fwp-admin%2F&reauth=1



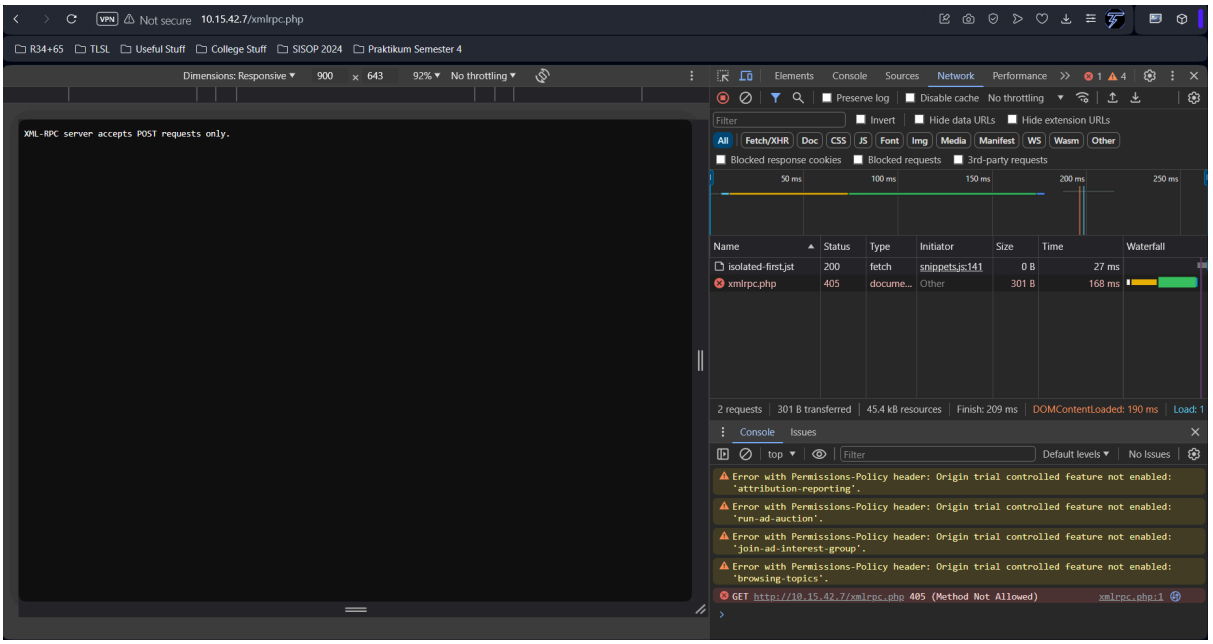
http://10.15.42.7/robots.txt



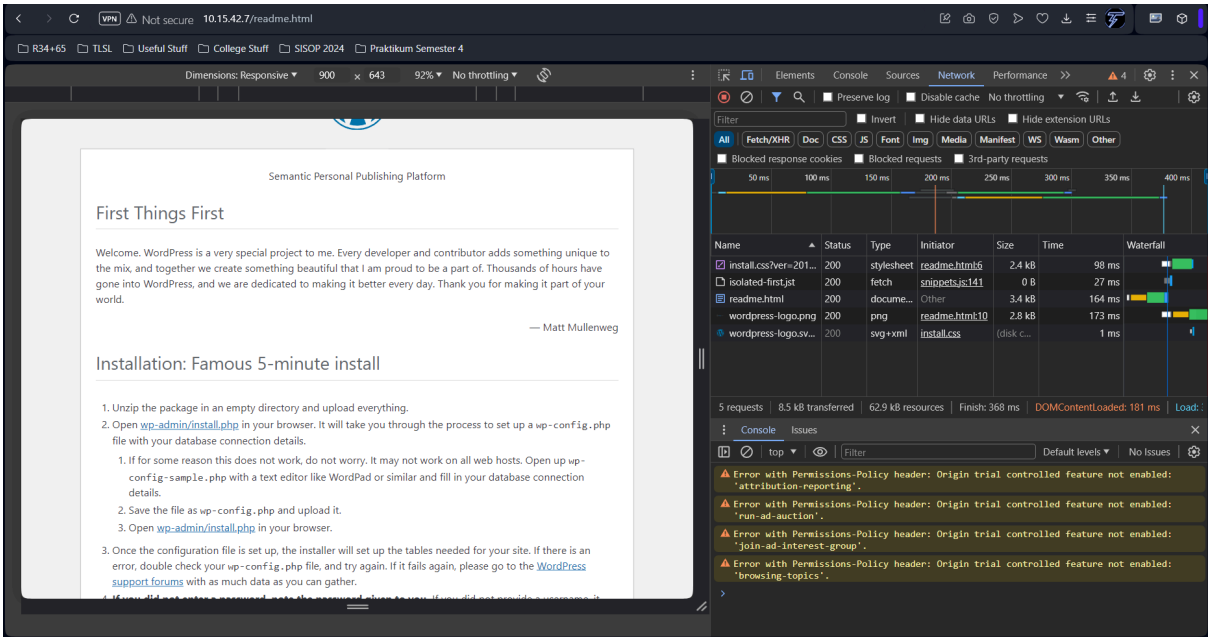
http://10.15.42.7/wp-admin/admin-ajax.php



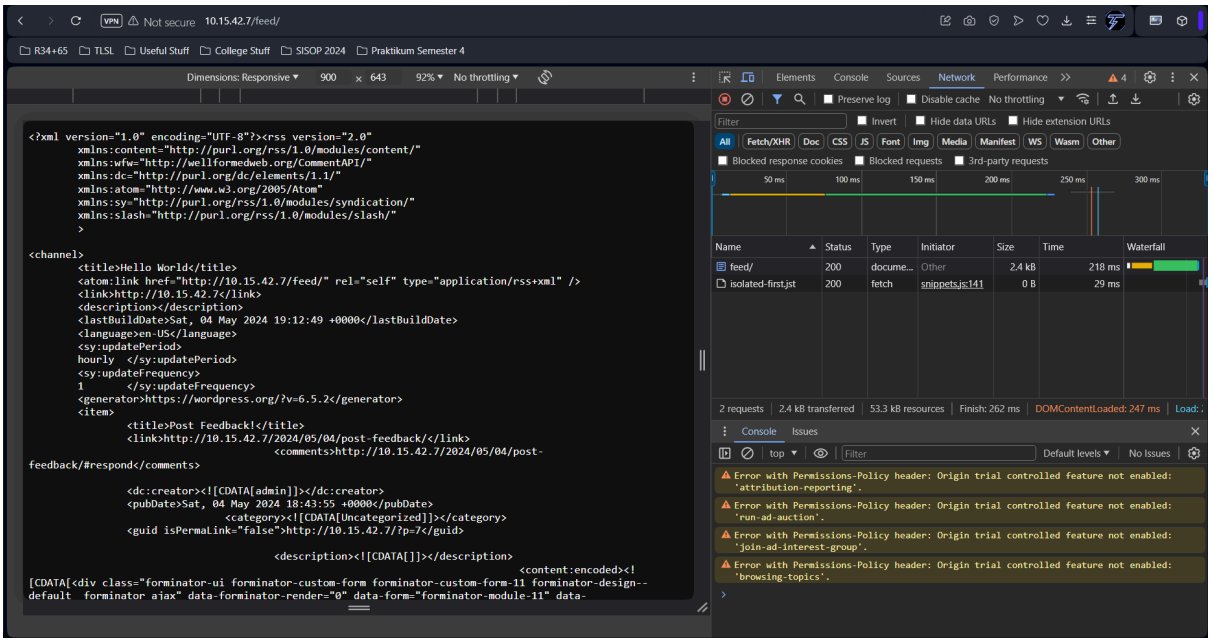
http://10.15.42.7/xmlrpc.php



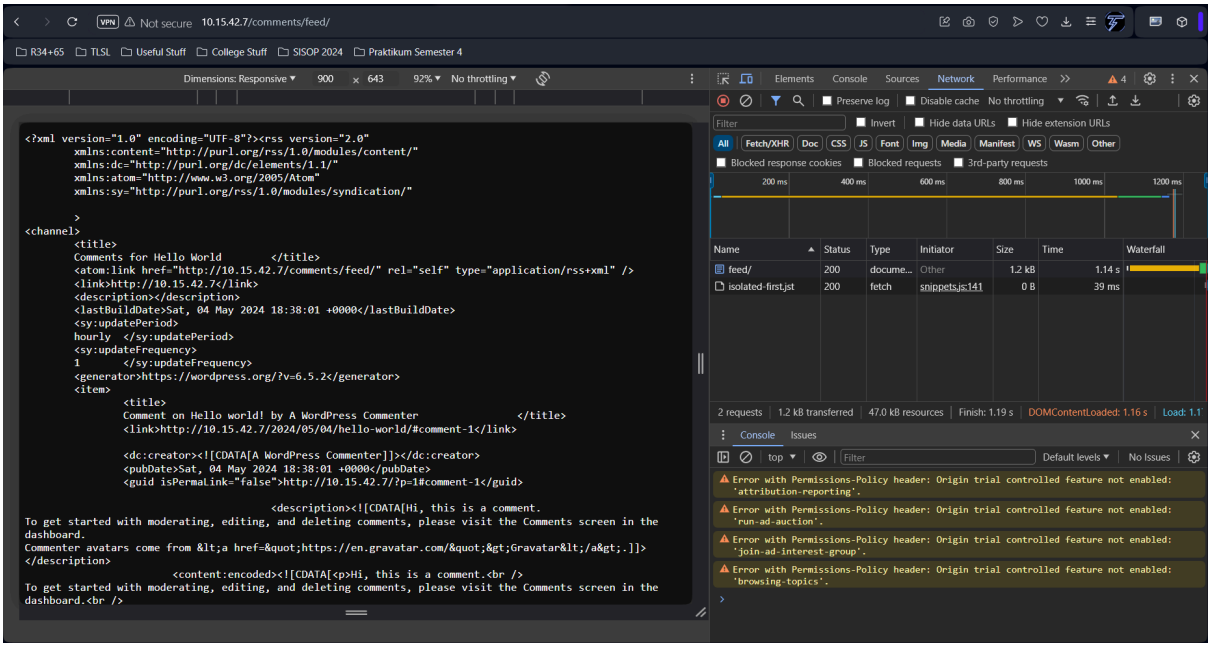
http://10.15.42.7/readme.html



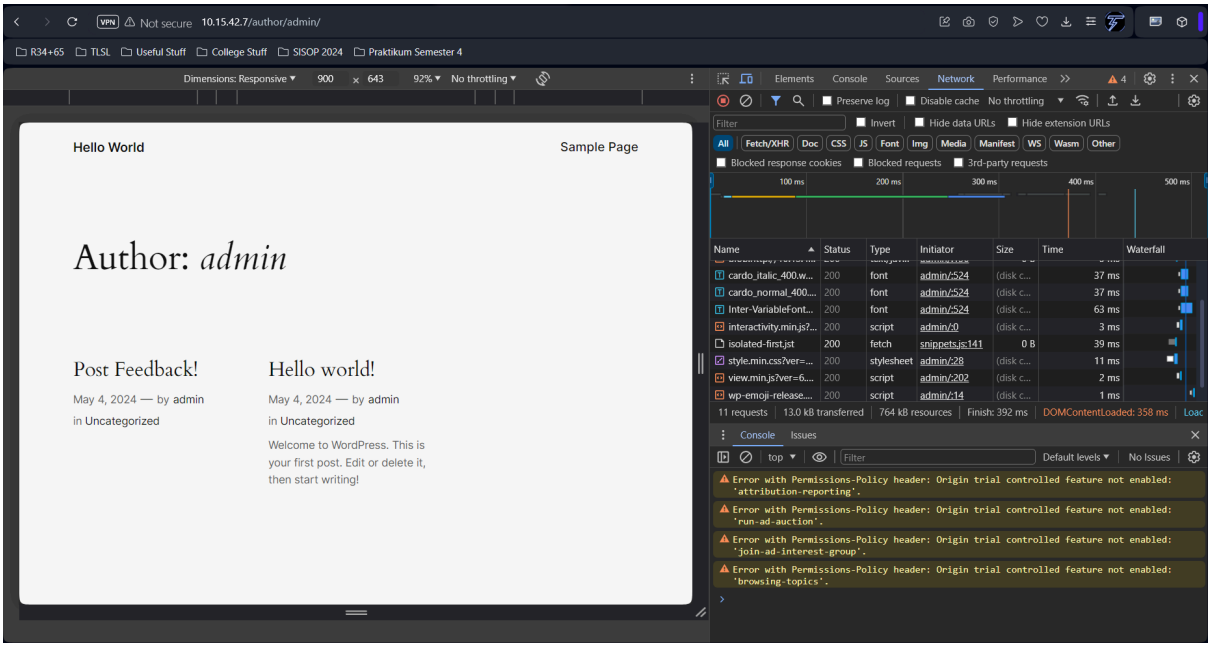
http://10.15.42.7/feed/



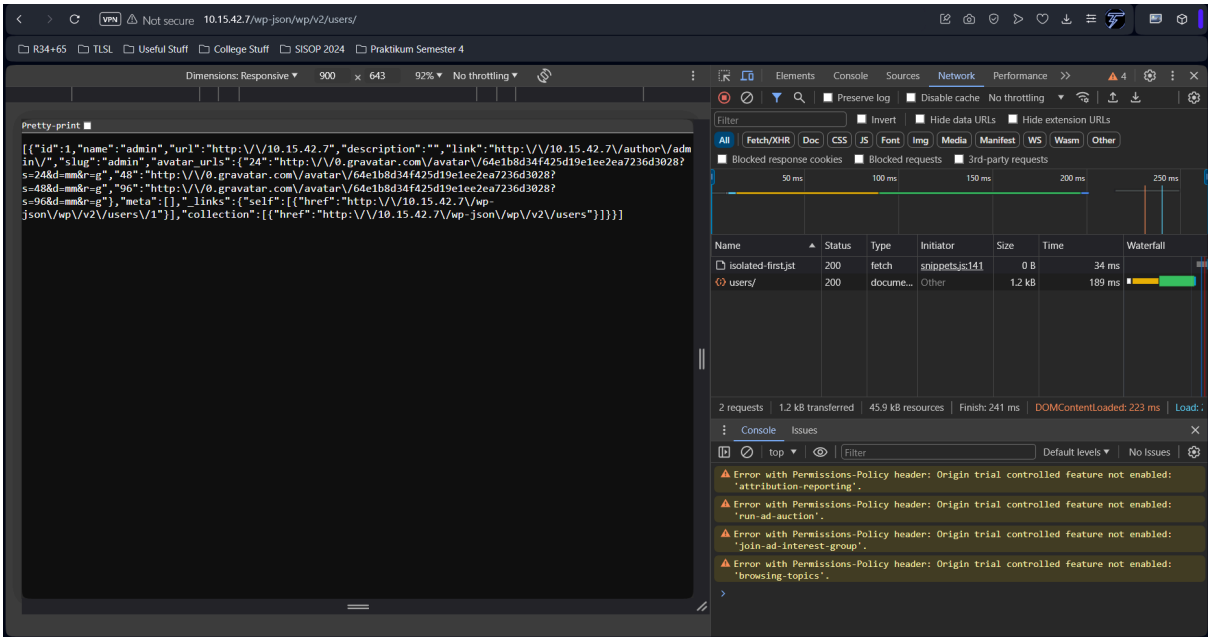
http://10.15.42.7/comments/feed/



http://10.15.42.7/?author=1



http://10.15.42.7/wp-json/wp/v2/users/



Vulnerabilities

1. [wp-user-enum], lewat link itu kita bisa tahu id dana nama usernya. Ditambah brute-force, kita bisa dapat passwordnya juga (https://hackertarget.com/wordpress-user-enumeration/)

2. [CVE-2023-48795], melalui man in the middle, kita bisa melemahkan SSH req, tapi siapa mannya?