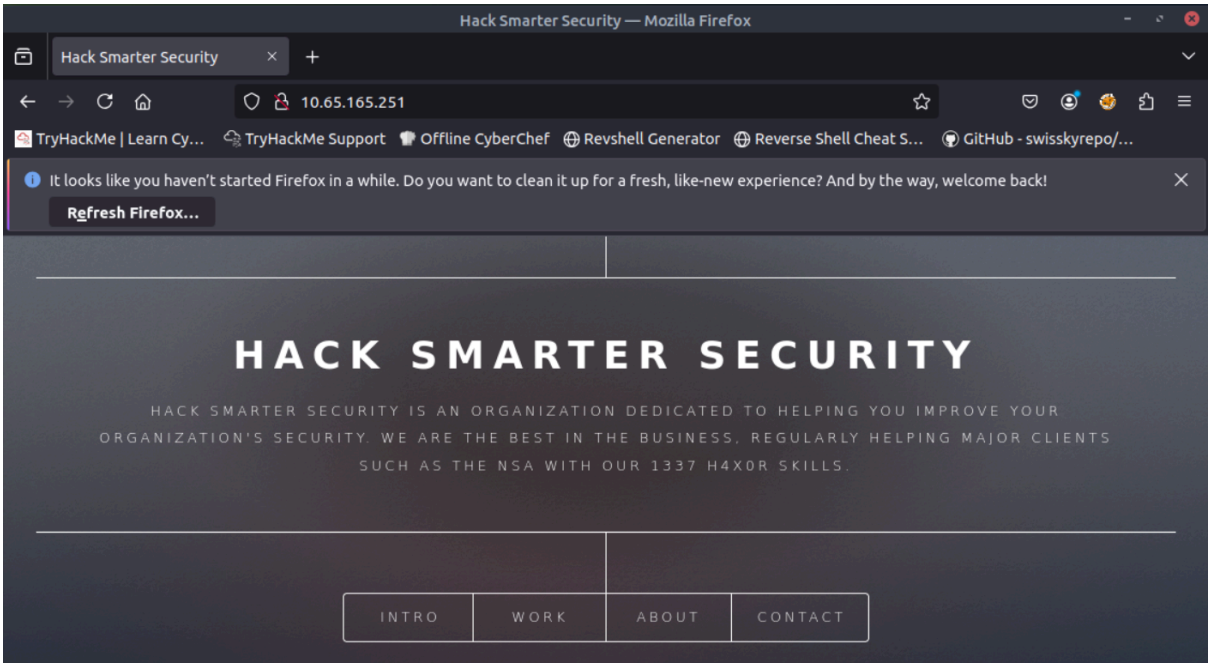
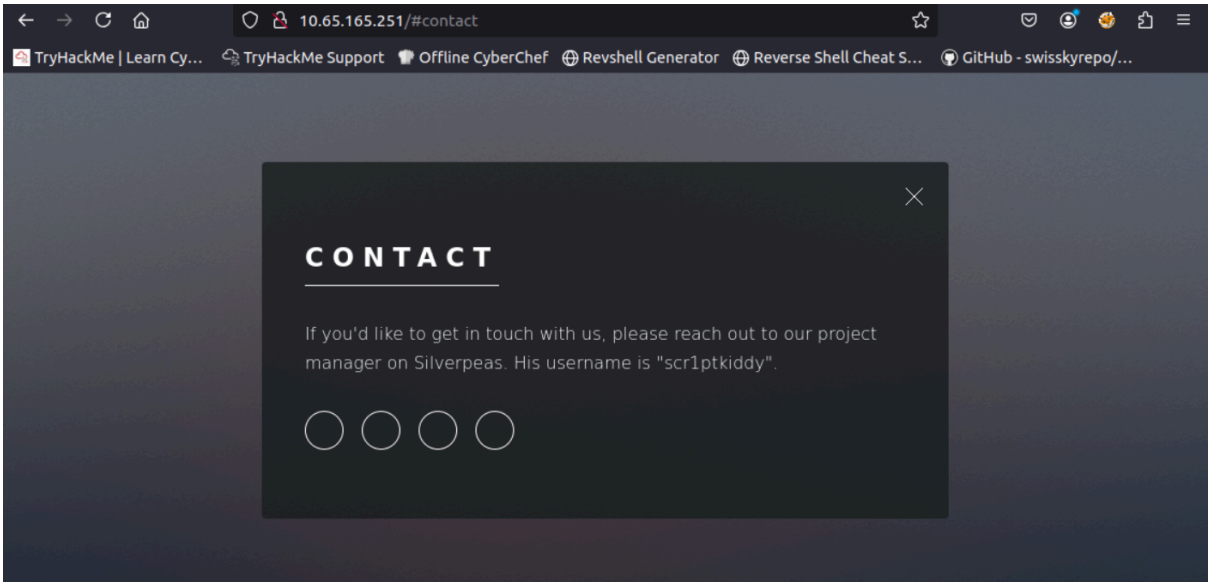
Write up CTF Silver Platter

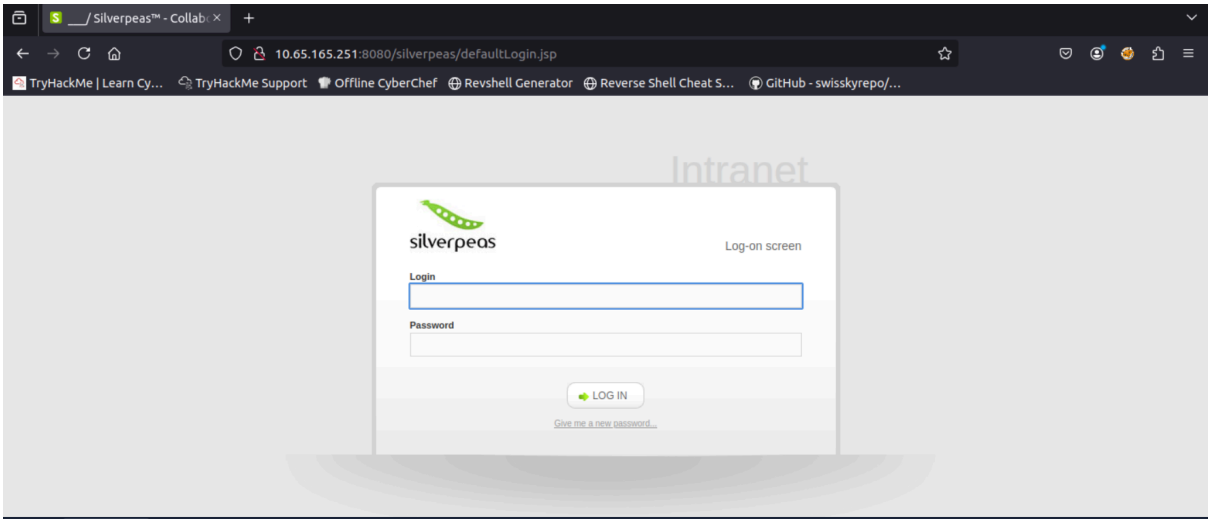
Inicialmente foi feita uma enumeração de portas no IP recebido pelo Nmap para saber o que estava rodando no servidor, foram descobertas as portas 22, 80 e um proxy na porta 8080, como a porta 80 normalmente recebe um serviço web, foi colocado o IP em um browser para ver qual site estava sendo executado:



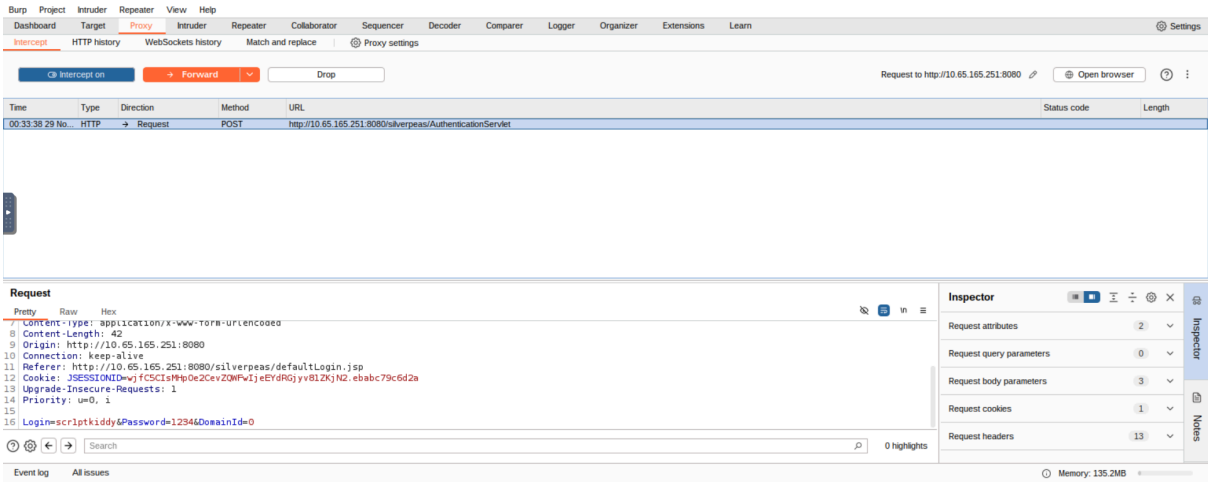
Na aba contact foi encontrado algo interessante, havia o serviço responsável pelo site, o Silverpeas e uma possível credencial de login.



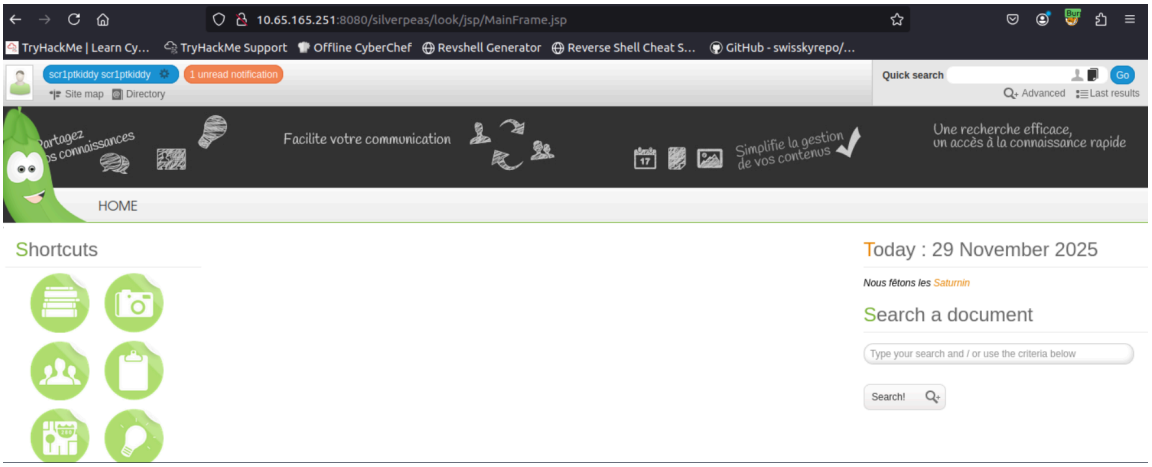
Pesquisando sobre o serviço, foi descoberto que ele roda no proxy mencionado anteriomente

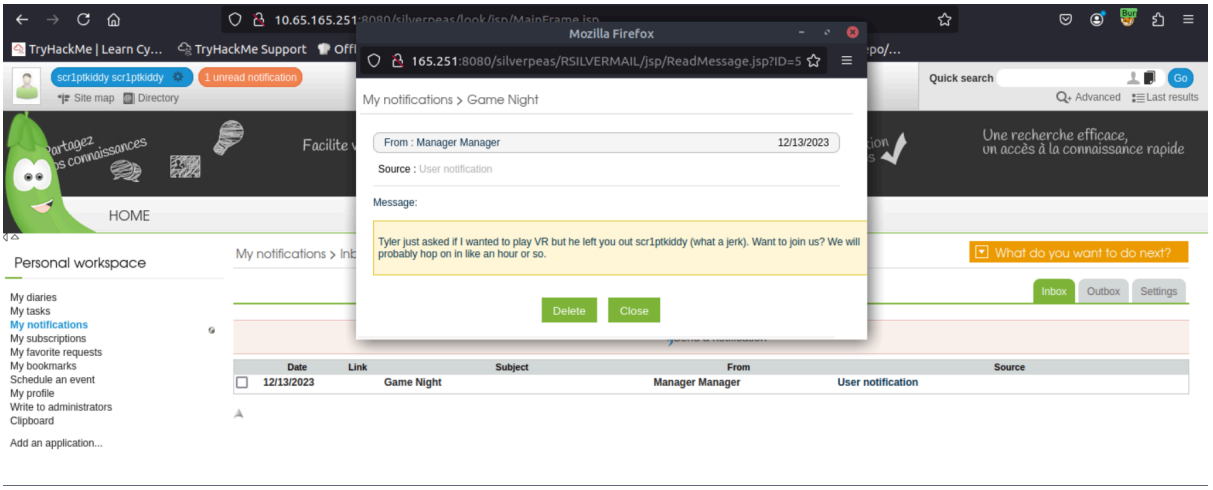


Pesquisando sobre possíveis vulnerabilidades desse serviço, foi encontrado a CVE--2024-36042, que se trata de um authentication bypass, onde podemos interceptar a requisição e apenas apagar o password da requisição para obter login.

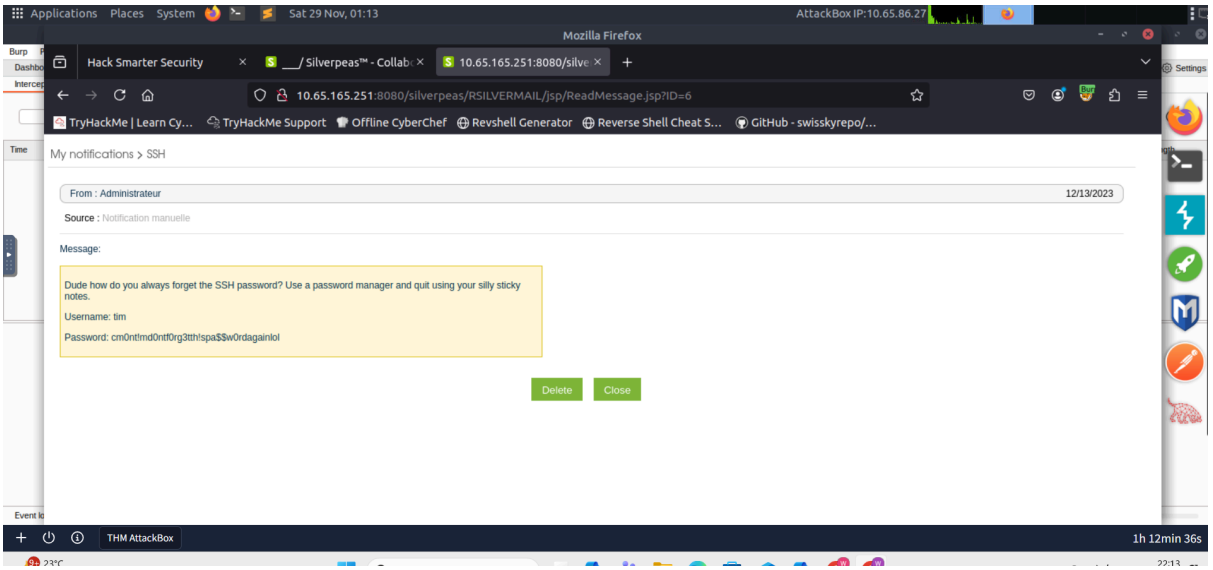


Executando a vulnerabilidade encontramos o seguinte sistema:





Na aba de notificações foi visto um possível IDOR, copiando o url e executando em uma nova aba com id=6, foi confirmado a vulnerabilidade e conseguimos ver a notificação de outro usuário que nos fornece as credências SSH do usuário “tim”.



Após o login, encontramos a flag user.txt.

```
Last login: Wed Dec 13 16:33:12 2023 from 192.168.1.20
tim@ip-10-65-165-251:~$ whoiam
whoiam: command not found
tim@ip-10-65-165-251:~$ whoami
tim
tim@ip-10-65-165-251:~$
```

Agora tentando escalar privilégios para encontrar a flag de root, vemos que há outro usuário no sistema, verificando as permissões no etc/passwd, vemos que o usuário tyler tem permissões de root, então ele passa a ser nosso alvo.

```
tyler:x:1000:1000:root:/home/tyler:/bin/bash
```

Indo para o diretório var/log, podemos ver as entradas que o usuário tyler inseriu no sistema com o comando grep -iR tyler, onde foi encontrado um login no postgres, que nos dar uma possível senha do usuário.

```
auth.log.2:Dec 13 15:38:57 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/apt install docker.io
auth.log.2:Dec 13 15:38:57 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
auth.log.2:Dec 13 15:40:33 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name postgresql -d -e POSTGRES_PASSWORD=_Zd_zx7N8
23/ -v postgresql-data:/var/lib/postgresql/data postgres:12.3
```

Colocando a senha no usuário tyler, foi obtido o login e posteriormente apenas executando sudo su com a mesma senha, obtemos acesso root e por fim a flag de root.

```
tim@ip-10-65-165-251:/var/log$ su tyler
Password:
tyler@ip-10-65-165-251:/var/log$ sudo su
[sudo] password for tyler:
root@ip-10-65-165-251:/var/log# cd ../..
root@ip-10-65-165-251:/# ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  snap  srv  sys  tmp  usr  var
root@ip-10-65-165-251:/# cd root
root@ip-10-65-165-251:~# ls
root.txt  snap  start_docker_containers.sh
root@ip-10-65-165-251:~#
```