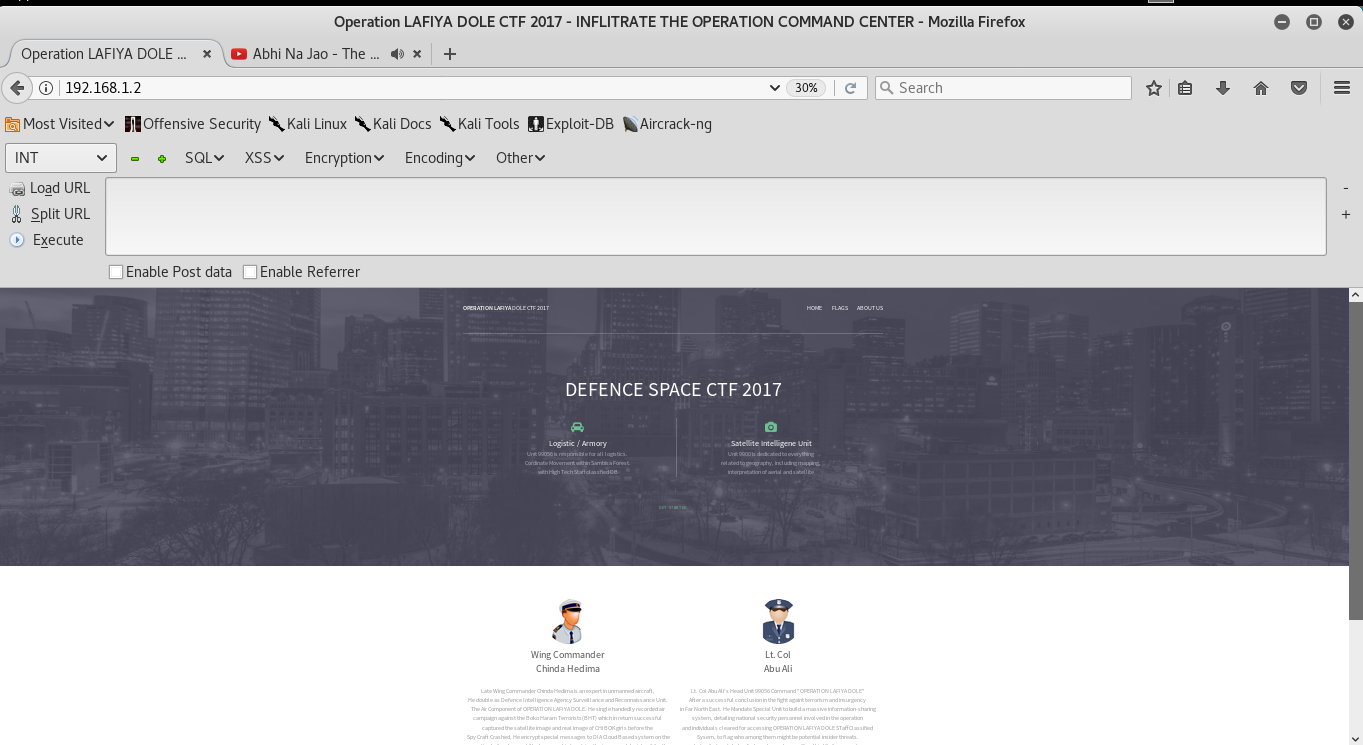
A walkthrough of Defence Space CTF 2017

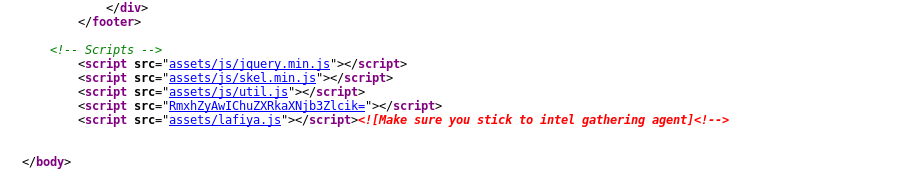
In this walkthrough i’ll show you how i find 7 flags, this CTF is provided by Silexsecure and his team. A big thanks to you guys :)



So the very first approach of every CTF is that, you should know how to gather information, read every small info related to CTF, this would help you to solve machines. In this CTF information gathering is playing a very important role. In this VM we have to find 7 flags and some data through file. Let’s the game begin, but before starting the CTF make sure you have done proper network settings in VM.

**Flag 1-**

The very first thing, do some information gathering, so i started looking at source code and at the last of source code i found some information. As you can see here i found some scripts.



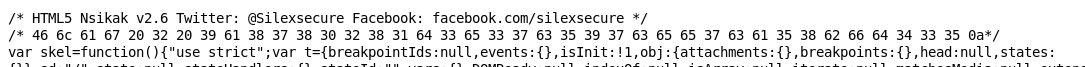
So i start looking at every script which is related to this CTF. But the attention i got in which script that was the base64 encoded code **“RmxhZyAwIChuZXRkaXNjb3Zlcik="** this code was include with script tag. So i found something fishy here, so i simply decode this encoded value and I got my **first flag** which is **Flag 0 (netdiscover).**

**Flag 2-**

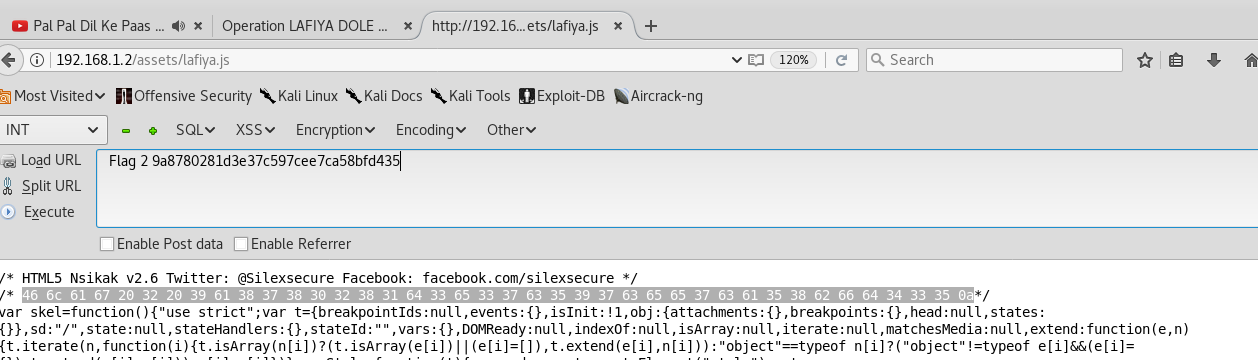
As i said, information gathering is the key to success and it will help you a lot to solve CTF challenges, so i start reading the source code of the application. First time when i read source code actually i was not getting anything and i was little bit confused, but later **script** part comes in my mind in which i attracted more into the **lafiya.js** file.



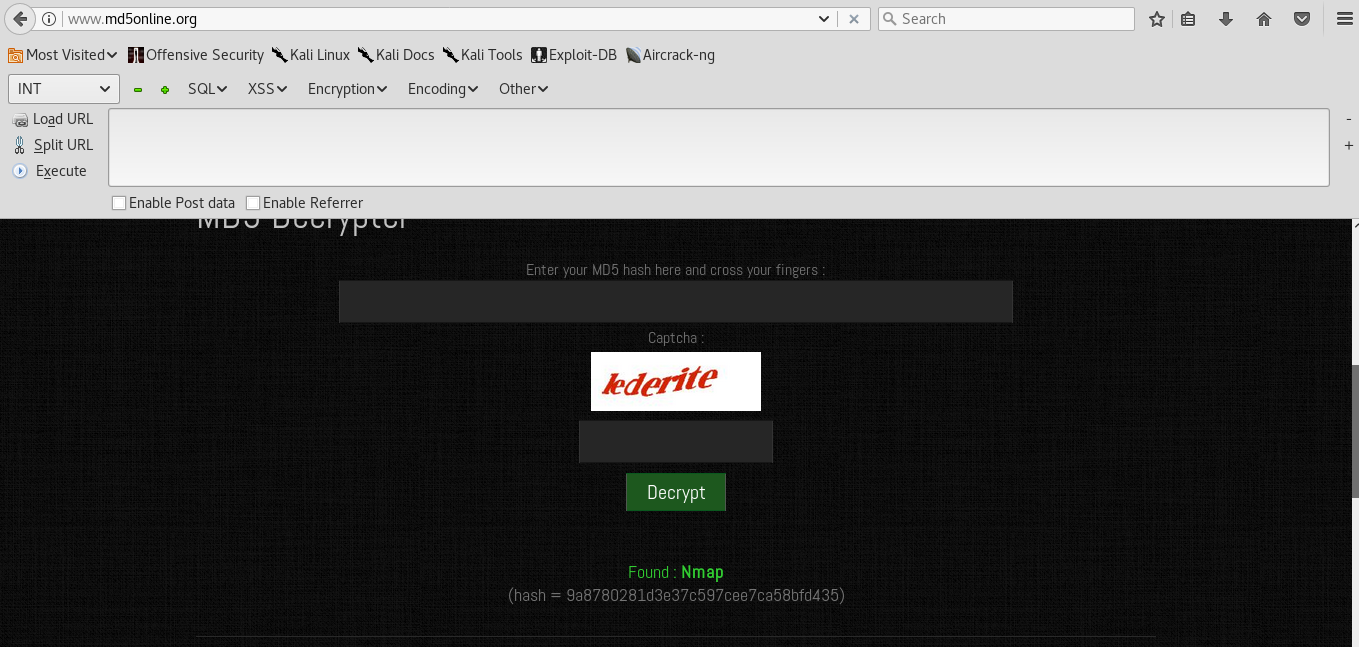
So I click on it and start reading the code. After landing into the **lafiya.js** file, i got more confused but i found a mail id, a date a google map code and a hex value on the top section of comment.



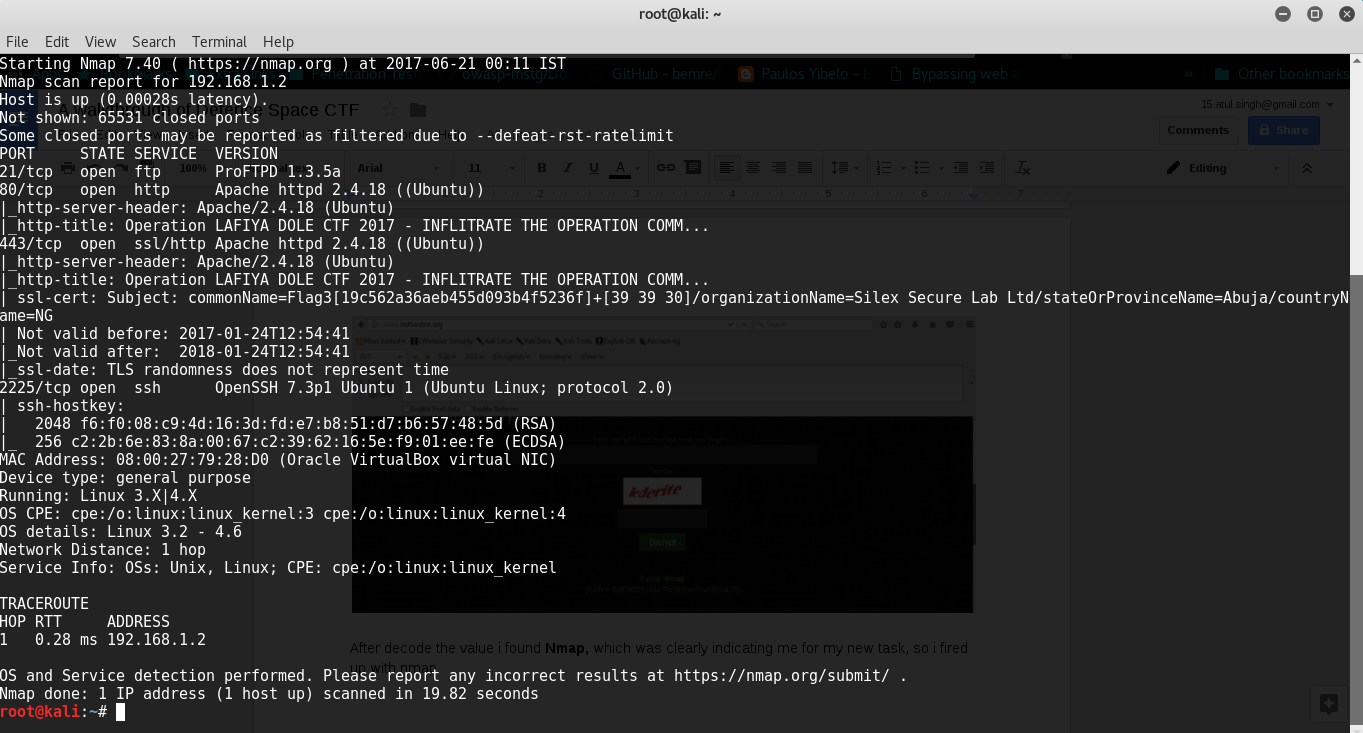
So i again fire up my hackbar :) to decode the value and i got my **second flag** which is **Flag 2 9a8780281d3e37c597cee7ca58bfd435.**



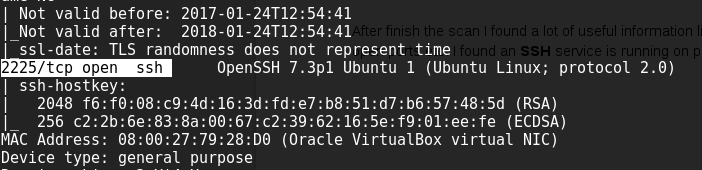
But still something was hidden and i was not getting, I just notice the flag 2 it was in encoded format, so I decide to decode it and try to get some information. Bingo :) I was correct there was a hidden code **Nmap**.



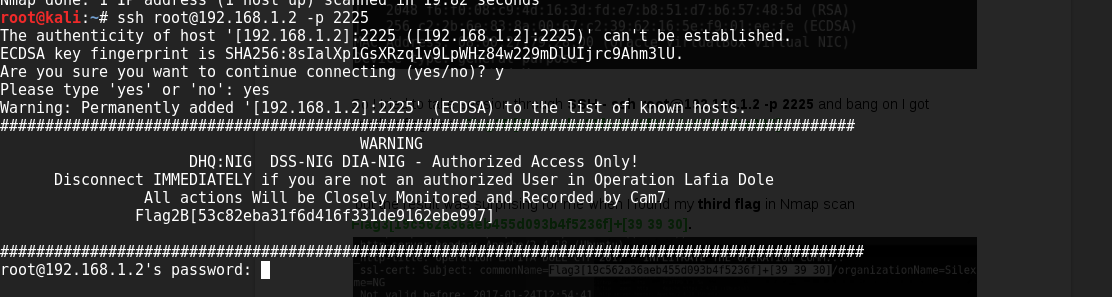
After decode the value i found **Nmap,** which was clearly indicating me for my new task, so i fired up with nmap



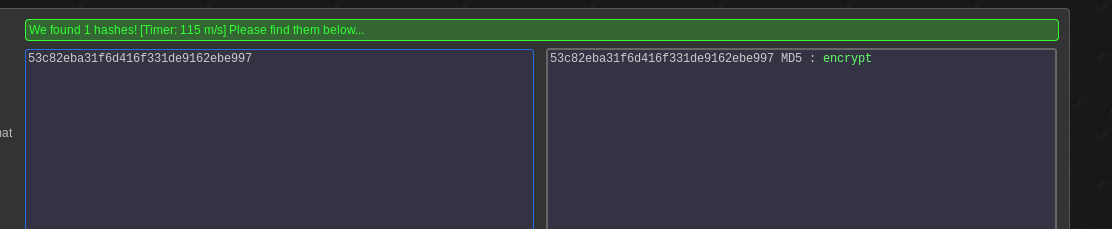
After finish the scan I found a lot of useful information like OS version, Web server information, open ports etc. I found an **SSH** service is running on **port 2225**.



So I tried to take session through **SSH - ssh root@192.168.1.2 -p 2225** and bang on I got another flag here **Flag2B[53c82eba31f6d416f331de9162ebe997].**

****

This flag was in MD5 hashes, so i decided to decrypt MD5 hash value and found my another clue **encrypt**.

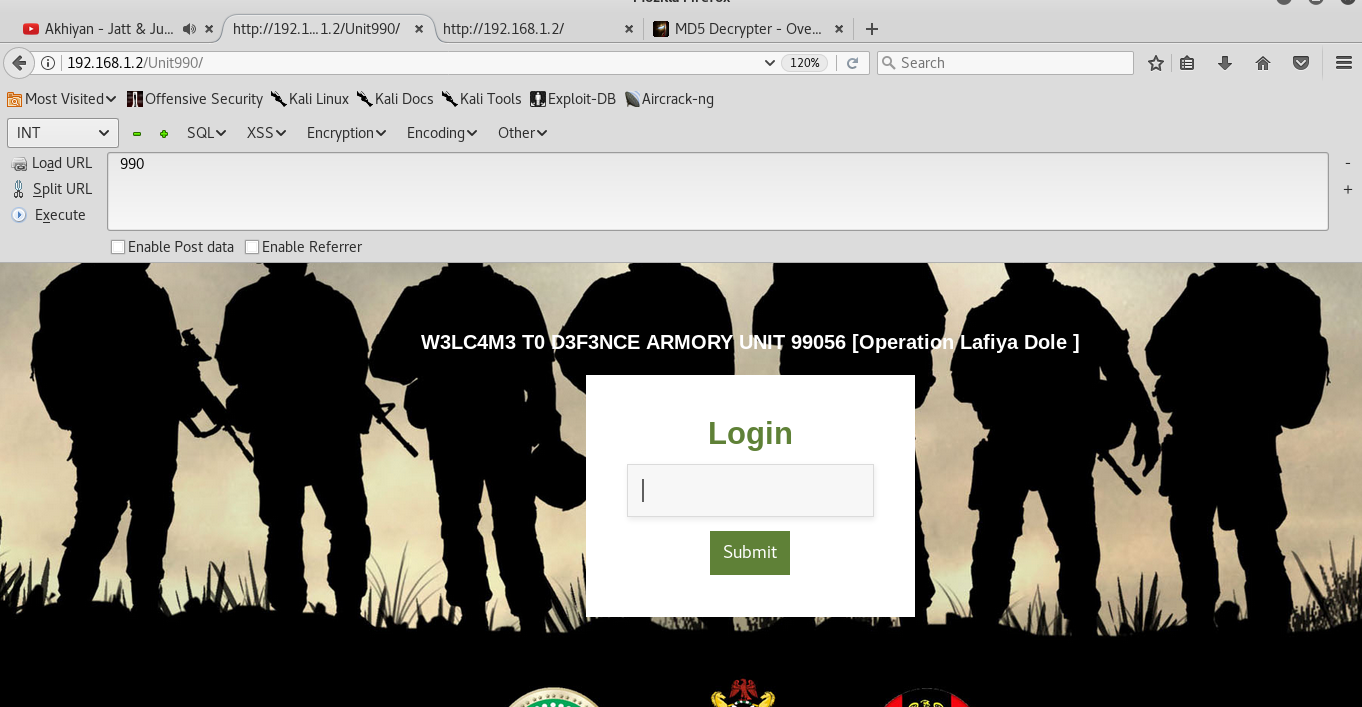


After getting another Flag I was so excited so again I look into the Nmap scan result, and the result was surprising for me when I found my **third flag** in Nmap scan **Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30].**

****

After getting 3 Flags in a row, I was on high now, I was trying to find the rest of the flags as soon as possible. As I got hint from my third flag, I tried to solve the decrypted value **19c562a36aeb455d093b4f5236f** and later I fireup md5decryptor and got this as result **Unit**, so I decided to go with only **39 39 30** when i decode this value to **Hex to Characters** another value i got **990**.

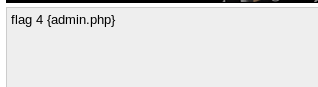
As we can see in source Unit 990 was managed by Lt. Col Abu Ali. So I put this with the browser URL which was [**http://192.168.1.2/Unit990/**](http://192.168.1.2/Unit990/) **,** so i fired this on my browser.

****

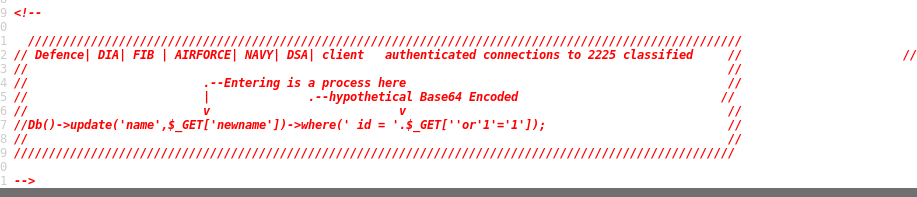
Quickly I start looking into the source code, so that I can get hint. In the source at the bottom I found a comment where i found this value **ZmxhZyA0IHthZG1pbi5waHB9**



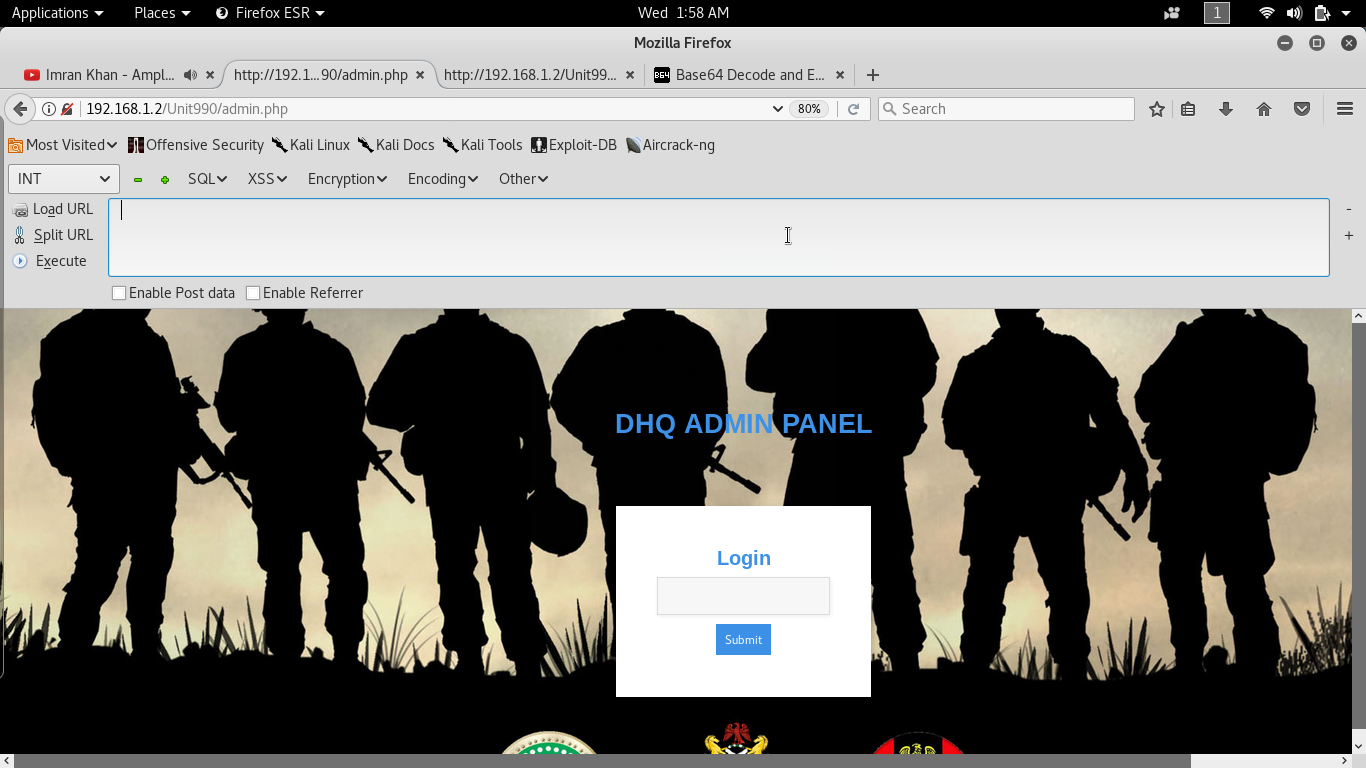
After decoding above value i found my **fourth flag** ;) and it was **admin.php**

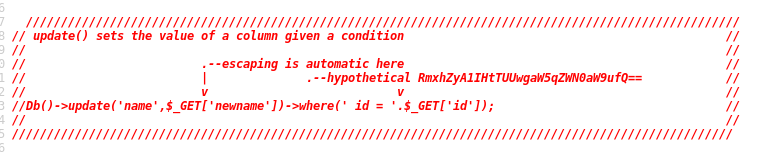


But it was not all over, after looking at the end of the source code i found a SQL Injection hint with some hints.



As our **fourth flag** we found another admin.php page, so i was excited to look into this.

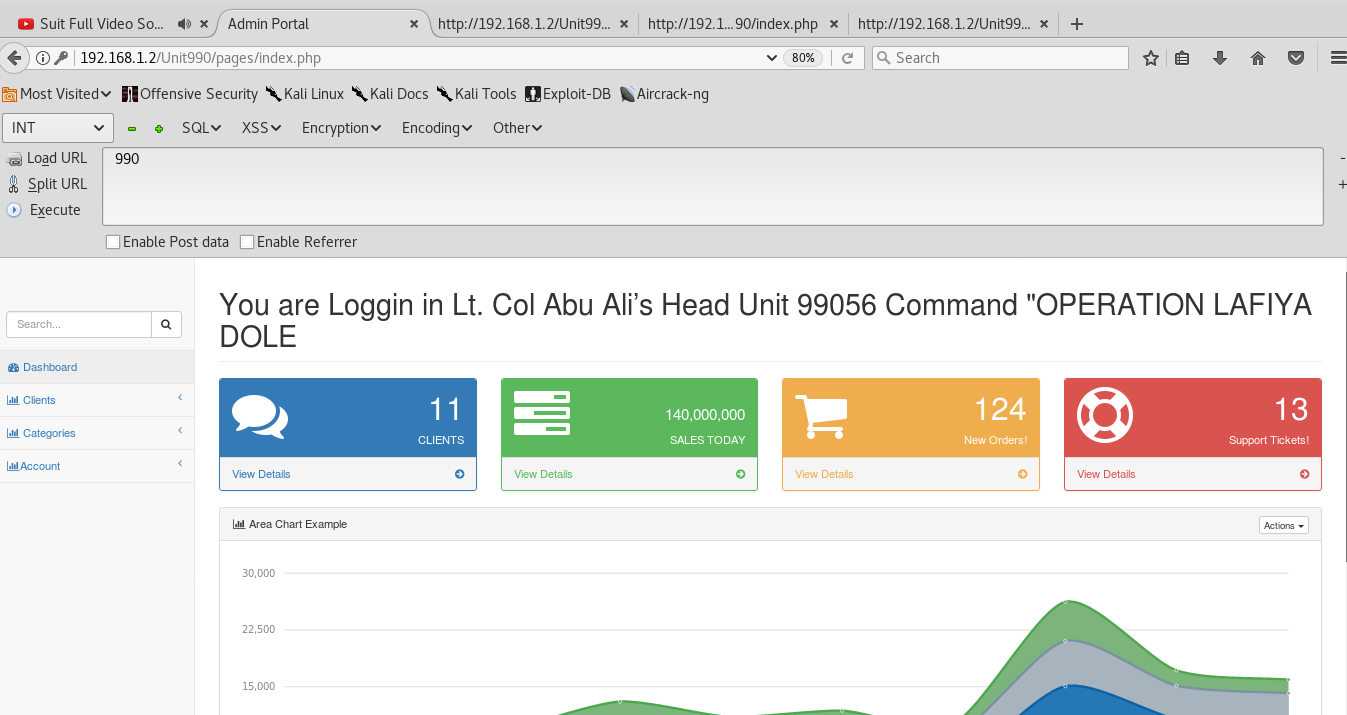




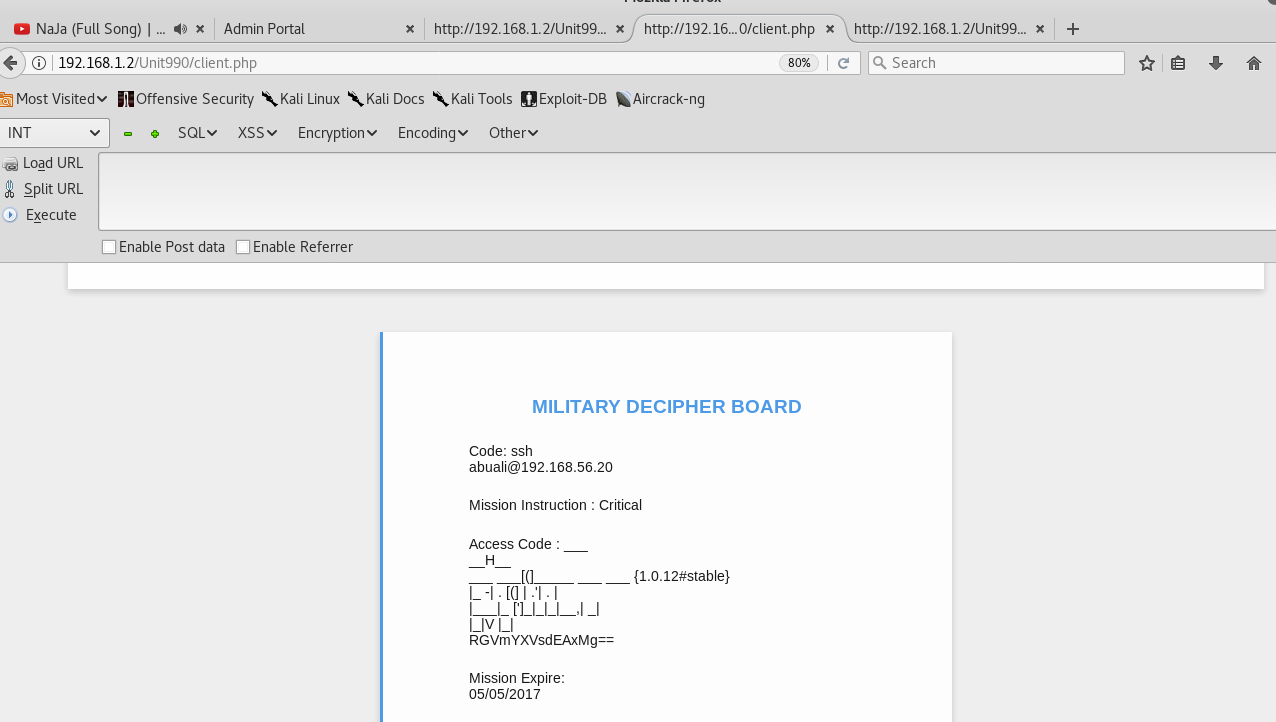
Here i found another base64 value **RmxhZyA1IHtTUUwgaW5qZWN0aW9ufQ==**, so i decode this value and found my another **fifth flag**, which is **Flag 5 {SQL injection}**.



It was time to try SQL Injection technique, so as i got hint from my fourth flag **admin.php**, where i found sql injection code, so I try that code **'or'1'='1** and boom i was in admin panel.

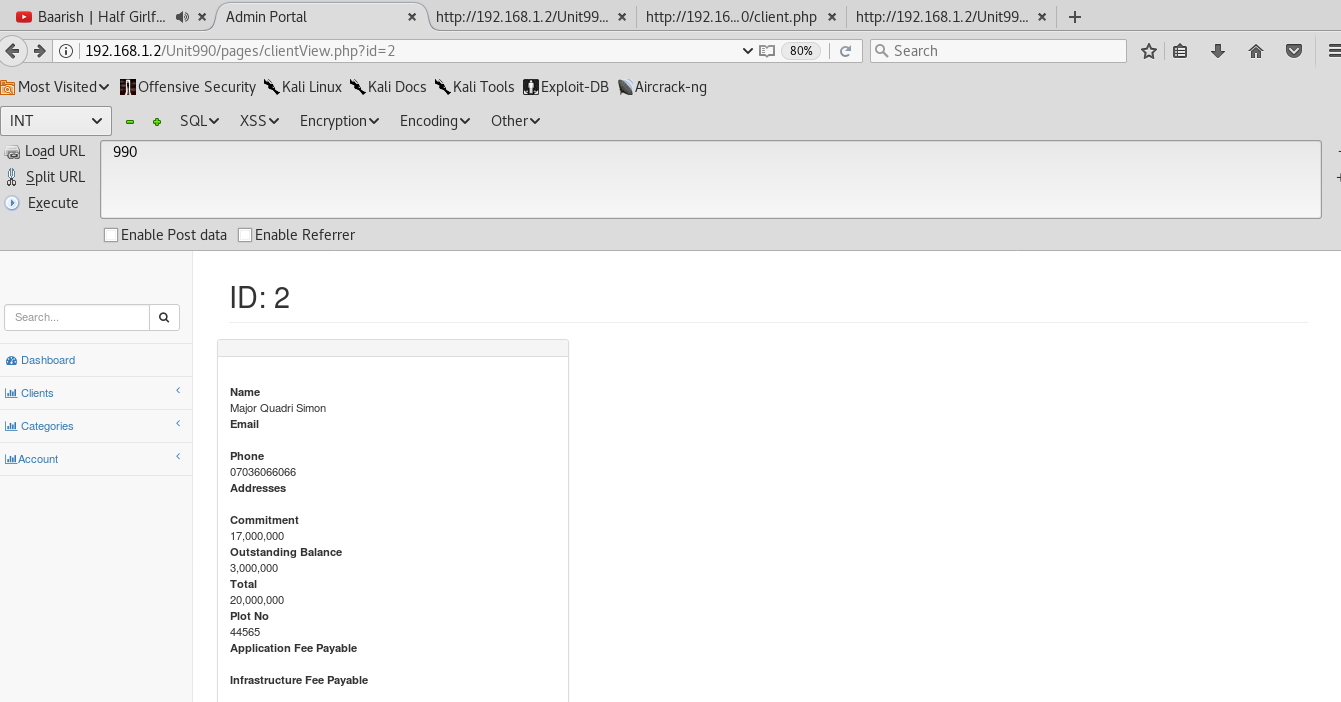


After logging into the admin panel of Lt. Col. Abu Ali’s i start looking for more information as much as i can get. I again went to the <http://192.168.1.2/Unit990/index.php> and login into this.

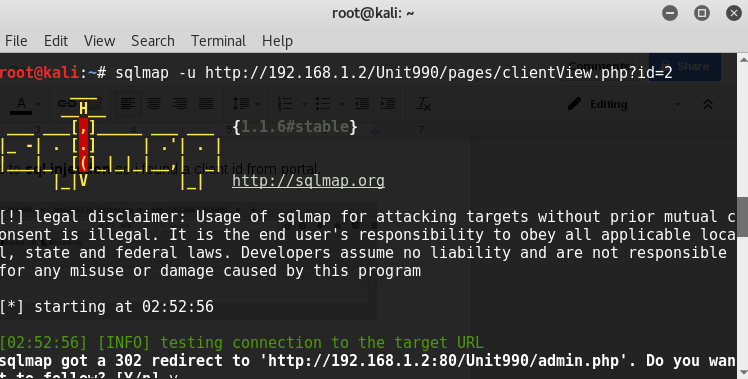


After logging into the application i again found a base64 code **RGVmYXVsdEAxMg==** after decoding the value i found **Default@12**.

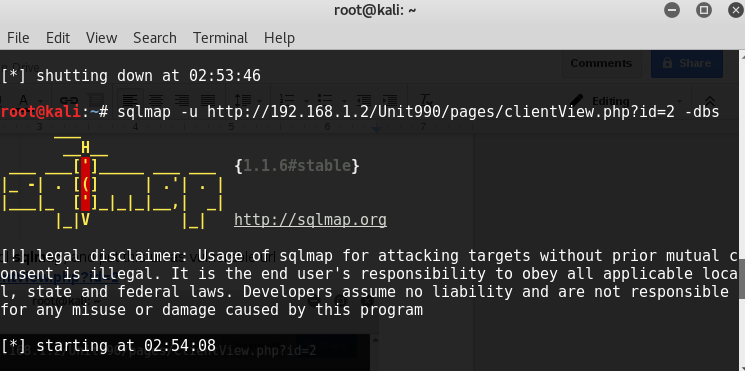
As per **fifth flag** next flag will be related to **sql injection** so i found a client id from portal.

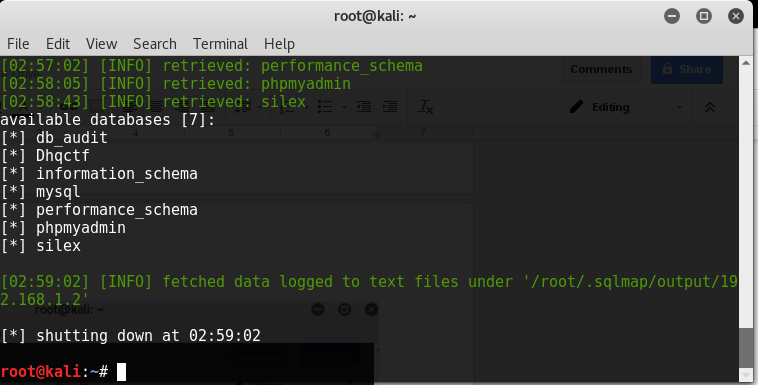


So i just go with one of my favourite tool **sqlmap**, and put this url as vulnerable url [**http://192.168.1.2/Unit990/pages/clientView.php?id=2**](http://192.168.1.2/Unit990/pages/clientView.php?id=2)

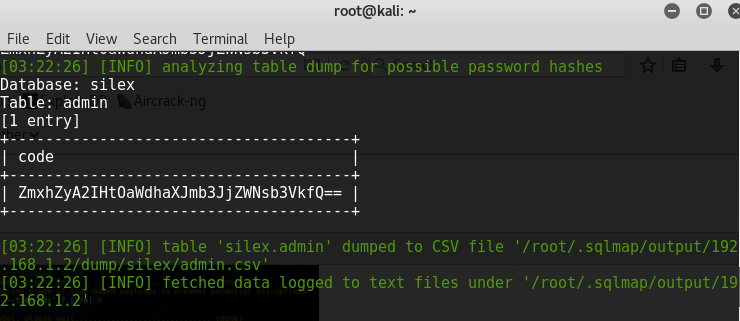
****

After the process, i tried to find the database,

****

****

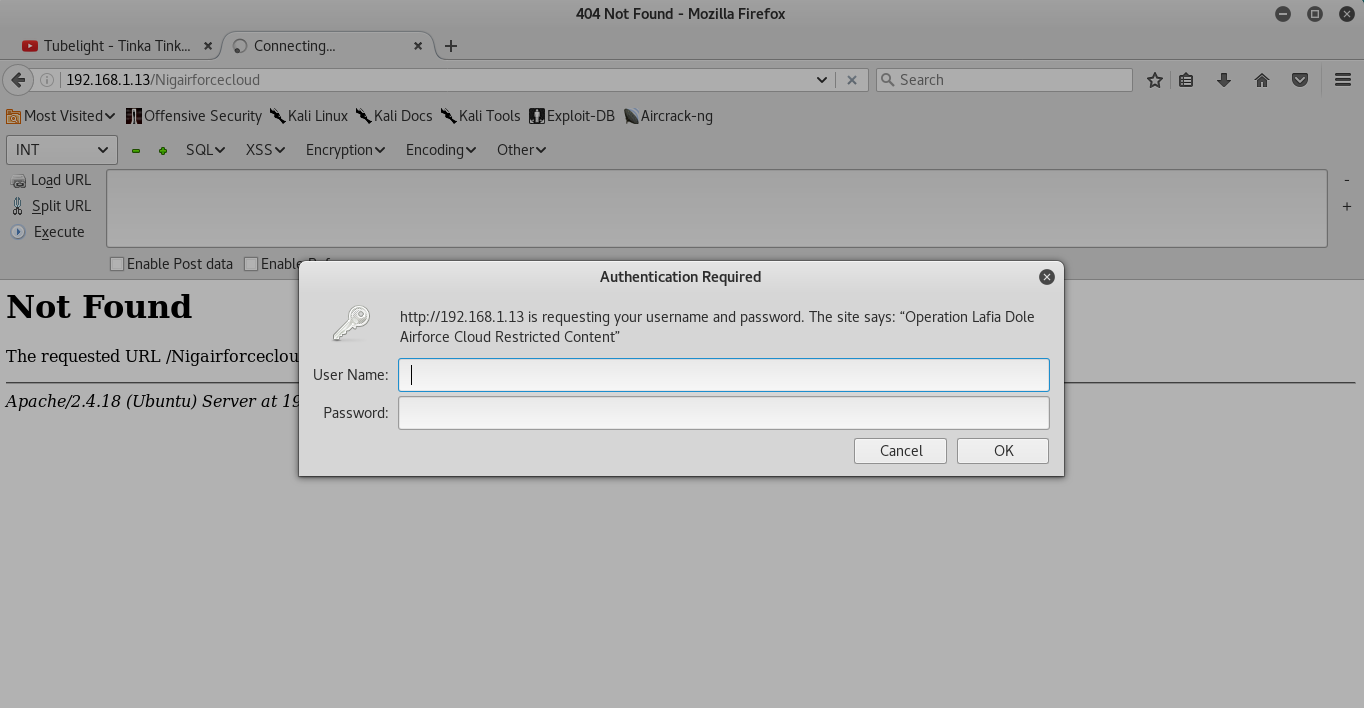
And luckily i got the database **silex**. Let’s try to get more details from database. After getting the database i tried to dump the password but again i got base64 value and seriously now i was fedup of getting too much base64 values, encoding, decoding etc. ;)



Here is the Code **ZmxhZyA2IHtOaWdhaXJmb3JjZWNsb3VkfQ==** or maybe i can say it was the path of my next flag ;) and it was really the path of my next **flag 6,** after decoding the value i found my **sixth flag** **flag 6 {Nigairforcecloud}**.

After getting sixth flag now i was on high weed again, was thinking about the next hint, anywhich case i had one hint which was **Nigairforcecloud**, so i put this flag with URL to see what will happen next. So i just fired up with **Nigairforcecloud**, to see what is going to happen next.

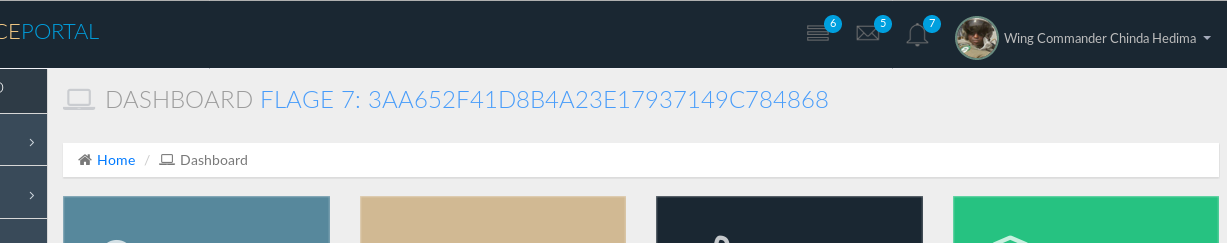
Here you will see the difference between my previous IP and this last IP, it happen because i need to take restart of my system so please don’t confuse between two different IPs :). So when i fired up it gives me a pop up which was asking for user credentials but what were those credentials even i was not aware, so i again start reading the lafiya.js file which we found during first flag.



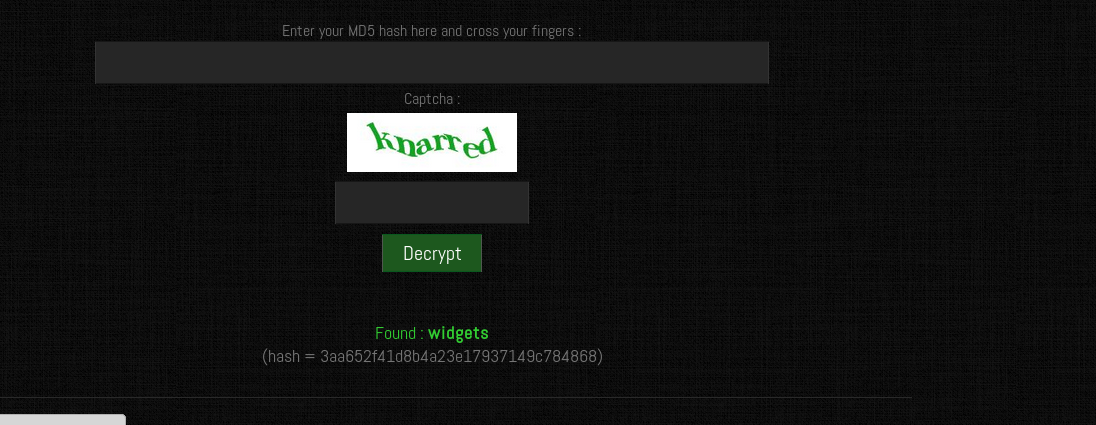
If you will look into the source code of lafiya.js there was a comment “**There is a big shoe to fill. Lord I need your feet”.** Here i found an email id(c.hedima@airforce.mil.ng) with a google map coordinate (maps/kanuri/Borno/@11.8664433,10.9088387,7z) which i already discussed.



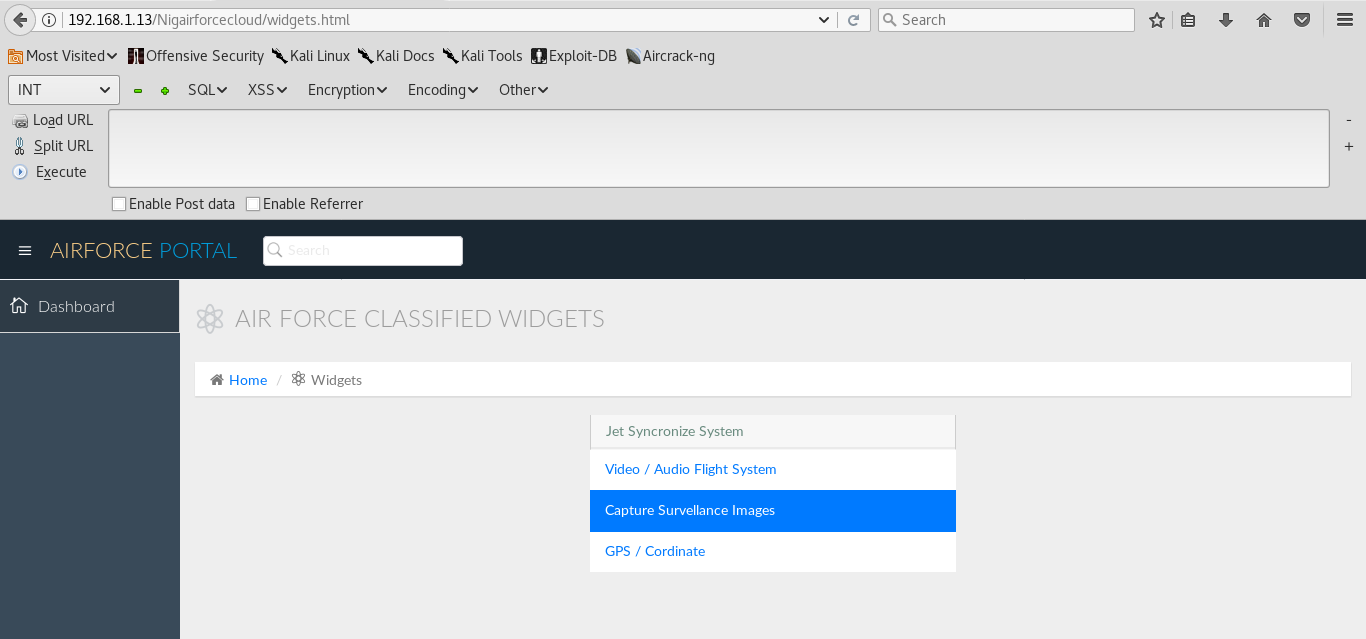
At this moment only one thing i can say i don’t have any single clue about password, and on email id i can trust as username only 10%. So one by one i went through every map coordinate as password and it was a double happines for me when i found Borno as a password :) and after login i found my final flag on dashboard **flage 7: 3aa652f41d8b4a23e17937149c784868**.



When i clicked on the flag 7 nothing happened. So i try to decrypt the value and found **widgets flag**.



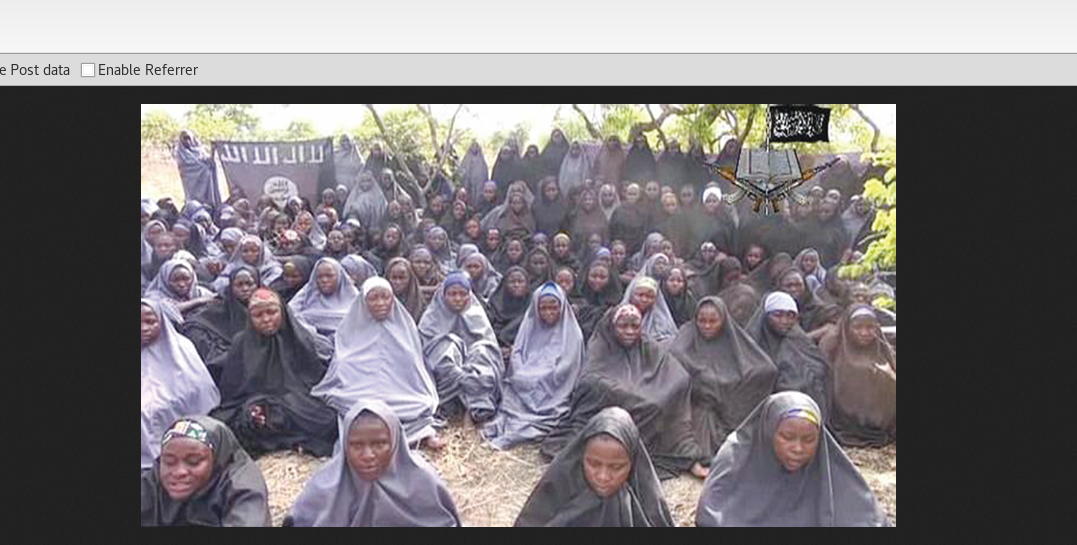
I was excited to know what information he was sending to Defense Intelligence. I start digging into the dashboard and in widgets section, there i found three files.



When i clicked on first link Video/Audio Flight Systems it popup and i saved this file.



Then i go with second link where i found a satellite image and i saved this image also.

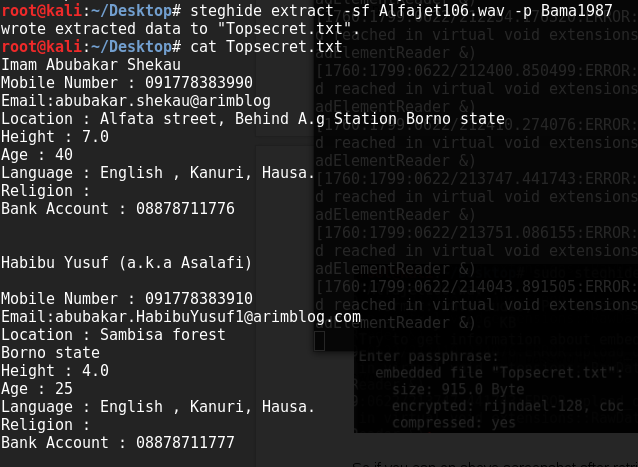


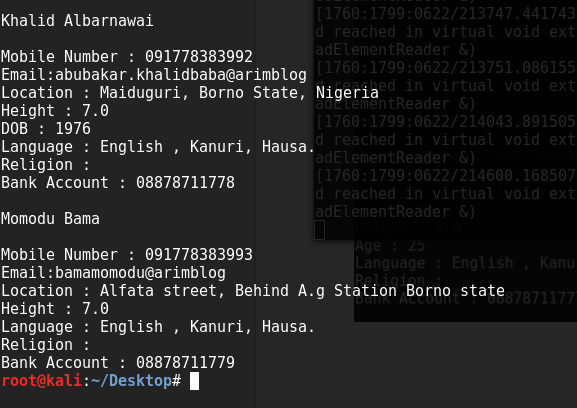
When i tried to click on GPS/Coordinate section nothing happened :( . As a security researcher i’m aware people sending messages via steganography i.e. hiding personal information in audio/video or behind images. So i go with very first file which i got .**wav file**.

While decoding the file it ask me for password, so i again went to **lafiya.js**, and found Bama1987 as password.



So if you can on above screenshot after retrieving data from Alfajet106.wav file it shows me an embedded file **“Topsecret.txt”.**





Below are the seven flags.

1. RmxhZyAwIChuZXRkaXNjb3Zlcik= - Flag 0 (netdiscover)
2. Flag2 9a8780281d3e37c597cee7ca58bfd435 (Nmap)
3. Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]
4. Flag 4 ZmxhZyA0IHthZG1pbi5waHB9 {admin.php}
5. Flag 5 RmxhZyA1IHtTUUwgaW5qZWN0aW9ufQ== {SQL injection}
6. Flag 6 ZmxhZyA2IHtOaWdhaXJmb3JjZWNsb3VkfQ== {Nigairforcecloud}
7. Flage 7: 3aa652f41d8b4a23e17937149c784868 (widgets)