

# BRUTE FORCE SALDIRILARI VE SAVUNMA

Öğretim Görevlisi A. Berika VAROL MALKOÇOĞLU

# İçindekiler

- Brute Force Saldırısı Nedir?
- Nasıl kourunulur?
- Nasıl uygulanır?

# Brute Force Nedir?

- Brute Force (kaba kuvvet saldırısı) kullanıcıya ait parolayı doğru bir şekilde tahmin etmek için birçok deneme yapma işlemidir.
- Saldırgan, doğru olanı bulana kadar tüm olası parolaları sistematik olarak kontrol eder.
- Bu saldırı türüne karşı önlem alınmadıysa sisteme istediğimiz kadar ya da oluşturduğumuz wordlist'teki kelime kadar deneme yapılabilir.
- Wordlist'teki kelime ve parola eşleşirse giriş başarıyla gerçekleşir.

# Nasıl Korunulur?

- Web sitelerinde güvenlik eklenti/yazılımları yüklü ve aktif durumda olmalı,
- İki faktörlü kimlik doğrulama sistemi kullanılabilir,
- Daha uzun şifre tercihi,
- Sizinle ilgili olmayan (doğum yılınızı ya da tuttuğunuz takımı içermesi gibi) şifreler,
- Aynı şifrenin birden fazla platformda kullanılmaması gerekir.

# Damn Vulnerable Web Application (DVWA) Nedir?

- Savunmasız bir PHP / MySQL web uygulamasıdır.
- Temel hedefleri, güvenlik uzmanlarının becerilerini ve araçlarını yasal bir ortamda test etmelerine yardımcı olmak
- Web geliştiricilerinin web uygulamalarını güvenli hale getirme süreçlerini daha iyi anlamalarına yardımcı olmak.
- Öğretmenlerin / öğrencilerin bir sınıf ortamında web uygulama güvenliğini öğretmelerine / öğrenmelerine yardımcı olmaktır.

# DVWA içerisinde bulunan zafiyetler;

- Zafiyeleri;
  - Brute Force
  - Command Execution
  - CSRF
  - File Inclusion
  - SQL Injection
  - Upload
  - XSS Reflected
  - XSS Stored
- Ayrıca DVWA Sisteminde 3 tane zorluk seçeneği vardır.Bunlar low,medium ve high dir.

# Kali'de DVWA Nasıl Kurulur?

- Öncelikle **service apache2 start** ve **service mysql start** komutları ile apache ve mysql servislerini başlatıyoruz.

```
root@kali:/# sudo /etc/init.d/apache2 start
[ ok ] Starting apache2 (via systemctl): apache2.service.
root@kali:/#
root@kali:/# sudo /etc/init.d/mysql start
[ ok ] Starting mysql (via systemctl): mysql.service.
root@kali:/#
```

# Kali'de DVWA Nasıl Kurulur?

```
root@kali:/# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: active (running) since Fri 2020-11-13 07:21:17 EST; 14min ago
   Process: 1374 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCE
   Main PID: 1385 (apache2)
   Tasks: 8 (limit: 4915)
   CGroup: /system.slice/apache2.service
           └─1385 /usr/sbin/apache2 -k start
           └─1386 /usr/sbin/apache2 -k start
           └─1387 /usr/sbin/apache2 -k start
           └─1388 /usr/sbin/apache2 -k start
           └─1389 /usr/sbin/apache2 -k start
           └─1390 /usr/sbin/apache2 -k start
           └─1391 /usr/sbin/apache2 -k start
           └─1985 /usr/sbin/apache2 -k start
```

```
Nov 13 07:21:17 kali systemd[1]: Starting The Apache HTTP Server.
Nov 13 07:21:17 kali apachectl[1374]: AH00558: apache2: Could not
Nov 13 07:21:17 kali systemd[1]: Started The Apache HTTP Server.
lines 1-19/19 (END)
```

```
root@kali:/# service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
   Loaded: loaded (/etc/init.d/mysql; generated; vendor preset: disabled)
   Active: active (running) since Fri 2020-11-13 07:21:42 EST; 14min ago
   Docs: man:systemd-sysv-generator(8)
   Process: 1420 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
   Tasks: 29 (limit: 4915)
   CGroup: /system.slice/mysql.service
           └─1447 /bin/bash /usr/bin/mysqld_safe
           └─1591 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/us
           └─1592 logger -t mysqld -p daemon error
```

```
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: mysql
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: performance_schema
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: Phase 6/7: Checking and upgrading table
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: Processing databases
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: information_schema
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: performance_schema
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: Phase 7/7: Running 'FLUSH PRIVILEGES'
Nov 13 07:21:43 kali /etc/mysql/debian-start[1645]: OK
Nov 13 07:21:43 kali /etc/mysql/debian-start[1674]: Checking for insecure root accounts.
Nov 13 07:21:43 kali /etc/mysql/debian-start[1678]: Triggering myisam-recover for all MyISA
```



# Kali'de DVWA Nasıl Kurulur?

- Sonra `cd /var/www/html` komutunu kullanarak `/www` dizinine geliyoruz.
- `git clone https://github.com/RandomStorm/DVWA.git` `dvwa` komutunu çalıştırarak DVWA dosyasını `dvwa` klasörünün içine git ile kopyalıyoruz.

```
root@kali:/var# cd www
root@kali:/var/www# ls
html
root@kali:/var/www# cd html
root@kali:/var/www/html# git clone https://github.com/RandomStorm/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (38/38), done.
remote: Total 3300 (delta 13), reused 29 (delta 5), pack-reused 3253
Receiving objects: 100% (3300/3300), 1.61 MiB | 1.75 MiB/s, done.
Resolving deltas: 100% (1462/1462), done.
root@kali:/var/www/html#
```

# Kali'de DVWA Nasıl Kurulur?

- Kullanıcı oluşturulur.

```
root@kali:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 82
Server version: 10.1.26-MariaDB-1 Debian unstable

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

```
MariaDB [(none)]> create user 'berika'@'localhost' identify by 'password'
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'identify by 'password'' at line 1
MariaDB [(none)]> create user berika;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> grant all on berika.* to berika@localhost identified by 'password'
-> ;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> grant all on berika.* to 'berika'@'%';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'on berika.* to 'berika'@'%' at line 1
MariaDB [(none)]> grant all on berika.* to 'berika'@'%';
Query OK, 0 rows affected (0.00 sec)
```

```
MariaDB [(none)]> select host,user,password from mysql.user;
+-----+-----+-----+
| host      | user  | password |
+-----+-----+-----+
| localhost | root  |          |
| %         | dvwa3 |          |
| localhost | dvwa3 | *6C0AB0774E8049C4C32B0762EC4C85160C9EBCD3 |
| %         | berika |          |
| localhost | berika | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
+-----+-----+-----+
5 rows in set (0.00 sec)
```

# Kali'de DVWA Nasıl Kurulur?

- Daha sonra **leafpad dvwa/config/config.inc.php** konfigürasyon dosyasını açarak password kısmını silip boş bırakarak kaydedip çıkıyoruz.

```
config.inc.php.dist
File Edit Search Options Help
<?php

# If you are having problems connecting to the MySQL database and all of th
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes
# Thanks to @digininja for the fix.

# Database management system to use
$dbms = 'MySQL';
#$dbms = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.

# If you are using MariaDB then you cannot use root, you must use create a
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'password';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings
```

```
// Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedi
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'berika';
$_DVWA[ 'db_user' ] = 'berika';
$_DVWA[ 'db_password' ] = 'password';
$_DVWA[ 'db_port' ] = '3306';

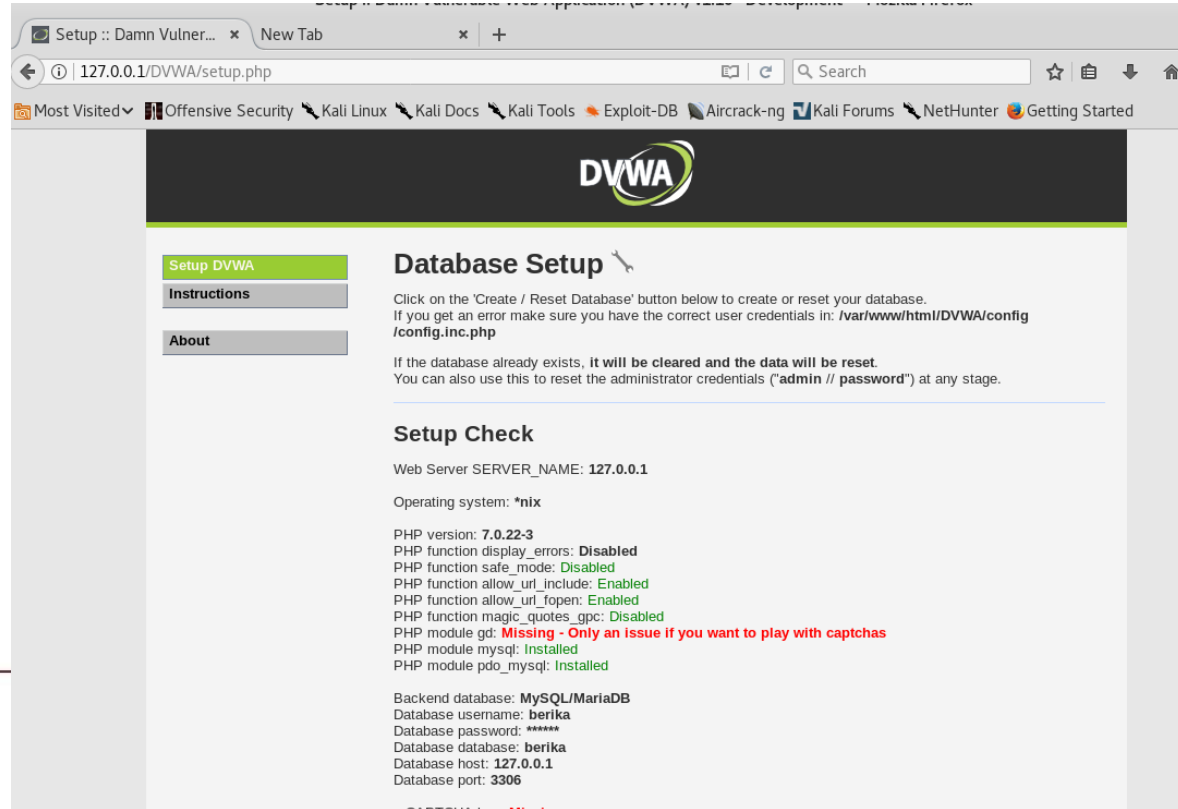
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'med
impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

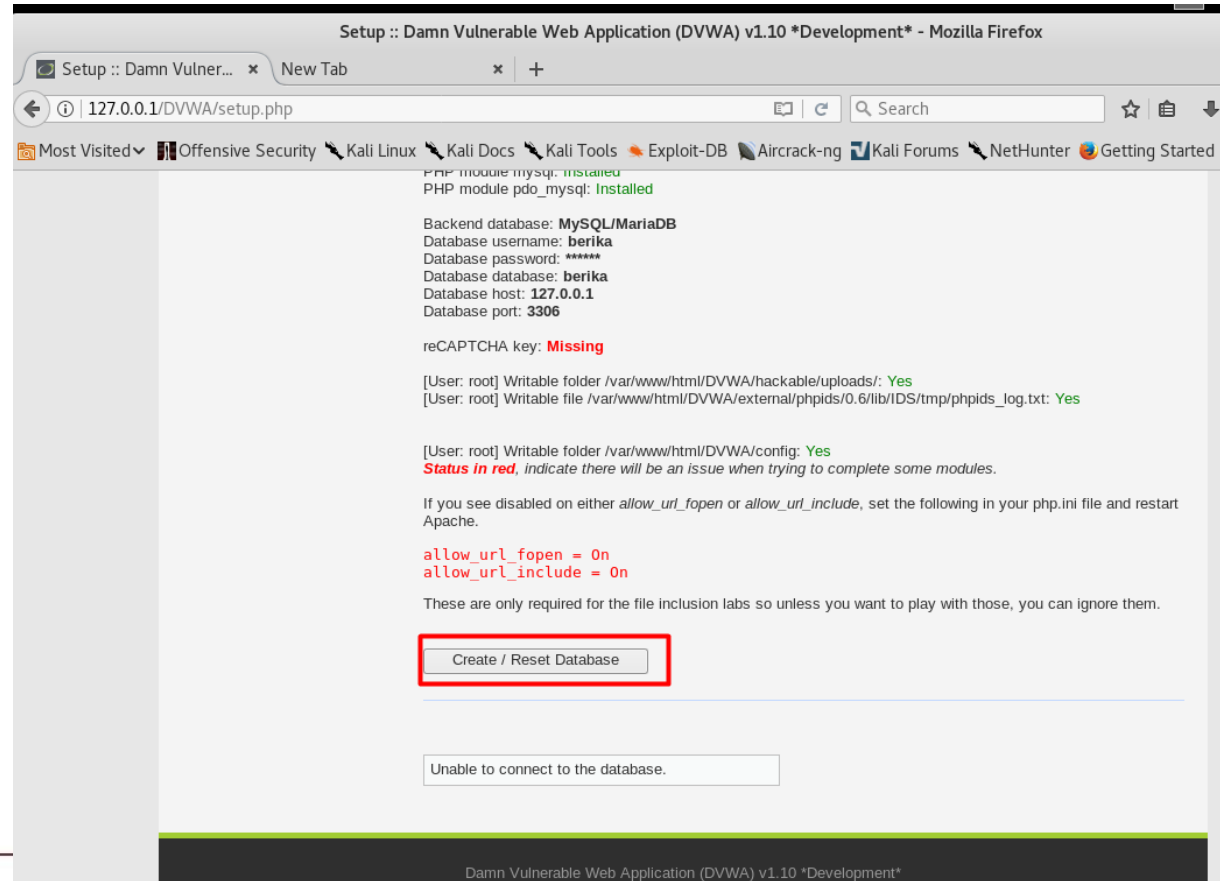
# Default PHPIDS status
# PHPIDS status with each session.
# The default is 'disabled'. You can set this to be either 'enabled' or 'disa
$_DVWA[ 'default_phpids_level' ] = 'disabled';
```

# Kali'de DVWA Nasıl Kurulur?

- İnternet tarayıcımıza **127.0.0.1** veya **localhost** yazıp gittiğimizde DVWA ın kurulum ve veri tabanı oluşturma sayfası gelmektedir.

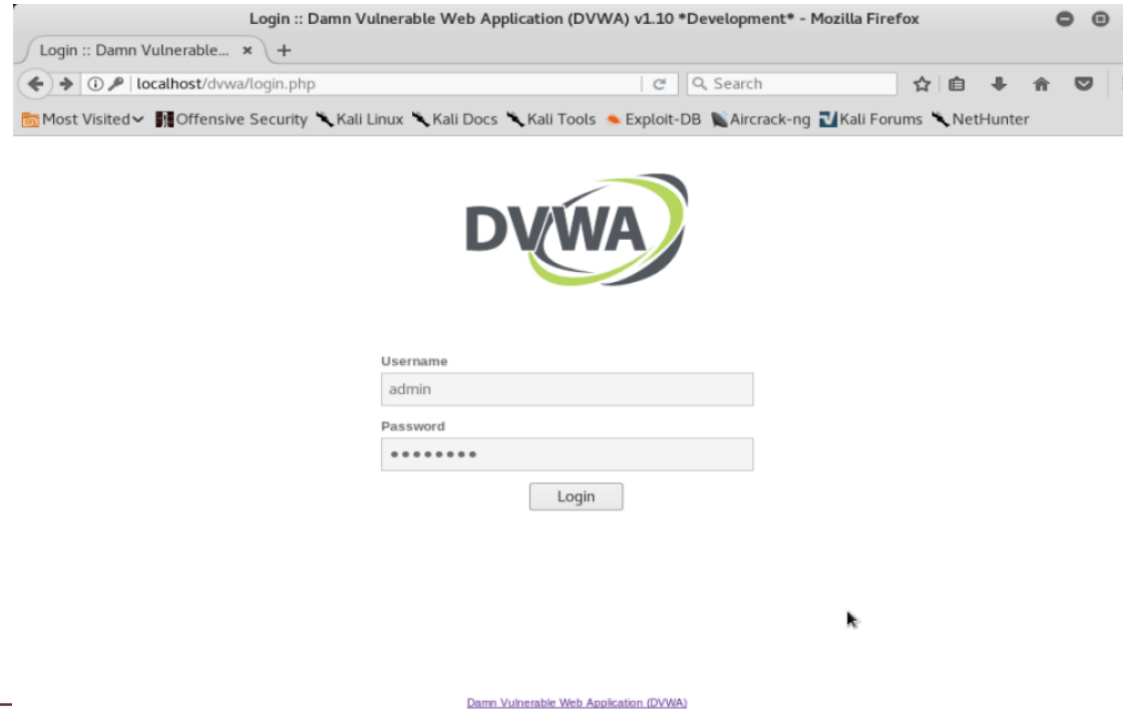


# Kali'de DVWA Nasıl Kurulur?

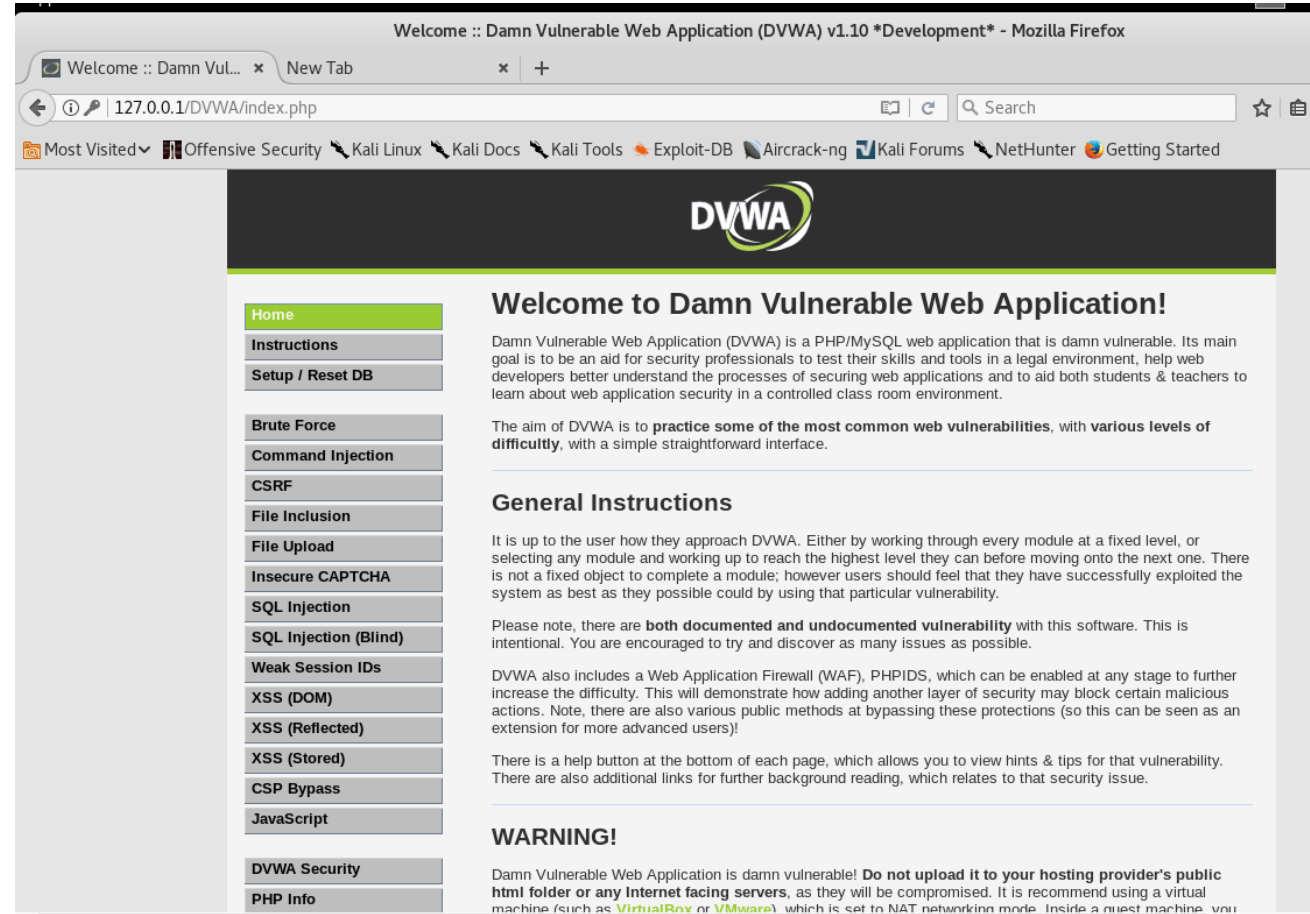


# Kali'de DVWA Nasıl Kurulur?

- Kullanıcı adı: admin, parola:password



# Kali'de DVWA Nasıl Kurulur?

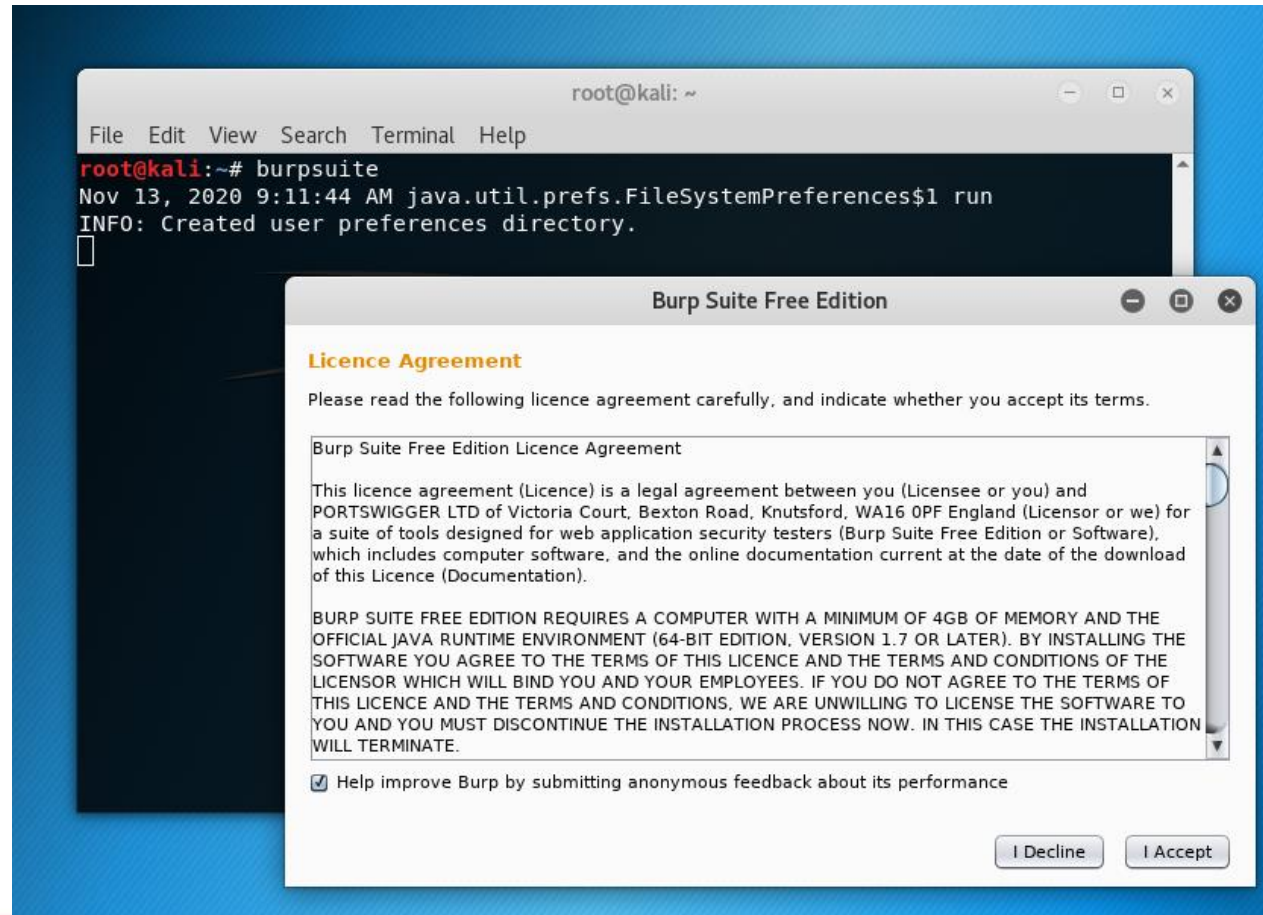


# Burp Suite Nedir?

- Burp bir proxy aracıdır.
- Web uygulamaları HTTP protokolünü kullanır ve HTTP protokolü ise istemci/sunucu mimarisi üzerine kurulu olan bir protokoldür.
- İstemci ve sunucu arasında proxy olarak kullanılan Burp Suite tüm istek ve cevapların ayrıntılı bir şekilde incelenebilmesine ve diğer özellikleri ile farklı işlemler yapılabilmesine olanak sağlayan bir araçtır.

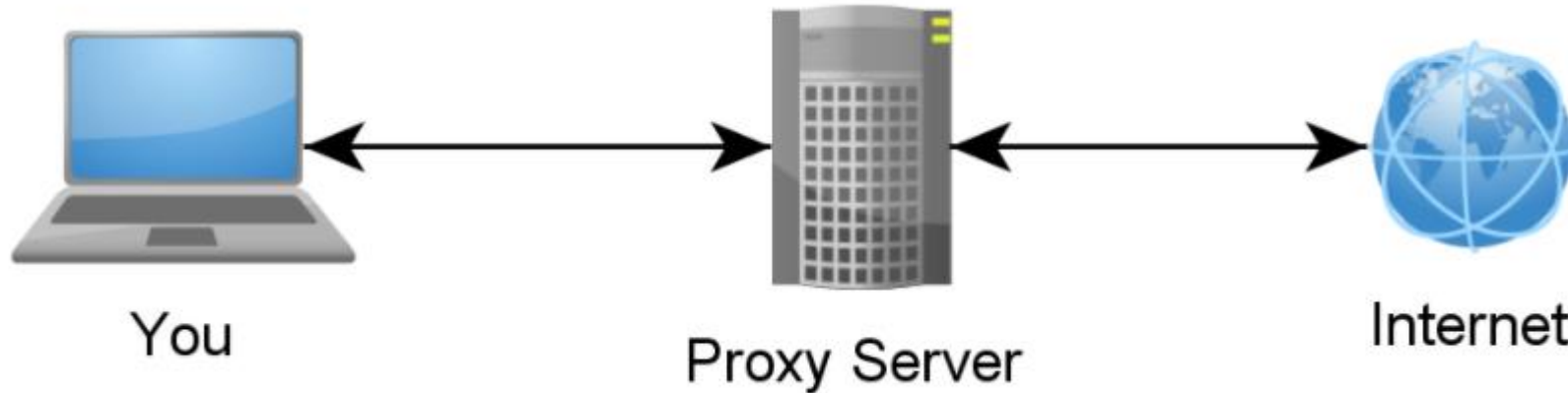


# Burp Suite Nasıl Kurulur?



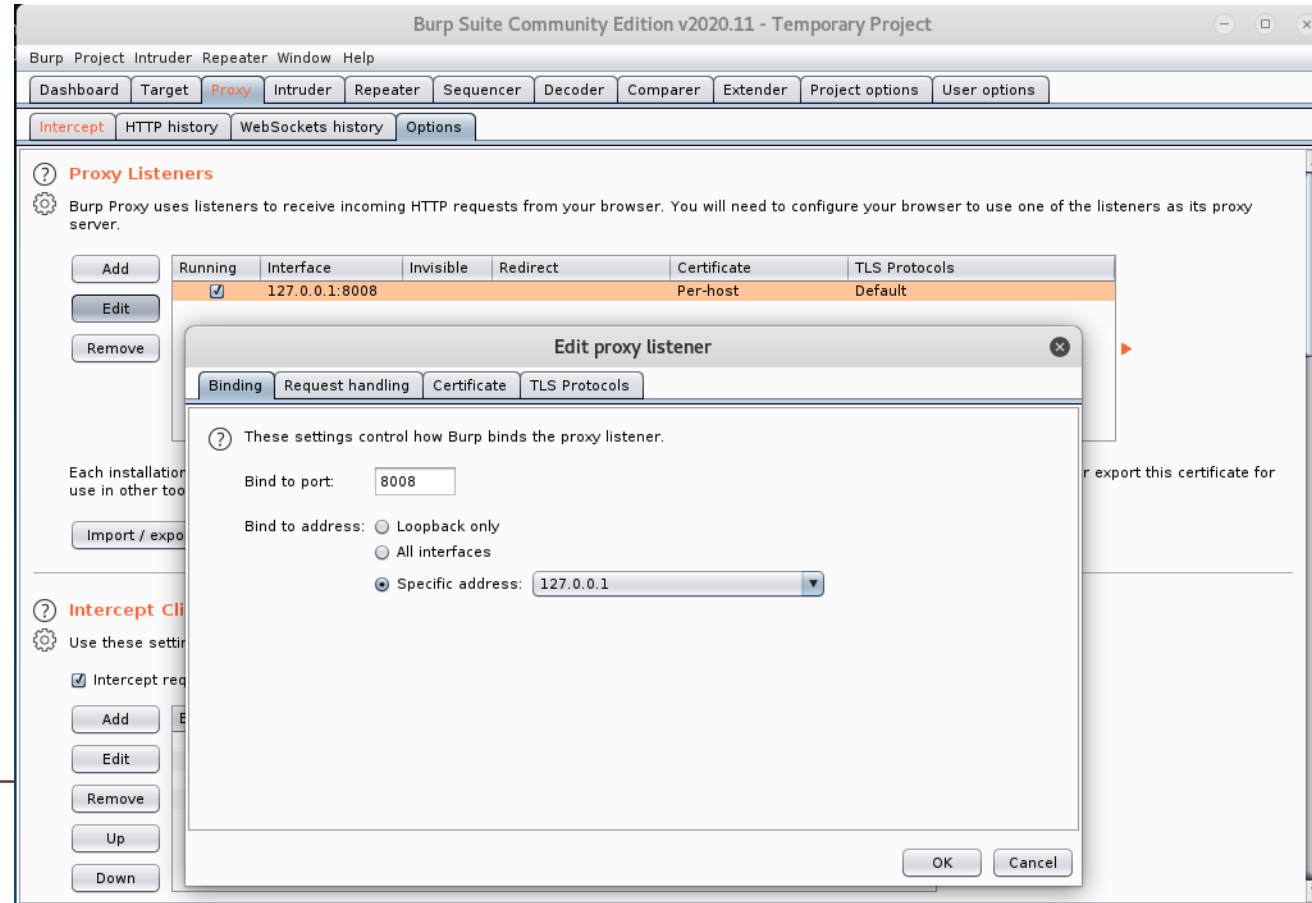
# Burp Suite Ayarları

- Proxy ayarları yapıp internetimizi Burp Suite üzerinden geçirmek.
- Böylece http paketlerimiz yorumlanacak ve verileri açık şekilde görebileceğiz.



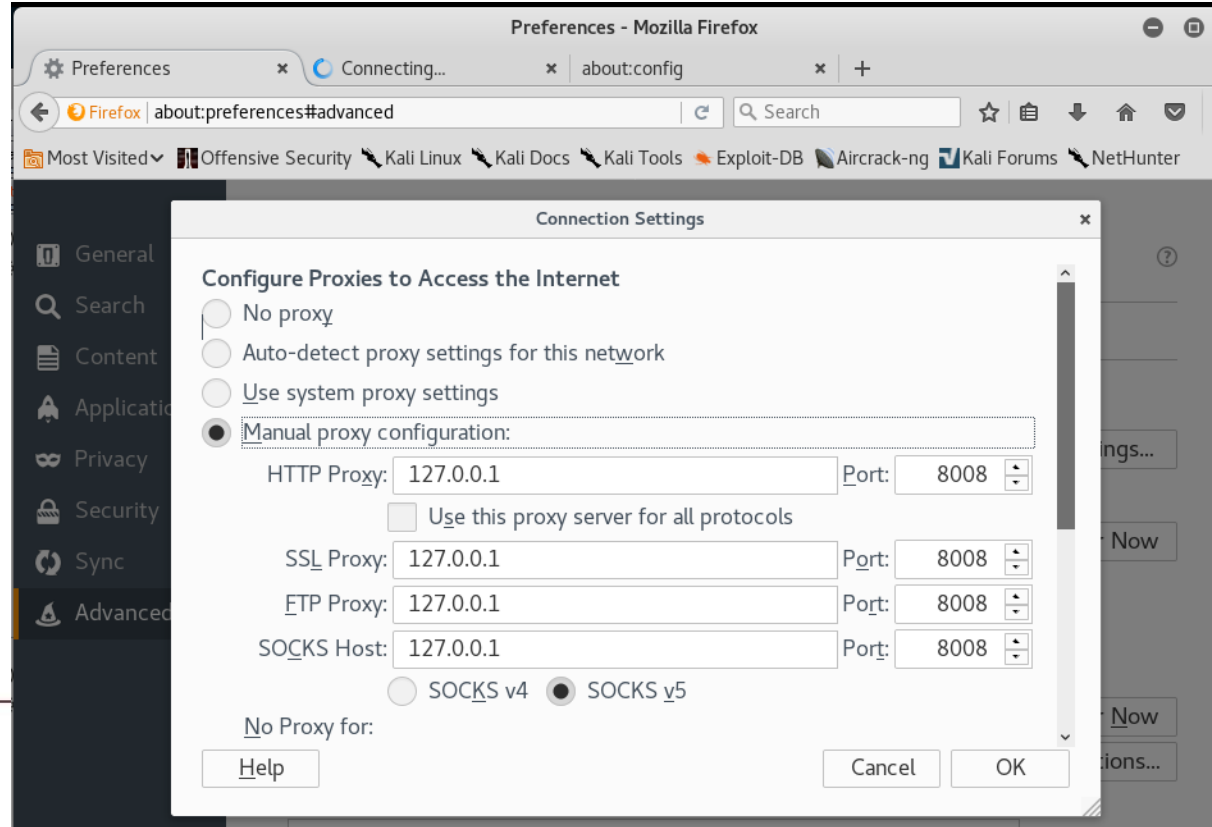
# Burp Suite Ayarları

- Proxy>options>edit



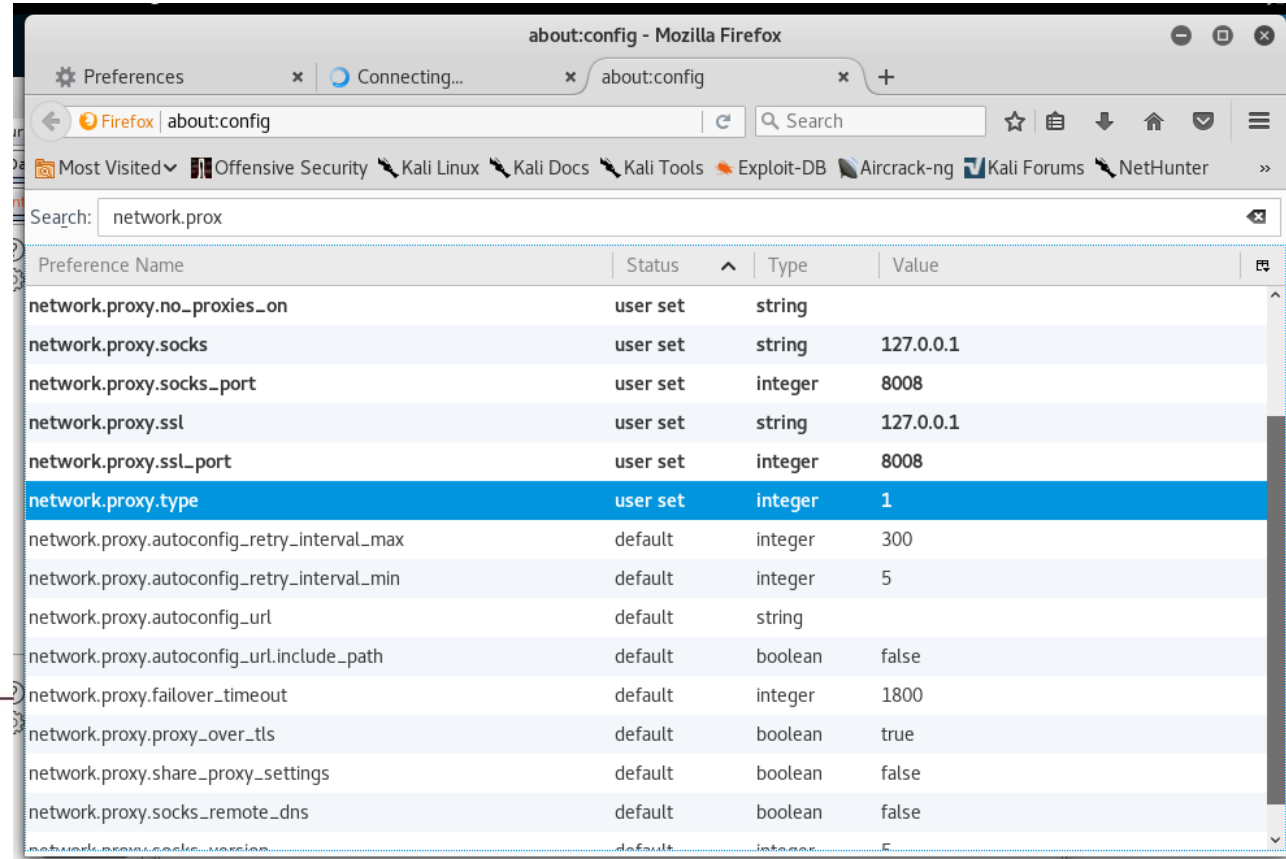
# Burp Suite Ayarları

- Firefox'un proxy ayarlamasını Tercihler->Gelişmiş->Ağ->Ayarlar sekmesinden yapıyoruz.



# Burp Suite Ayarları

- Firefox'un config ayarlarında network.proxy.type 0 ise 1 yapıyoruz.



# Brute Force Saldırısı

Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\* - Mozilla Firefox

Preferences x Vulnerability: Brute F... x about:config x +

localhost/DVWA/vulnerabilities/brute/?username=deneme&password=... Search

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

**DVWA**

**Vulnerability: Brute Force**

**Login**

Username:  
deneme

Password:  
...

Login

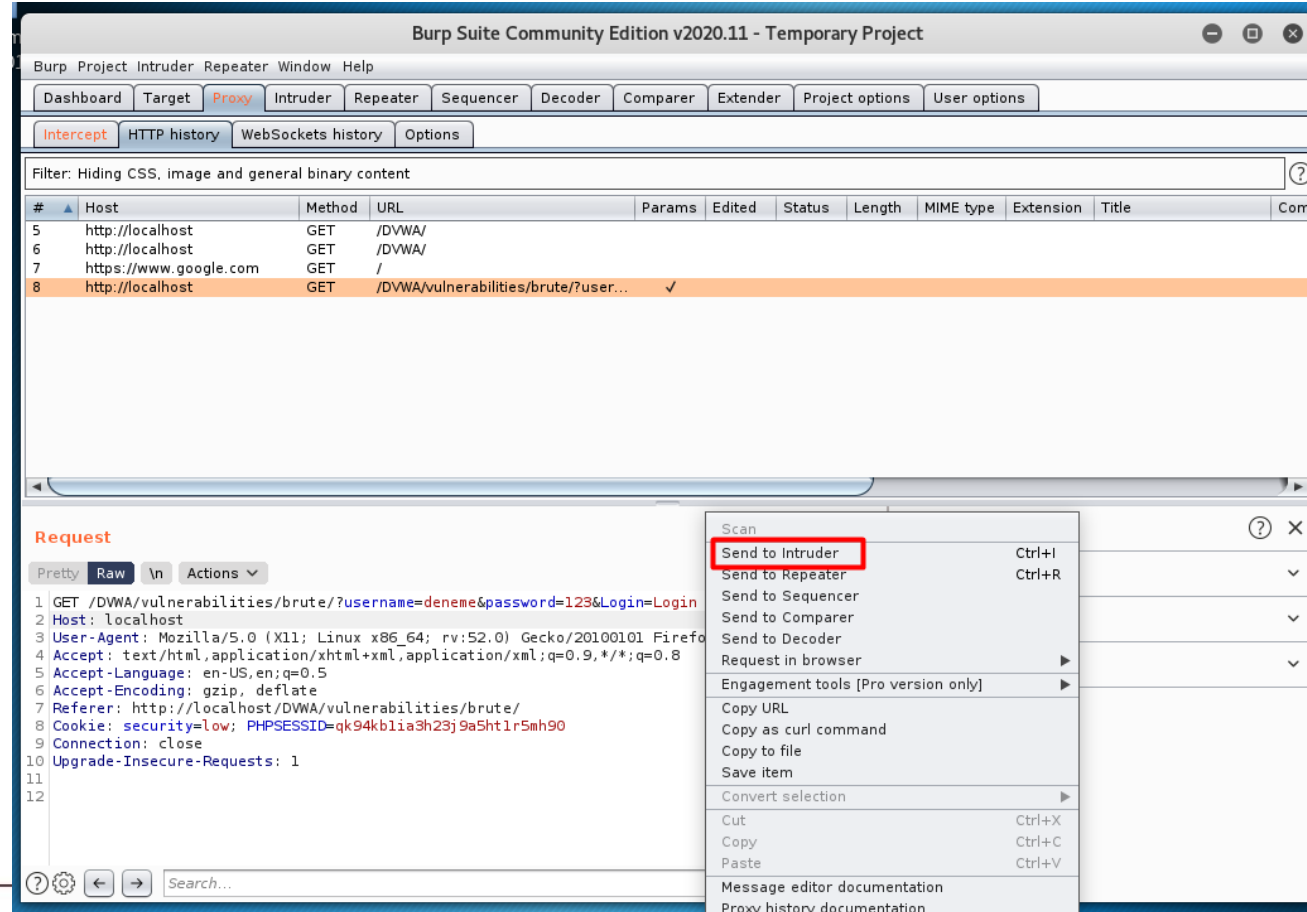
Username and/or password incorrect.

**More Information**

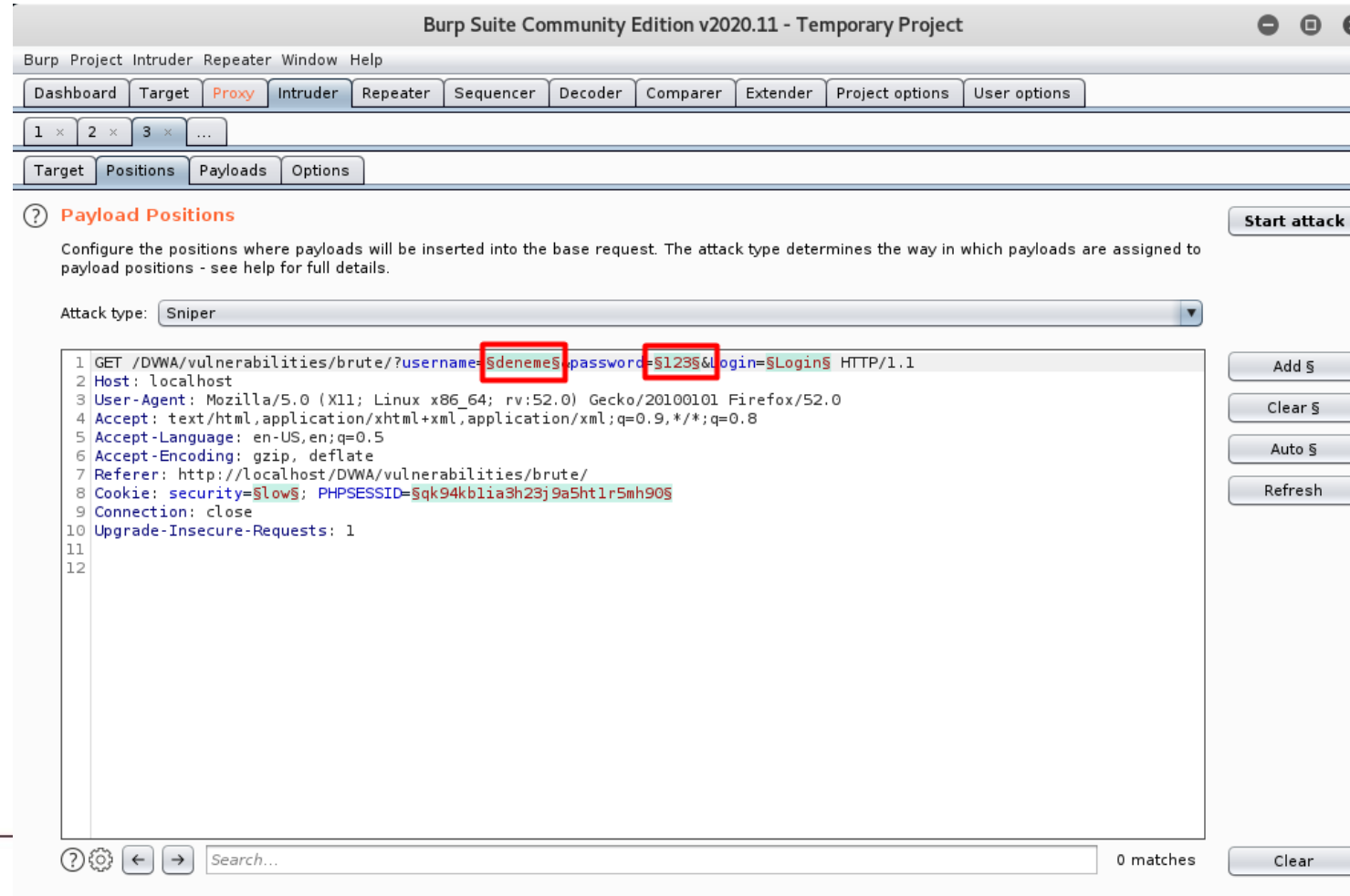
- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack)
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Home  
Instructions  
Setup / Reset DB  
**Brute Force**  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)

# Brute Force Saldırısı



# Brute Force Saldırısı





# Brute Force Saldırısı

Burp Suite Community Edition v2020.11 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Target Positions Payloads Options

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

Start attack

1 GET /DVWA/vulnerabilities/brute/?username=\$deneme\$&password=\$123\$&Login=Login HTTP/1.1

2 Host: localhost

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:52.0) Gecko/20100101 Firefox/52.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Referer: http://localhost/DVWA/vulnerabilities/brute/

8 Cookie: security=low; PHPSESSID=qk94kb1ia3h23j9a5ht1r5mh90

9 Connection: close

10 Upgrade-Insecure-Requests: 1

11

12

Add \$

Clear \$

Auto \$

Refresh

0 matches

Clear

2 payload positions

Length: 491

# Brute Force Saldırısı

Burp Suite Community Edition v2020.11 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x ...

Target Positions Payloads Options

### ? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

1 GET /DV  
2 Host: 1  
3 User-Agent: Pitchfork  
4 Accept: **Cluster bomb**  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Referer: http://localhost/DVWA/vulnerabilities/brute/  
8 Cookie: security=low; PHPSESSID=qk94kb1ia3h23j9a5ht1r5mh90  
9 Connection: close  
10 Upgrade-Insecure-Requests: 1  
11  
12

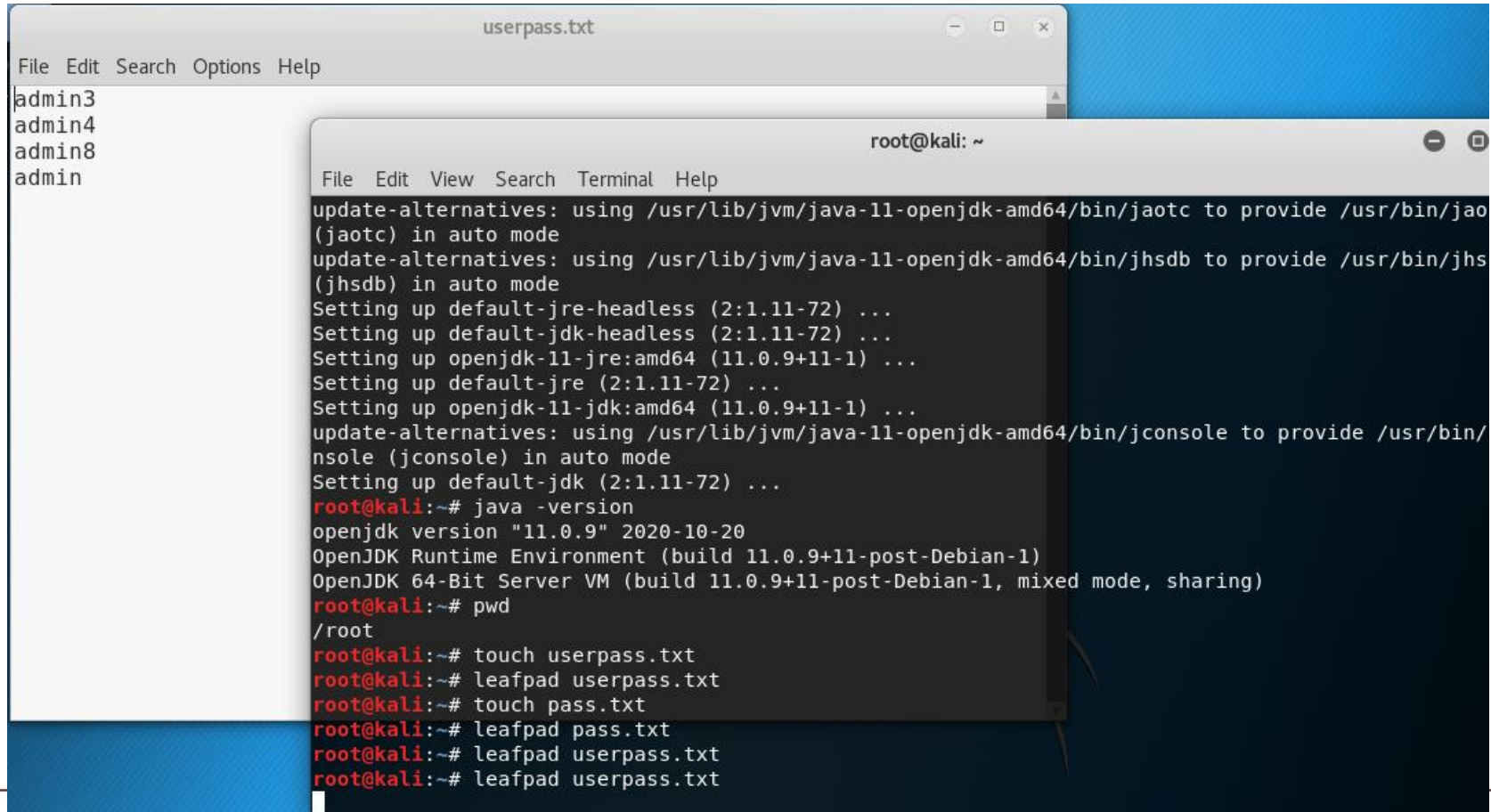
Start attack

Add §  
Clear §  
Auto §  
Refresh

0 matches  
Clear

2 payload positions  
Length: 491

# Brute Force Saldırısı

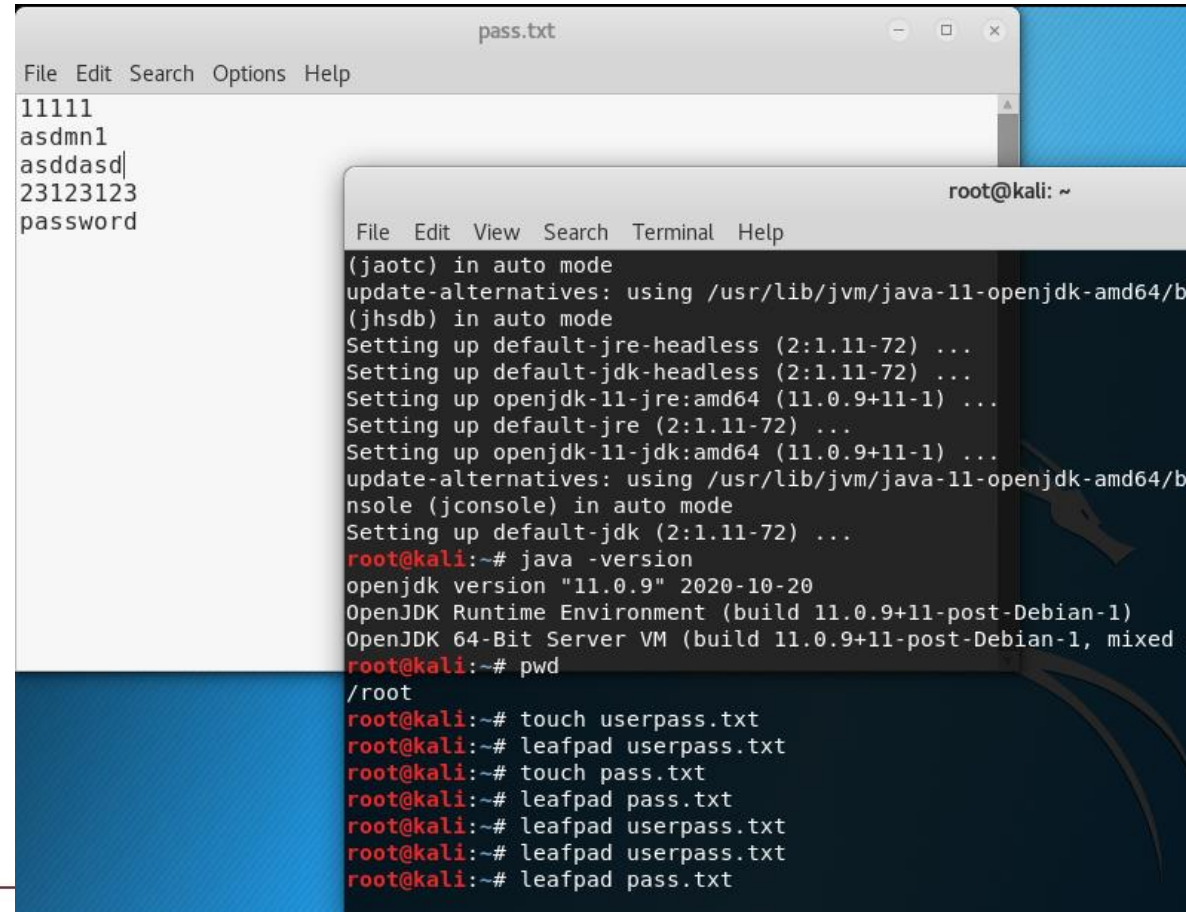


The image shows a Kali Linux desktop environment. In the background, a text editor window titled 'userpass.txt' is open, displaying a list of usernames: 'admin3', 'admin4', 'admin8', and 'admin'. In the foreground, a terminal window titled 'root@kali: ~' is open, showing the output of several system update and configuration commands. The terminal output includes messages about updating alternatives for 'jaotc' and 'jhsdb', setting up default JRE and JDK for headless mode, and verifying the Java version (11.0.9). The user then runs 'pwd' showing they are in the root directory, and finally creates and opens 'userpass.txt' and 'pass.txt' files using 'touch' and 'leafpad' commands.

```
File Edit Search Options Help
admin3
admin4
admin8
admin

root@kali: ~
File Edit View Search Terminal Help
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jaotc to provide /usr/bin/jaotc in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jhsdb to provide /usr/bin/jhsdb in auto mode
Setting up default-jre-headless (2:1.11-72) ...
Setting up default-jdk-headless (2:1.11-72) ...
Setting up openjdk-11-jre:amd64 (11.0.9+11-1) ...
Setting up default-jre (2:1.11-72) ...
Setting up openjdk-11-jdk:amd64 (11.0.9+11-1) ...
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole in auto mode
Setting up default-jdk (2:1.11-72) ...
root@kali:~# java -version
openjdk version "11.0.9" 2020-10-20
OpenJDK Runtime Environment (build 11.0.9+11-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.9+11-post-Debian-1, mixed mode, sharing)
root@kali:~# pwd
/root
root@kali:~# touch userpass.txt
root@kali:~# leafpad userpass.txt
root@kali:~# touch pass.txt
root@kali:~# leafpad pass.txt
root@kali:~# leafpad userpass.txt
root@kali:~# leafpad userpass.txt
```

# Brute Force Saldırısı



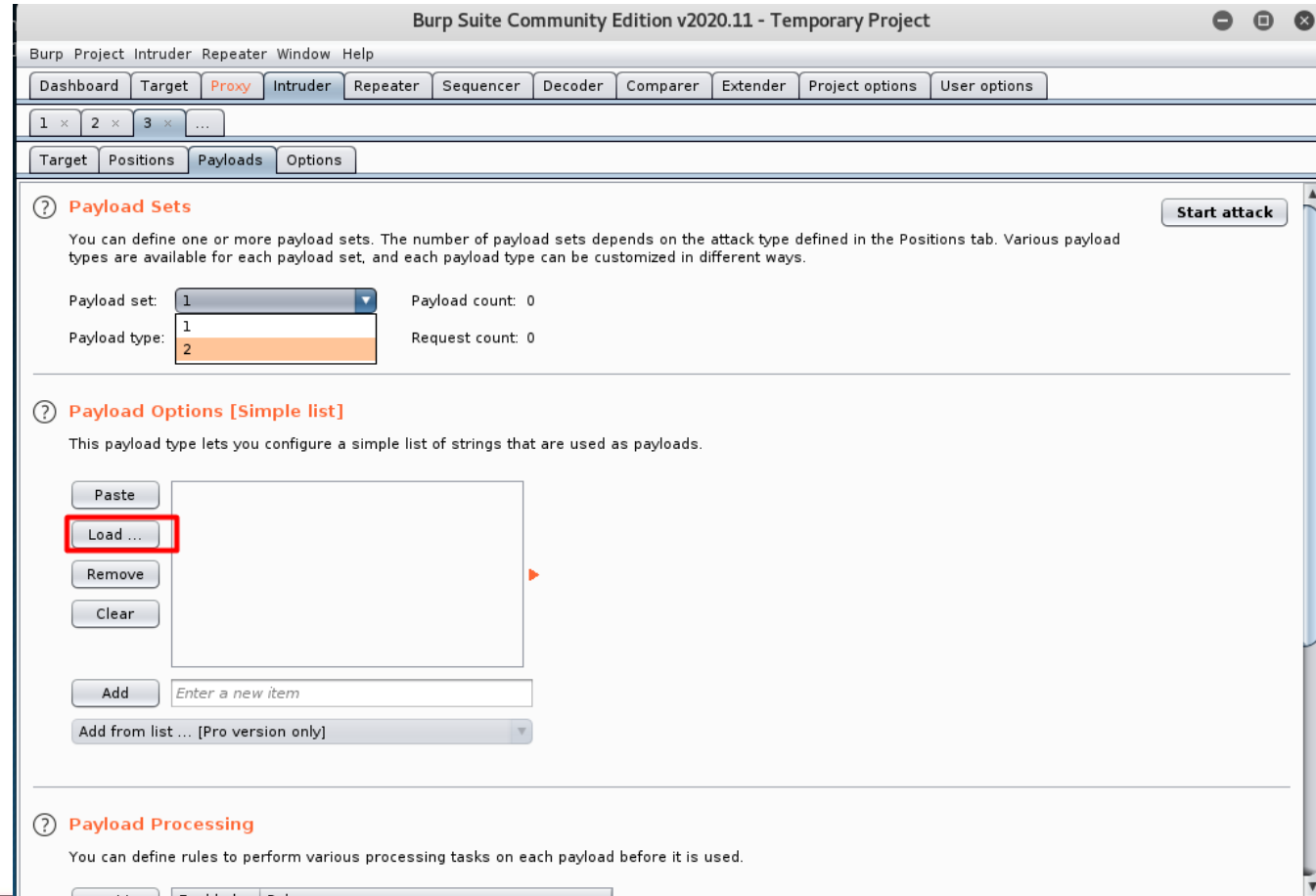
The image shows a Kali Linux desktop environment. In the background, a text editor window titled 'pass.txt' contains the following text:

```
11111
asdmn1
asddasd|
23123123
password
```

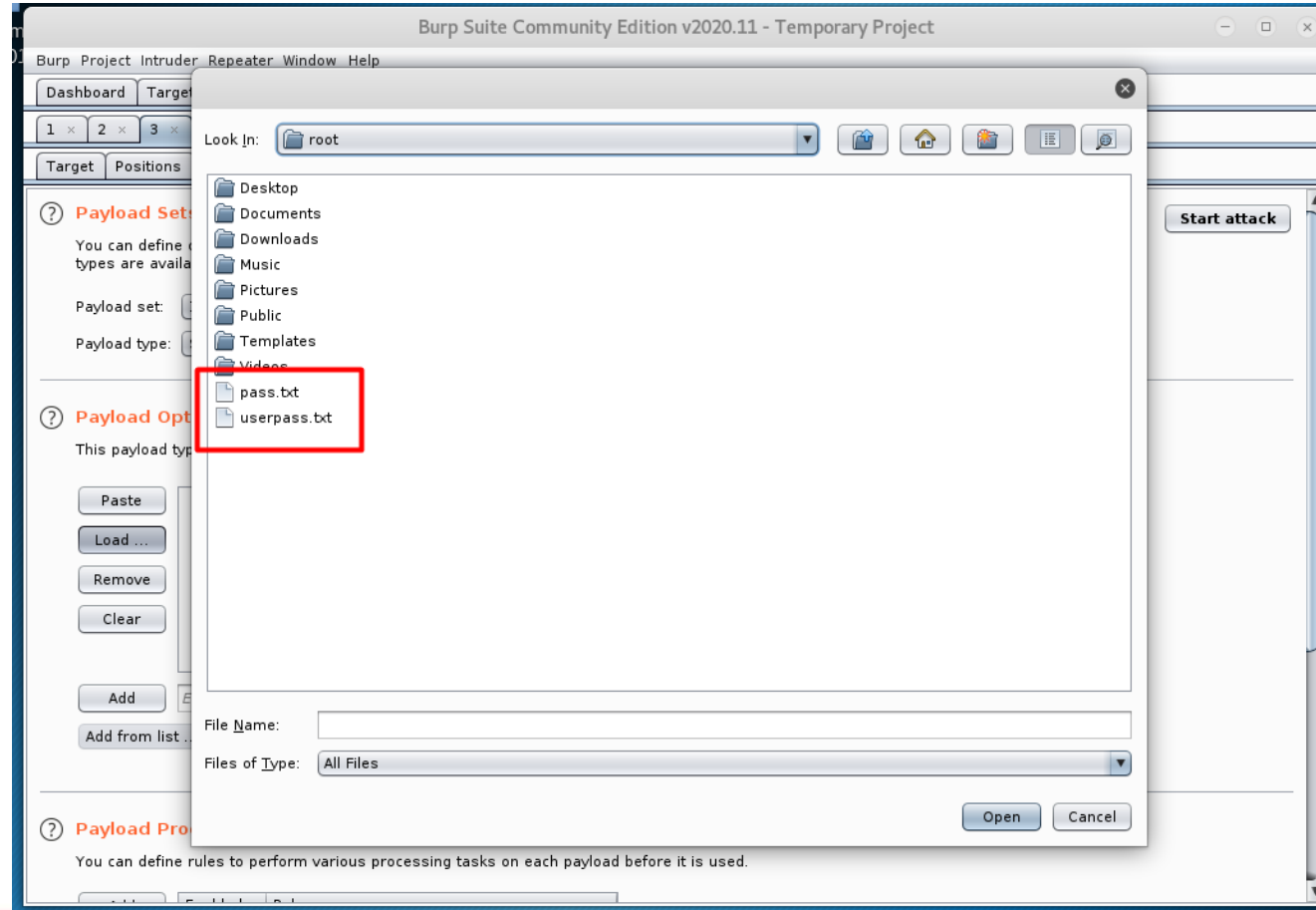
In the foreground, a terminal window titled 'root@kali: ~' shows the following commands and output:

```
(jaotc) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/java to provide /usr/bin/java in auto mode
(jhsdb) in auto mode
Setting up default-jre-headless (2:1.11-72) ...
Setting up default-jdk-headless (2:1.11-72) ...
Setting up openjdk-11-jre:amd64 (11.0.9+11-1) ...
Setting up default-jre (2:1.11-72) ...
Setting up openjdk-11-jdk:amd64 (11.0.9+11-1) ...
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/java to provide /usr/bin/java in auto mode
nsole (jconsole) in auto mode
Setting up default-jdk (2:1.11-72) ...
root@kali:~# java -version
openjdk version "11.0.9" 2020-10-20
OpenJDK Runtime Environment (build 11.0.9+11-post-Debian-1)
OpenJDK 64-Bit Server VM (build 11.0.9+11-post-Debian-1, mixed mode, sharing)
root@kali:~# pwd
/root
root@kali:~# touch userpass.txt
root@kali:~# leafpad userpass.txt
root@kali:~# touch pass.txt
root@kali:~# leafpad pass.txt
root@kali:~# leafpad userpass.txt
root@kali:~# leafpad userpass.txt
root@kali:~# leafpad pass.txt
```

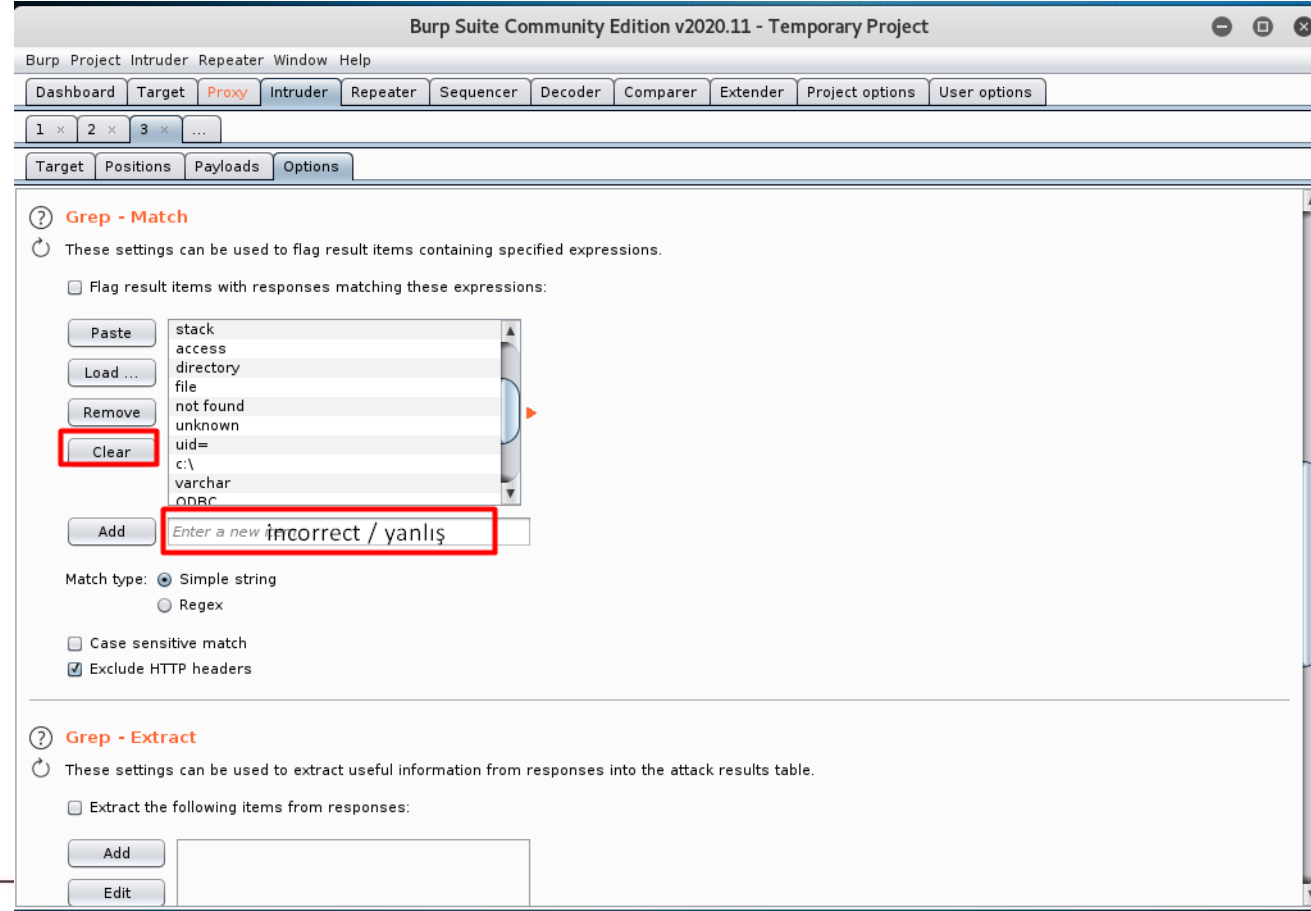
# Brute Force Saldırısı



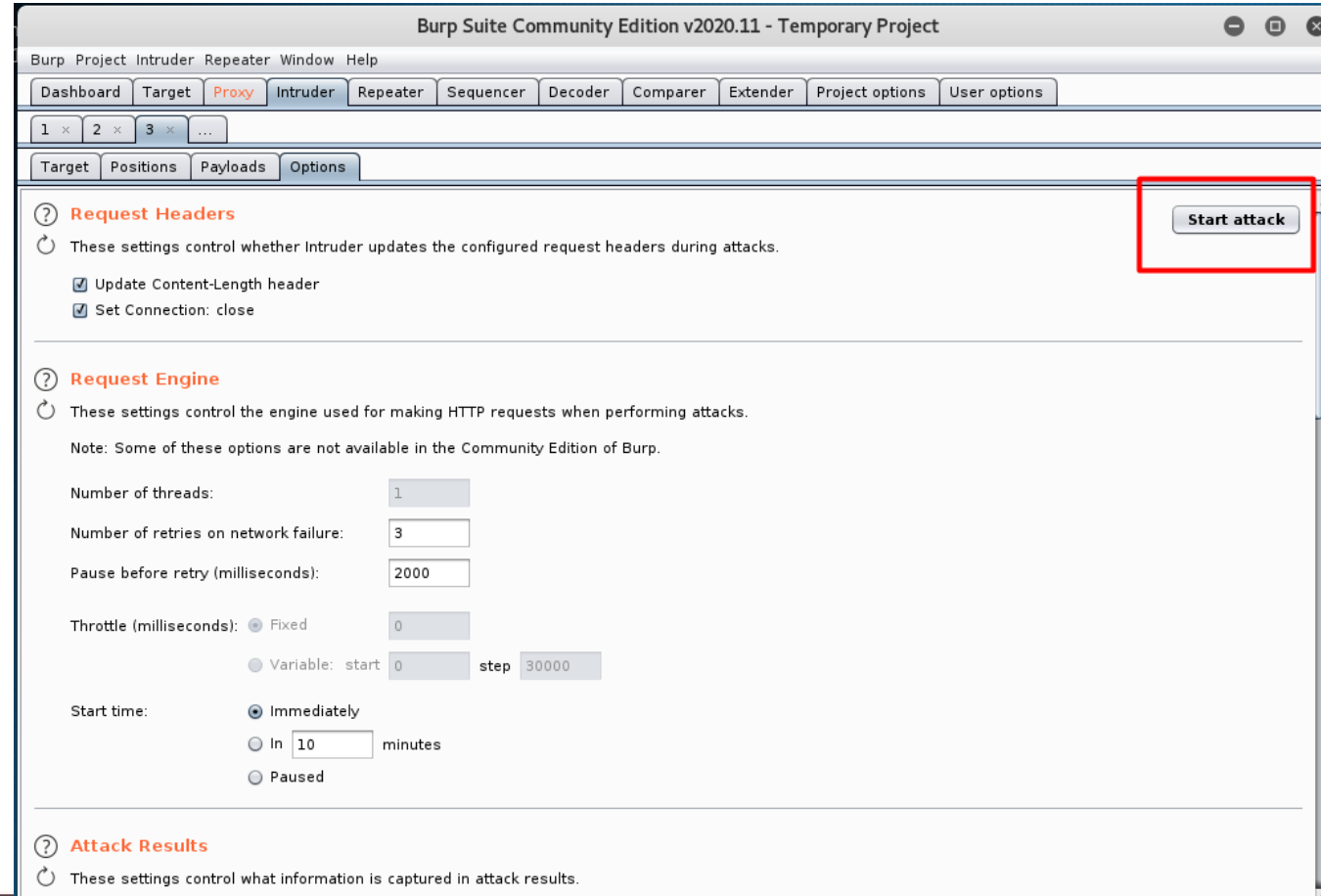
# Brute Force Saldırısı



# Brute Force Saldırısı



# Brute Force Saldırısı





# Brute Force Saldırısı

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	incorr...	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
1	admin4	asdmn1	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
2	admin8	asdmn1	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
3	admin	asdmn1	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
4	admin4	asddasd	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
5	admin8	asddasd	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
6	admin	asddasd	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
7	admin4	23123123	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
8	admin8	23123123	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
9	admin	23123123	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
10	admin4	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
11	admin8	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4528	<input checked="" type="checkbox"/>	
12	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4571	<input type="checkbox"/>	

Finished

# Brute Force Saldırısı

The image displays two screenshots of the Damn Vulnerable Web Application (DVWA) v1.10 \*Development\* interface, specifically the Brute Force vulnerability page. Both screenshots are taken from a Mozilla Firefox browser window.

**Left Screenshot:** The browser address bar shows the URL `localhost/DVWA/vulnerabilities/brute/?username=admin&password=`. The page title is "Vulnerability: Brute Force". The left sidebar menu has "Brute Force" selected. The main content area shows the "Login" form with "Username:" and "Password:" fields. The "Username:" field contains "admin" and the "Password:" field contains ".....". Below the form, a red error message states: "Username and/or password incorrect." The "More Information" section lists three links: [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack), <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>, and <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>.

**Right Screenshot:** The browser address bar shows the URL `localhost/DVWA/vulnerabilities/brute/?username=admin&password=`. The page title is "Vulnerability: Brute Force". The left sidebar menu has "Brute Force" selected. The main content area shows the "Login" form with "Username:" and "Password:" fields. The "Username:" field contains "admin" and the "Password:" field contains ".....". Below the form, a green success message states: "Welcome to the password protected area admin". A small image of a person is displayed below the message. The "More Information" section lists three links: [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack), <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>, and <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>.