

bWAPP Kurulumu

bWAPP Kurulumu yazısı hazırlanırken kullanılan işletim sistemi GNU/Linux [Parrot Os](#) 5.10.0 sürümüdür. Bazı işlemler çok küçük farklılıklarla olsa bile Debian tabanlı sistemler üzerinde genel olarak verilen adımlar izlenerek kurulum yapılması mümkündür.

bWAPP Nedir ?

bWAPP [itsecgames](#) tarafından geliştirilen ,[open source](#) ve ücretsiz bir web güvenlik zafiyetleri penetrasyon testi laboratuvarıdır. Detaylı bilgi için [tıklayınız](#).

Bwapp üzerinde bulunan bazı zafiyetler :

- SQL, HTML, iFrame, SSI, OS Command, XML, XPath, LDAP and SMTP injections
- Blind SQL and Blind OS Command injection
- Bash Shellshock (CGI) and Heartbleed vulnerability (OpenSSL)
- Cross-Site Scripting (XSS) and Cross-Site Tracing (XST)
- Cross-Site Request Forgery (CSRF)
- AJAX and Web Services vulnerabilities (JSON/XML/SOAP/WSDL)
- Malicious, unrestricted file uploads and backdoor files
- Authentication, authorization and session management issues
- Arbitrary file access and directory traversals
- Local and remote file inclusions (LFI/RFI)
- Configuration issues: Man-in-the-Middle, cross-domain policy files, information disclosures,...
- HTTP parameter pollution and HTTP response splitting
- Denial-of-Service (DoS) attacks: Slow HTTP and XML Entity Expansion
- Insecure distcc, FTP, NTP, Samba, SNMP, VNC, WebDAV configurations
- HTML5 ClickJacking, Cross-Origin Resource Sharing (CORS) and web storage issues
- Unvalidated redirects and forwards, and cookie poisoning
- Cookie poisoning and insecure cryptographic storage
- Server Side Request Forgery (SSRF)
- XML External Entity attacks (XXE)

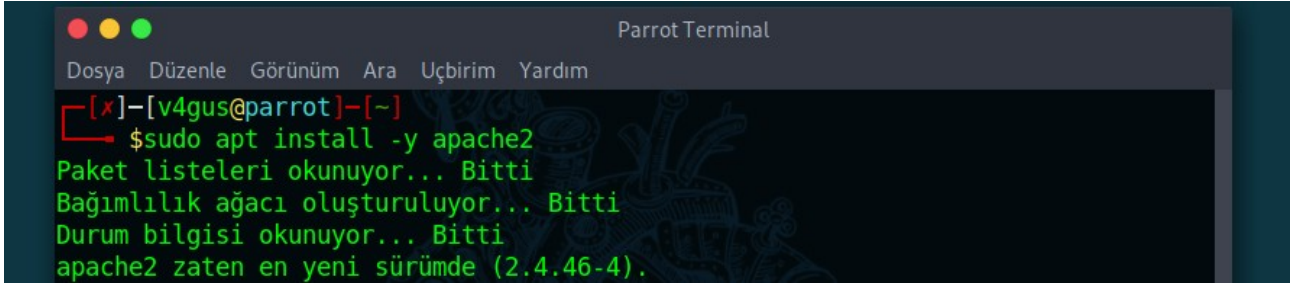
Zafiyetler hakkında daha fazla bilgi için [buraya](#) bakabilirsiniz.

Apache2 Kurulumu

Apache2 server, Gnu/Linux distrolarında genellikle default olarak gelir.

sudo apt install -y apache2

komutu eğer sistemimiz üzerinde apache kurulu değilse kurulum işlemine , eğer kurulu ise versiyon bilgilerini görüntüleyecektir.



```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[v4gus@parrot]-[~]
$ sudo apt install -y apache2
Paket listeleri okunuyor... Bitti
Bağımlılık ağacı oluşturuluyor... Bitti
Durum bilgisi okunuyor... Bitti
apache2 zaten en yeni sürümde (2.4.46-4).
```

Mysql Kurulumu

Mysql veya Mariadb de çoğu dağıtımda yüklü olarak geliyor. Kali-Linux ve Parrot-Linux (Security) üzerinde ise genellikle Mariadb geliyor. İki program üzerinde de çalışmamız mümkün olduğu için hangisi üzerinde daha rahat olacaksınız onu seçmenizi tavsiye ederim.

apt install -y mysql-server

komutu ile mysql

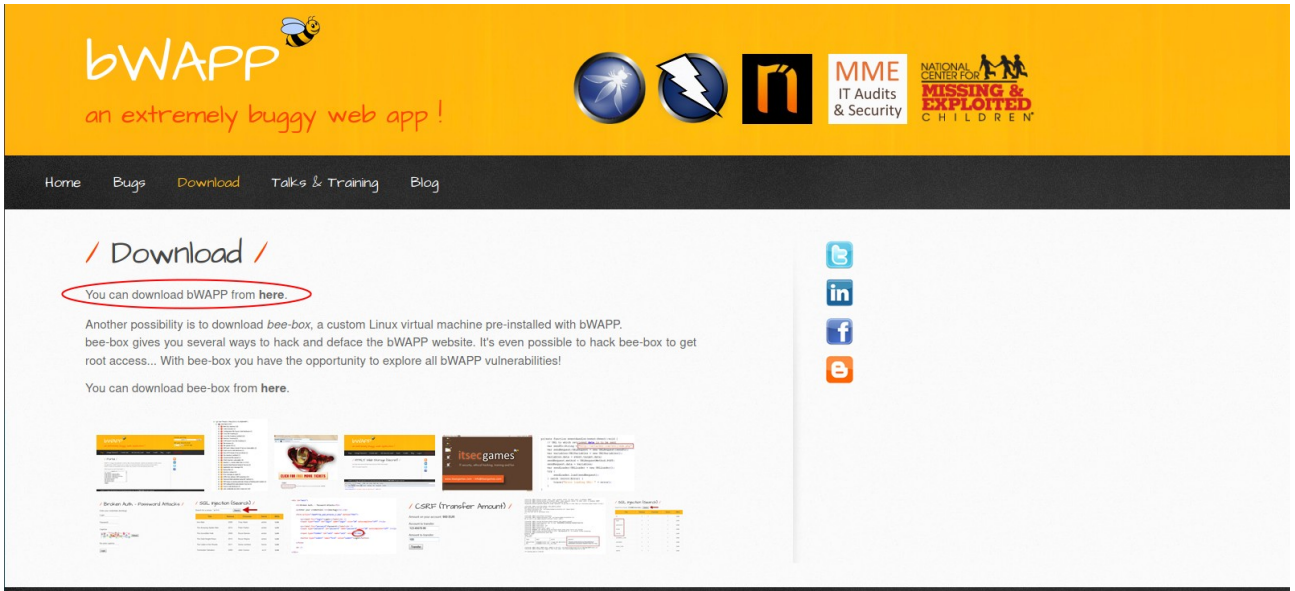
apt install -y mariadb-server

komutu ile mariadb kurulumu gerçekleştirilir.

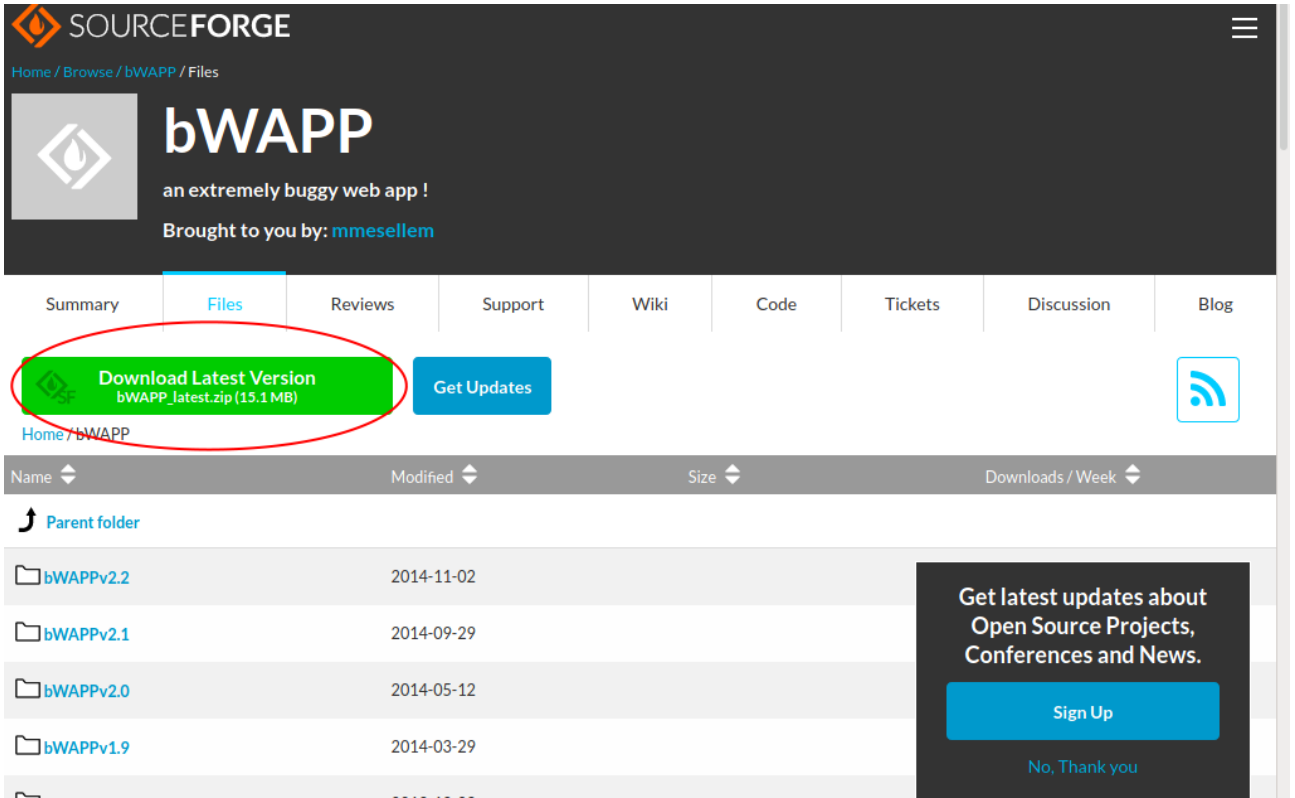
Bu işlemlerin ardından bWAPP kurulumuna geçebiliriz.

bWAPP'in Debian Tabanlı GNU/Linux Dağıtımlarına Kurulumu

<http://www.itsecgames.com/> adresinden Download sekmesine gelip en üstteki seçeneği seçiyoruz.



Yönlendirildiğimiz adresten en son versionu indir seçeneğini seçiyoruz.



Arşivi indirdiğimiz dizine gidip `unzip bWAPP_lastes.zip -d bWAPP` komutu ile bWAPP dizinine unzip edelim.

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[v4gus@parrot]--[~/Downloads]
$unzip bwAPP_latest.zip -d bwAPP
```

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[v4gus@parrot]--[~/Downloads]
$unzip bwAPP_latest.zip -d bwAPP
Archive: bwAPP_latest.zip
  inflating: bwAPP/apache2/default
  inflating: bwAPP/apache2/httpd.conf
  inflating: bwAPP/bwAPP/666
    creating: bwAPP/bwAPP/admin/
  inflating: bwAPP/bwAPP/admin/index.php
  inflating: bwAPP/bwAPP/admin/phpinfo.php
  inflating: bwAPP/bwAPP/admin/settings.php
  inflating: bwAPP/bwAPP/aim.php
    creating: bwAPP/bwAPP/apps/
  inflating: bwAPP/bwAPP/apps/movie_search
  inflating: bwAPP/bwAPP/ba_captcha_bypass.php
  inflating: bwAPP/bwAPP/ba_forgotten.php
  inflating: bwAPP/bwAPP/ba_insecure_login.php
  inflating: bwAPP/bwAPP/ba_insecure_login_1.php
  inflating: bwAPP/bwAPP/ba_insecure_login_2.php
  inflating: bwAPP/bwAPP/ba_insecure_login_3.php
  inflating: bwAPP/bwAPP/ba_logout.php
  inflating: bwAPP/bwAPP/ba_logout_1.php
  inflating: bwAPP/bwAPP/ba_pwd_attacks.php
```

Arşivdeki dosyalar çıkarıldığında aşağıdakine benzer bir dizin elde etmiş olacağız:

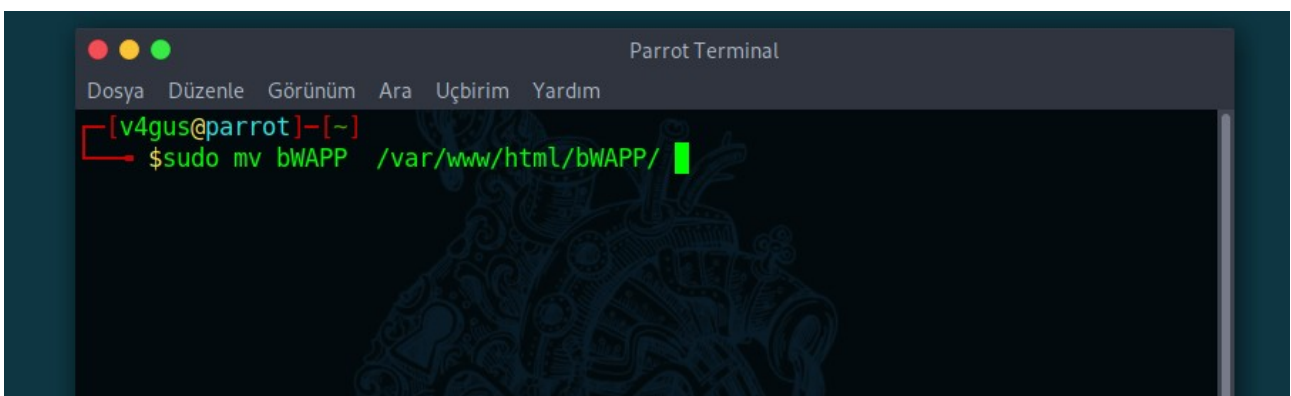
```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[v4gus@parrot]--[~/Downloads/bwAPP]
$ls
apache2          ClientAccessPolicy.xml  INSTALL.txt
bwAPP            crossdomain.xml         README.txt
bwAPP_intro.pdf  evil                    release_notes.txt
[v4gus@parrot]--[~/Downloads/bwAPP]
$
```

Download dizini içerisindeki bWAPP dizinini `/var/www/html` dizinine taşımamız gerekiyor.

Bu dizinde bulunan dosya ve dizinlere normal kullanıcıların yazma yetkisi olmadığı için super user olarak işlemimize devam edeceğiz.

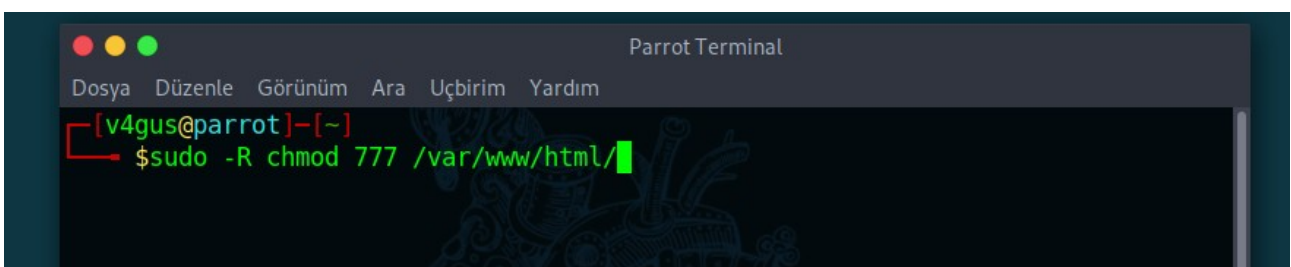
```
sudo mv bWAPP /var/www/html/bWAPP/
```

komutu ile bWAPP dizini `/var/www/html/bWAPP` içerisine taşıma işlemi yapılır.



Şimdi taşıdığımız bWAPP dizinine normal kullanıcı gurpları için erişim yetkisi verelim.

```
sudo -R chmod 777 /var/www/html/
```



Ardından `var/www/html/bWAPP/admin` dizini altında bulunan `settings.php` içerisindeki

```
$db_username = "user_name";  
$db_password = "user_password";
```

değerlerini kendi ayarlarımıza göre değiştirmemiz gerekiyor.

Eğer mysql kurulumu sonrasında değişiklik yapmamışsanız

```
service mysql start
```

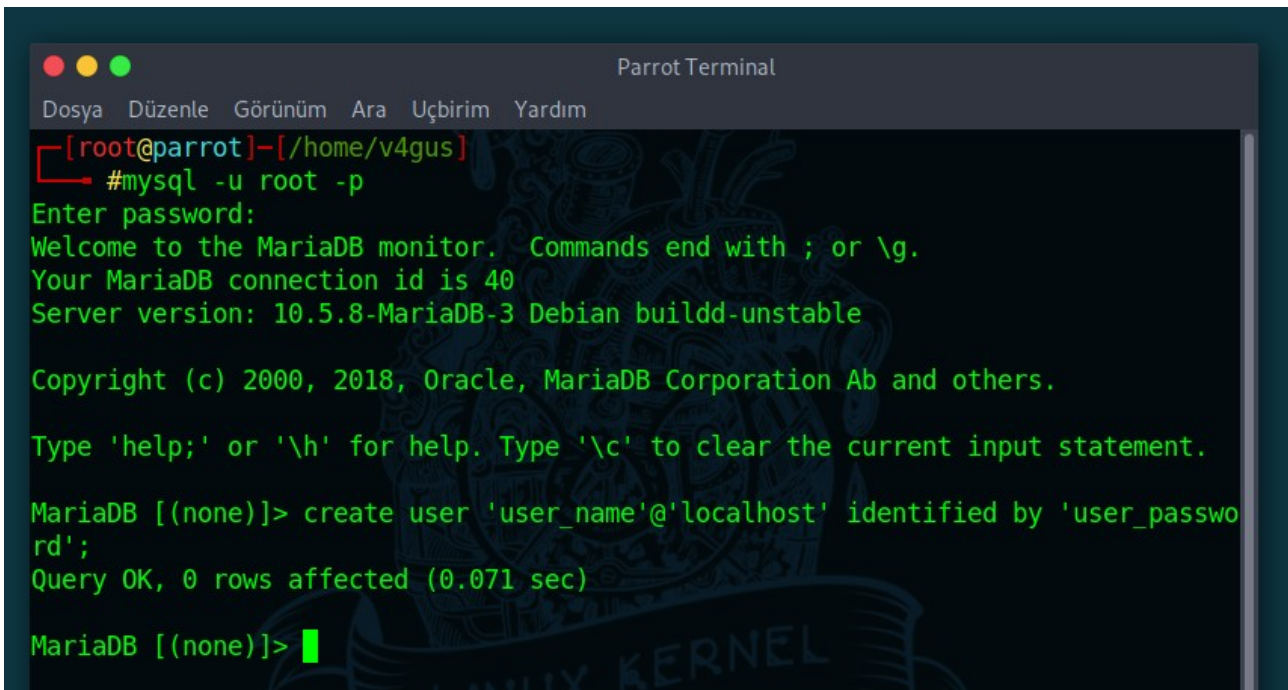
komutunu verdikten sonra

```
mysql -u root -p
```

komutu ile mysql bağlantısı kurabilirsiniz. Bağlantı kurulduktan sonra

```
create user 'user_name'@'localhost' identified by 'user_password';
```

komutu ile *user_name* isimli *user_password* parolalı bir kullanıcı oluşturulacaktır. Siz *user_name* ve *user_password* kısımlarına istediğiniz ismi ve parolayı verebilirsiniz.



```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[root@parrot]-[/home/v4gus]
#mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 40
Server version: 10.5.8-MariaDB-3 Debian buildd-unstable

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

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

MariaDB [(none)]> create user 'user_name'@'localhost' identified by 'user_passwo
rd';
Query OK, 0 rows affected (0.071 sec)

MariaDB [(none)]> █
```

Şimdi bWAPP içerisinde gelmiş olan database ismine yani oluşturduğumuz kullanıcıyı yetkilendirelim. Database ismi bWAPP.

```
grant all privileges on bWAPP.* to 'user_name'@'localhost' identified by 'user_password' ;
```

komutu ile yeni kullancımızın bu database üzerinde tam yetkili olmasını sağlarız.

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
MariaDB [(none)]> grant all privileges on bwAPP.* to 'user_name'@'localhost' identified by 'user_password' ;
Query OK, 0 rows affected (0.023 sec)

MariaDB [(none)]> █
```

Yeni kullanıcımızın yetkilerinden emin olmak için son bir sorgu daha çalıştıralım.

show grants for 'user_name'@'localhost';

bu sorgu ile yeni kullanıcımızın yetkilerini görüntüleriz.

```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
MariaDB [(none)]> show grants for 'user_name'@'localhost';
+-----+
+-----+
| Grants for user_name@localhost |
+-----+
+-----+
| GRANT USAGE ON *.* TO `user_name`@`localhost` IDENTIFIED BY PASSWORD '*ADC3B5B27617732CD6320A2DA976258E149A7EC8' |
| GRANT ALL PRIVILEGES ON `bwAPP`.* TO `user_name`@`localhost` |
+-----+
+-----+
2 rows in set (0.020 sec)

MariaDB [(none)]> █
```

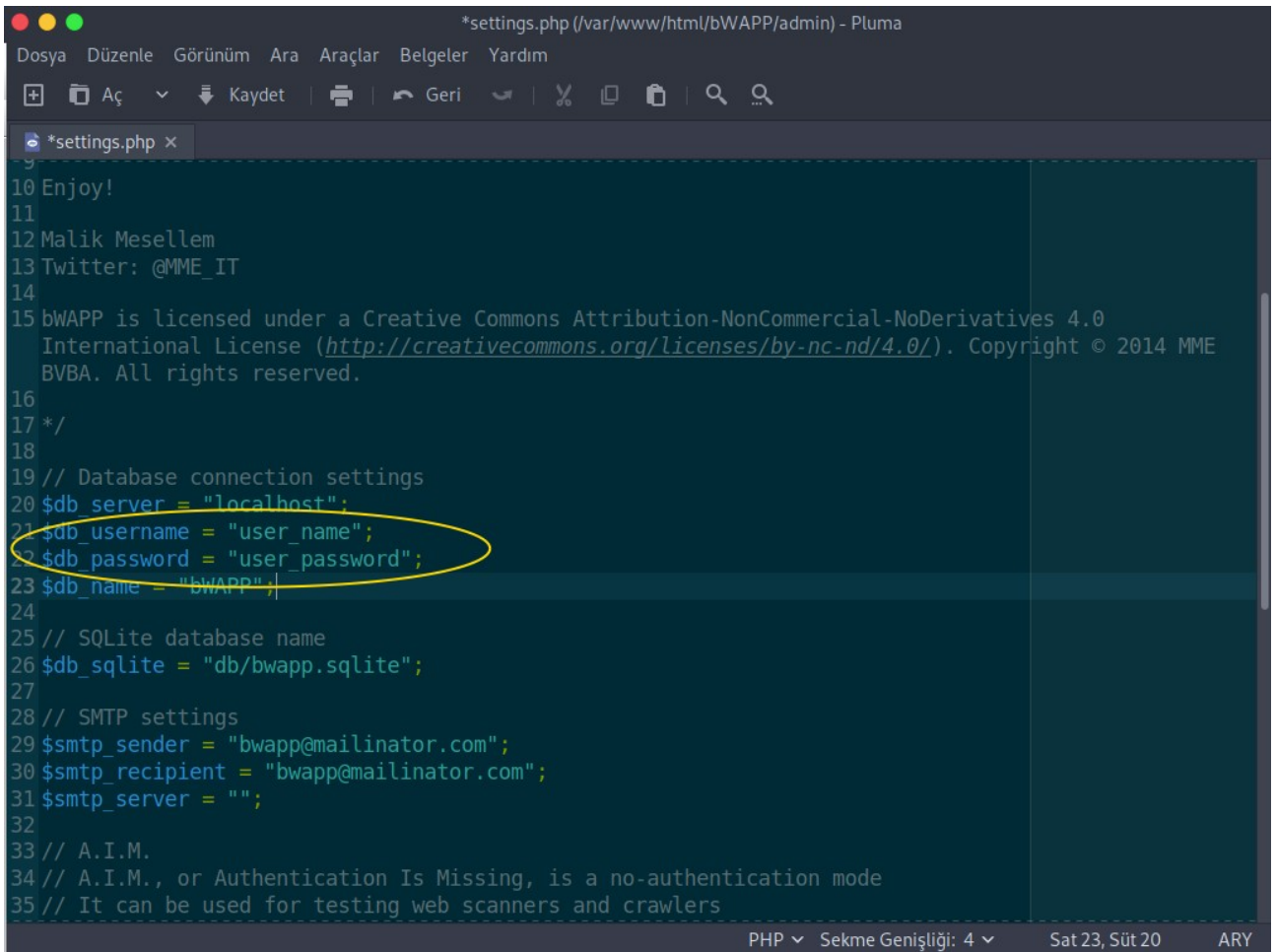
Görüldüğü gibi yetkilendirme tanımlanmış.

Şimdi dosyamıza dönüp

\$db_username = "user_name";

\$db_password = "user_password";

değişikliklerini yapalım.



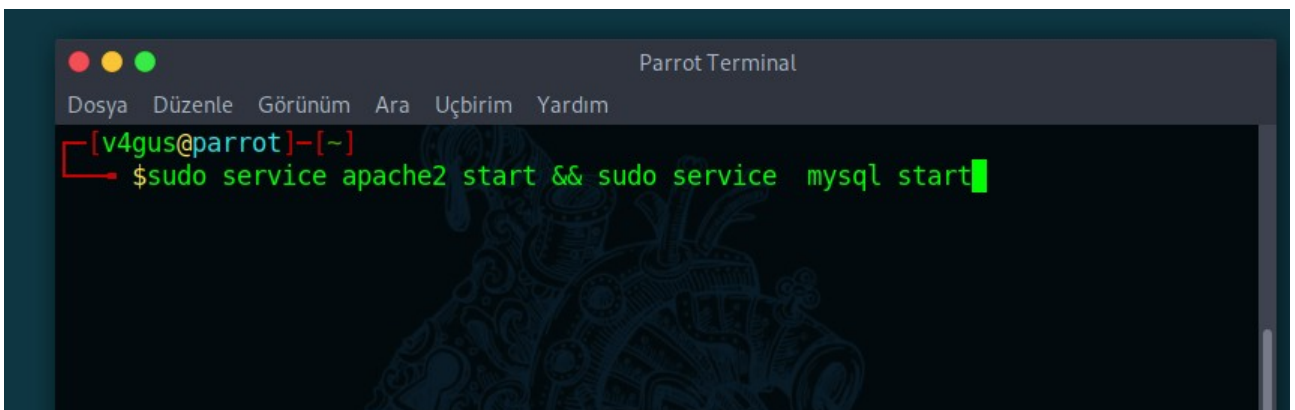
```
*settings.php (/var/www/html/bWAPP/admin) - Pluma
Dosya Düzenle Görünüm Ara Araçlar Belgeler Yardım
+ Aç Kaydet | | | | | | | | | |
*settings.php x
10 Enjoy!
11
12 Malik Mesellem
13 Twitter: @MME_IT
14
15 bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0
  International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME
  BVBA. All rights reserved.
16
17 */
18
19 // Database connection settings
20 $db_server = "localhost";
21 $db_username = "user_name";
22 $db_password = "user_password";
23 $db_name = "bWAPP";
24
25 // SQLite database name
26 $db_sqlite = "db/bwapp.sqlite";
27
28 // SMTP settings
29 $smtp_sender = "bwapp@mailinator.com";
30 $smtp_recipient = "bwapp@mailinator.com";
31 $smtp_server = "";
32
33 // A.I.M.
34 // A.I.M., or Authentication Is Missing, is a no-authentication mode
35 // It can be used for testing web scanners and crawlers
PHP Sekme Geniřlięi: 4 Sat 23, Süt 20 ARY
```

bWAPP'i Çalıştırma

Apache2 ve mysql servislerini çalıştıralım.

sudo service apache2 start && sudo service mysql start

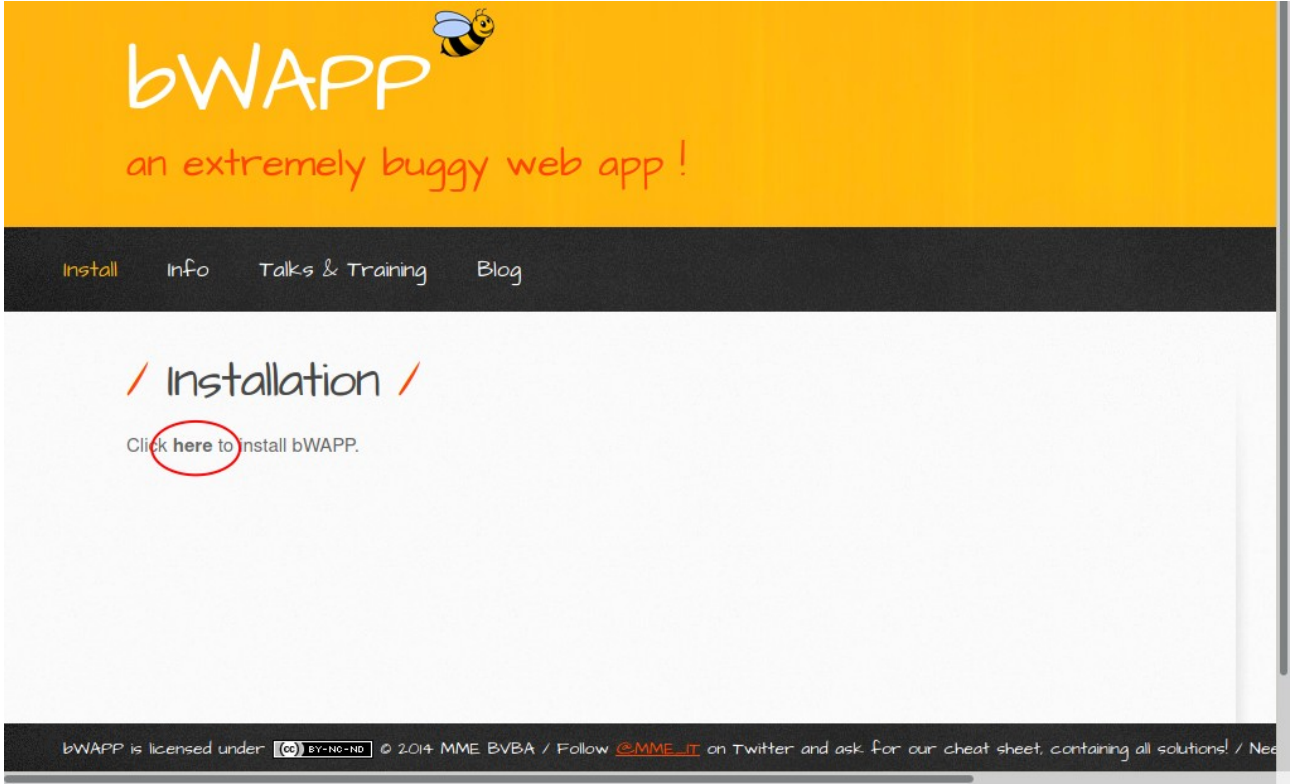
komutu ile iki servisi tek bir komut ile çalıştırabiliriz.



```
Parrot Terminal
Dosya Düzenle Görünüm Ara Uçbirim Yardım
[v4gus@parrot]~$ sudo service apache2 start && sudo service mysql start
```


Bir web browser üzerinden <http://127.0.0.1/html/bWAPP/install.php> veya <http://localhost/html/bWAPP/install.php> üzerinden erişim sağlayabilirsiniz.

Ardından gelen sayfada kalın olarak yazılan 'here' a tıklayıp kurulumu bitiririz.



Sayfanın üst kısmında bulunan menüden Login'i seçerek login sayfasına gelerek



an extremely buggy web app !

[Login](#)
[New User](#)
[Info](#)
[Talks & Training](#)
[Blog](#)

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:

low

Login








bWAPP is licensed under  © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training](#)?

Login: bee

Password: bug



an extremely buggy web app !

Choose your bug

bWAPP v2.2

Hack

Set your security level:

low

Set

Current: low

[Bugs](#)
[Change Password](#)
[Create User](#)
[Set Security Level](#)
[Reset](#)
[Credits](#)
[Blog](#)
[Logout](#)
[Welcome Bee](#)

/ Portal /

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project! It is for security-testing and educational purposes only.

Which bug do you want to hack today? :)

bWAPP v2.2

/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)

Hack








bWAPP is licensed under  © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training](#)?

ile giriş yapınca çalışmak istediğimiz zafiyetleri ve güvenlik seviyesini belirleyebiliriz. İyi eğlenceler ...

Kaynak