

Zayıf Web Uygulaması

Doküman

Zayıf Web Uygulaması web uygulama güvenliği alanında kendini geliştirmek isteyen pentesterlar ve güvenlik ile uğraşan kimseler için PHP ile oluşturulmuş içinde belli web zafiyetlerini barındıran bir eğitim sistemidir.

Bu proje Kocaeli Üniversitesinin Bilgisayar Mühendisliği bölümündeki Yazılım Laboratuvarı 2 (Proje III) ders projesi kapsamında geliştirilmiştir. Güvenlik uzmanlarının arasında meşhur Damn Vulnerable Web Application (DVMA) zayıf web uygulamasından ilham alıp bu projeni geliştirdik.

Uygulamamızın temel amacı güvenlik uzmanlarının becerilerini yasal bir ortamda geliştirmelerine, web geliştiricilerinin uygulamalarını daha iyi anlamalarına ve güvenli yazılımlar geliştirmelerine, hem öğrencilerin hem de öğretmenlerin kontrollü bir sınıfta web uygulaması güvenliği hakkında bilgi edinmelerine yardımcı olmak.

Her zafiyetin bulunduğu her bir sayfada **Yardım** bağlantısına tıklandığında pop-up şeklinde açılan bir sayfada ilgili zafiyetin sömürmek için örnek bir URL, bir paragraflık açıklaması, kaynak koddaki hangi kısımdan dolayı ve neden bu zafiyetin ortaya çıktığı, kaynak koddaki hangi değişiklikle ve nasıl bu zafiyetin engellenebileceği hakkında bilgi edinebilirsiniz.

UYARI!

Geliştirdiğimiz Zayıf Web Uygulamasını denemek için bir web hostinge veya internet'e açık sunuculara yüklemeyiniz. NAT ağ moduna ayarlanmış bir sanal makine ([VirtualBox](#) veya [VMware](#) gibi) veya [XAMPP](#) uygulamasını kullanmanızı öneririz. Herhangi birinin uygulamamızı kullanımı ile ilgili sorumluluk kabul etmiyoruz. Uygulamamızın yukarıda belirttiğimiz amaçlar dışında (kötü niyetle vs.) kullanmamlısınız. Bu uygulama kurulu web sunucunuz tehlikeye girerse sorumluluğumuz değil, yükleyen kişinin sorumluluğu altındadır.

Lisans (LICENSE)

Zayıf web uygulamamız ücretsiz bir yazılımdır. GNU Genel Kamu Lisansı 3'üncü (GPLv3) versiyonu altında yayınlanmıştır. Free Software Foundation tarafından yayınlanan şartlar altında dağıtılabilir ve/veya değiştirebilirsiniz.

GNU Genel Kamu Lisansı'nın bir kopyası bu yazılımla birlikte almışsınızdır, eğer almadıysanız <http://www.gnu.org/licenses/> link'inden bakabilirsiniz.

İndir

Uygulamamız github üzerinden geliştiriliyor ve dağıtılıyor ve [Github Link](#) indirebilirsiniz veya bilgisayarınızda git kuruluysa:

```
git clone https://github.com/ataniazov/Zayif-Web-Uygulamasi.git
```

Kurulum

Zayıf Web Uygulamasını kurmanın en kolay yolu [XAMPP](#) uygulamasının indirilip üzerine kurulmasıdır. XAMPP, esas olarak Apache HTTP sunucusu, MySQL veritabanı dağıtımı olup, PHP ve PERL programlama dilleri ile yazılmış çapraz platform web sunucusu çözümü ve ücretsiz, açık kaynaklı yığın paketidir. Oldukça popüler olan bir PHP geliştirme ortamı yazılımıdır. Windows, Mac OS X ve Linux için uygun paketleri bulunmaktadır.

XAMPP <https://www.apachefriends.org/> linkinden indirebilirsiniz.

[Github Link](#) uygulamamızın sıkıştırılmış dosyasını çıkartıp, XAMPP uygulamasının genel html klasörüne yerleştirin, ardından tarayıcınıza aşağıdaki adresi giriniz: <http://127.0.0.1/>

Ubuntu + XAMPP

Zayıf Web Uygulaması [Ubuntu](#) linux dağıtımının 16.04.2, [XAMPP](#) uygulamasının 5.6.30 versiyonunda test edilmiştir. Ubuntu linux dağıtımına XAMPP kurulumu:

```
wget
https://www.apachefriends.org/xampp-files/5.6.30/xampp-linux-x64-5.6.30-0-installer.
run
chmod u+x ./xampp-linux-x64-5.6.30-0-installer.run
sudo ./xampp-linux-x64-5.6.30-0-installer.run
```

Komut enjeksiyonu zafiyetinin düzgün çalışması için bilgisayarınızda **whois** uygulamasının kurulu olması gerekmektedir.

```
sudo apt update && apt install whois
```

Ardından yukarıda belirtilen kurulum aşamalarını izlemeniz yeterlidir.

Veritabanı ayarları

Veritabanını kurmak için, ana menüde **Kur / Sıfırla** düğmesine tıklayın. Bu sizin için bazı verilerle

veritabanını oluşturacak / sıfırlayacaktır. Veritabanınızı oluşturmaya çalışırken bir hata mesajı alırsanız ./config/config.inc.php içinde veritabanının bağlantı ayarlarının doğru olduğundan emin olun. Veritabanının bağlantı ayarları varsayılan olarak aşağıdaki şekildedir:

```
$_DNRDB[ 'db_server' ]    = '127.0.0.1';
$_DNRDB[ 'db_database' ] = 'dnrdb';
$_DNRDB[ 'db_user' ]      = 'root';
$_DNRDB[ 'db_password' ] = '';
$_DNRDB[ 'db_port ' ]     = '3306';
```

Sorun giderme

En son sorun giderme bilgileri için lütfen [Github Issues](#) ziyaret edin.

```
In open source, no one can hear you scream;)
Please use Google before asking questions.
```

Bağlantılar

Proje Ana Sayfası: <https://github.com/ataniazov/Zayif-Web-Uygulaması/>

Ata Niyazov tarafından yazılmış ve geliştirilmiştir
