DVWA

Friday, February 5, 2016 8:20 AM

DAMN VULNERABLE WEB APPLICATION

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.
The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface. Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

License

Download

DVWA is available either as a package that will run on your own web server or as a Live CD:

- DVWA v1.9 Source (Stable) - [1.3 MB] Download ZIP - Released 2015-10-05
- DVWA v1.0.7 LiveCD - [480 MB] Download ISO - Released 2010-09-08
- DVWA Development Source (Latest) Download ZIP // `git clone https://github.com/RandomStorm/DVWA`

Installation

Windows + XAMPP

Installation video: https://www.youtube.com/watch?v=GzIj07jt8rM
The easiest way to install DVWA is to download and install XAMPP if you do not already have a web server setup.
XAMPP is a very easy to install Apache Distribution for Linux, Solaris, Windows and Mac OS X. The package includes the Apache web server, MySQL, PHP, Perl, a FTP server and phpMyAdmin.
XAMPP can be downloaded from: https://www.apachefriends.org/en/xampp.html
Simply unzip dvwa.zip, place the unzipped files in your public html folder, then point your browser to: http://127.0.0.1/dvwa/setup.php

Linux Packages

If you are using a Debian based Linux distribution, you will need to install the following packages *(or their equivalent)*:

```
apt-get -y install apache2 mysql-server php5 php5-mysql php5-gd
```

Database Setup

To set up the database, simply click on the `Setup DVWA` button in the main menu, then click on the `Create / Reset Database` button. This will create / reset the database for you with some data in.
If you receive an error while trying to create your database, make sure your database credentials are correct within `./config/config.inc.php`.
The variables are set to the following by default:

```
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_database' ] = 'dvwa';
```

Other Configuration

Depening on your Operating System as well as version of PHP, you may wish to alter the default configuration. The location of the files will be different on a per-machine basis. Note, You are unable to use PHP v7.0 or later with DVWA.
Folder Permissions:

- `./hackable/uploads/` - Needs to be writable by the web service (for File Upload).
- `./external/phpids/0.6/lib/IDS/tmp/phpids_log.txt` - Needs to be writable by the web service (if you wish to use PHPIDS).

PHP configuration:

- `allow_url_include = on` - Allows for Remote File Inclusions (RFI) [allow_url_include]
- `allow_url_fopen = on` - Allows for Remote File Inclusions (RFI) [allow_url_fopen]
- `safe_mode = off` - (If PHP <= v5.4) Allows for SQL Injection (SQLi) [safe_mode]
- `magic_quotes_gpc = off` - (If PHP <= v5.4) Allows for SQL Injection (SQLi) [magic_quotes_gpc]
- `display_errors = off` - (Optional) Hides PHP warning messages to make it less verbose [display_errors]

File: `config/config.inc.php`:

- `$_DVWA[ 'recaptcha_public_key' ]` & `$_DVWA[ 'recaptcha_private_key' ]` - These values need to be generated from: https://www.google.com/recaptcha/admin/create

Default Credentials

Default username = `admin`
Default password = `password`
...can easily be brute forced ;)
Login URL: http://127.0.0.1/dvwa/login.php

Troubleshooting

For the latest troubleshooting information please visit: https://github.com/RandomStorm/DVWA/issues
+Q. SQL Injection wont work on PHP v5.2.6.
-A.If you are using PHP v5.2.6 you will need to do the following in order for SQL injection and other vulnerabilities to work.
In `.htaccess`:
Replace:

```
<IfModule mod_php5.c>
    php_flag magic_quotes_gpc off
    #php_flag allow_url_fopen on
    #php_flag allow_url_include on
</IfModule>
```

With:

```
<IfModule mod_php5.c>
    magic_quotes_gpc = Off
    allow_url_fopen = On
    allow_url_include = On
</IfModule>
```

+Q. Command Injection won't work.
-A. Apache may not have high enough priviledges to run commands on the web server. If you are running DVWA under Linux make sure you are logged in as root. Under Windows log in as Administrator.
+Q. My XSS payload won't run in IE.
-A. If you're running IE8 or above, IE actively filters any XSS. To disable the filter you can do so by setting the HTTP header `X-XSS-Protection: 0` or disable it from internet options. There may also be ways to bypass the filter.

Links

Homepage: http://www.dvwa.co.uk/
Project Home: https://github.com/RandomStorm/DVWA
Created by the DVWA team

From <https://github.com/RandomStorm/DVWA/blob/master/README.md>