

Damn Vulnerable Web Application



Saugos testavimo įrankis

Reikalinga programinė įranga

- XAMPP

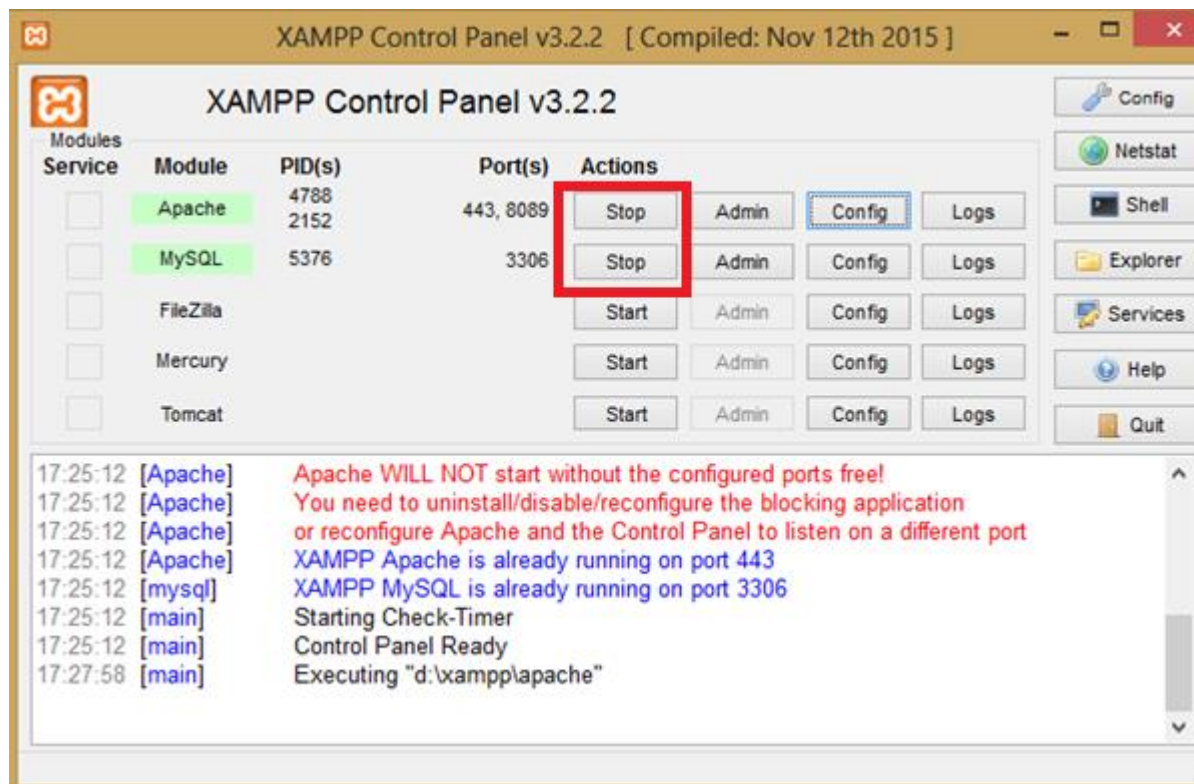
<https://www.apachefriends.org/download.html>

- Damn Vulnerable Web Application

<http://www.dvwa.co.uk/>

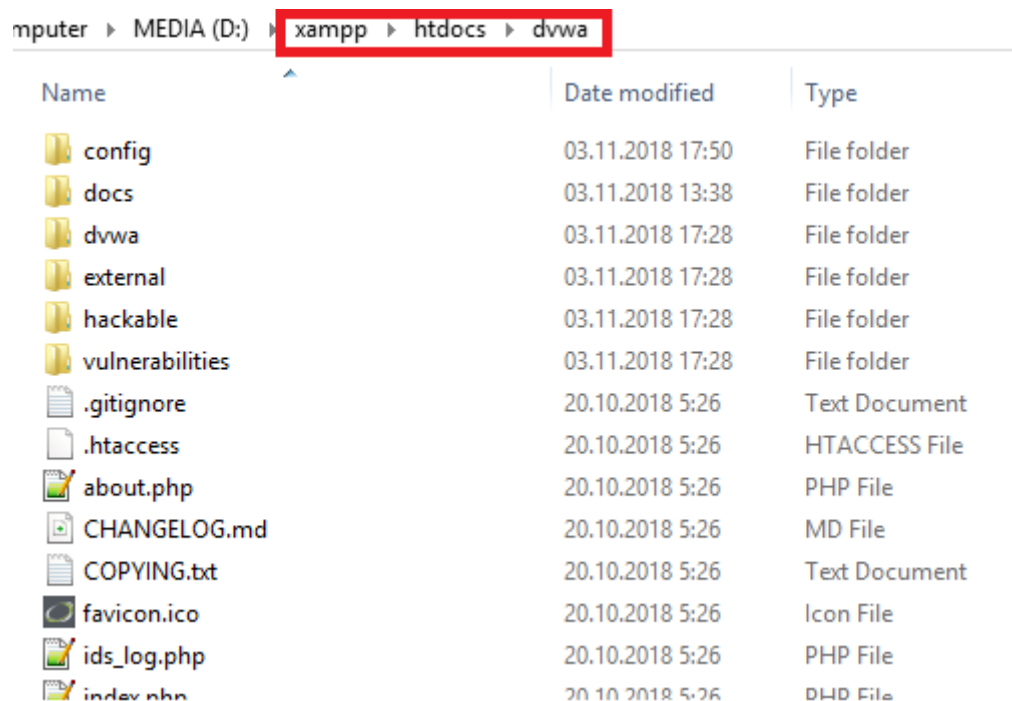
XAMPP paleidimas

- Parsisiųsti, įsidiegti, pasileisti:



Įdiegimas. Failai (1)

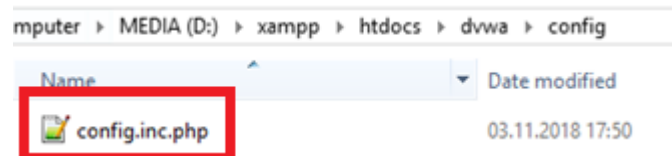
- Parsisiųstus *dvwa* failus patalpinti į *XAMPP*



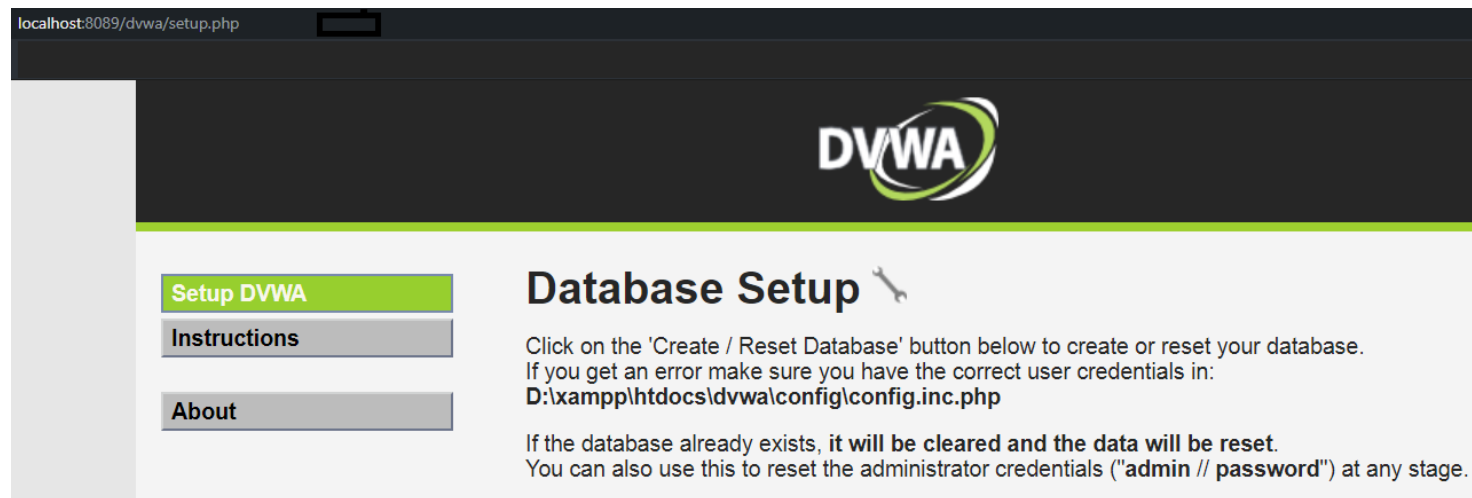
| mputer > MEDIA (D:) > xampp > htdocs > dvwa | | |
|---|------------------|---------------|
| Name | Date modified | Type |
| config | 03.11.2018 17:50 | File folder |
| docs | 03.11.2018 13:38 | File folder |
| dvwa | 03.11.2018 17:28 | File folder |
| external | 03.11.2018 17:28 | File folder |
| hackable | 03.11.2018 17:28 | File folder |
| vulnerabilities | 03.11.2018 17:28 | File folder |
| .gitignore | 20.10.2018 5:26 | Text Document |
| .htaccess | 20.10.2018 5:26 | HTACCESS File |
| about.php | 20.10.2018 5:26 | PHP File |
| CHANGELOG.md | 20.10.2018 5:26 | MD File |
| COPYING.txt | 20.10.2018 5:26 | Text Document |
| favicon.ico | 20.10.2018 5:26 | Icon File |
| ids_log.php | 20.10.2018 5:26 | PHP File |
| index.php | 20.10.2018 5:26 | PHP File |

Įdiegimas. Failai (2)

- Pervadinti *config* failą į:



- Paleisti aplikaciją:



Įdiegimas. CAPTCHA (1) [optional]

- **CAPTCHA** (angl. *Completely Automated Public Turing test to tell Computers and Humans Apart*) – testas, naudojamas kompiuteriuose ir skirtas nustatyti ar naudotojas yra žmogus, ar ne.
- Ką matome *localhost/dvwa*:

reCAPTCHA key: **Missing**

- Atsidarome *config* failą. Kai užsiregistruosime *google* (sekanti skaidrė), į *public* ir *private key* vietas reikės patalpinti iš *google* gautus raktus:

```
26 # ReCAPTCHA settings
27 #   Used for the 'Insecure CAPTCHA' module
28 #   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin/create
29 $_DVWA[ 'recaptcha_public_key' ] = '';
30 $_DVWA[ 'recaptcha_private_key' ] = '';
```

- Raktams gauti einame į <https://www.google.com/recaptcha/admin>

Įdiegimas. CAPTCHA (2) [optional]

- Registruojamės *google captcha* raktams gauti:

Label

Choose the type of reCAPTCHA ⓘ

☐ reCAPTCHA v3
Validate requests with a score.

☒ reCAPTCHA v2

☒ Checkbox
Validate requests with the "I'm not a robot" checkbox.

☐ Invisible
Validate requests with your own button.

☐ Android
Validate requests in your android app.

Domains
(one per line)

For example:
example.com
example.net
example.org

☒ Accept the reCAPTCHA Terms of Service.
By accessing or using the reCAPTCHA APIs, you agree to the Google APIs [Terms of Use](#), Google [Terms of Use](#), and to the [Additional Terms](#) below. Please read and understand all applicable terms and policies before accessing the APIs.
▸ reCAPTCHA Terms of Service

☒ Send alerts to owners ⓘ



Register

Įdiegimas. CAPTCHA (3) [optional]

- Saugojamės raktus į *dvwa config* failą:

① Adding reCAPTCHA to your site

▼ Keys

| Site key | Secret key |
|---|---|
| public key | private key |
| Use this in the HTML code your site serves to users. | Use this for communication between your site and Google. Be sure to keep it a secret. |
|  |  |

▼ Step 1: Client side integration

Paste this snippet before the closing `</head>` tag on your HTML template:

```
<script src='https://www.google.com/recaptcha/api.js'></script>
```

Paste this snippet at the end of the `<form>` where you want the reCAPTCHA widget to appear:

```
<div class="g-recaptcha" data-sitekey="6LfYIHgUAAAAADZLXH3DHypiaLpTyzDcFYETwnOn" /div>
```

The [reCAPTCHA documentation site](#) describes more details and advanced configurations.

- Atnaujiname *localhost/dvwa*:

reCAPTCHA key: 6LfYIHgUAAAAADZLXH3DHypiaLpTyzDcFYETwnOn

Įdiegimas. URL [optional]

- Jeigu neįjungta:

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

- Įjungti (neužmirštami *XAMPP*):

To solve the issue, go to:

```
C:\xampp\php\php.ini
```

And change:



```
allow_url_include=Off
```


To:

```
allow_url_include=On
```

Įdiegimas. db (1)

- Sukuriama *localhost/phpmyadmin* nauja db:

 **Create database** 

Įdiegimas. db (2)

- Sukuriamas naujas vartotojas su *root* teisėm:

The screenshot shows the 'User accounts' tab in phpMyAdmin. A red box labeled '1' highlights the 'User accounts' tab. A red box labeled '2' highlights the 'root' user entry in the table. A red box labeled '3' highlights the 'Add user account' button at the bottom.

Warning: A user account allowing any user from localhost to connect is present. This will prevent other users from connecting from any (%) host.

| | User name | Host name | Password | Global privileges | User group | Grant | Action |
|-------------------------------------|-----------|-----------|----------|-------------------|------------|-------|------------------------|
| <input type="checkbox"/> | Any | % | No | USAGE | | No | Edit privileges Export |
| <input type="checkbox"/> | Any | localhost | No | USAGE | | No | Edit privileges Export |
| <input type="checkbox"/> | pma | localhost | No | USAGE | | No | Edit privileges Export |
| <input checked="" type="checkbox"/> | root | 127.0.0.1 | No | ALL PRIVILEGES | | Yes | Edit privileges Export |
| <input type="checkbox"/> | root | ::1 | No | ALL PRIVILEGES | | Yes | Edit privileges Export |
| <input type="checkbox"/> | root | localhost | No | ALL PRIVILEGES | | Yes | Edit privileges Export |

Check all With selected: Export

New Add user account

Įdiegimas. db (3)

- Sukuriamas naujas vartotojas su *root* teisėm:

The screenshot shows the MySQL User Accounts configuration interface. Red annotations highlight key steps:

- 1**: The **User accounts** tab in the top navigation bar is highlighted.
- 2**: The **Login Information** section is highlighted, showing the following fields:
 - User name**: A dropdown menu with "parag" selected.
 - Host name**: A dropdown menu with "Local" selected.
 - Password**: A text field with "****" and a strength indicator labeled "Very weak".
 - Re-type**: A text field with "****".
 - Authentication Plugin**: A dropdown menu with "Native MySQL authentication" selected.
 - Generate password**: A button labeled "Generate" next to an empty text field.
- 3**: The **Global privileges** section is highlighted, showing a checkbox labeled "Check all" which is checked.

{diegimas. db (4)

- *db config:*

```
17 $_DVWA = array();  
18 $_DVWA[ 'db_server' ] = '127.0.0.1';  
19 $_DVWA[ 'db_database' ] = 'dvwa';  
20 $_DVWA[ 'db_user' ] = 'parag';  
21 $_DVWA[ 'db_password' ] = 'root';
```

- *localhost/dvwa:*

Create / Reset Database

Prisijungimas

- Pasižiūrime prisijungimus prie *dvwa* ir prisijungiamo *localhost/dvwa*:



<https://www.md5online.org>

| user_id | first_name | last_name | user | password | for decrypt |
|---------|------------|-----------|---------|----------------------------------|-------------|
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f260853678922e03 | |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b | |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 | |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 | |



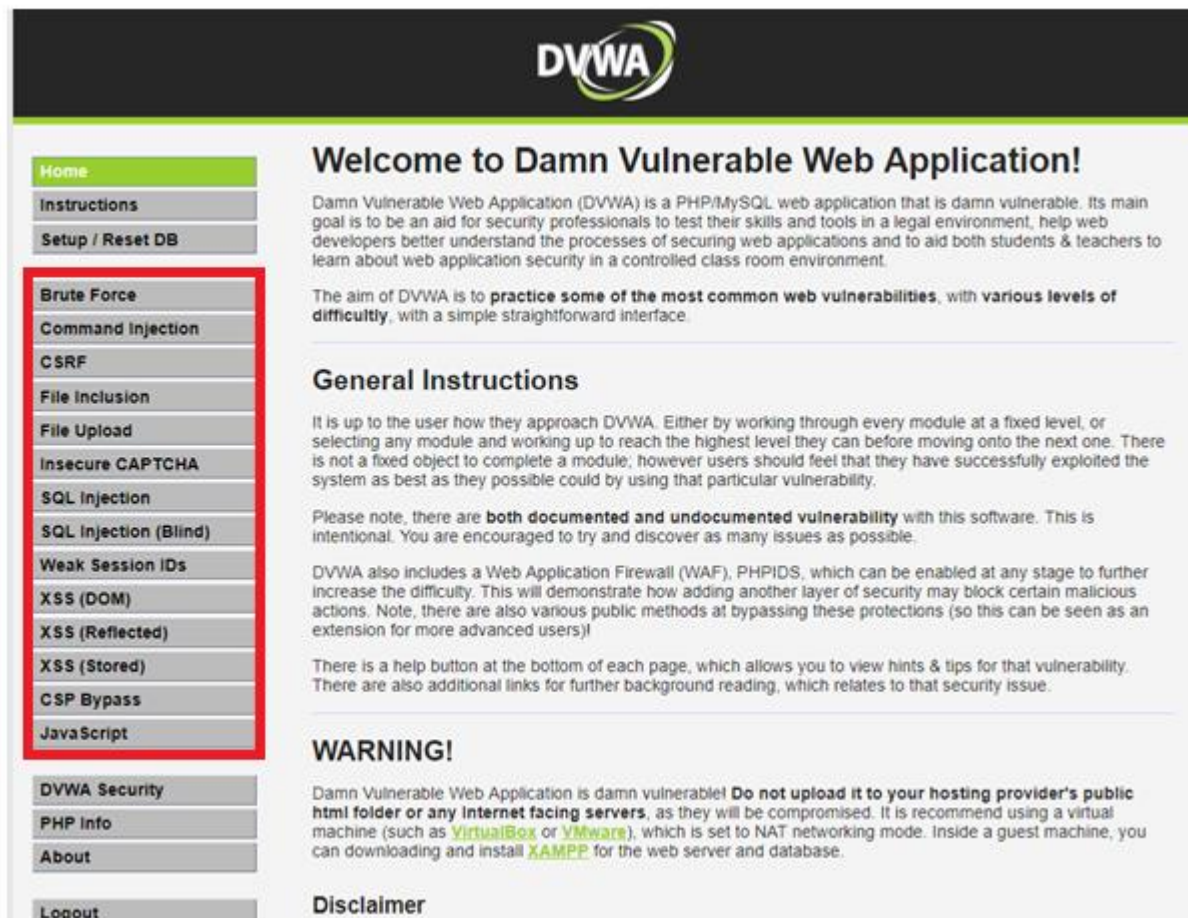
Username
admin

Password

Login

Naudojimas (1)

- Prisijungus prie *dvwa* matome tokį vaizdą:



The screenshot displays the DVWA homepage. On the left is a sidebar menu with the following items: 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), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, About, and Logout. The 'Brute Force' through 'JavaScript' items are highlighted with a red border. The main content area has a dark header with the DVWA logo and the title 'Welcome to Damn Vulnerable Web Application!'. Below the title, it describes DVWA as a PHP/MySQL web application for testing security skills. It states the aim is to practice common web vulnerabilities with varying difficulty levels. A 'General Instructions' section follows, explaining the user's approach and the application's security features like WAF and PHPIDS. A 'WARNING!' section advises against uploading the application to public servers and recommends using a virtual machine. A 'Disclaimer' section is at the bottom.

Welcome to 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 vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

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.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

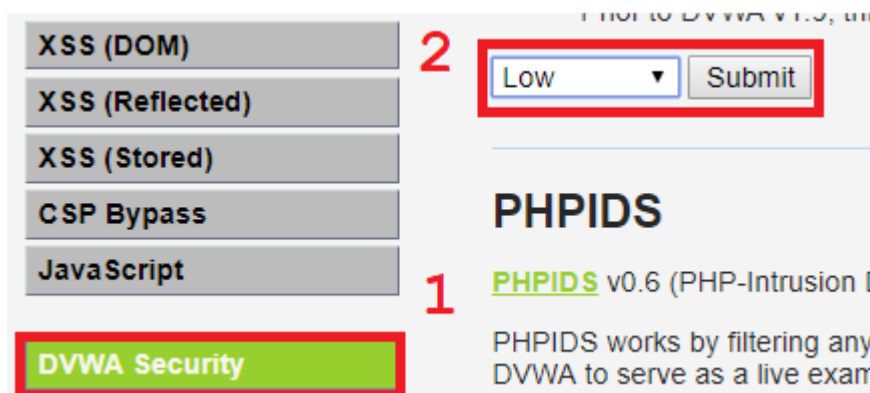
WARNING!

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

Naudojimas (2)

- Nustatome apsaugos lygį testavimui:



- Pasitikriname:

Username: admin
Security Level: low
PHPIDS: disabled

Veikimo testas

- Pabandome atlikti *SQL Injection*:

Vulnerability: SQL Injection

User ID:

ID: ' or 1=1 #
First name: admin
Surname: admin

ID: ' or 1=1 #
First name: Gordon
Surname: Brown

ID: ' or 1=1 #
First name: Hack
Surname: Me

ID: ' or 1=1 #
First name: Pablo
Surname: Picasso

ID: ' or 1=1 #
First name: Bob
Surname: Smith

Testavimo pratybos su dvwa

- Atliekame *dvwa* sistemos testavimą pagal skaidres '*Pagrindiniai web sistemų pažeidžiamumai ir saugos būdai*'

Literatūra

- How to setup DVWA (Damn Vulnerable Web Application) on Windows with XAMPP or WAMP- Installation Guru:

https://www.youtube.com/watch?v=DCRVa_my8rE