

# Презентация по второму этапу индивидуального проекта

## Информационная безопасность

---

Арабтова В. П.

22 марта 2025

Российский университет дружбы народов, Москва, Россия

## Цель работы

---

Установить DVWA в гостевую систему к Kali Linux.

## Задание

---

Установите DVWA в гостевую систему к Kali Linux.

## Теоретическое введение

---

Некоторые из уязвимостей веб приложений, который содержит DVWA:

Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.

Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.

Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.

Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.

SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение.

## Выполнение лабораторной работы

---



Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию /var/www/html. Затем клонирую нужный репозиторий GitHub, указанный в задании к этому этапу индивидуального проекта

```
(vparbatova@vparbatova)-[~]  
$ cd /var/www/html  
  
(vparbatova@vparbatova)-[/var/www/html]  
$ sudo git clone https://github.com/ethicalhack3r/DVWA  
[sudo] пароль для vparbatova:  
Клонирование в «DVWA»...  
remote: Enumerating objects: 5105, done.  
remote: Counting objects: 100% (91/91), done.  
remote: Compressing objects: 100% (24/24), done.  
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)  
Получение объектов: 100% (5105/5105), 2.49 МиБ | 350.00 КиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
  
(vparbatova@vparbatova)-[/var/www/html]  
$
```

Рис. 1: Клонирование репозитория

Проверяю, что всё правильно скопировалось и добавляю права на этот файл, чтобы у меня был полный доступ к нему

```
(vparbatova@vparbatova)-[/var/www/html]
$ ls
DVWA index.html index.nginx-debian.html

(vparbatova@vparbatova)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис. 2: Добавляю права

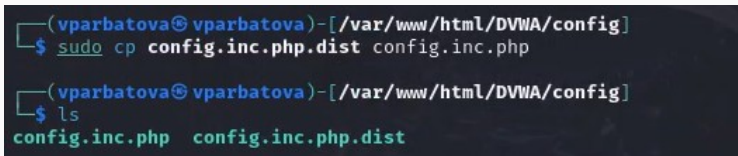
Перехожу в папку и смотрю, какие в ней файлы

```
(vparbatova@vparbatova)-[/var/www/html]
$ cd DVWA/config

(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
$ ls
config.inc.php.dist
```

Рис. 3: Перехожу в папку

Копирую файл и проверяю, как он скопировался. Делаю это для того, чтобы в случае, если что-то пойдет не так, у меня был запасной вариант

A terminal window with a dark background and light blue text. The prompt is (vparbatova@vparbatova)-[/var/www/html/DVWA/config]. The first command is \$ sudo cp config.inc.php.dist config.inc.php. The second command is \$ ls. The output of the ls command is config.inc.php config.inc.php.dist.

```
(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist
```

Рис. 4: Копирование файла

Открываю файл в текстовом редакторе

A terminal window with a dark background. The prompt shows the user 'vparbatova' on a host 'vparbatova' in the directory '/var/www/html/DVWA/config'. The command 'sudo nano config.inc.php' is entered, with 'sudo' in green, 'nano' in blue, and 'config.inc.php' in white. A white cursor is at the end of the command.

```
(vparbatova@vparbatova)-[/var/www/html/DVWA/config]  
$ sudo nano config.inc.php
```

Рис. 5: Открываю файл в редакторе

## Меняю информацию об имени пользователя и пароле

```
GNU nano 8.2                                config.inc.php *
# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv( 'DB_SERVER' ) ? : '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'userDVWA';
$_DVWA[ 'db_password' ] = 'dvwa';
$_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/admin
$_DVWA[ 'recaptcha_public_key' ] = getenv( 'RECAPTCHA_PUBLIC_KEY' ) ? : '';
$_DVWA[ 'recaptcha_private_key' ] = getenv( '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', 'medium', 'high' or
$_DVWA[ 'default_security_level' ] = getenv( 'DEFAULT_SECURITY_LEVEL' ) ? : 'impossible';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.

Имя файла для записи [Формат DOS]: config.inc.php
^G Справка          М-D Формат DOS      М-A Доп. в начало    М-B Резерв. копия
^C Отмена           М-M Формат Mac      М-P Доп. в конец   ^T Обзор
```

Рис. 6: Меняю имя пользователя и пароль

Запускаю mysql, он изначально установлен в Kali Linux, поэтому скачивать не надо и проверяю, запустился ли

```
└─$ sudo systemctl start mysql
vparbatova@vparbatova:~$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-03-20 20:12:28 MSK; 25s ago
     Invocation: a860e12aa3ef40808b8e2f9de62f2f7e
       Docs: man:mariadb(8)
             https://mariadb.com/kb/en/library/systemd/
   Process: 7578 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 7588 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 7591 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/usr/bin/galera_recovery" (code=exited, status=0/SUCCESS)
   Process: 7674 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 7676 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 7652 (mariabdd)
   Status: "Taking your SQL requests now..."
    Tasks: 14 (limit: 30079)
  Memory: 242.5M (peak: 247M)
     CPU: 2.148s
   CGroup: /system.slice/mariadb.service
           └─7652 /usr/sbin/mariabdd

mar 20 20:12:27 vparbatova mariabdd[7652]: 2025-03-20 20:12:27 0 [Note] Plugin 'FEEDBACK' is disabled
mar 20 20:12:27 vparbatova mariabdd[7652]: 2025-03-20 20:12:27 0 [Note] Plugin 'wsrep-provider' is disabled
mar 20 20:12:27 vparbatova mariabdd[7652]: 2025-03-20 20:12:27 0 [Note] InnoDB: Buffer pool(s) built
mar 20 20:12:27 vparbatova mariabdd[7652]: 2025-03-20 20:12:27 0 [Note] Server socket created on
mar 20 20:12:28 vparbatova mariabdd[7652]: 2025-03-20 20:12:28 0 [Note] mariabdd: Event Scheduler
mar 20 20:12:28 vparbatova mariabdd[7652]: 2025-03-20 20:12:28 0 [Note] /usr/sbin/mariabdd: ready for
mar 20 20:12:28 vparbatova mariabdd[7652]: Version: '11.4.3-MariaDB-1' socket: '/run/mysqld/mysq
mar 20 20:12:28 vparbatova systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.
```

Рис. 7: Запуск mysql

Авторизуюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением “MariaDB”, далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php

```
(vparbatova@vparbatova)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0,028 sec)
```

Рис. 8: Авторизация



Выдаю пользователю все привилегии и выхожу

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';  
Query OK, 0 rows affected (0,005 sec)  
  
MariaDB [(none)]> exit  
Bye
```

Рис. 9: Выдаю привилегии

Теперь надо настроить сервер apache2, для этого перехожу в соответствующую директорию

A terminal window with a dark background. The prompt shows the user is vparbatova@vparbatova in the directory /var/www/html/DVWA/config. The command 'cd /etc/php/8.2/apache2' has been entered and executed.

```
(vparbatova@vparbatova)-[/var/www/html/DVWA/config]  
$ cd /etc/php/8.2/apache2
```

Рис. 10: Переход в директорию

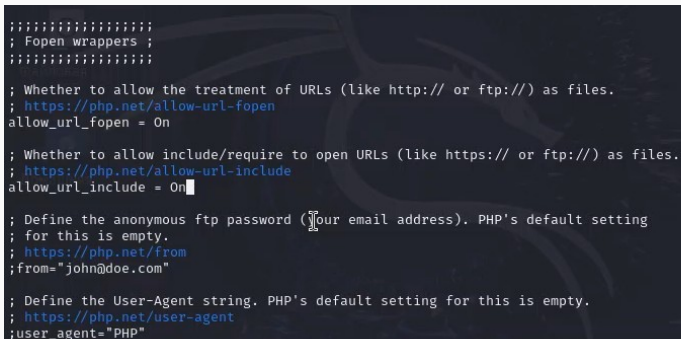
Открываю файл в текстовом редакторе

A terminal window with a dark background. The prompt is '(vparbatova@vparbatova)-[/etc/php/8.2/apache2]'. The command '\$ sudo nano php.ini' is entered, with a cursor at the end of the line.

```
(vparbatova@vparbatova)-[/etc/php/8.2/apache2]  
$ sudo nano php.ini
```

Рис. 11: Открытие файла

Нахожу параметры allow\_url\_fopen и allow\_url\_include. Эти параметры должны быть on



```
;;;;;;;;;;  
; Fopen wrappers ;  
;;;;;;;;;;  
  
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.  
; https://php.net/allow-url-fopen  
allow_url_fopen = On  
  
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.  
; https://php.net/allow-url-include  
allow_url_include = On  
  
; Define the anonymous ftp password (your email address). PHP's default setting  
; for this is empty.  
; https://php.net/from  
;from="john@doe.com"  
  
; Define the User-Agent string. PHP's default setting for this is empty.  
; https://php.net/user-agent  
;user_agent="PHP"
```

Рис. 12: Редактирование файла

Запускаю apache2 и проверяю статус, чтобы убедиться, что он действительно запущен

```
(vparbatova@vparbatova)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(vparbatova@vparbatova)-[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-03-20 20:30:06 MSK; 18s ago
 Invocation: 79d41f25b74d48999a6aff9f76923a71
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 15846 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 15862 (apache2)
     Tasks: 6 (limit: 4557)
    Memory: 20.1M (peak: 20.5M)
       CPU: 135ms
    CGroup: /system.slice/apache2.service
            └─15862 /usr/sbin/apache2 -k start
              └─15865 /usr/sbin/apache2 -k start
                └─15866 /usr/sbin/apache2 -k start
                  └─15867 /usr/sbin/apache2 -k start
                    └─15868 /usr/sbin/apache2 -k start
                      └─15869 /usr/sbin/apache2 -k start

map 20 20:30:06 vparbatova systemd[1]: Starting apache2.service - The Apache HTTP Server ...
map 20 20:30:06 vparbatova systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Рис. 13: Запуск

В браузере вбиваю 127.0.0.1/DVWA и попадаю на сайт, где нужно авторизироваться

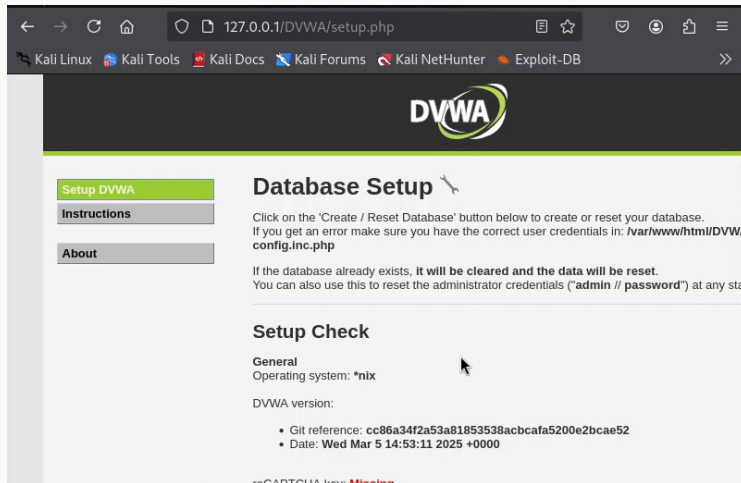


Рис. 14: Переход на сайт

Прокручиваем страницу вниз и нажимаем на кнопку

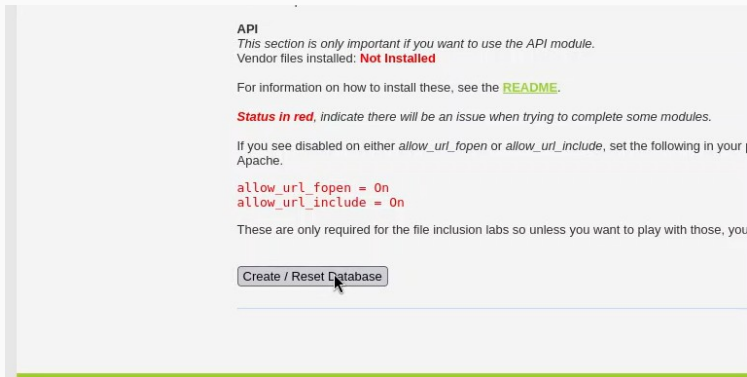
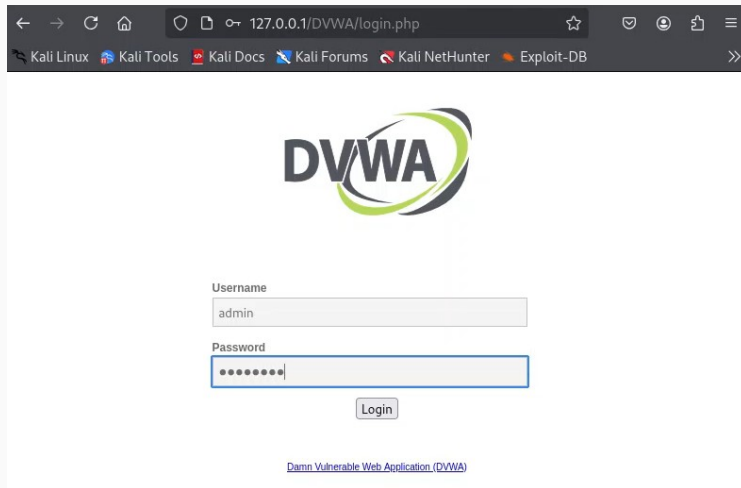


Рис. 15: Кнопка

Вхожу с данными, предложенными по умолчанию



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/DVWA/login.php`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. The main content area features the DVWA logo, which consists of the letters "DVWA" in a bold, black, sans-serif font, with a green and black swoosh graphic to the right. Below the logo are two input fields: "Username" with the text "admin" and "Password" with masked characters (dots). A "Login" button is positioned below the password field. At the bottom of the page, there is a link that reads "Damn Vulnerable Web Application (DVWA)".

Рис. 16: Вход



## Выводы

---

Установила DVWA в гостевую систему к Kali Linux.