

Отчёт по ИП 2 этап

Установка DVWA

Хрусталев Влад Николаевич

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	10

List of Figures

List of Tables

1 Цель работы

Установить DVMA, изучить основные возможности

2 Теоретическое введение

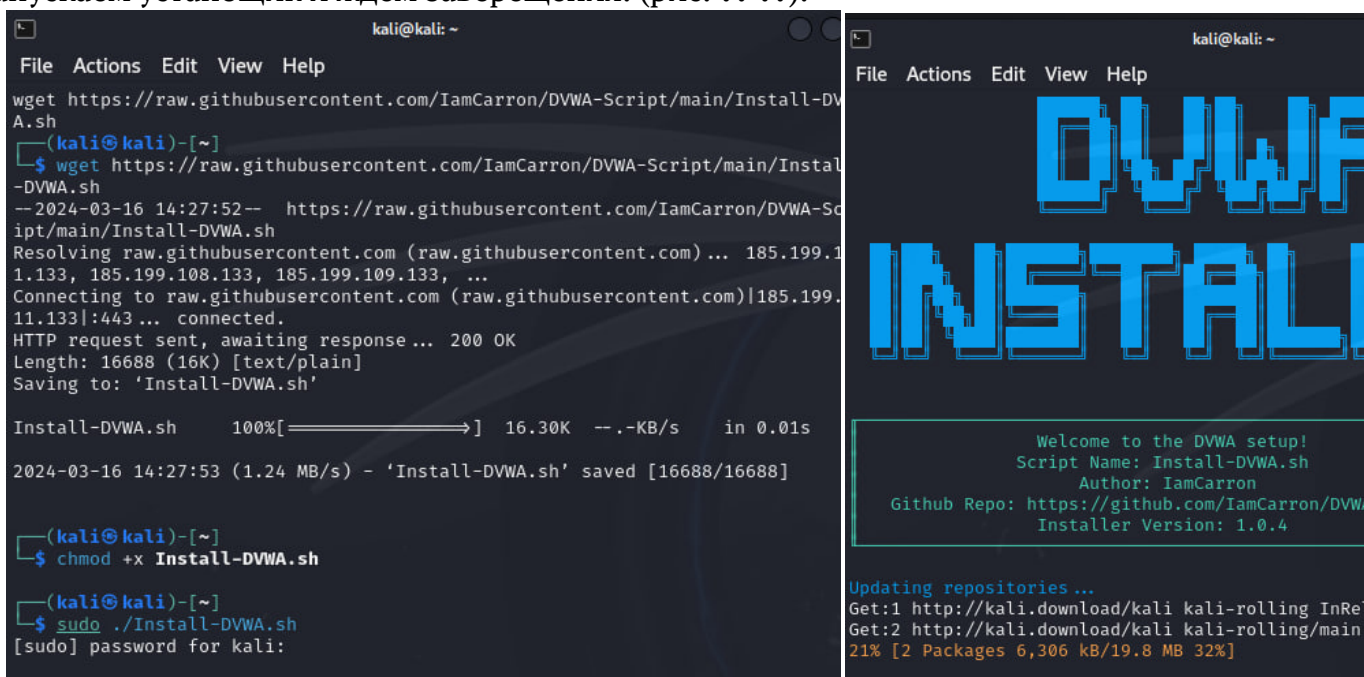
Некоторые из уязвимостей веб приложений, который содержит DVWA: - Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. - Исполнение (внедрение) команд: Выполнение команд уровня операционной 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. - Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер. - Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS. - Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: - Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. - Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях. - Средний — этот уровень без-

опасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу. - Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

3 Выполнение лабораторной работы

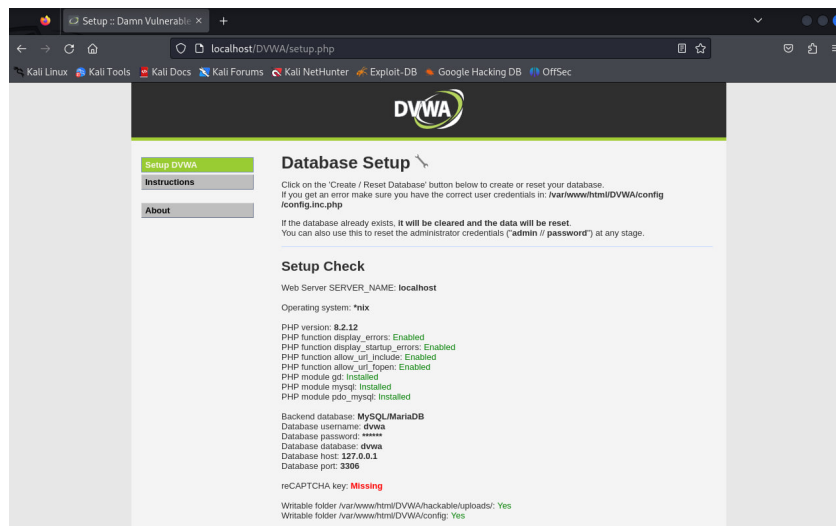
Скачиваем установщик командой: `wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh` Выдаём верные права: `chmod +x Install-DVWA.sh`
Запускаем установщик и ждём завершения. (рис. ?? ??).



```
kali@kali: ~  
File Actions Edit View Help  
wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh  
(kali@kali)-[~]  
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh  
--2024-03-16 14:27:52-- https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh  
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.111.133, 185.199.108.133, 185.199.109.133, ...  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443 ... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: 16688 (16K) [text/plain]  
Saving to: 'Install-DVWA.sh'  
  
Install-DVWA.sh 100%[=====>] 16.30K --.-KB/s in 0.01s  
2024-03-16 14:27:53 (1.24 MB/s) - 'Install-DVWA.sh' saved [16688/16688]  
  
(kali@kali)-[~]  
$ chmod +x Install-DVWA.sh  
  
(kali@kali)-[~]  
$ sudo ./Install-DVWA.sh  
[sudo] password for kali:  
  
kali@kali: ~  
File Actions Edit View Help  
DVWA  
INSTALL  
  
Welcome to the DVWA setup!  
Script Name: Install-DVWA.sh  
Author: IamCarron  
Github Repo: https://github.com/IamCarron/DVWA-Script  
Installer Version: 1.0.4  
  
Updating repositories ...  
Get:1 http://kali.download/kali kali-rolling InRelease [4096 B]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [6306 B]  
21% [2 Packages 6,306 kB/19.8 MB 32%]
```

После этого на локальном хосту через браузер мы можем посмотреть кто рабо-

ту, протестировать функции.(рис. ??).



4 Выводы

В ходе выполнения работы мы разобрались, что такое DVWA и для чего он служит.