

Основы информационной безопасности

Индивидуальный проект. Этап №3. Использование Hydra

Нзита Диатезилуа Катенди

Содержание

Постановка задачи	4
Теоретические сведения	5
Выполнение лабораторной работы	7
Выводы	12
Список литературы	13

Список иллюстраций

1	Уровень защиты DVWA	7
2	Уязвимая форма для ввода пароля	8
3	Распаковка rockyou.txt.gz	9
4	файл rockyou.txt. с наиболее популярными паролями	9
5	Данные о запросе на вход	10
6	Запрос к Hydra	10
7	Проверка полученного пароля	11

Постановка задачи

Целью данной работы является использование Hydra для подбора пароля.

Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~@dvwa]. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

DVWA (Damn Vulnerable Web Application) — это приложение, предназначенное для практики работы с распространёнными веб-уязвимостями, предлагая пользователю интуитивно понятный интерфейс. Оно содержит как документированные, так и недокументированные уязвимости, позволяя исследовать безопасность веб-приложений на разных уровнях сложности.

Некоторые из уязвимостей, представленных в DVWA, включают:

- **Брутфорс:** Атака на формы входа, используемая для тестирования инструментов, позволяющих подбирать пароли, и демонстрации уязвимости слабых паролей.
- **Выполнение команд:** Позволяет злоумышленнику исполнять команды на уровне операционной системы.
- **Межсайтовая подделка запроса (CSRF):** Позволяет злоумышленнику изменять пароль администратора.
- **Внедрение файлов:** Злоумышленник может подключать удалённые или локальные файлы к веб-приложению.
- **SQL-внедрение:** Позволяет вставлять SQL-код в запросы через поля ввода,

включая слепое и основанное на ошибках внедрение.

- **Небезопасная выгрузка файлов:** Позволяет загружать вредоносные файлы на сервер.
- **Межсайтовый скриптинг (XSS):** Злоумышленник может внедрять свои скрипты в веб-приложение или базу данных, включая отражённые и сохранённые XSS.
- **Пасхальные яйца:** Раскрытие путей к файлам, обход аутентификации и другие уязвимости.

DVWA предлагает четыре уровня безопасности, которые меняют уязвимость веб-приложений:

- **Невозможный:** Уровень безопасности, при котором приложение защищено от всех уязвимостей. Используется для сравнения уязвимого кода с безопасным.
- **Высокий:** Уровень сложности с элементами более сложных и альтернативных плохих практик, который снижает возможности эксплуатации.
- **Средний:** Уровень, показывающий примеры плохих практик безопасности, где разработчик пытался обеспечить безопасность, но не смог.
- **Низкий:** Полностью уязвимый уровень, предназначенный для демонстрации плохих практик программирования и обучения базовым методам эксплуатации.

Выполнение лабораторной работы

Установим самый низкий уровень защиты DVWA (рис. @fig:001)



Рис. 1: Уровень защиты DVWA

Откроем страницу для проведения атаки brute force, которая представляет собой простейшую уязвимую форму с паролем (рис. @fig:002).

DVWA

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
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout

Vulnerability: Brute Force

Login

Username:

Password:

Username and/or password incorrect.

Alternative, the account has been locked because of too many failed logins.
If this is the case, **please try again in 15 minutes.**

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 2: Уязвимая форма для ввода пароля

В Kali лежит файл с наиболее популярными паролями, который мы распакуем(рис. @fig:003).


```
(dknzita@dknzita)-[/usr/share/wordlists]
$ cd /usr/share/wordlists

(dknzita@dknzita)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst   nmap.lst   wfuzz
dirb       fasttrack.txt  legion    rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi   metasploit sqlmap.txt

(dknzita@dknzita)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for dknzita:
gzip: rockyou.txt.gz: No such file or directory

(dknzita@dknzita)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz

(dknzita@dknzita)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst   nmap.lst   wfuzz
dirb       fasttrack.txt  legion    rockyou.txt  wifite.txt
dirbuster  fern-wifi   metasploit sqlmap.txt
```

Рис. 3: Распаковка rockyou.txt.gz

Можно увидеть, что уже в начале есть пароль, который установлен по умолчанию для нашего аккаунта(рис. @fig:004, @fig:005).

```
(dknzita@dknzita)-[/usr/share/wordlists]
$ head -12 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel

(dknzita@dknzita)-[/usr/share/wordlists]
$
```

Рис. 4: файл rockyou.txt. с наиболее популярными паролями

Рассмотрим данные о запросе на вход(рис. @fig:005).

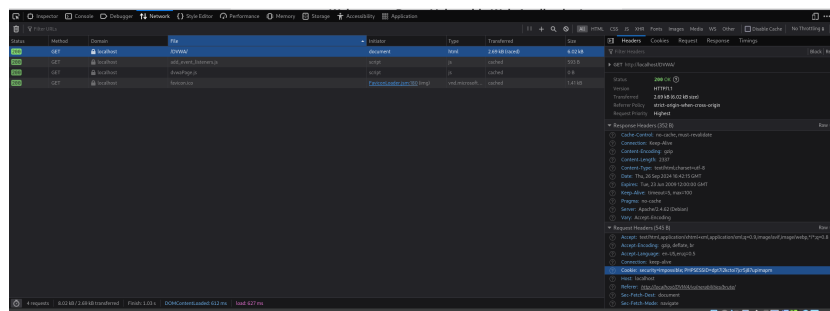


Рис. 5: Данные о запросе на вход

Исходные данные:

- IP сервера 127.0.0.1(localhost);
- Сервис http на стандартном 80 порту;
- Для авторизации используется html форма, которая отправляет по адресу `http://localhost/DVWA/vulnerabilities/brute` методом GET запрос вида `username=admin&password=test_password`;
- В случае неудачной аутентификации пользователь наблюдает сообщение `Username and/or password incorrect`.

Запрос к Hydra будет выглядеть так(рис. @fig:006):

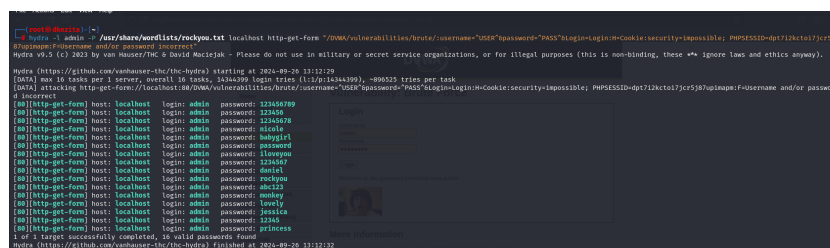



Рис. 6: Запрос к Hydra

В результате получим нужный пароль(рис. @fig:007):



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

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Vulnerability: Brute Force


Login

Username:

Password:

Login

Welcome to the password protected area admin



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 7: Проверка полученного пароля

Выводы

В результате выполнения работы была использована Hydra, для атаки типа brute force.

Список литературы

.....