

Индивидуальный проект

Этап 3. Использование Hydra

Морозов Михаил Евгеньевич

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	10
	Список литературы	11

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Теоретическое введение

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. [1]

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»

щему» 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. [2]

3 Выполнение лабораторной работы

Сменили уровень безопасности на Low.

Зашли в раздел brute force.

Посмотрим код этой страницы.

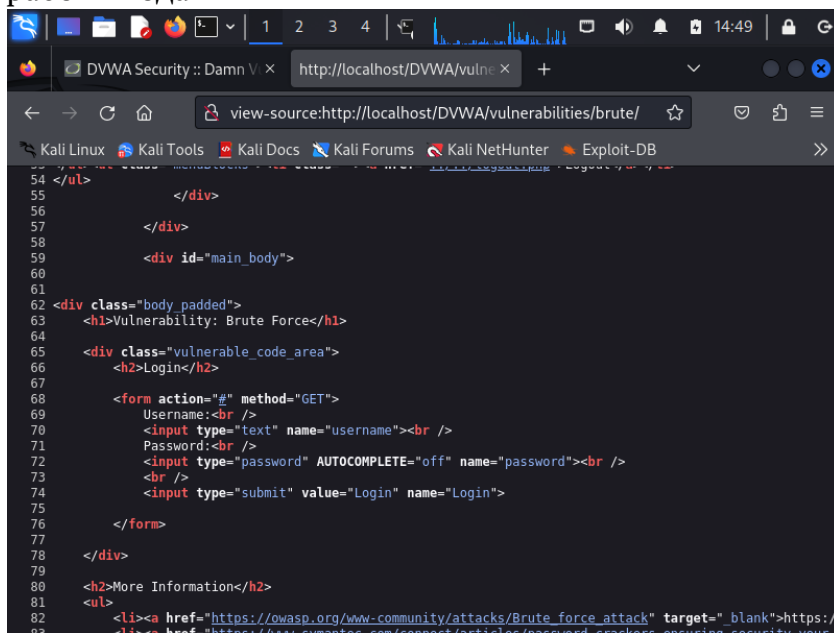
Посмотрим содержимое файла.

Найдем в куки PHPSESSID.

Запустим командой подбор паролей.

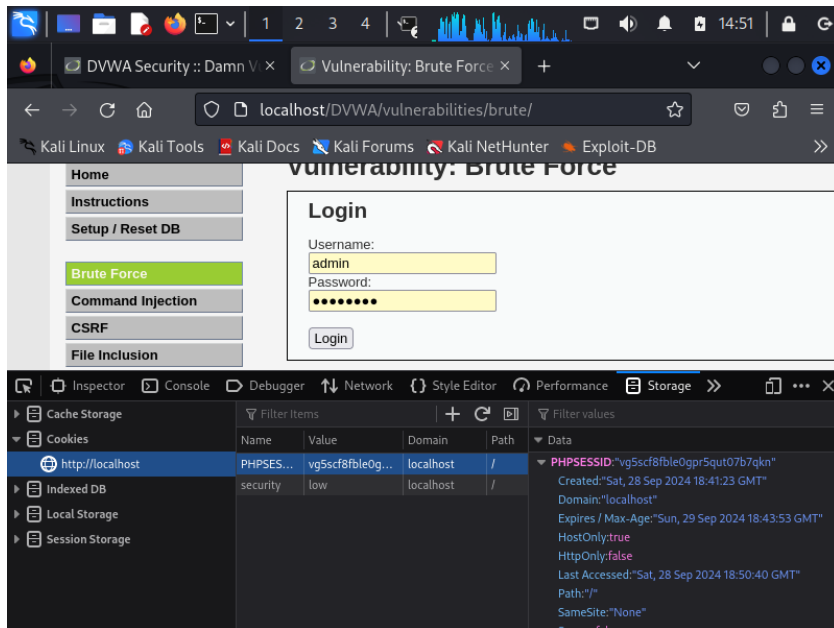
Проверим работу кода

Результат работы кода

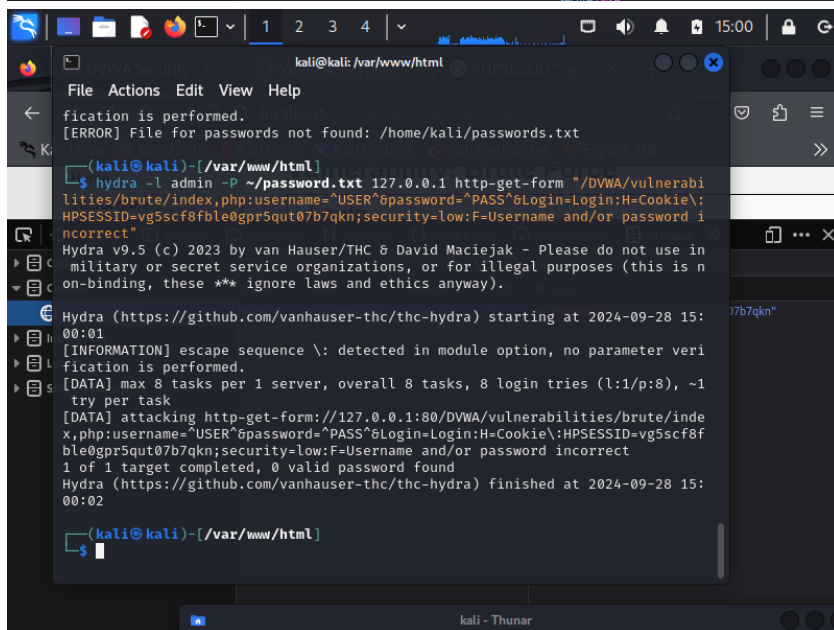


```
54 </ul>
55 </div>
56 </div>
57 </div>
58 <div id="main_body">
59 <div class="body_padded">
60 <h1>Vulnerability: Brute Force</h1>
61 <div class="vulnerable_code_area">
62 <h2>Login</h2>
63 <form action="#" method="GET">
64 Username:<br />
65 <input type="text" name="username"><br />
66 Password:<br />
67 <input type="password" AUTOCOMPLETE="off" name="password"><br />
68 <input type="submit" value="Login" name="Login">
69 </form>
70 </div>
71 <h2>More Information</h2>
72 <ul>
73 <li><a href="https://owasp.org/www-community/attacks/Brute_force_attack" target="blank">https://
74 <li><a href="https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-
75
```

1 (рис. ??)



2 (рис. ??)



3 (рис. ??)

4 Выводы

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

Список литературы

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