Индивидуальный проект. Этап 5

Использование Burp Suite. Уязвимости DVWA

Татьяна Александровна Буллер

Содержание

# 1 Цель работы

Знакомство со сканером уязвимостей набором инструментов Burp Suite и тестирование его возможностей на примере DVWA. Исследование прочих типов уязвимостей, для эксплуатации которых нет необходимости применять дополнительный инструментарий.

# 2 Ход работы

## 2.1 Command Execution

Command Execution - тип уязвимости, позволяющий злоумышленнику запускать на сервере произвольные команды. Чаще всего встречается в приложениях, где реализована и не профильтрована должным образом передача пользовательского ввода в командную строку сервера. Нас странице этой уязвимости в DVWA видим форму, которая позволяет осуществить команду ping.

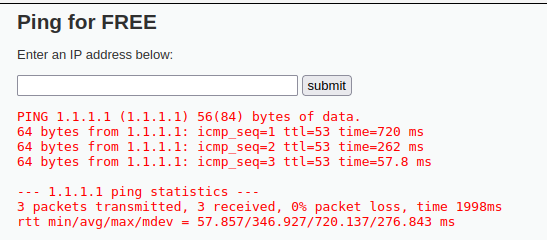


Рис. 1: ping

Для эксплуатации данной уязвимости нам необходимо объеденить ввод для команды ping со следующей командой, которую мы хотим подать на сервер, чтобы они запустились последовательно. Сделаем это, использовав знак разделения ;, и получим вывод, которого не должны видеть по изначальной логике приложения.

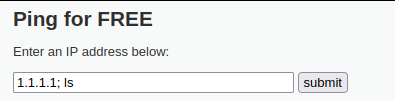


Рис. 2: Две команды

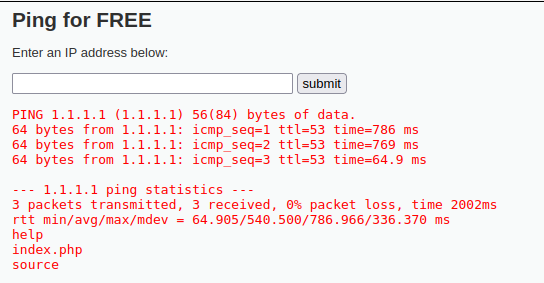


Рис. 3: Вывод двух команд

## 2.2 Cross Site Request Forgery (CSRF)

Cross Site Request Forgery (CSRF) - уязвимость, позволяющая злоумышленнику подделывать запросы, отправляемые на сайт, через свои домены. На странице этой уязвимости видим форму замены пароля.



Рис. 4: Страница CSRF

Открыв код страницы сочетанием клавиш Ctrl+U видим html-код этой формы. Это все, что нам нужно для эксплуатации: мы можем создать аналогичную форму на локальном сервере, скопировав код и подменив файл form action на адрес страницы, которой хотим подделать запрос.

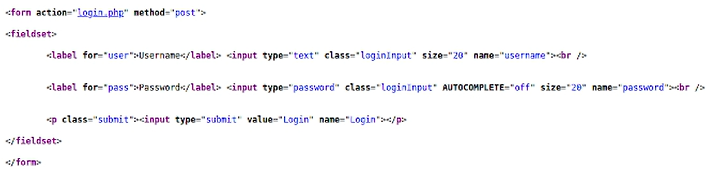


Рис. 5: Код страницы

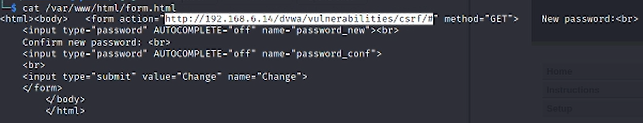


Рис. 6: Подделанная форма

Открыв файл подделанной формы на локальном сервере, введем новый пароль и нажмем кнопку “заменить”. После этого нас перенаправит на страницу уязвимости, которую мы рассматривали ранее, где будет сообщено, что пароль успешно изменен. При попытке зайти со старым паролем, действительно, логин провалится, тогда как новый пароль сработает.

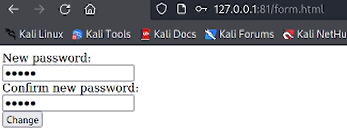


Рис. 7: Смена пароля

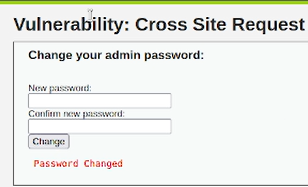


Рис. 8: Редирект на уязвимую страницу

## 2.3 File Inclusion (LFI) и Burp Suite

File Inclusion - уязвимость небезопасного включения файлов с сервера. Так, на странице этой уязвимости в DVWA мы можем видеть, что страница в параметре page подключает файл include.php. Можно предположить, что мы можем подключить и какой-то другой файл. Возможно, даже тот, который находится вне данной директории. Как раз для этого используем Burp Suite.

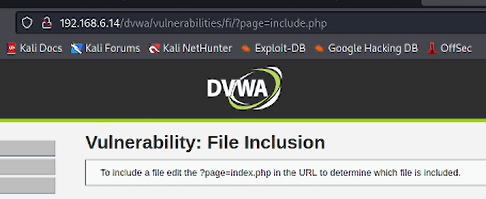


Рис. 9: Страница LFI

Для работы с Burp Suite было использовано расширение FoxyProxy. Прокси настроен на порт 8080 на локалхост. Это позволит Burp Suite перехватывать отправляемые запросы.

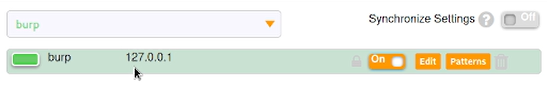


Рис. 10: Прокси

Включив прокси, запустив перехват трафика в Burp и перезагрузив страницу, получим перехваченный GET-запрос к ней. Видим здесь интересующий нас параметр: имя подключаемого файла. Далее можно пойти двумя путями. Либо перебирать варианты и отправлять запросы вручную через Repeater, либо составить (или раздобыть) список полезных нагрузок и автоматизировать процесс через Intruder. Список я дам. Поэтому выбираю второй вариант.



Рис. 11: GET-запрос с выделенным местом для вставки пэйлоада

Тип атаки, который будем проводить в данном (и всех последующих) случаях - Sniper. Эта атака использует один набор полезной нагрузки и подставляет его во все выделенные места. Список нагрузок возьму из стандартных словарей Kali для фаззинговой утилиты wfuzz.

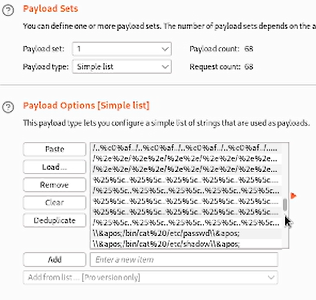


Рис. 12: Полезные нагрузки

Отсортировав ответы по длине, видим, что нам удалось подключить файл /etc/passwd.

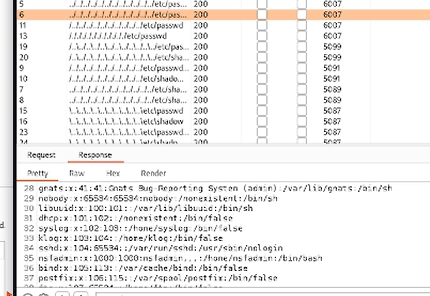


Рис. 13: Результат атаки

## 2.4 SQL Injection и Blind SQL Injection

SQL - язык, используемый для написания баз данных. В случае, когда пользовательский ввод фильтруется недостаточно, пользователь может передавать команды базе данных и получать содержимое, которое он видеть не должен. Для атаки используем тот же режим Sniper в Intruder, словарь - словарь SQL-инъекций для wfuzz.

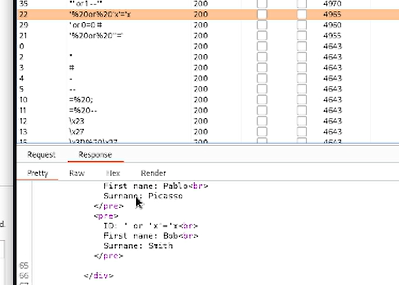


Рис. 14: Результат атаки SQLi

Особенность Blind SQLi в том, что, в отличие от обычного случая, база данных не дает никакого ответа об ошибках, на которые можно было бы ориетироваться. Так, если до этого мы встречали ответы сервера абсолютно крохотной длины (460), содержащие только сообщения об ошибках, теперь все неудачные атаки дают ответ длины 4671 и на них сложно ориентироваться, пытаясь составить правильный запрос к базе.

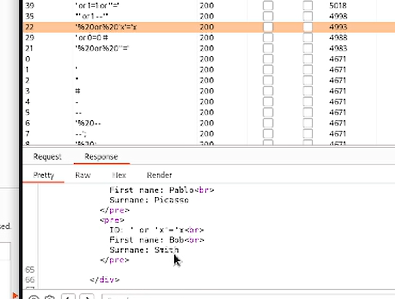


Рис. 15: Результат атаки Blind SQLi

## 2.5 File Upload

File Upload - уязвимость загрузки и исполнения произвольных пользовательских файлов на сервере. В самом простейшем ее варианте, который рассмотрим здесь, файлы, загружаемые пользователем, не проверяются вообще никак. В других случаях страницы также могут быть уязвимы к подмене MIME-type в запросе или двойным расширениям. Так, отправляя php файл, я могу перехватить запрос и заменить в теле Content-Type: application/php на image/jpeg, или отправить файл .jpeg.php, что можно так же реализовать через Burp Proxy. Для данного примера был использован реверс-шелл pentestmonkey, по умолчанию включенный в Kali Linux.



Рис. 16: php-reverse-shell.php

{#fig:017 width=70%

Загрузив этот файл на уязвимую страницу, открываем netcat на прослушивание порта 1234, который оставили для подключения в шелле.

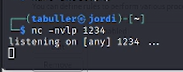


Рис. 17: netcat

После того, как мы попытаемся перейти на страницу, куда загружен этот файл, скрипт запустится, и netcat получит подключение от сервера. Теперь мы можем разбирать машину изнутри.

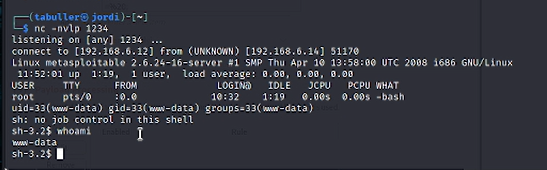


Рис. 18: Работа reverse shell

# 3 Выводы

Была освоена работа с набором инструментов Burp Suite и протестированы его возможности на примере DVWA. Были исследованы прочие типы уязвимостей (CSRF, Commang injection), для эксплуатации которых нет необходимости применять дополнительный инструментарий.