# Выполнение практики

Для выполнения задания практики было использовано программное обеспечение Burp Suite для сканирования web-приложения (перебора логина и пароля).

Burp Suite включает в себя следующие утилиты (Рисунок 1):

* Proxy – прокси сервер, перехватывающий сообщения проходящие по протоколу HTTP(S) в режиме man-in-the-middle. Находясь между браузером и целевым веб-приложением, он позволит вам перехватывать, изучать и изменять трафик идущий в обоих направлениях.
* Spider – веб-паук, позволяющий вам в автоматическом режиме собирать информацию о содержимом и функционале приложения.
* Scanner – мощная утилита для автоматического раскрытия уязвимостей в веб-приложениях.
* Intruder – максимально гибкая в настройках утилита, позволяющая в автоматическом режиме производить атаки различного вида. Например, перебор идентификаторов, сбор важной информации, фаззинг и прочее.
* Repeater – инструмент для ручного изменения и повторной отсылки отдельных HTTP-запросов, а также для анализа ответов приложения.
* Sequencer – Утилита для анализа качества генерации случайных данных приложения (например идентификаторов сессий) на возможность предсказания их алгоритма.
* Decoder – утилита для ручного или автоматического (де)кодирования данных приложения.
* Comparer – инструмент для поиска визуальных различий между двумя вариациями данных.
* Extender – инструмент для добавления расширений в BurpSuite



Рисунок 1 – Циркуляция потоков данных

# Burp Intruder

Burp Intruder – это утилита для автоматизированного проведения атак на веб-приложения.

Можно сделать с использованием любимого браузера (Chrome, Mozilla, Opera) и Burp Proxy для того, чтобы осуществлять перехват и просмотр запросов, и ответов, генерируемых приложением.

Burp Intruder обладает очень гибкой системой настроек, благодаря чему может быть использован для автоматизации множества видов атак. Можно использовать его и для выполнения иных задач, например, подбора пользовательских идентификаторов, сбора важной информации или фаззинга (техники тестирования программного обеспечения). Типы возможных атак зависят от особенностей конкретного приложения и могут включать: проверку на наличие SQL-инъекций, XSS, переполнение буфера, обход директории; bruteforce-атаки по различным схемам аутентификации, перебор значений, манипуляции с содержимым параметров; поиск скрытого содержимого и функционала, вычисление идентификаторов сессий и их перехвата, сбор данных, организация параллельных атак, реализация DoS-атак связанных с особенностями целевого приложения.

Burp Intruder содержит множество заранее подобранных списков с особо сформированными данными (строками, позволяющими обнаружить наличие уязвимостей). Кроме того, он содержит большое количество утилит для динамической генерации векторов атак, подходящих под конкретное приложение. Также в него могут быть загружены дополнительные списки, которые будут объединены с тем, что есть на данный момент (например, списки с именами пользователей или выражения для фаззинг-атак ранее неизвестного вида).

Основу работы каждой атаки составляет отсылка определённого количества HTTP-запросов. Их содержимое генерируется на основе первоначального запроса, обнаруженного ранее. BI (Burp Intruder) изменяет основной запрос несколькими способами, для того, чтоб попытаться обнаружить как можно большее количество уязвимостей. Это делается по средствам замены частей основного запроса различными опасными выражениями. Процесс выполнения и интервал проведения каждой атаки может быть настроен отдельно. Кроме того, запросы могут формироваться таким образом, чтобы не попасть под внимание IDS (англ. **I**ntrusion **D**etection **S**ystem, система обнаружения вторжений). Режим отказа в обслуживании может использоваться для бомбардировки сервера запросами с игнорированием содержимого его ответов.

Во время выполнения атаки будет показана таблица с детальным описанием всего происходящего. В ней будут отображаться ответы сервера, полученные на каждый запрос. Результаты будут содержать всю релевантную информацию с помощью которой можно будет с высокой точностью сказать о том, что данный запрос может быть интересен. В дополнение к стандартным результатам, являющимся общими для каждого вида атак, можно проводить множество гибко настраиваемых тестов в режиме реального времени в отношении получаемых результатов. Например, BI может быть настроен таким образом, чтоб извлекать определённую информацию из HTML-страниц (например, персональные данные на странице с профилем пользователя), и записывать её вместе с основным результатом. Все результаты могут быть экспортированы для дальнейшего изучения или использованы в качестве входных данных для работы других утилит Burp Suite.

# **Настройка Burp Intruder**

Панель управления Burp Intruder позволяет настраивать одновременно одну или более атак в их вкладках. Можно создавать новые вкладки или переименовывать существующие с использованием меню Intruder.

Настройка каждой атаки состоит из работы с несколькими вкладками: (target, positions, payloads, options). Самый простой вариант создания новой атаки состоит в том, чтобы найти необходимый базовый запрос в результатах одной из Burp-утилит (например, в истории Burp Proxy или карты сайта) и в контекстном меню выбрать "send to intruder". Это действие приведёт к автоматическому заполнению вкладок "target" и "position". Можно использовать меню "Intruder" для контроля над тем, как будут заполнятся вкладки "payloads" и "options" при создании новой атаки. Можно выбрать использование конфигурации атаки по умолчанию, скопировать конфигурацию с первой вкладки или с вкладки последней проведённой атаки. К примеру, можно создать стандартную конфигурацию атаки на самой первой вкладке (например, фаззинг найденных параметров и сбор сообщений об ошибках) и автоматически распространять её на каждую новую атаку посылаемую в Burp Intruder. Кроме того, можно копировать настройки между двумя любыми вкладками, или сохранять и загружать их, используя меню Intruder.

# Вкладка Target

Она используется для указания данных целевого сервера:



Рисунок 2 – Вкладка Intruder

Поле (Рисунок 2) "host" используется для указания IP-адреса или имени хоста целевого сервера. Поле "port" используется для установки номера порта HTTP(S)-сервиса. Галочка "use SSL" позволяет использовать для атаки Secure Sockets Layer-соединения.

# Вкладка Positions

Данная вкладка используется для создания шаблона для каждого HTTP-запроса, генерируемого в ходе атаки (Рисунок 3):



Рисунок 3 – Вкладка Positions

Основной текстовый редактор используется для указания содержимого базового запроса. Также в нём можно указать место, куда будут помещаться опасные данные. Кроме того, тут есть контекстное меню, предоставляющее доступ ко всем основным функциям.

Простейшим путём создания шаблона для атаки является обнаружение интересующего запроса с помощью любой Burp-утилиты и клика по пункту "send to intruder" контекстного меню. Можно отправить запрос из любого места Burp Suite, где есть отображение HTTP-запросов или ответов, а также из истории Burp Proxy, дерева карты сайта или её таблицы, и из уже проводящей атаки BI (Рисунок 4):



Рисунок 4 – Вкладка Proxy

Позиции размещения опасных данных обозначаются парами символов §, которые ограждают текст, находящийся между ними. Когда специально сформированные данные помещаются внутрь текущего запроса, они заменяют собой всё, что находится между § (в т.ч. и эти символы). Если для текущего запроса не требуется вставка опасных данных, то § просто удаляются без внесения каких-либо изменений.

Когда отдает BI запрос из любой Burp-утилиты, он автоматически обозначает самые лучшие позиции вхождения опасных данных. Это параметры, находящиеся в теле запроса и в URL, а также cookies. Для большего удобства сами маркеры (§), и текст внутри них, специальным образом подсвечиваются. В Intruder-меню указывают как именно должны вести себя опасные данные при вставке в обозначенные места – заменять имеющееся значение или добавляться к нему. Чуть выше редактора запроса отображается количество имеющихся позиций и размер текущего шаблона.

Используют кнопки на этой вкладке (Рис. 6.0.1) для контроля размещения позиций опасных данных:

1. add § – добавить одиночный маркер § в место нахождения курсора.
2. Clear § – удалить все маркеры либо из всего шаблона, либо из выделенной его части, если таковая имеется.
3. Auto § – при нажатии данной кнопки маркеры во всём шаблоне, или выделенной его части, расставляются автоматически. При этом все созданные до этого маркеры удаляются. Эта функция очень полезна в тех случаях, когда нужно обозначить все возможные позиции вхождения опасных данных для быстрой проверки на общие виды уязвимостей (например, такие как SQL-инъекции или XSS), в то время как их ручное указание больше подходит для более конкретных или сложных атак, когда уязвимое место уже обнаружено.
4. Refresh – обновить цветовую подсветку элементов в редакторе.
5. Clear – удалить все маркеры.

Механизм автоматического размещения маркеров умеет распознавать XML-данные. Некоторые приложения отсылают их в теле запроса, например, в таком виде:

POST /wp-login.php HTTP/1.1

Host: 192.168.217.130

User-agent: Mozilla/5.0 (X11; Linux x86\_64; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://192.168.217.130/wp-login.php

Content-Type: application/x-www-form-urlencoded

Content-Length: 104

Cookie: wordpress\_test\_cookie=§WP+Cookie+check§

Connection: close

Upgrade-Insecure-Requests: 1

Log=§admin§pwd=admin§wp-sumbit=§Log+In§&redirect\_to=§http%3A%2F%2F192.168.217.130%2Fwp-admin%2F§testcookie=§1§

Если использовать авто-размещение маркеров на сообщении целиком, то Intruder пометит весь XML-блок как одну цельную позицию вхождения опасных данных. Если же вручную выделить XML-блок, то функция авто-размещения отметит каждый XML-параметр отдельно.

Выпадающее меню «attack type» используется для установки ключевых аспектов поведения BI. Значение, находящееся в нём, определяет метод размещения опасных данных в обозначенных позициях каждого запроса.

Четыре возможных вида атак описываются ниже:

1. sniper – при этом виде атак используется отдельный набор опасных данных. BI начинает по очереди брать все обозначенные маркерами позиции в запросе и помещать отдельно в каждую специально сформированные данные. Остальные позиции не обрабатываются – их маркеры удаляются из тела запроса, а содержимое остаётся нетронутым. Данный тип атак полезен при индивидуальном тестировании полей на наличие общих уязвимостей (таких как XSS). Итоговое количество отправляемых запросов здесь может быть посчитано путём умножения количества позиций для опасных данных на количество вариантов этих данных в используемом наборе.
2. battering ram – здесь используется отдельный набор опасных данных. Перебирая записи в нём, BI помещает проверочный текст сразу во все позиции, отмеченные маркерами. Это может пригодиться, когда для осуществления атаки необходимо помещать одни и те же данные сразу во множество мест. Например, имя пользователя в Cookie и в тело запроса. Итоговое количество запросов равняется количеству записей в наборе проверочных данных.
3. pitchfork – этот вид атак использует несколько наборов проверочных данных. Таким образом, для каждого отрезка, обозначенного маркерами (максимум 8) устанавливаются свои специально сформированные строки. BI перебирает наборы тестовых строк одновременно и помещает данные из них в каждый обозначенный участок запроса. Например, при первом запросе первая строка из первого проверочного набора будет помещена на первое место, обозначенное маркерами. А первая строка из второго набора поместится на вторую позицию. При формировании второго запроса на первое место будет помещена вторая строка из первого набора, а на второе – вторая строка из второго набора, и так далее. Такой вид атак может пригодиться в ситуациях, когда приложению нужно отсылать всё время разные, но каким-то образом взаимосвязанные данные. Например, если необходимо отправлять имя пользователя в одном поле и его ID в другом. Общее количество запросов, совершаемых при проведении атак такого рода, измеряется количеством строк в наименьшем используемом проверочном наборе.
4. cluster bomb – данный вид атак использует несколько проверочных наборов. Для каждого отрезка, обозначенного маркерами (максимум 8) устанавливаются свои специально сформированные строки. При проведении атаки BI проверяет все возможные комбинации выражений из всех тестовых наборов. То есть если у вас есть 2 проверочных набора, то при первом запросе Intruder поместит на первую позицию первую строку из первого набора, на вторую первую строку из второго. При втором запросе на первом месте останется первая строка первого набора, а на вторую будет помещена вторая строка второго набора. Потом третья, и так далее. Данный вид атак может быть полезен в ситуациях, когда требуется помещать в запрос разные, никак не связанные между собой данные. Например, имя пользователя в один параметр и неизвестный пароль в другой. Общее количество запросов, генерируемых при реализации данной атаки, может быть большим.

# Вкладка Payloads

Данная вкладка (Рисунок 5) используется для настройки одного или более набора проверочных данных. Если выполняется работа с атаками типа «pitchfork» или «cluster bomb», то указывают несколько наборов проверочных данных, по одному на каждую позицию, обозначенную маркерами в теле запроса (максимум 8). Для этого используют выпадающие списки «payload set».

Для каждого проверочного набора указывают вид проверочных данных (preset list, character blocks, brute forcer и т.д.), а также дополнительную его обработку, которой будут подвергаться все значения из набора. Большое количество таких видов уже встроено в Burp Intruder. Некоторые из них очень гибко настраиваемы и могут быть полезны при проведении широкого диапазона атак.



Рисунок 5 – Вкладка Payloads

# Вкладка Options

Данная вкладка (Рисунок 6) содержит различные опции, позволяющие контролировать процесс проведения отдельных атак.

Эти опции используются для управления HTTP-заголовками в генерируемых запросах.



Рисунок 6 – Вкладка Options

Если отметить поле «update Content-Length header», то Burp Intruder будет добавлять или изменять HTTP-заголовок «Content-Length» в каждом генерируемом запросе, в соответствии с длиной данных в их телах. Эта возможность является необходимой при проведении атак, основанных на помещении в тело запросов специально сформированных данных постоянно меняющейся длины. Спецификация HTTP и большинство веб-серверов требуют, чтобы в данном заголовке использовалось корректное значение. Если же его нет, целевой сервер может вернуть ошибку, не до конца обработать запрос, или же станет ожидать от клиента передачи неопределённо большого количества данных.

Если отмечено поле «set Connection: close», то Burp Intruder будет добавлять или изменять соответствующим образом заголовок «Connection» в каждом формируемом запросе. В некоторых случаях (когда сервер не возвращает верное значение в заголовках Content-Length или Transfer-Encoding), эта опция может позволить ускорить процесс проведения атак.

Опция «concurrent request threads» позволяет определять, будут ли запросы при проведении атаки отсылаться синхронно в одном потоке, либо же для работы будут использованы несколько потоков. Использование последнего варианта пригодится при проведении атак, в которых главным является временный фактор. Например, задержка между принятием запроса и выдачей ответа. Кроме того, данная возможность может быть использована при поиске уязвимостей, связанных с обработкой приложением множества запросов, полученных за короткий промежуток времени.

Следующие 2 опции определяют, как много раз Burp будет повторять запрос при возникновении ошибки работы с сетью (отказ в соединении, таймаут), и сколько времени он будет ожидать между попытками.

Опция «throttle» позволяет установить временную задержку между отправкой запросов. Нефиксированная задержка может служить простым (хотя и малоэффективным) способом сокрытия каких-либо иных действий или же использоваться для периодического выполнения простейших запросов, направленных, например, на сохранение активности идентификатора сессии. Изменяемое время задержки может пригодиться, например, для определения времени жизни сессии.

Опция «start» позволяет определить, будет ли атака начата сразу после её запуска, или же это произойдёт через какое-то определённое время, или BI будет ожидать команду «resume». Эта функция может быть использована в случаях, когда необходимо запустить атаку в заранее известное время, или же сохранить её на будущее.

Настройки хранения определяют, как в процессе атаки будет сохраняться содержимое отдельных запросов и ответов. Запись данного материала происходит во временную директорию. Эта функция позволяет полностью наблюдать за процессом атаки, повторять отдельные запросы, если это необходимо и отправлять их в другие Burp-утилиты.

Если отмечено поле «make unmodified baseline request», то в дополнение к основной настройке атаки Burp будет отправлять запрос-шаблон с начальными значениями изменяемых параметров. Он будет показан в таблице результатов под номером 0.

Если включить «DoS mode», то атака будет брать текущий запрос и слать его серверу, не дожидаясь ответа на предыдущий. Как только запрос будет полностью передан, BI сразу же закроет TCP-соединение. Данная функция может использоваться для обнаружения уязвимостей, приводящих к отказу в обслуживании на уровне приложения, что, в свою очередь, позволит выделить самые высоконагруженные задачи, выполняемые на сервере.

Опция «store full payloads» указывает Burp Intruder, что необходимо у каждого результата записывать специально-сформированные данные в полном объёме. Это «съест» дополнительный объём памяти, но позволит во время проведения атаки выполнять такие действия, как модификацию правил раздела «grep» или изменять шаблон основного запроса.

Настройки из раздела «grep» используются на шаблонном поиске данных в ответах сервера. Здесь есть три типа проверок:

* grep match – они (Рисунок 7) используются для проверки каждого ответа сервера на наличие в нём определённой фразы или на совпадение с простым регулярным выражением, составленном в стиле Perl. Для каждого отдельного выражения будет создана колонка в результирующей таблице, содержащая информацию о том, где было найдено совпадение. Стандартный набор выражений имеет очень широкий диапазон использования: при атаках, связанных с перебором пароля, для сканирования на выражения типа «password incorrect» или «login successful»; для поиска признаков SQL-инъекций – поиск выражений, содержащих «ODBC», «error» и т.д.

Если выражения используются для поиска совпадений, то они могут содержать символы новой строки.



Рисунок 7 – grep match

* grep extract – вкладка (Рисунок 8) используется для проверки всех получаемых ответов сервера на совпадение с указанными выражениями, а также, если необходимо, для немедленного извлечения совпадений (от найденного выражения до указанного символа или по указанную длину). Для каждого отдельного выражения в результирующей таблице будет своя колонка, в которую будет помещён извлечённый с его помощью текст. Эта функция может быть использована для поиска страниц, содержащих чувствительную информацию, и автоматизированного её извлечения, если в этом возникнет необходимость. Например, если получен доступ к странице управления пользовательскими аккаунтами, которая отображает данные того или иного пользователя в зависимости от переданного в URL ID, то можно запустить атаку, которая будет перебирать возможные ID и извлекать из полученных страниц логин и пароль каждого пользователя. Если совпадения с выражениями встречаются BI несколько раз подряд, то записано будет каждое из них. Это бывает полезно в ситуациях, когда важные данные содержатся, например, в нескольких строках в HTML-таблице, но не имеют какого-то определённого признака для точечного их извлечения.



Рисунок 8 – grep extract

* grep payloads – используется для проверки каждого ответа сервера на наличие в нём строк со специально-сформированными данными (Рисунок 9). Это может помочь при поиске XSS, и других инъективных уязвимостей, при наличии которых принимаемые от пользователя данные отображаются в ответе приложения. Если выбрана опция «match against pre-encoded payloads», то в ответах происходит поиск каждой тестовой строки в чистом виде, перед применением к ней доступных вариантов кодирования.



Рисунок 9 – grep payloads

Настройки переадресации позволяют контролировать поведение BI в случаях встречи с ответами, содержащими соответствующие коды (т.е. статус-коды 3хх и заголовок Location, содержащий новый URL) в процессе проведения атаки. Если Burp Intruder следует редиректам (автоматическая переадресация пользователей с одного URL-адреса на другой), то при их встрече он проследует по указанному в заголовке URL (максимальное количество переходов подряд – 10) и запишет результат только конечного адреса. В отдельной колонке, в таблице результатов, запросы с переадресацией будут особым образом отмечены. Также можно настроить BI на следование переадресациям только в области исследуемого сайта (т.е. по адресам с тем же протоколом, хостом и портом), внутри границ работы (Вкладка Target => Scope), или на полное их игнорирование.

Включение следования редиректам может пригодиться в том случае, когда приложение, принимая какие-нибудь данные, возвращает ответ с кодом 3хх, перебрасывая клиента на страницу с интересной информацией об обработке его запроса. Например, при фаззинге параметров приложения оно может совершать переадресацию клиента на страницу с описанием ошибки, содержащую данные о природе возникшего сбоя, что поможет определить наличие той или иной уязвимости.

Если включена опция «process cookies in redirects», то любые cookies, передаваемые клиенту вместе с ответом с кодом 3хх, будут переданы целевой странице. Это может пригодиться в случаях, когда проводят подбор пароля, а скрипт авторизации перебрасывает вас на отдельную страницу с её результатами.

# Вкладка Results

Пример, приведённый ниже (Рисунок 10), показывает таблицу результатов атаки, производящей перебор содержимого на целевом веб-сайте.



Рисунок 10 – Результат атаки

Данная атака использует тип «sniper» для осуществления запросов к нескольким, наиболее часто встречающимся, именам веб-директорий. Для этого вида атак в таблице результатов по умолчанию отображается номер каждого запроса, позиция тестовой строки (если их более чем одна), саму проверочную строку, код HTTP-ответа полученный от сервера, зафиксировано или нет ошибки или таймаута, и длина ответа сервера. В дополнительных колонках могут быть отображены таймеры «received response» и «finished response» («начало передачи ответа» и «ответ передан» соответственно, всё в милисекундах – п.п.), а также полученные cookies. Различные опции, типа grep, добавляют в результат дополнительные колонки. Каждая колонка может быть скрыта или показана с помощью меню «view». Результаты могут быть отсортированы по содержимому любой колонки с помощью клика на соответствующем заголовке.

Ключевая часть эффективной интерпретации результатов атаки состоит в обнаружении интересных или успешных ответов сервера, и идентификации запросов, которые к ним привели. Интересные ответы, чаще всего, могут быть разделены на следующие группы:

* Различные статус-коды;
* Разная длина ответа;
* Присутствие или отсутствие определённого выражения;
* Возникновение ошибки или таймаута; или время начала или окончания генерации ответа.

При раскрытии контента на запрос существующего объекта сервер должен ответить кодом «200» с ответом изменяющейся длины. Когда запрос отправляется к несуществующему объекту, сервер может ответить кодом «404» или же с «200», но содержащем сообщение об ошибке фиксированной длины. В случае же с подбором пароля, неудачная попытка авторизации может привести к ответу с кодом «200», и генерации страницы, содержащей фразу «login failed». При успешной попытке сервер может ответить кодом «302», или «200» со словом «welcome» в теле ответа.

Burp Intruder предоставляет функционал для отсева страниц по вышеописанным признакам. Функция поиска текста поможет отмечать ответы, содержащие заданные ключевые слова, или извлекать интересную информацию из определённых частей страниц. В таблице результатов записи могут быть отсортированы кликом на заголовке колонки. [1][2]

# Список использованных источников

1. Burp Suite documentation [Электронный ресурс]. – Режим доступа: https://portswigger.net/burp/documentation/contents (Дата обращения: 02.08.2019).
2. Burp [Электронный ресурс]. – Режим доступа: http://itsecwiki.org/index.php/Burp (Дата обращения: 02.08.2019).