Burp

Открытые курсы по Burp от разработчиков.

Структура сканера

Процесс прохождения пакета и точки настройки

1. Входящий пакет попадает на proxy.
2. Происходит проверка совпадения со Scopes.
3. В случае совпадения отправляется в инструменты. Иначе отправляется обратно в Proxy.
4. Производится обработка, модификация пакета, далее отправляется обратно в Proxy
5. Пакет отправляется на выход в соответствии с правилами

Настройки

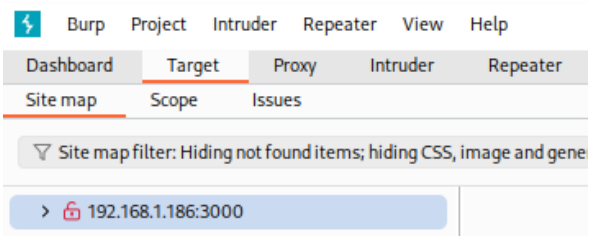
Проект Настройки бывают пользователя и проекта. Проект = данные + настройки. В Community Edition можно сохранить только настройки, данные придется получать каждый раз. Для каждого блока можно сохранить / загрузить настройки отдельно.

Scopes

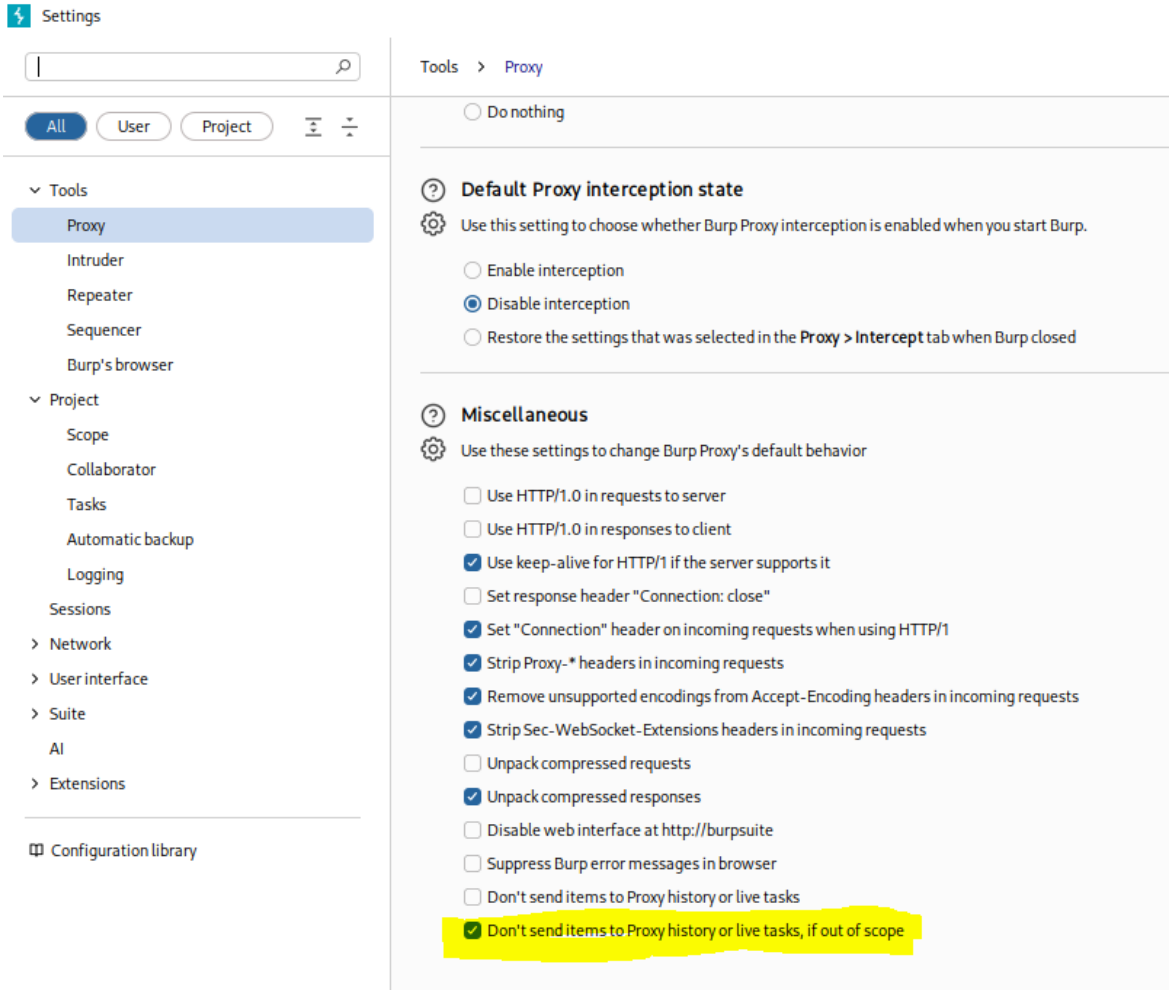
Site map. Агрегация данных о структуре сайта. Раздел Display - расширенные инструменты фильтрации отображения, есть регулярки. Можно подсветить нужные запросы (ПКМ - highlight) и/или добавить комментарии, затем по ним отфильтровать. После применения Scopes, исключенные пакеты отображаются в сером цвете.

В Pro версии можно найти отличия между двумя Site Map.

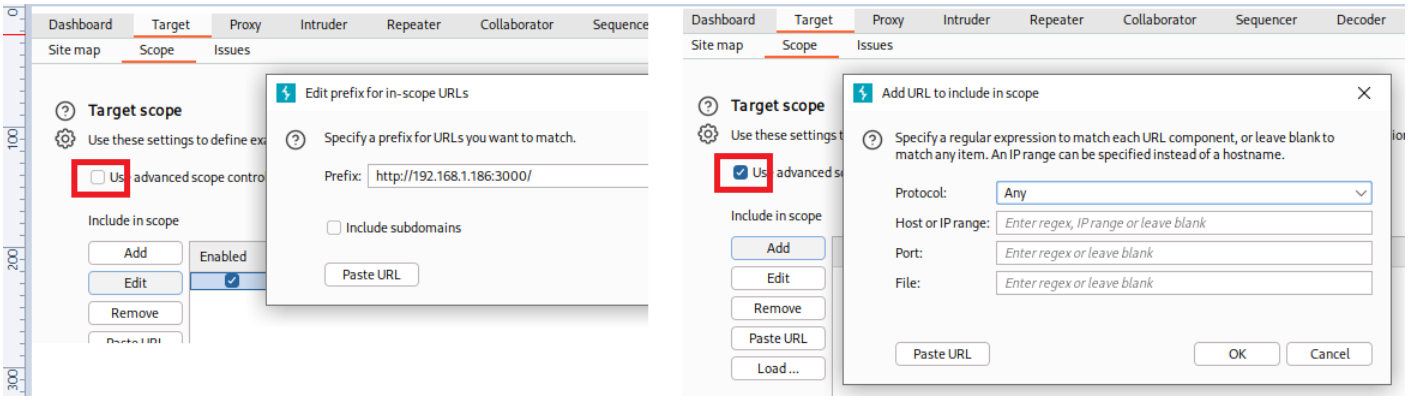
Scope. Ограничение области действия (домен, папка, файлы). Файл в терминах Burp - например для запроса http://one.ru/two/index.php будет index.php. Вариант настройки - запустить браузер и перейти в нем на нужный сайт. Все посещенные сайты в пределах текущей сессии отображаются в разделе Target-Site map



ПКМ-Add to scope По умолчанию для нового проекта все посещенные страницы попадают в историю и другие инструменты. После добавления в scope будет задан вопрос - сохранять ли запросы вне scope. Можно включить обратно.



Есть обычный и расширенный режимы настройки scope. В обычном настраивается только префикс, в расширенном можно ограничить протокол и использовать регулярные выражения для определения сайта, порта, файла.



Страница попадает/исключается при полном совпадении условий.

Можем загрузить список из текстового файла без указания протокола, например в виде

```
web.cyber-ed.ru
wiki.cyber-ed.ru
www.cyber-ed.ru
```

В других разделах настраиваются более точные параметры для фильтрации. В разделе Project - Scope есть настройка Drop all out-of-scope requests. Если предыдущие настройки определяли правила попадания страниц в историю, то это блокирует запросы вне scope.

Proxy

В этом разделе есть 3 блока настроек: входящие параметры, перехват трафика и исходящие параметры.

Отправка трафика на другой прокси настраивается в разделе Network-Connections Поддерживаются http и socks. Пример настройки socks для TOR сети.

По умолчанию принимает локальные входящие соединения на 8080 порту http. Можно настроить в режиме прокси для внешних соединений. В Settings - Tools - Proxy нужно добавить Proxy Listeners. Это можно использовать для проксирования внешнего трафика.

Обработка https запросов. Нужно чтобы burp распаковывал трафик, предоставлял возможности модификации и обратно запаковывал трафик.

- Перейти в браузере по адресу http://burp и скачать CA Certificate.
- Преобразовать сертификат

  ```
  openssl x509 -inform DER -in cacert.der -out cacert.pem
  ```

- Установить приложение и сертификат

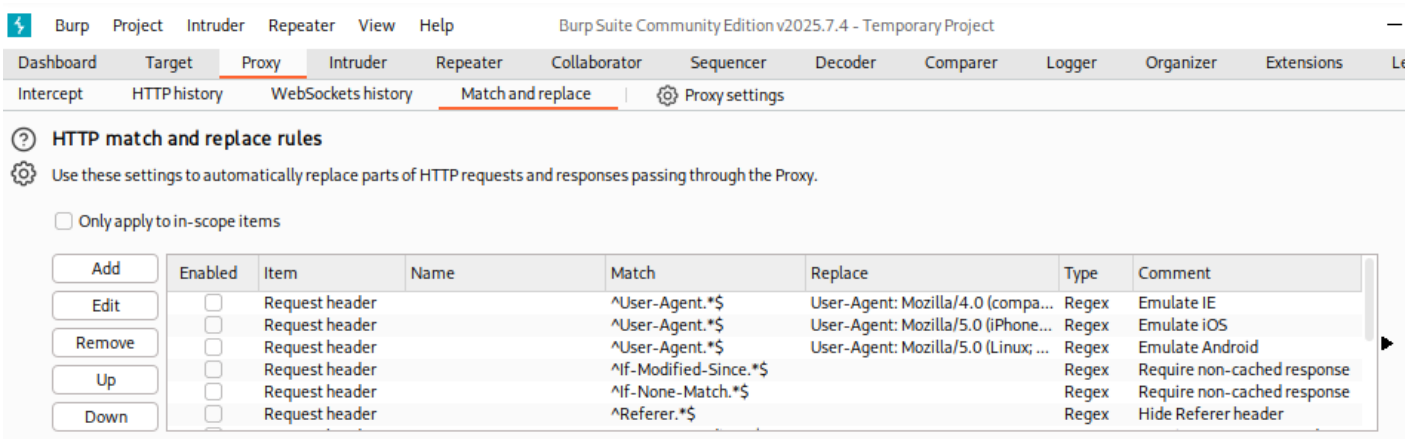
```
sudo apt install libnss3-tools
certutil -d sql:$HOME/.pki/nssdb -A -t "C,," -n "Burp Suite" -i cacert.pem
```

- Перезапустить браузер

Еще дополнительно можно настроить SSL pass-through в случае ошибки SSL

"Незаметный proxy" В случае отсутствия у клиента возможности работать через proxy. На клиенте в host файле меняем ссылку на нужный ресурс.

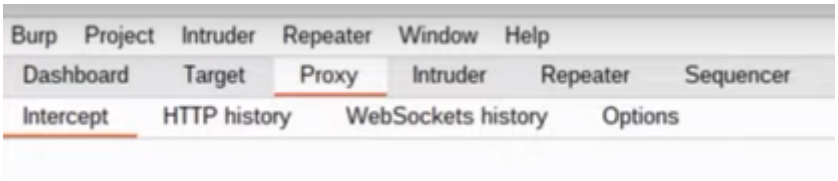
Поиск и замена данных



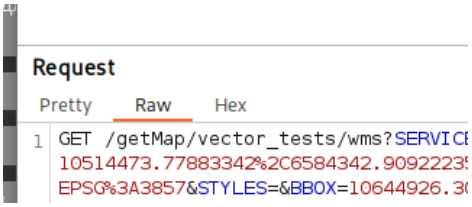
Позволяет модифицировать запрос / ответ перед отправкой / возвратом.

Перехват трафика

Перейти во вкладку Proxy->Intercept



Proxy используется в режимах выключенного и включенного перехвата. При включенном перехвате пакеты перед отправкой останавливаются и ожидают, в какой инструмент будут направлены. В разделе Raw можно редактировать данные.



Включить Intercept и открыть браузер

При включенном Intercept, при обращении к странице выводится запрос, и вариант - пропустить или блокировать. Доступна вкладка http history, где можно увидеть историю запросов и просмотреть запрос и ответ.

По умолчанию перехватываются запросы. Можно перехватывать ответы.

Инструменты.

Передача в инструмент копирует данные для анализа. Не отправляет данные дальше.

Repeater - ручной просмотр данных с возможностью редактирования

Intruder - для автоматизированной атаки. Работает по принципу подстановки элементов из словарей

Macros - можно выполнить предварительные действия

Decoder - модуль для кодирования JS скриптов для XSS атак. В связи с близостью XML и html разметки, это необходимо.

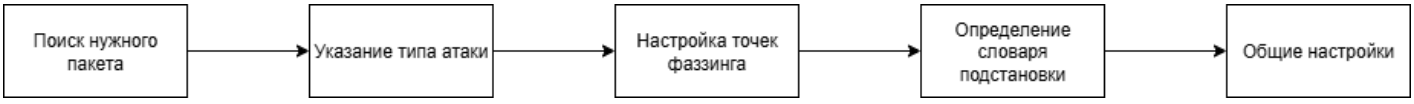
Repeater

Модификация http запросов

Перед отправкой, запрос можно модифицировать. Во вкладке http history будут запросы. правая кнопка - отправить в repeater позволяет скопировать запрос, модифицировать и отправить его.

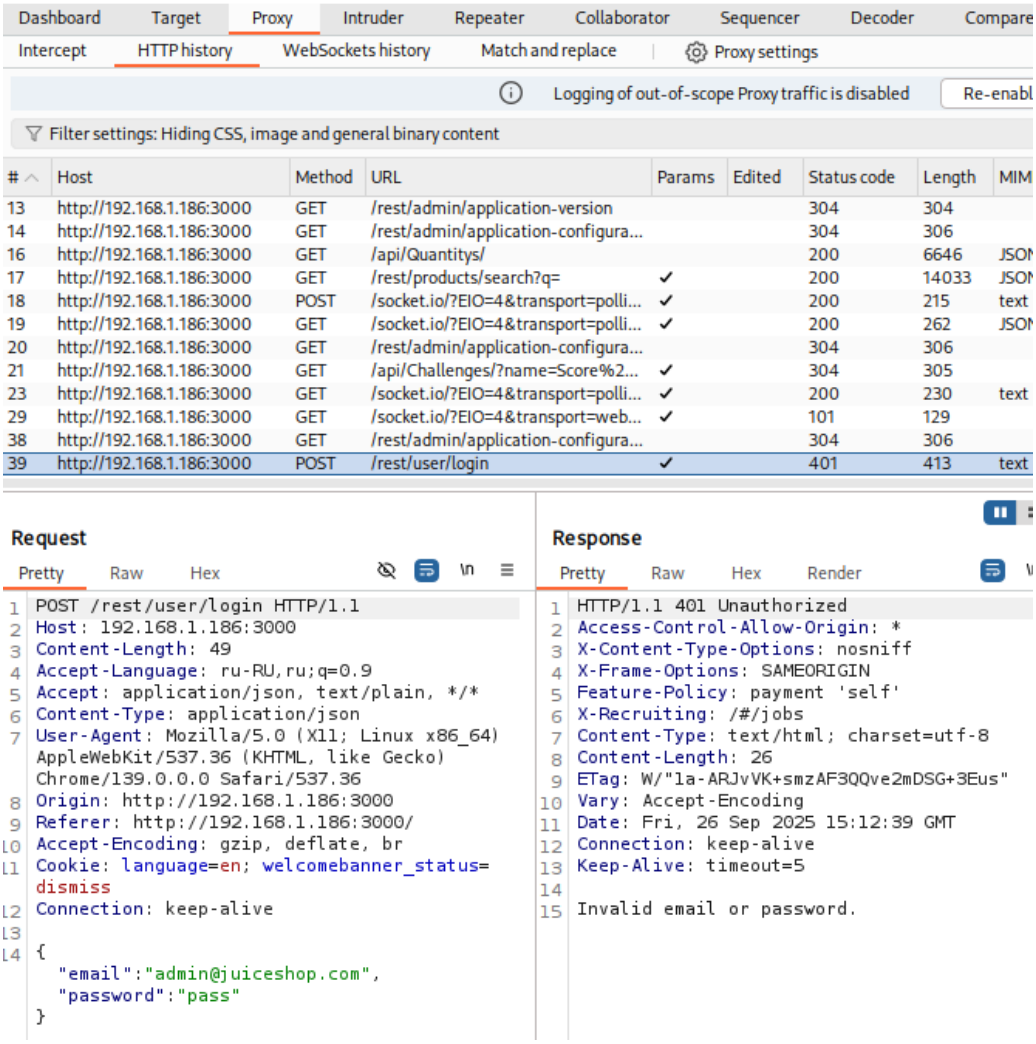
Intruder

Пример подбора пароля. Общая идея:

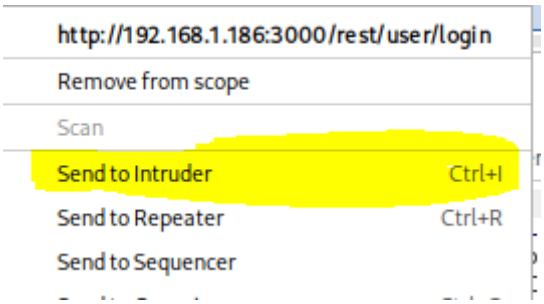


Поиск нужного пакета

Добавили в Scope адрес сайта, запустили Interception, перешли на страницу авторизации, отправили тестовые данные. В истории находим пакет, который отправлял запрос с логином и паролем:



Отправляем данный пакет в Intruder



Указание типа атаки

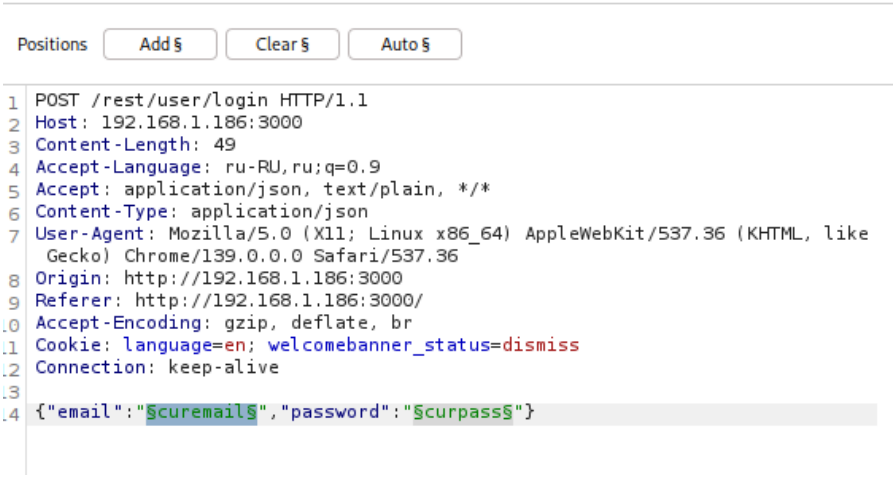
От типа атаки зависит дальнейшая настройка. Возможные атаки:

Sniper	Один словарь. Обычно используется с одной позицией. Когда позиций несколько - перебор такой: П.1-Эл.1 П.2-значение по умолчанию ... До конца списка. Затем П.1-значение по умолчанию П.2- Эл.1 ... до конца списка. Т е количество запросов будет Длина списка X Кол-во позиций. Значение по умолчанию - значение, прописанное между $ перед стартом атаки.

Battering Ram	Один словарь. Каждый элемент размещается на всех позициях. Кол-во запросов = Длина списка.
Pitchfork	Для каждой позиции свой словарь. Элементы подставляются по очереди из каждого словаря последовательно. Т е Позиция 1: Словарь 1 элемент 1 Позиция 2: Словарь 2 элемент 1. Позиция 1: Словарь 1 элемент 2 Позиция 2: Словарь 2 элемент 2
Cluster Bomb	Для каждой позиции свой словарь. Перебираются все комбинации элементов для каждого словаря.

Настройка точек фаззинга

Для настройки выделяем элемент и нажимаем Add. Вокруг появляется символ $.



Определение словаря подстановки

Дальше интереснее. Можно использовать возможности Burp. Тогда настройка делается через интерфейс. Словарь определяется в разделе Payload. Есть ряд типов словарей, Simple - это простой список. Можно проводить дополнительную модификацию элементов словаря.

Все методы в community версии медленно работают. Можно использовать fuff clusterbomb для ускорения отправки запросов.

Sequencer

Проверка степени случайности данных. Можно ли по некоторому количеству псевдослучайных данных сказать, насколько они случайны, или есть какая-то вычисляемая закономерность?

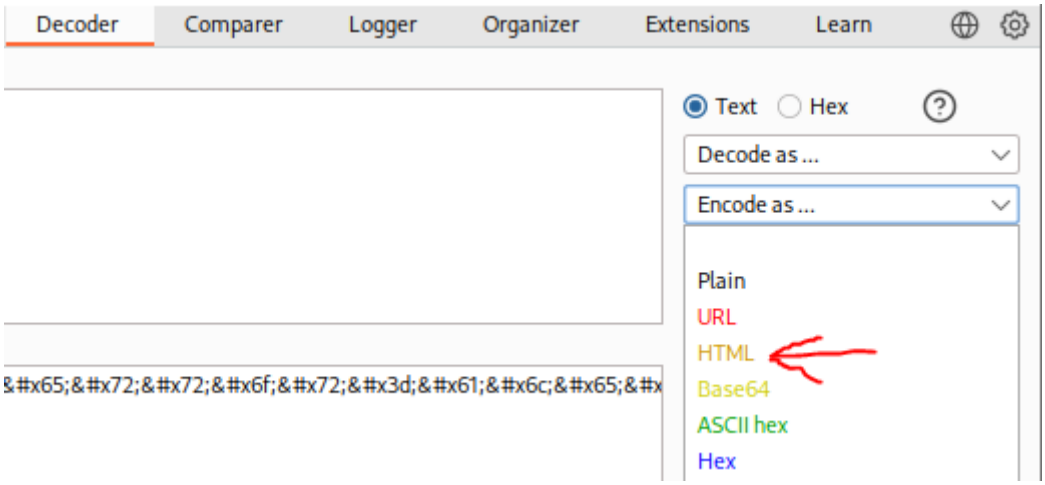
Decoder

Этот инструмент позволяет преобразовывать текст скрипта в закодированный текст, воспринимаемый системой как валидный текст для сохранения, но хранящий внутри

исполняемый код. Например для преобразования строки

```
"><img src=x onerror=alert(1) />
```

нужно зайти в Decoder и нажать кнопку Encode as -> HTML



В результате появится второе поле ввода, в котором будет результат.

Обратное преобразование - используя Decode as.

Comparer

Сравнение запросов или ответов.

Расширения

Есть магазин расширений и API для создания собственных (Java, Python, Ruby). Для Python и Ruby требуется настройка окружения Java-...

Revision #22
Created 1 September 2025 16:55:50 by Admin
Updated 29 September 2025 14:46:34 by Admin