

5 этап индивидуального проекта

Основы информационной безопасности

Волгин Иван Алексеевич

01 января 1970

Российский университет дружбы народов, Москва, Россия

Цель работы

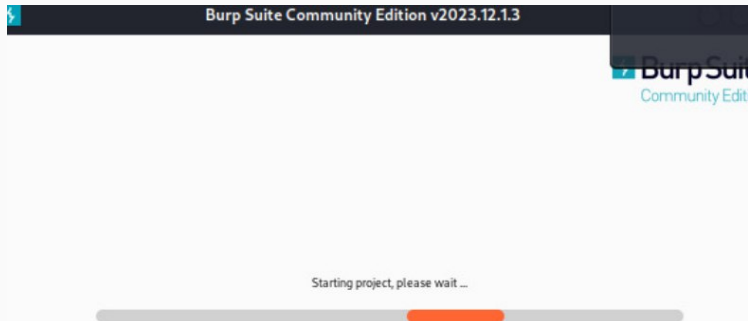
Ознакомление с Burp Suite.

Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения.

Выполнение лабораторной работы

1. С помощью `systemctl start apache2` и `systemctl start mysql` я запускаю локальный сервер, на котором после открою веб-приложение DVWA. Запускаю Burp Suite (рис. (fig:001?)).



2. Захожу в сетевые настройки браузера и меняю некоторые из них (рис. (fig:002?)).

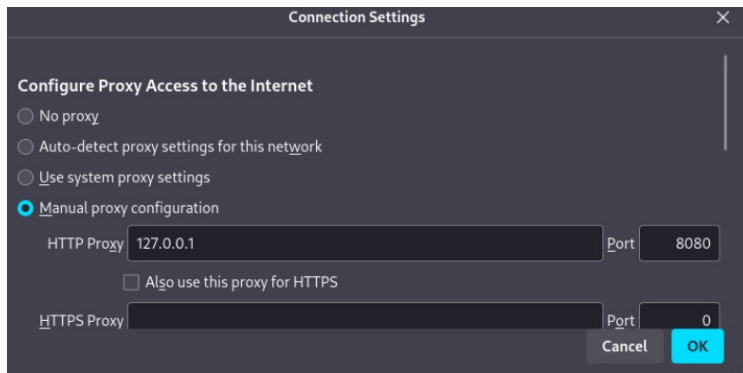
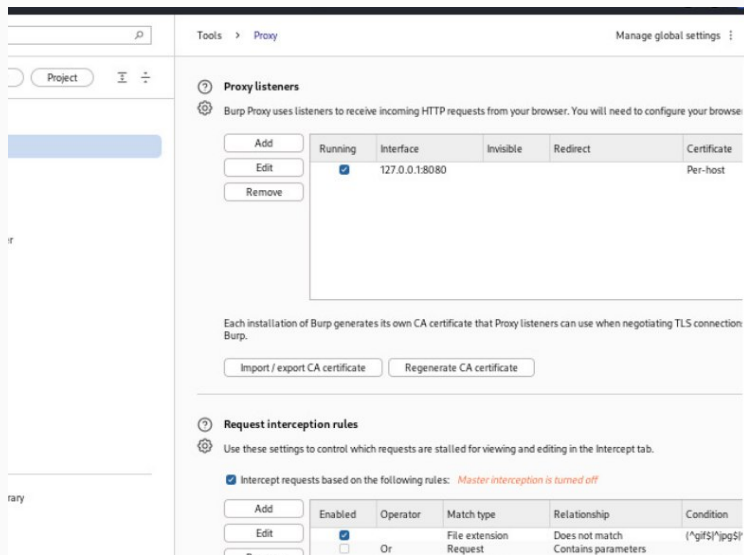


Рис. 2: изменение сетевых настроек браузера

3. Также меняю проху настройки самого инструмента. Во вкладке проху устанвливаю “intercept is on” (рис. (fig:003?)).



The screenshot shows the Burp Suite interface with the 'Tools > Proxy' menu path highlighted. The 'Proxy listeners' section is active, showing a table with one listener configured on interface 127.0.0.1:8080. Below this, there is a note about CA certificates and buttons to import/export or regenerate them. The 'Request interception rules' section is also visible, showing a checkbox for 'Intercept requests based on the following rules' which is checked, and a table for defining rules.

Tools > Proxy Manage global settings

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connection: Burp.

Import / export CA certificate Regenerate CA certificate

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension Request	Does not match Contains parameters	(^gif\$ ^jpg\$ ^
<input type="checkbox"/>	Or			

4. В браузере устанавливаю данный параметр (рис. (fig:004?)).

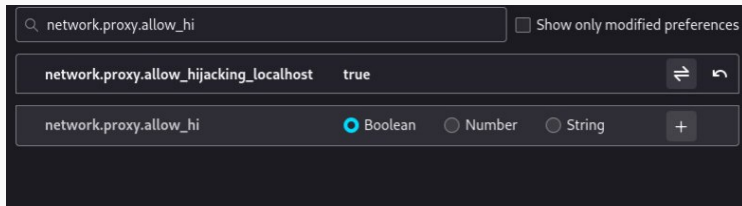
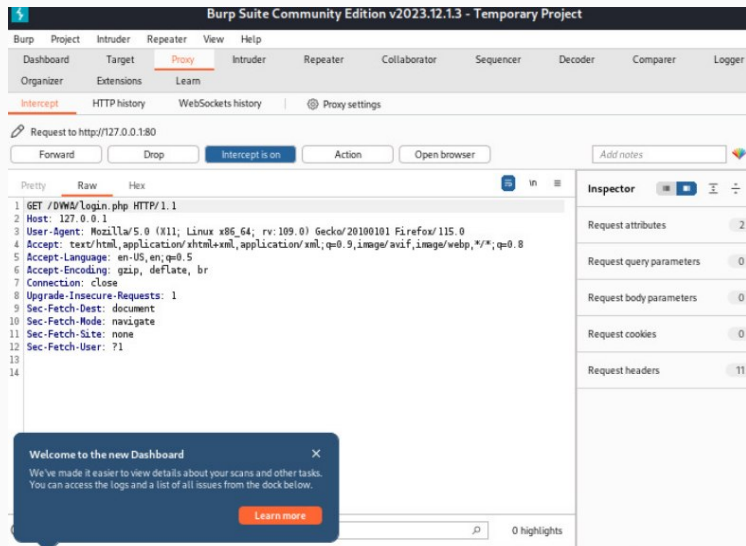


Рис. 4: настройка браузера

5. После этого при попытке зайти на DVWA в браузере, во вкладке проху появляется запрос (рис. (fig:005?)).



6. Во вкладке `target` находится история запросов, во вкладке `intruder` можно посмотреть тип атаки, который можно изменить, и запрос.

Я ознакомилась с Burp Suite.

Спасибо за внимание!