Lab 3 - SQL Injection with Burp Suite

Submission Guidelines

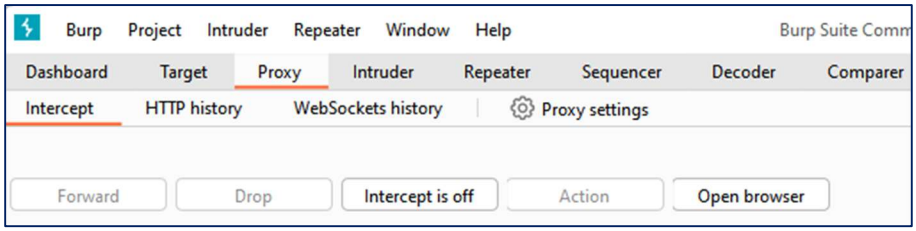
- This is due on **March 6 at midnight**.
- This is worth 5 points and graded as pass/fail.
- Use the "Lab 3 - Outcome.docx" file to submit your work.
- Use the following naming convention: Lab, lab#, last name, and extension (e.g., Lab_3_Ahmed.docx).
- Zoom in your screenshots, please.

Preparations

1) Go to the following website and create an account. The password is automatically created and e-mailed to your account. You cannot change the password. While conducting this lab, you must remain on the browser. When you exit the browser, you must receive a new password. https://portswigger.net/users
2) Please use your own computer for this lab. You may use your Windows or Mac machine for the lab. Go to the following site and download and install the latest **Burp Suite community edition**. Burp Suite is available for Mac OSX as well. https://portswigger.net/burp/communitydownload
3) Burp Suite is installed on Windows Server VM in the Proxmox server. But the browser in the Burp Suite is not launched. Therefore, do not perform this lab on the Proxmox server.

On Burp Suite

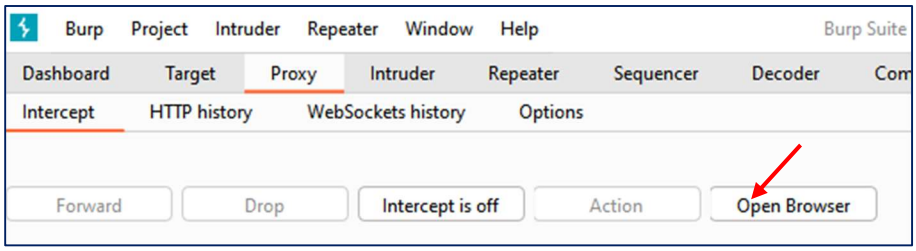
- On your machine, open Burp Suite. Select Temporary project > Next > Select Use Burp Suite default > Start Burp.



- On Proxy, use the following controls. Below is a copy from the following site: https://portswigger.net/burp/documentation/desktop/tools/proxy/intercept-messages.
  a) **Forward** - After you review or edit the message, click **Forward** to send the message to the target.
  b) **Drop** - To cancel the request so that it never reaches the target server, click **Drop**.
  c) **Interception is on/off** - Use this button to toggle all interception on and off:
  d) If the button shows **Intercept is on**, messages are intercepted. You can also configure messages to be forwarded automatically using the settings for interception of HTTP and WebSocket messages.
  e) If the button shows **Intercept is off**, Burp forwards all messages automatically.

f) **Action** - This shows the context menu for the main panel. From here, you can perform a range of actions such as running scans or sending requests to other Burp tools.

- Go to **Burp Suite** > **Proxy** > **Open Browser**. Make sure **Intercept is Off**.
- Click on **Open Browser**. The proxy setting on the browser is already turned on. So, you do not need to do an extra setting on the browser.



- Go to the following site. You need to login to be able to perform the labs.
  - https://portswigger.net/web-security/sql-injection

Tasks

1. Retrieving hidden data

https://portswigger.net/web-security/sql-injection

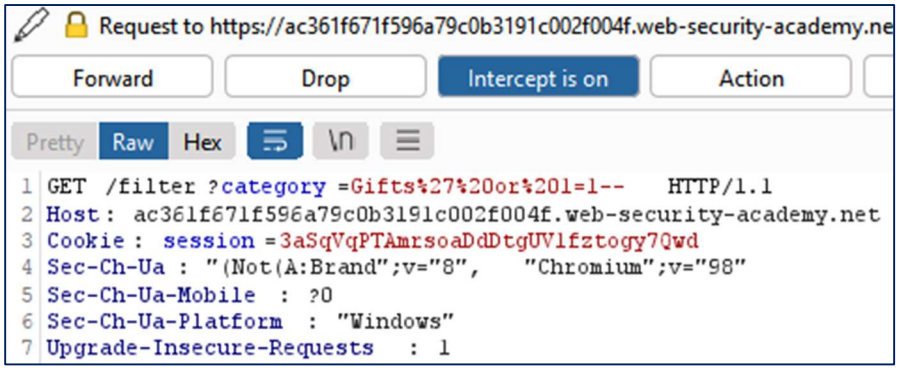
- Read all the instructions carefully.

- Go to the site for the injection. You are asked to select a category on the menu below.

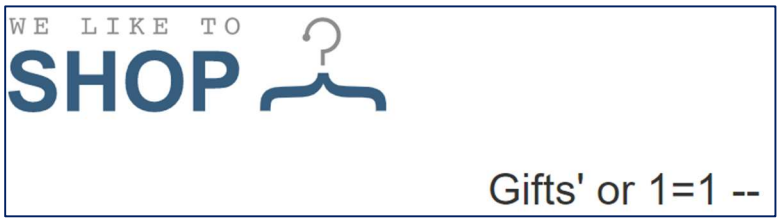
- Before you select a category, you need to turn on **Intercept**.
- Perform the injection following the steps in **solution**. You can perform the injection in two ways. Try both to see how they work.
  1) **On Burp Suite**: Editing the injection on Burp Suite is clunky. Alternatively, you may use **Notepad** as shown below. While working on Burp Suite, you need to replace **quote** with **%27** and **space** with **%20**.

2) **Using URL box**: You can directly enter an injection on the URL. Capture the injection using the proxy and check how the injection was handled internally.

- After testing the injection in both ways, perform an injection with a different category **using the proxy**.
- Before you execute the injection on the proxy (i.e., click on **Forward**), take a screenshot of the content of the injection that is displayed on the proxy. (Please do your own work!)



- Take a screenshot of the outcome like below. (Please do your own work!)

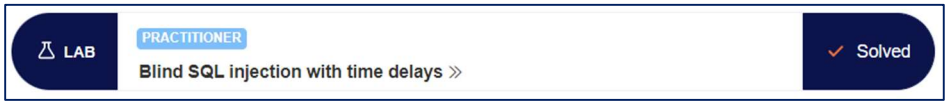


2. Blind SQL injection

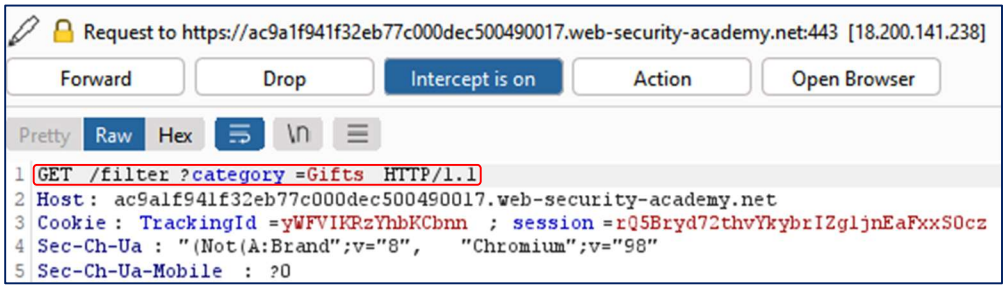
https://portswigger.net/web-security/sql-injection/blind

Lab: Blind SQL injection with time delays

https://portswigger.net/web-security/sql-injection/blind/lab-time-delays



- For this lab, you must use the proxy server. Before you click a category, you need to turn on **Intercept**.
- The following does not have an injection yet.



- Perform an injection using the solution.
- Before you execute the injection on the proxy (i.e., click on **Forward**), take a screenshot of the content of the injection that is displayed on the proxy.
- Take a screenshot of the outcome like below.