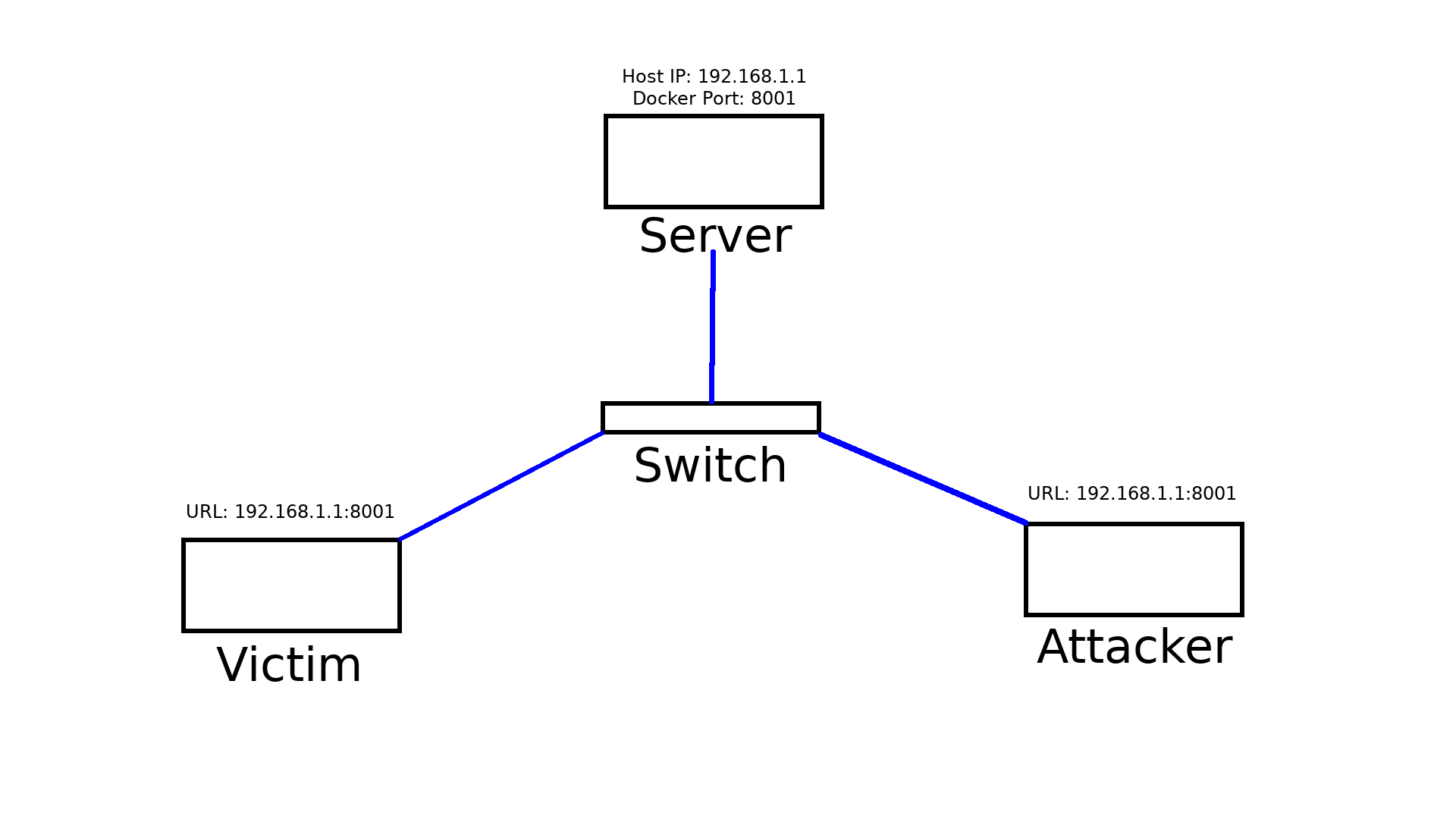
Lab 4

Session Hijacking

Session Hijacking is when an attacker finds the victims session ID and uses it to gain unauthorized access to a web service. For this lab there will need to be three nodes. These include the attacker, the victim, and the web server. The web server will be running the Docker LAMP and both the attacker and victim will have access to the server through the URL of their browser. Bellow is a diagram of how to set this up.



Part 1. (Victim)

For this lab only the victim needs an account. They should navigate to **Registration** and create one.



Part 2. (Attacker)

Once everything is setup the attacker must try to trick the victim into navigating to the **Stealsession.php** page(we assume this page was created in advance by the attacker). This may be accomplished in a variety of ways. A good place to start however would be to insert a link or a script into the **Persistent XSS** page.

Part 3. (Victim)

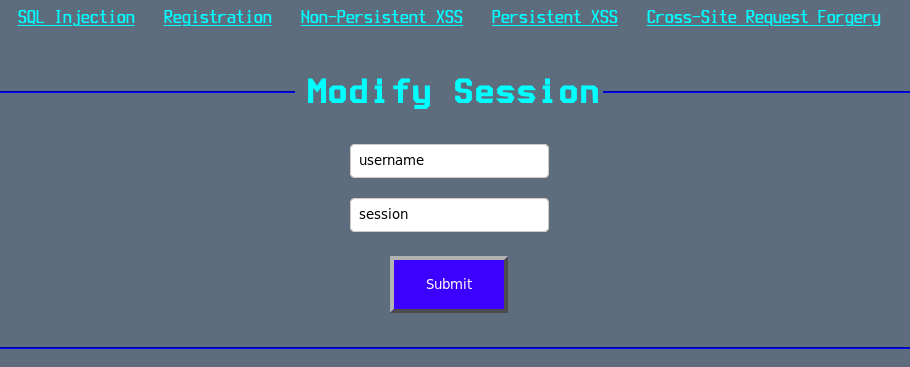
Since the victim in this lab already knows what to expect they should play along and click the exploit (normally they would not know what is happening).

Part 4. (Attacker)

After the victim has been redirected to Stealsession.phptheir session information will be posted on **Persistent XSS**. The attacker will need to save this information for the next step.

Part 5. (Attacker)

Once the attacker saves the information they should navigate to **mod\_session.php**(we assume this page was created in advance by the attacker). Here they can enter the victim’s username and session ID to hijack their account.



Part 6. (Attacker)

Finally the attacker should navigate to Persistent XSS and make a comment. Their comment should now reflect the victim’s username.

Questions

1. What code was injected to redirect the victim?

2. Include a screenshot of the victim’s session information displayed on the **Persistent XSS** page.