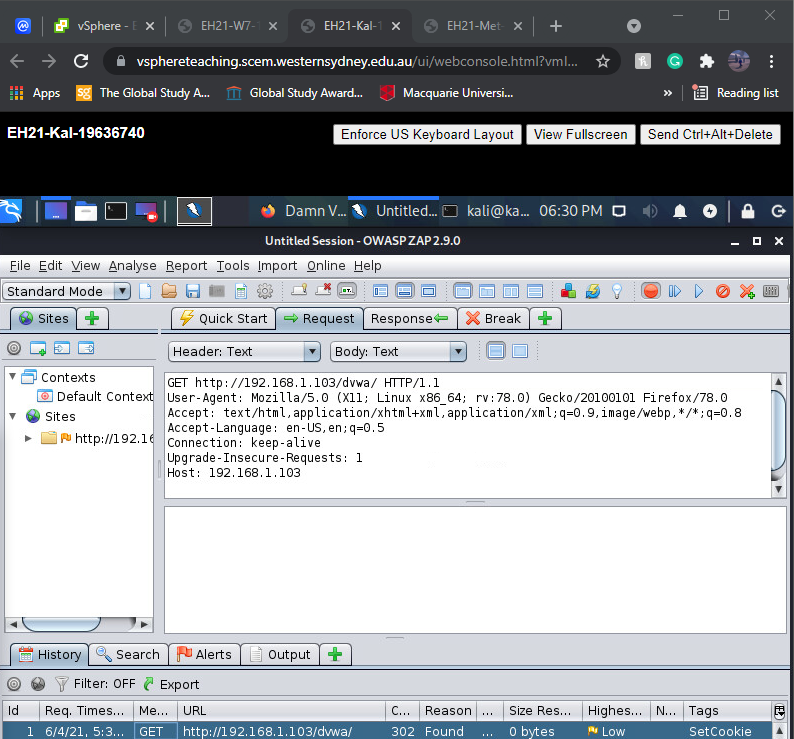
# Using ZAP to intercept and observe HTTP messages

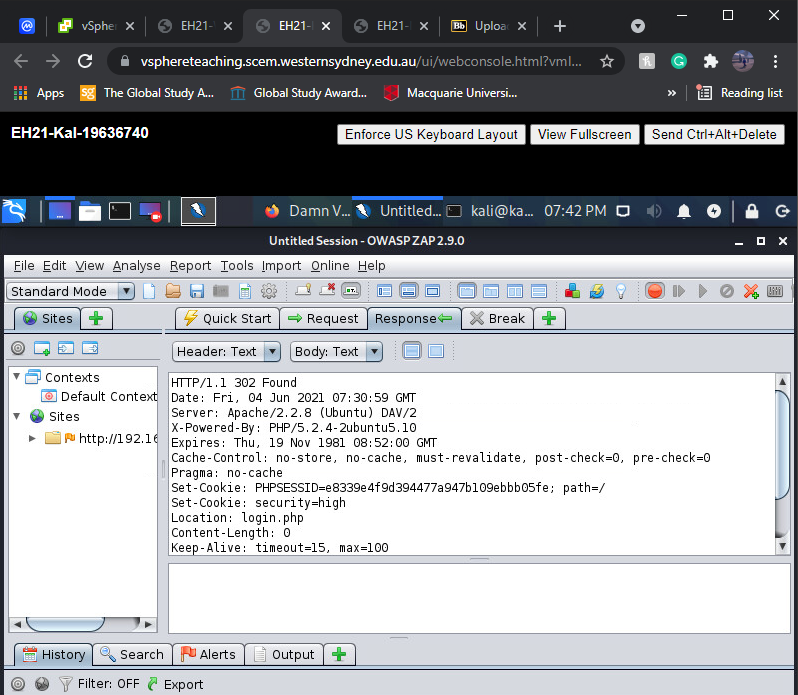
* 1. **Step (c)**

1. [**http://192.168.1.103**](http://192.168.1.103)**/dvwa/**
2. **There is no body part for this message.**



* 1. **Step (e)**

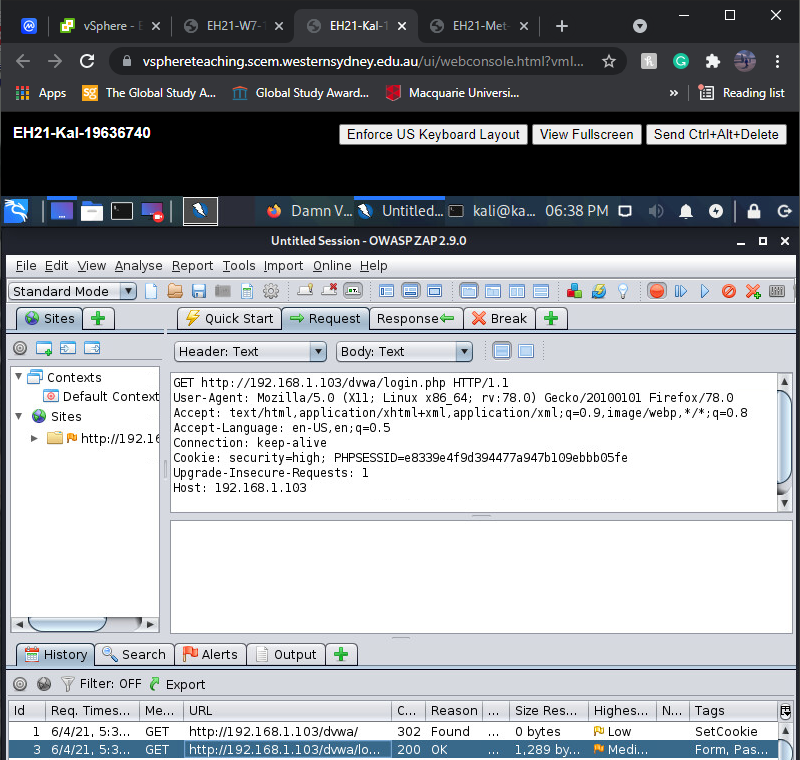
1. Cookie 1: PHPSESSID= e8339e4f9d394477a947b109ebbb05fe Cookie 2: security=high
2. login.php



* 1. **Step (f)**

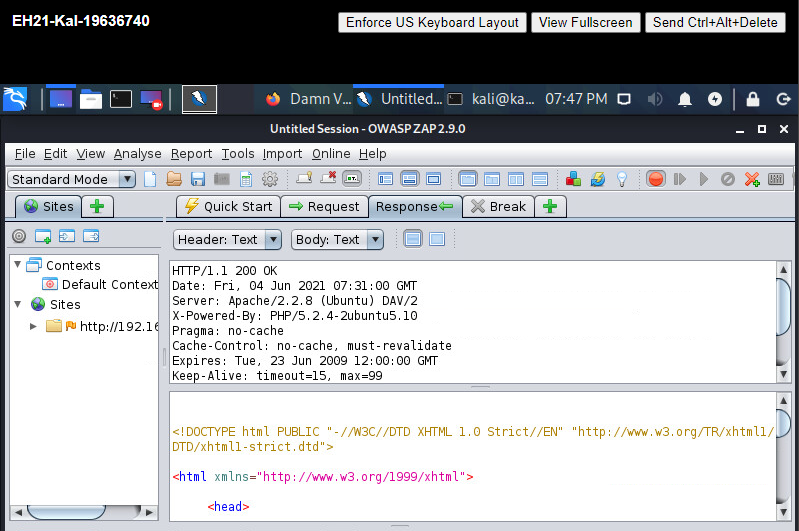
1. **<http://192.168.1.103>/dvwa/**login.php
2. Cookie 1: PHPSESSID=e8339e4f9d394477a947b109ebbb05fe

Cookie 2: security=high

1. Yes, the cookies have the same names and values as those in the 1.2 step.
2. 

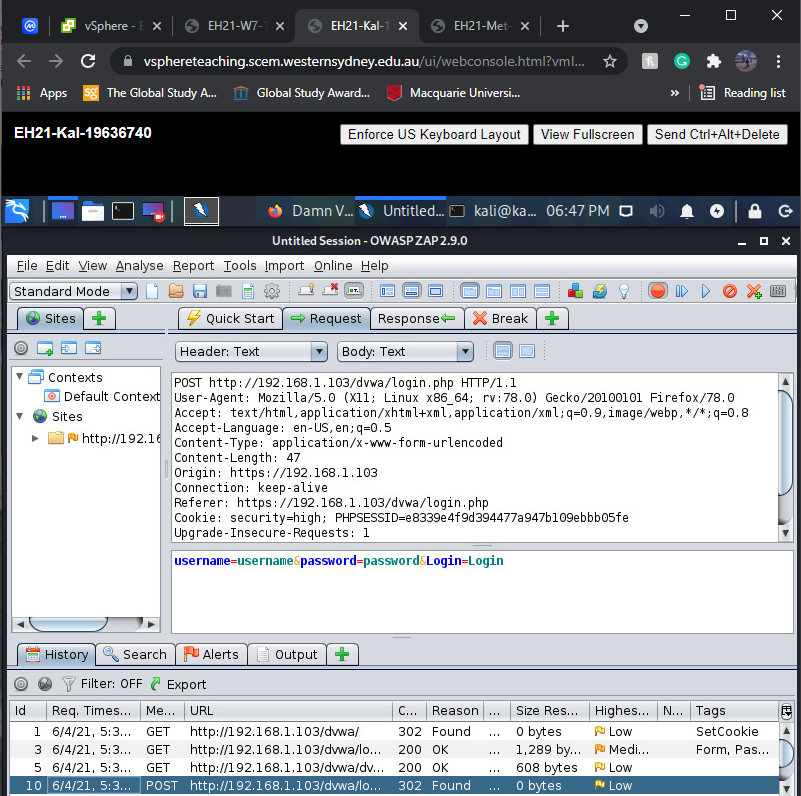
**1.4 Step (g)**

1. Yes, this message has a body part.
2. This body part contains the HTML script for the login screen of the website.
3. Because the session cookie will be derived from the login information provided by the user.



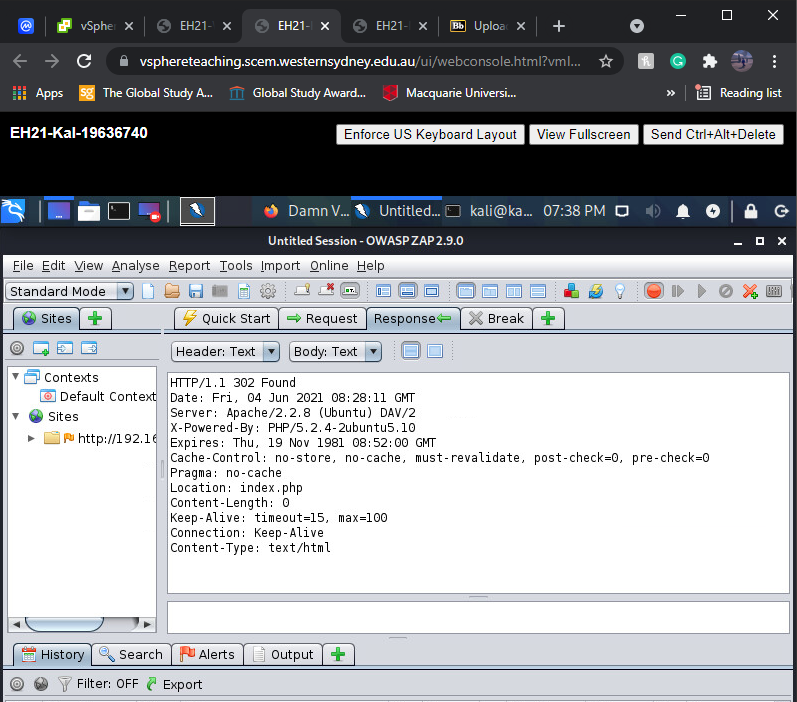
**1.5 Step (i)**

1. The method used in this message is POST.
2. The body part contains the inputs provided by the user: username, password, and Submit/Login button.



* 1. **Step (j)**

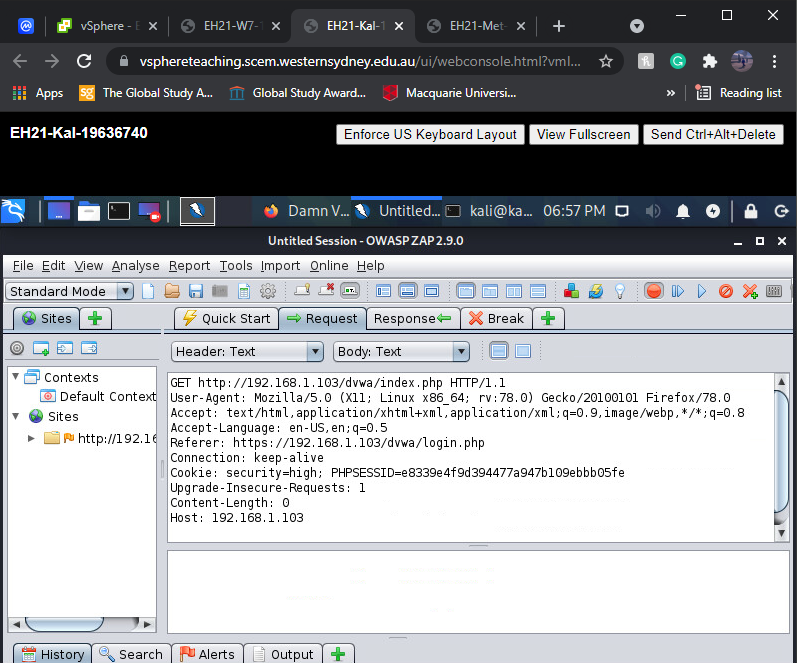
1. Yes.
2. Because the **Location** header indicates that the user will be redirected to the **index.php** page.



**1.7 Step (k)**

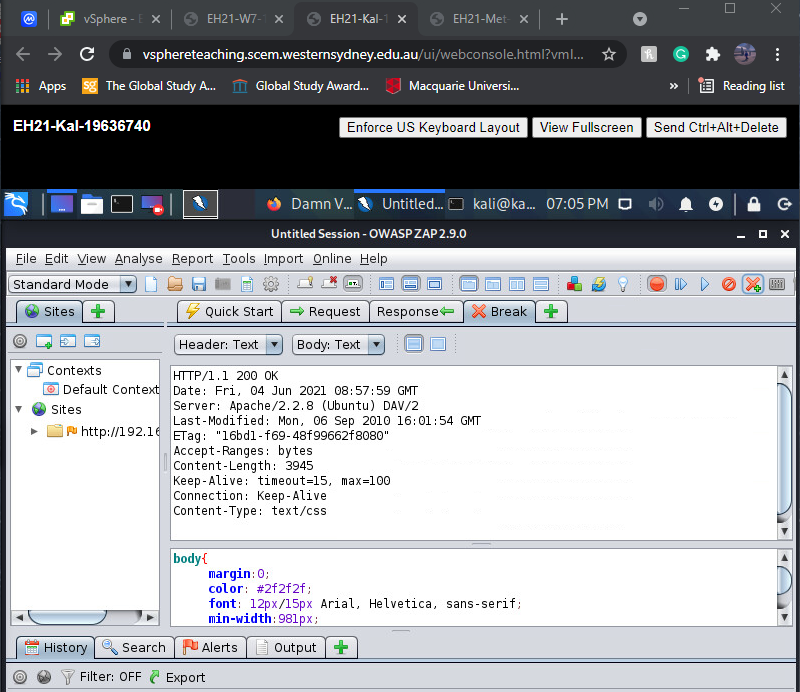
1. [**http://192.168.1.103**](http://192.168.1.103)**/dvwa/**login.php
2. Cookie 1: PHPSESSID=e8339e4f9d394477a947b109ebbb05fe

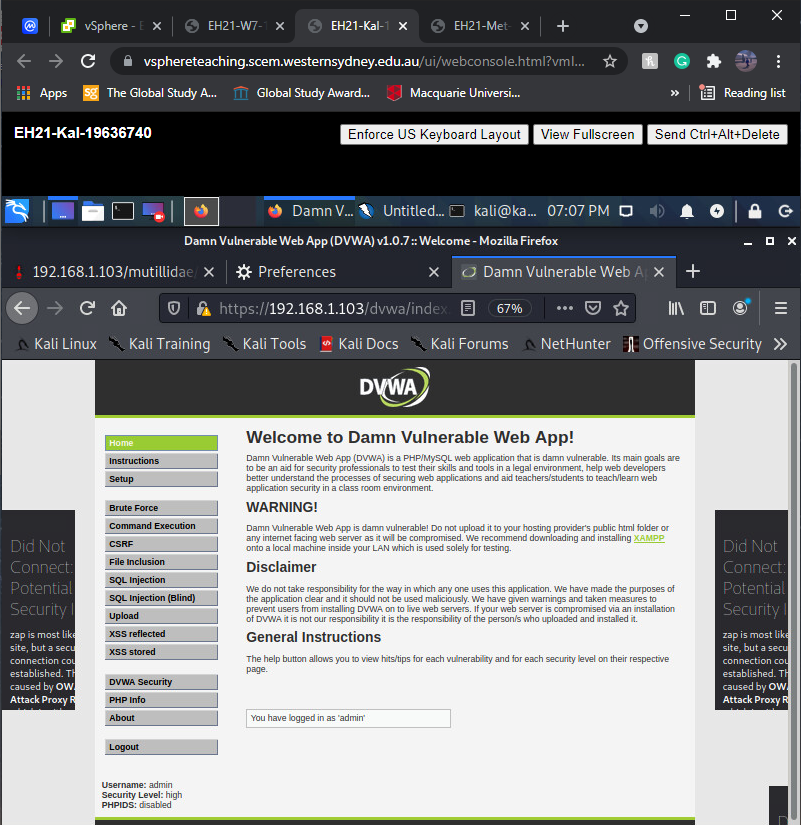
Cookie 2: security=high



* 1. **Step (l)**

1. Its body part contains the HTML page generated by **'index.php',** which is DVWA dashboard.





* 1. **History**

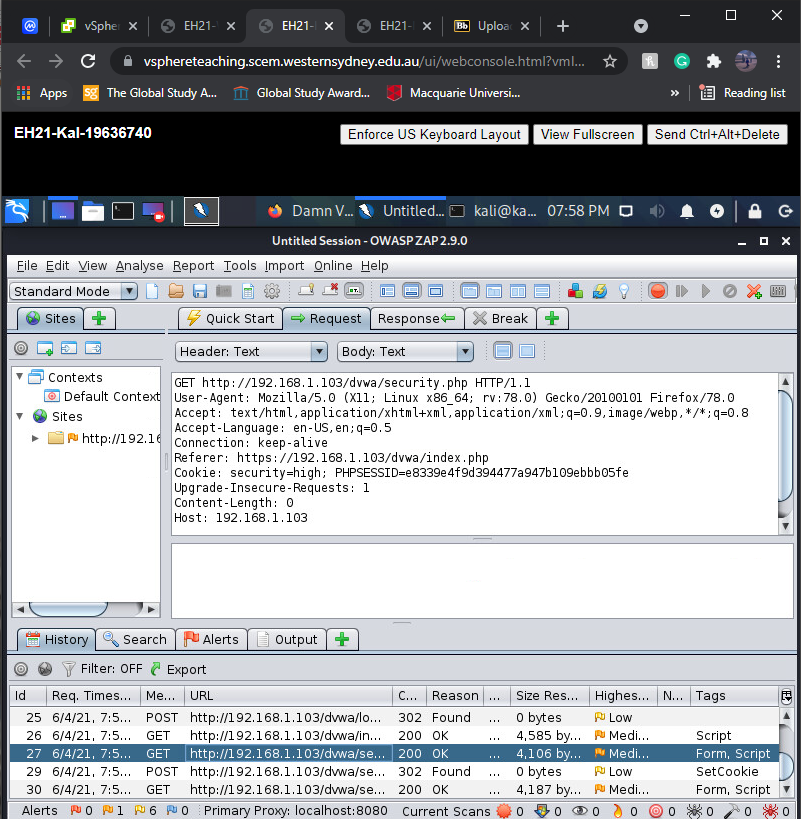
The **login.php** page was requested twice but for different methods. The first one was to GET the username and password inputs and does not contain cookies, while the second was to POST the cookies and establish the session.

# 2. Using ZAP to modify HTTP messages

**2.1 Step (a)**

**(i)** There are 3 pairs messages

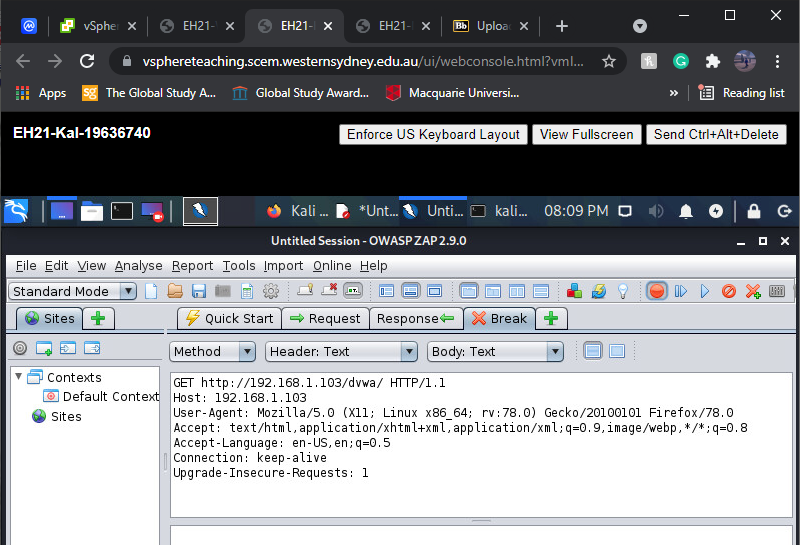
**(ii)**



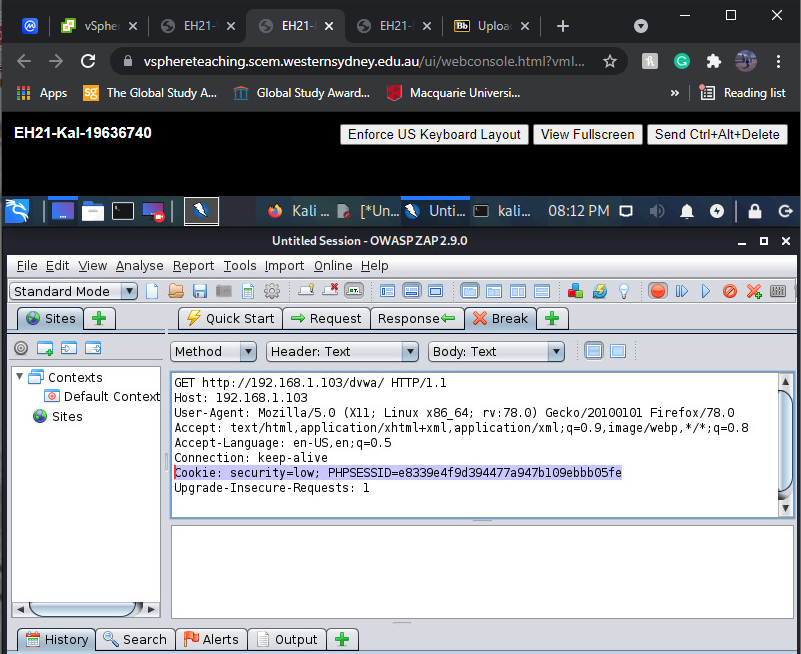
**2.2 Step (c)**

**(i)** Because the session was ended when the browser was closed, and Firefoxremoved both cookies from its memory.

**(ii)**

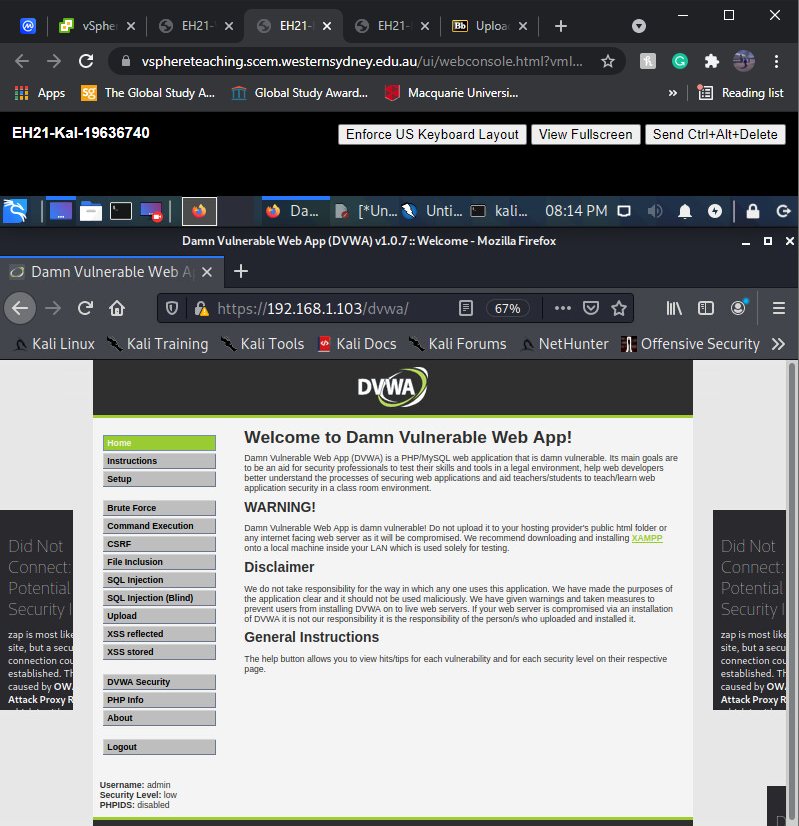


**2.3 Insertion**



**2.4 Step(j)**

**(i)**

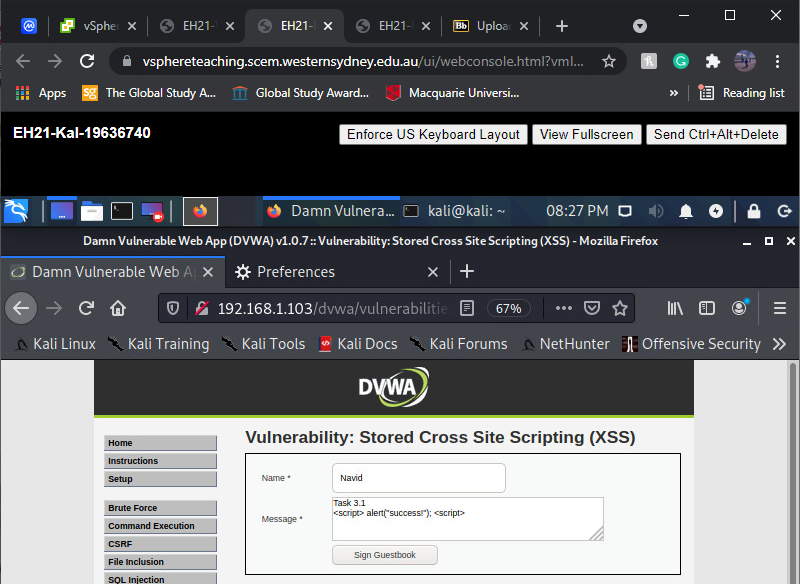


**(ii)** Because in the previous session, we set the security level to low. We copied the cookies of the previous session and inserted it to this new session which in turn inherited the security level settings of the previous one.

# 3. Stored XSS

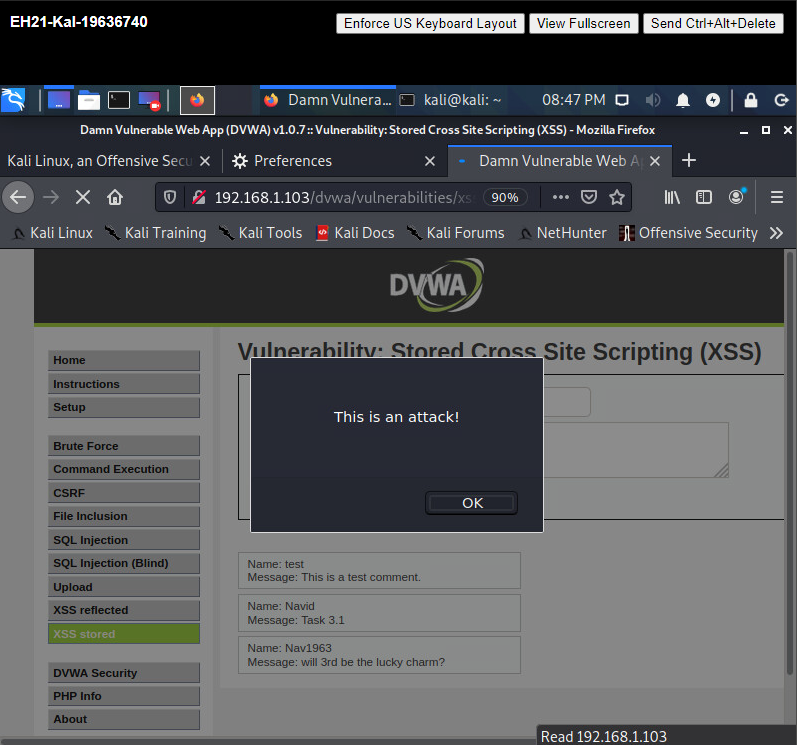
3.1 Example 1

i.



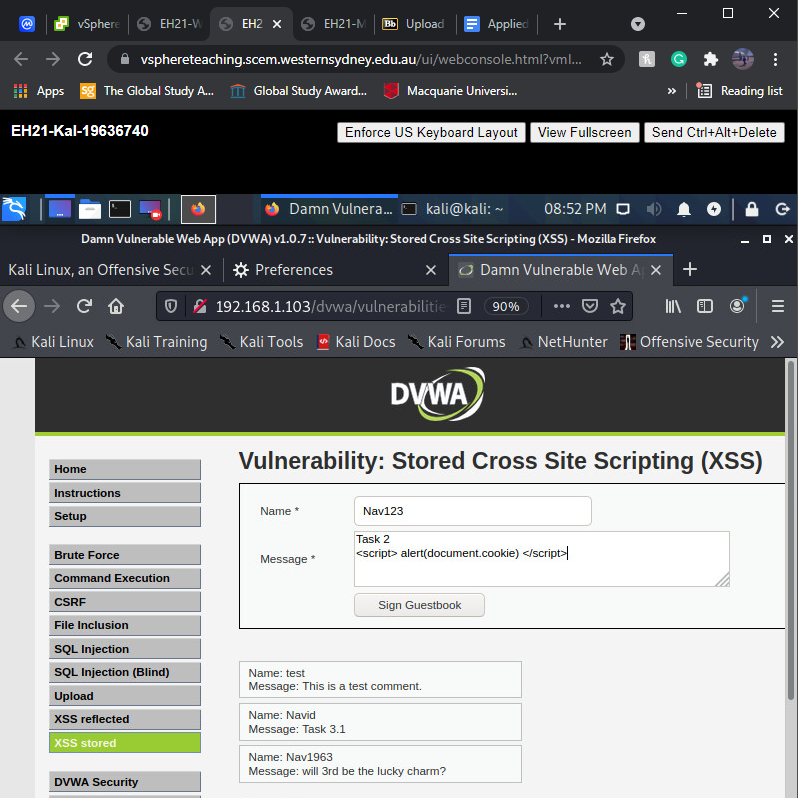
ii.

the output is different as initially it did not show mw any alert box!

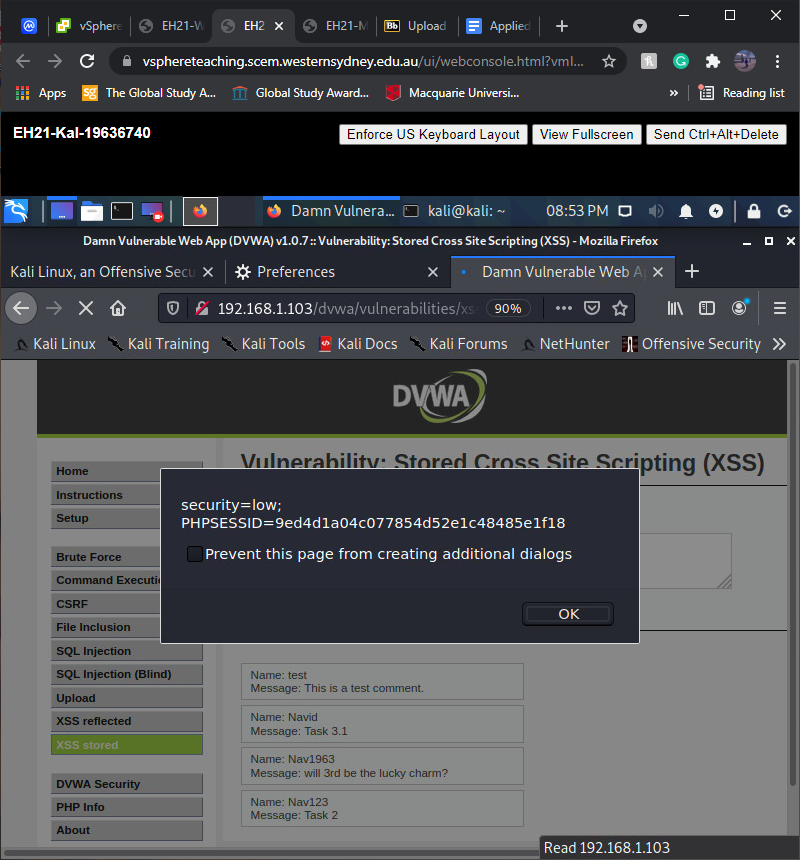


3.2 Example 2

i.

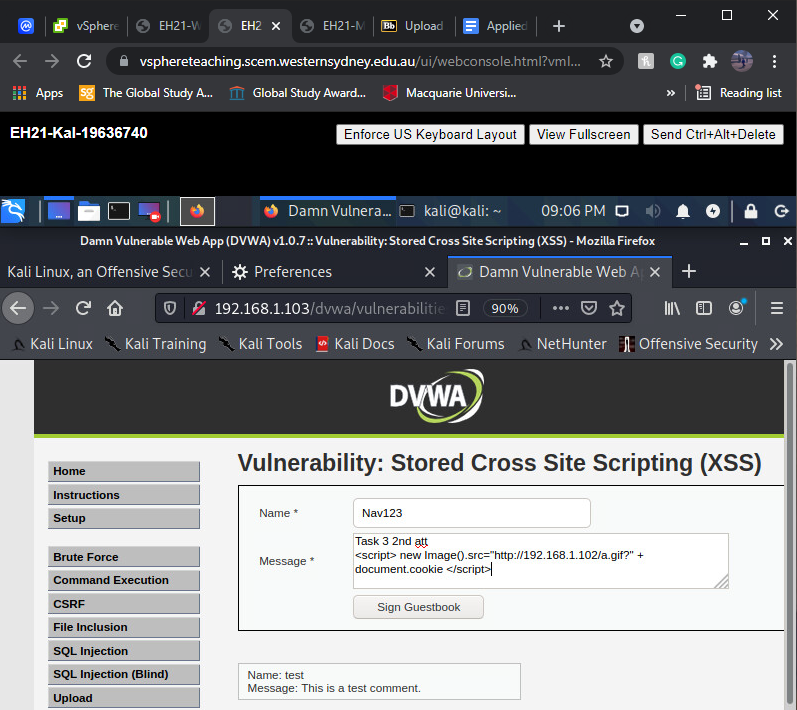


ii.

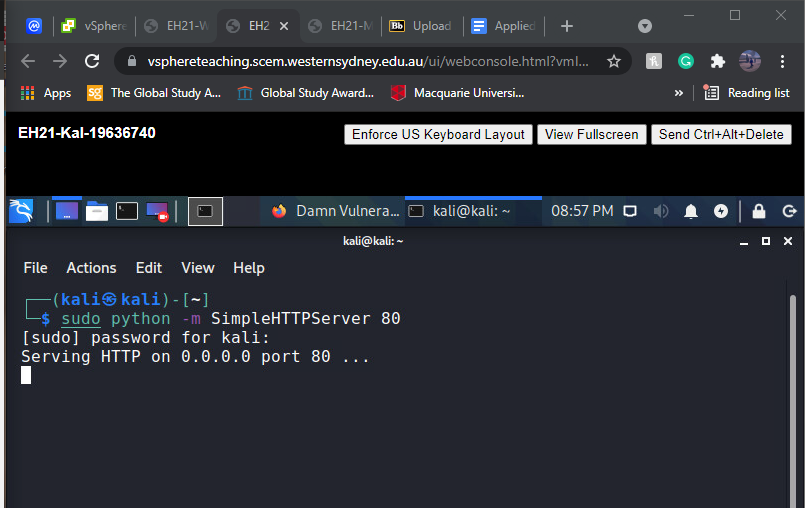


3.3 Example 3

i.



ii.



iii) result

