**Assignment 6**

**Title: Obtain threats associated with web Servers & Applications i.e. Session Hijacking**

**Theory:**

**Prerequisites:**

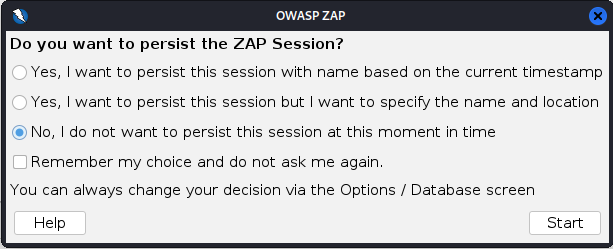
1. **You must know the IP ADDRESS of the attacker's system and target system.**

**Windows: (Target) (IP A)**

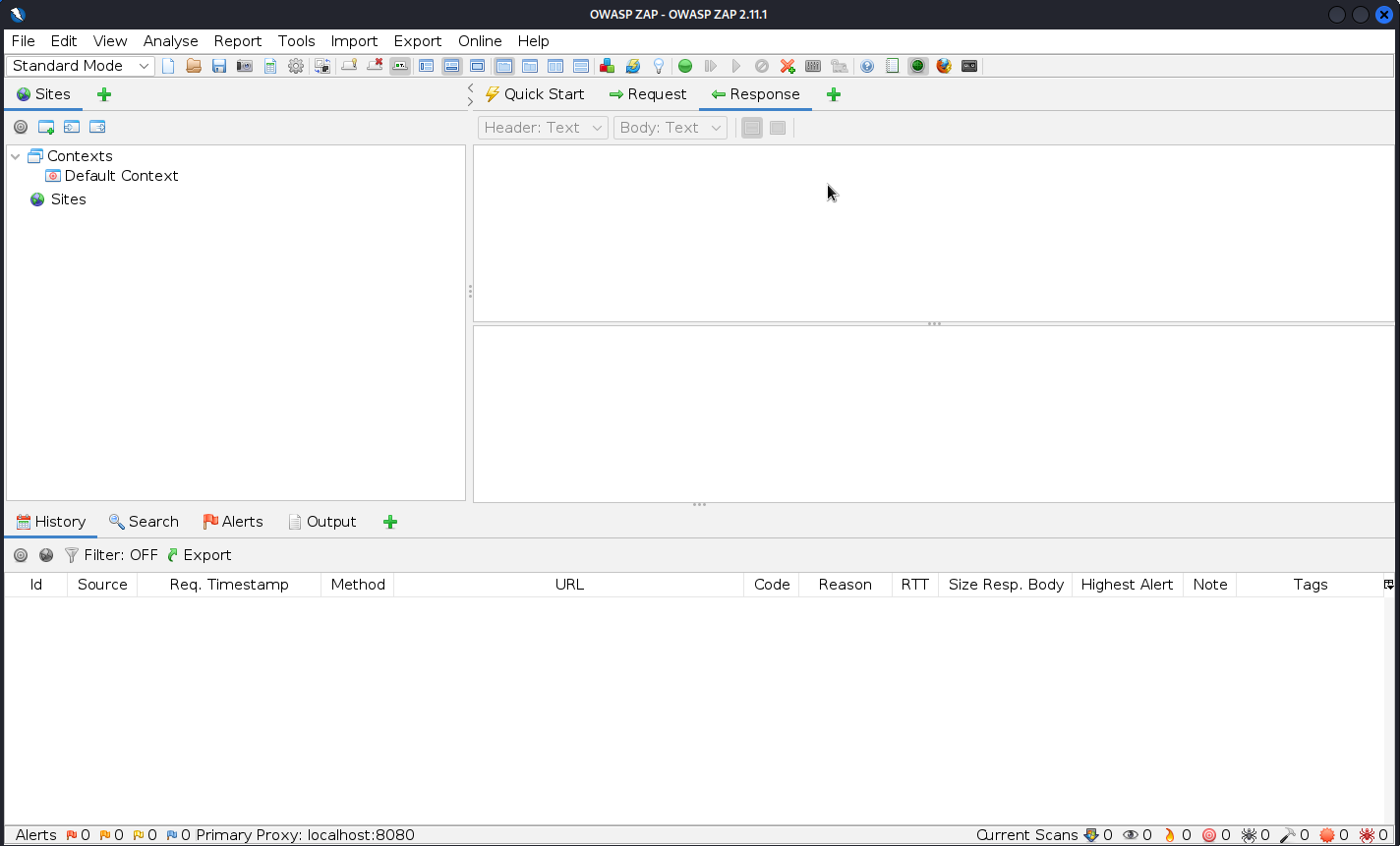
1. **Open browser - goto setting- goto proxy settings- edit manual proxy settings and write IP B and port no 8080- click on Save button.**

**Kali (ZAP): Attacker’s (IP B)**

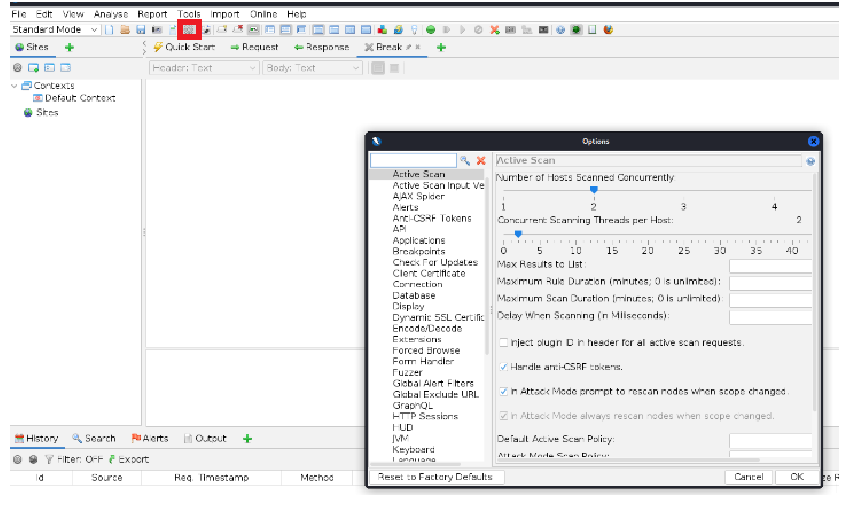
1. **Open ZAP**

**hit on start button**

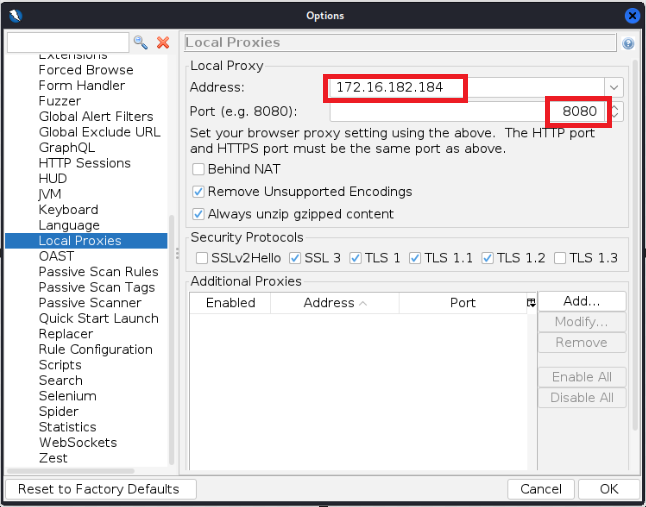
1. **this window will appears**

****

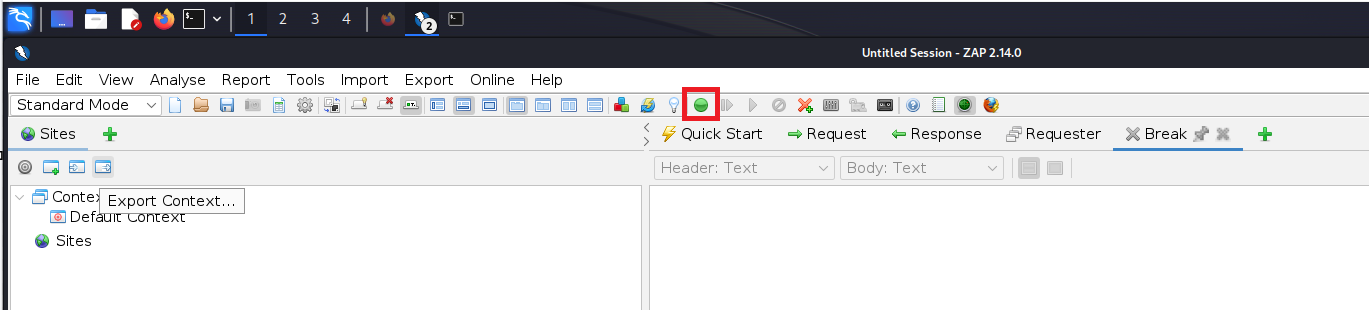
1. **Hit on + button (next to request response) and select break option and then hit on option (gearbox symbol, highlighted in red colour here)**

****

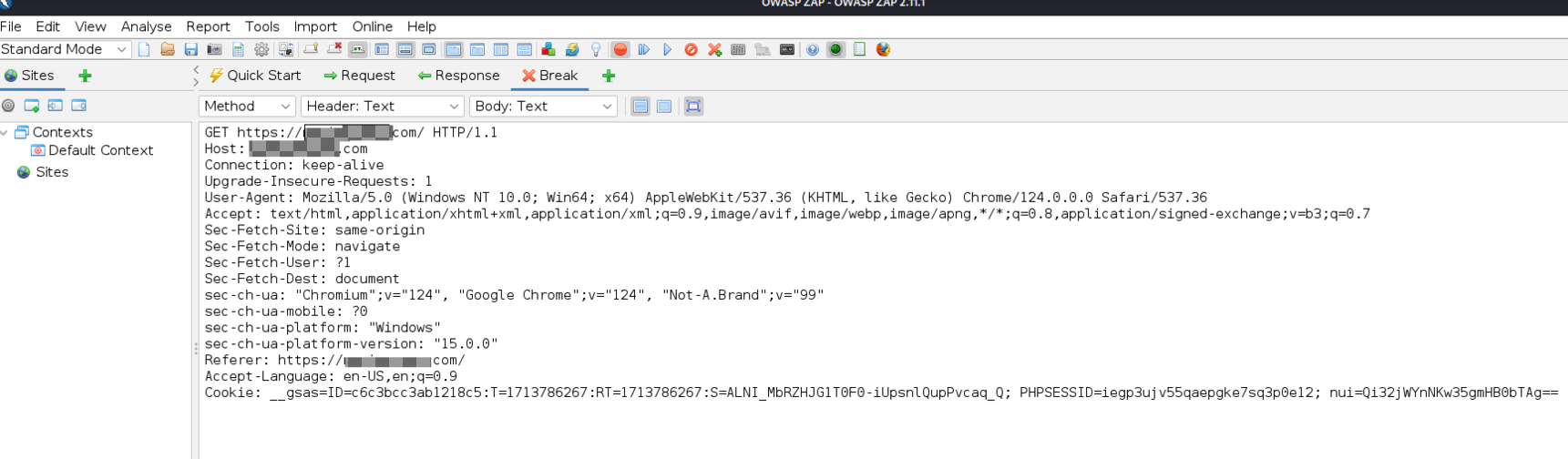
1. **Select local proxies option and set the values**

****

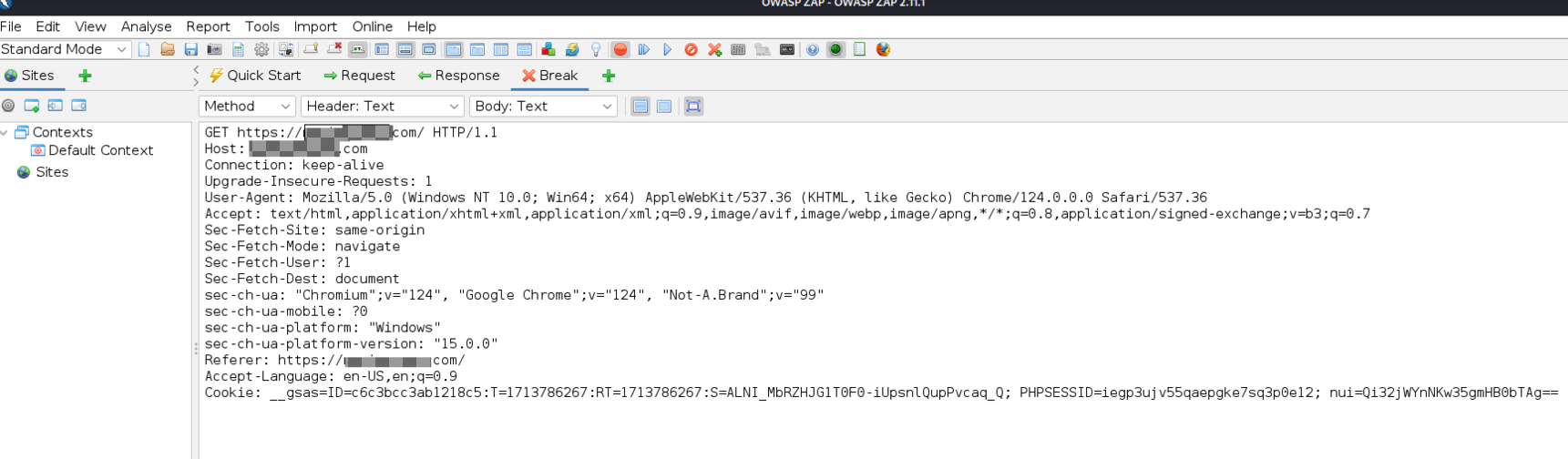
1. **hit on= Set break for all requests and response**

****

1. **Goto your target machine , open the browser and enter any URL EX.** [**www.xyz.com**](http://www.xyz.com)
2. **A message appears, stating that Your connection is not private. Click the Advanced button.**
3. **On the next page, click Proceed to www.xyz.com (unsafe) to open the website.**
4. **Your attacker’s system starts capturing the request as below**

****

1. **Look in the Break tab and click the Submit and step to next request or response icon on the toolbar to capture the www.xyz.com request (arrow directing to right hand side/ next to red button).**

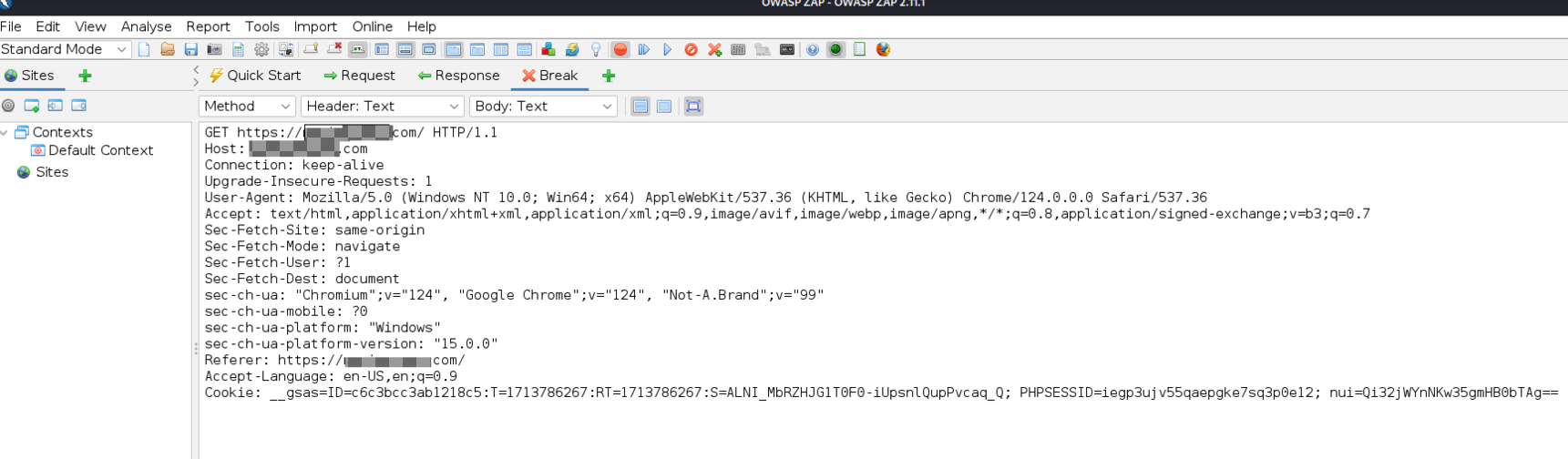
****

1. **You can see like this**

**A HTTP response appears; click the Submit and step to the next request or response icon again on the toolbar.**

****

1. **click the Submit and step to the next request or response icon again on the toolbar. you will get like this:**

****

**Now, in the Break tab, modify www.xyz.com to www.pqr.com in all the captured GET requests.**

**Note: If you find any URL starting with https, modify it to http.**

1. **Once you have modified the GET requests, click the Submit and step to the next request or response icon on the toolbar to forward the traffic to the victim’s machine.**
2. **In all the HTTP Not Found requests, click the Submit and step to the next request or response icon on the toolbar to forward the traffic.**
3. **In a similar way, modify every GET request captured by OWASP ZAP until you see the www.pqr.com page in the victim’s machine.**
4. **Note: It takes multiple iterations to open the pqr site in the victim’s machine.**
5. **The victim has navigated to www.xyz.com, but now sees www.pqr.com; while the address bar displays www. xyz.com, the window displays www.pqr.com.**

**Conclusion:**

1. **What is session hijacking**
2. **Tools to perform SH and tools to detect SH**
3. **Difference between XSS and CSRF**
4. **What is HTTP/1.1**
5. **What is HTTP/1.1 302 Found**