Vulnerability Report

- Arpit Mathur

Website name- http://testasp.vulnweb.com/

Testing Environment- Windows 11, Burpe Suite

Vulnerability name- Use of HTTP protocol

About Vulnerability- Website uses hypertext transfer protocol (HTTP) for communication between the server and clients.

Use of this protocol, leaves website and its users vulnerable to a plethora of attacks for example- cross-site scripting(XSS), HTTP request smuggling to name a few.

Also, due to sending plaintext credentials via HTTP, there is a constant risk of sensitive user credentials falling into wrong hands. Theft of these user credentials can lead to a different set of problems like- user impersonation etc.

Steps-

1. Open Burp Suite.
2. Now, in Burp Suite go to proxy page and open the Burp Suite browser.

3. Open the website in the browser.
4. Go to the login page of the website.
5. Fill the username and password space with valid login credentials(username=admin password=admin).
6. On proxy page and turn on the intercept.
7. Press login on the website having the valid credentials filled.
8. On the proxy page of Burp Suite, the login request with exact, unencrypted login credentials will appear.

Impact- This vulnerability makes the website vulnerable to the following attacks-

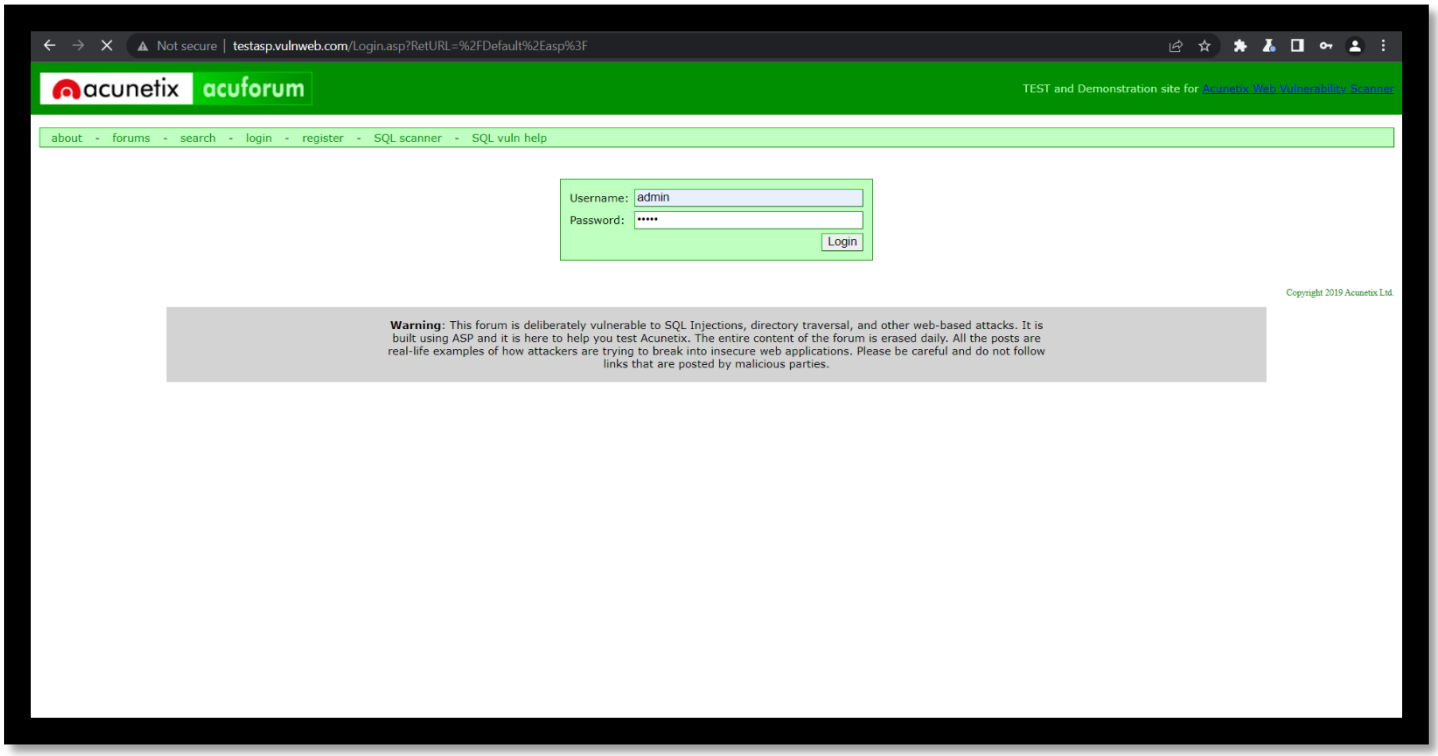
1. Cross-site scripting(XSS)
2. HTTP request smuggling
3. Sensitive user information leak
4. Denial Of Service(DOS) attack
5. Garbage flood attack

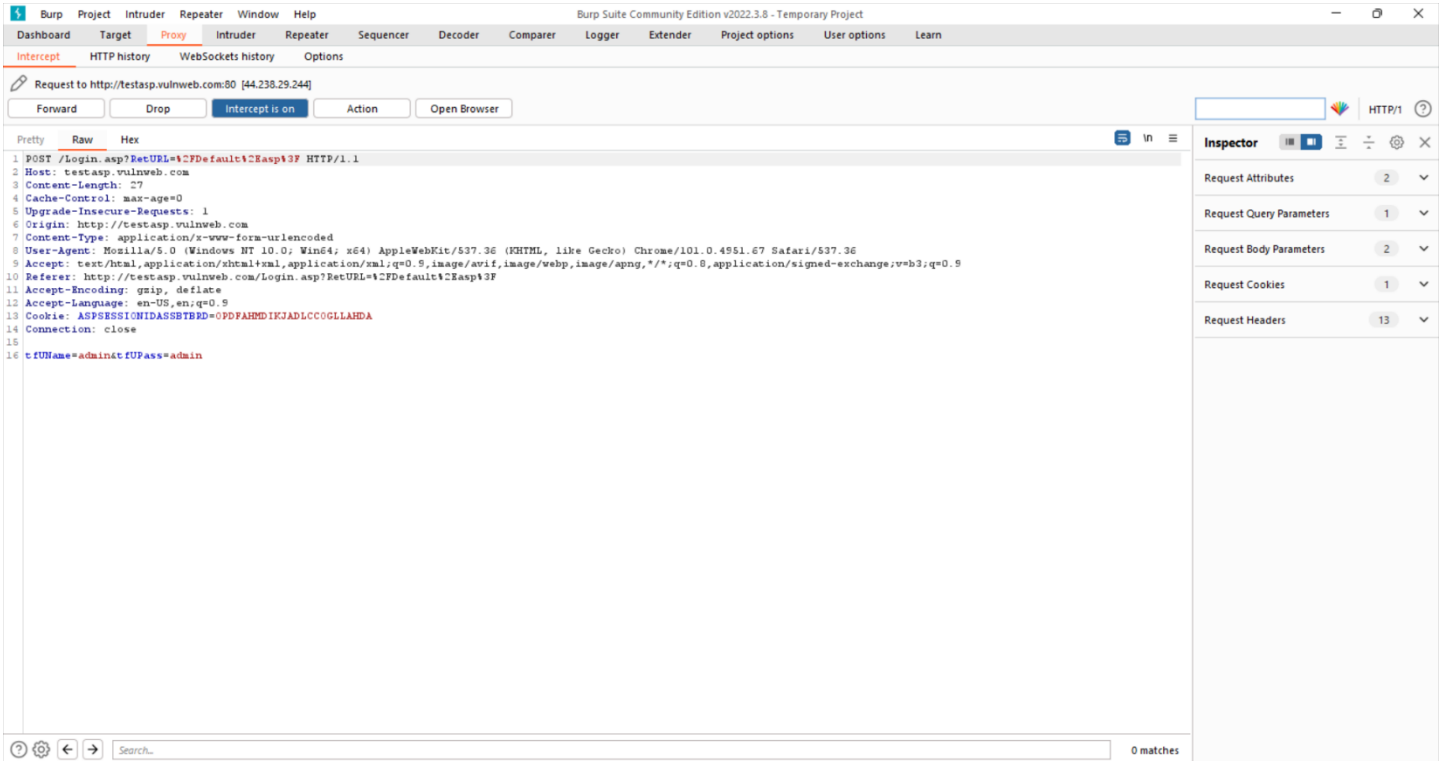
and many more.

Solution- A solution of the above vulnerability is the use of hypertext transfer protocol secure (HTTPS) instead of using the HTTP, which uses encryption to secure the communicated messages between clients and server.

Proof Of Concept-

Screenshots





Video

It has been uploaded on the GitHub repository in the Task-3 folder as Recording_Task-3.wbm