Title : SQL INJECTION

Domain: vulnweb.com

Steps to reproduce :

Step1: visit <http://testsasp.vulnweb.com/>

Step2: on the top of the bar you find a login option.

Step3: click on it yow will prompted with the login credentials.

Step4:Give a basic payloads like 1’or ‘1’= ‘1 for both username and password.

Step5:you can intercept the request in Burpsuit.

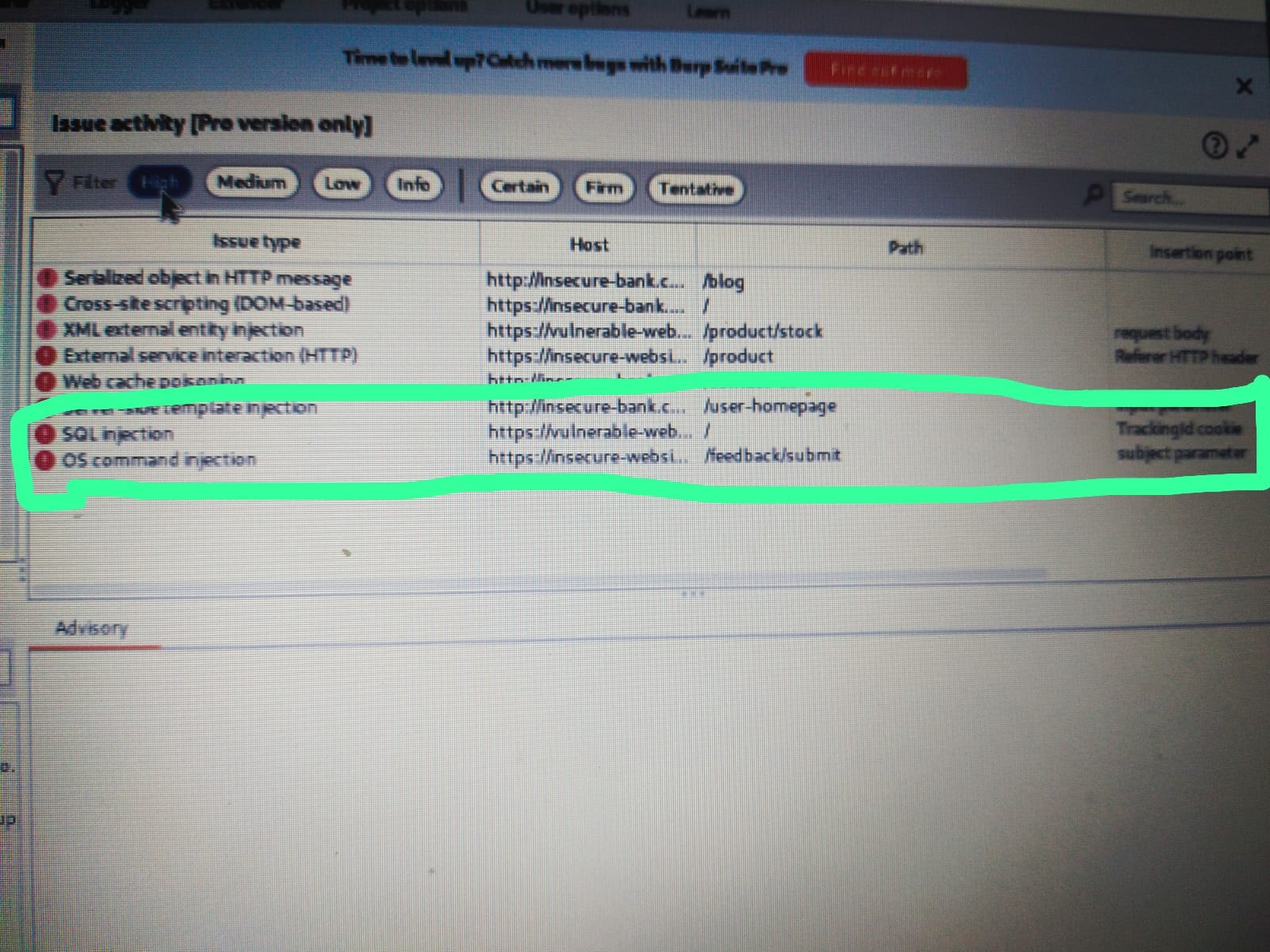
Step6:Now you can see that the page is logged with have any credential’s.

Step7:And you can watch how severity the payload is and what it is effecting.

Impact :

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Severity: high



Mitigations:

1. Use prepared statements and parameterized queries - Parameterized statements ensure that the parameters passed into the SQL statements are treated safely.
2. Object-relational mapping - Most development teams prefer to use Object Relational Mapping frameworks to translate SQL result sets into code objects more seamlessly.
3. Escaping inputs - It is a simple way to protect against most SQL injection attacks. Many languages have standard functions to achieve this. You need to be aware while using escape characters in your code base where an SQL statement is constructed.

