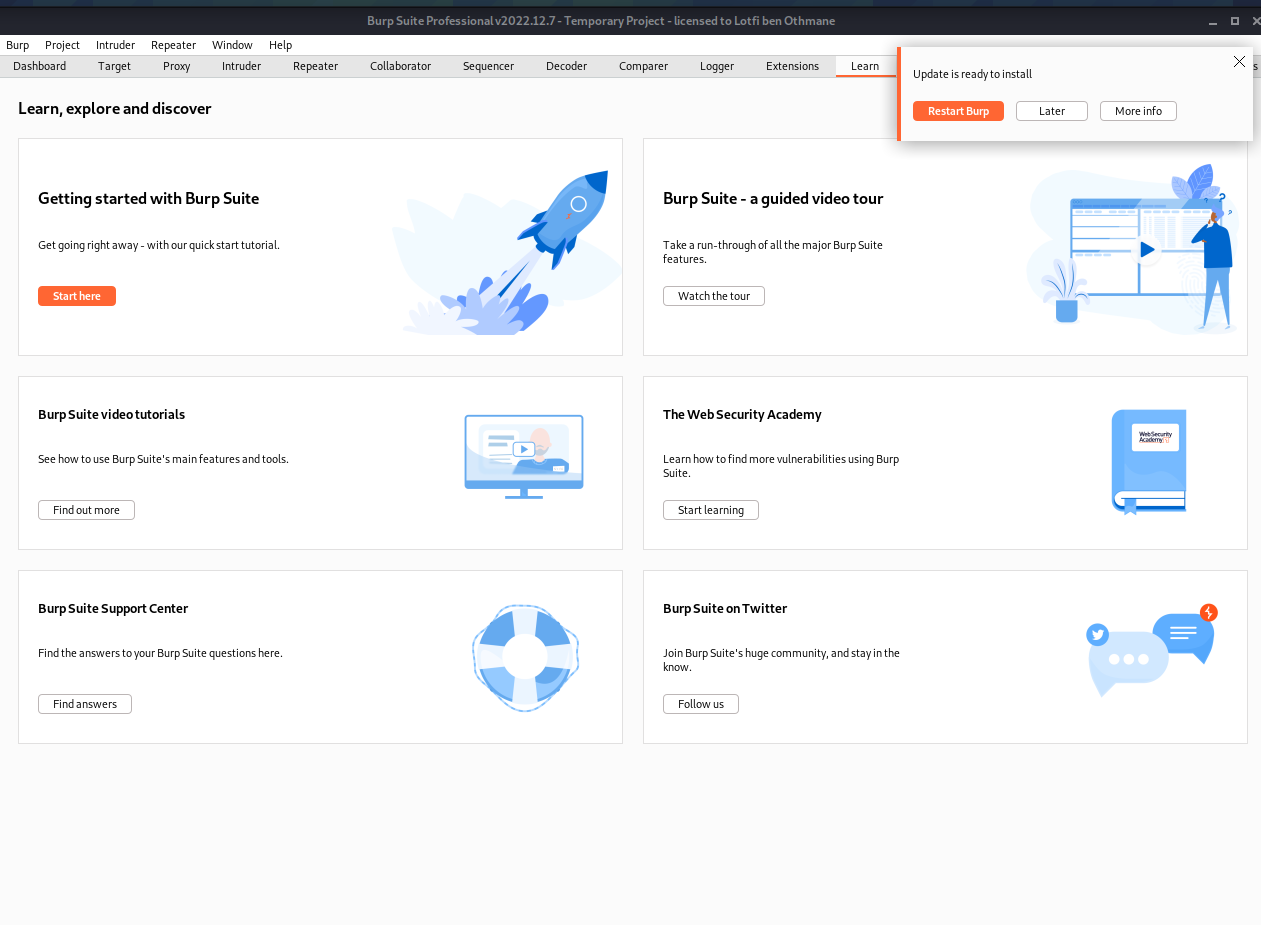
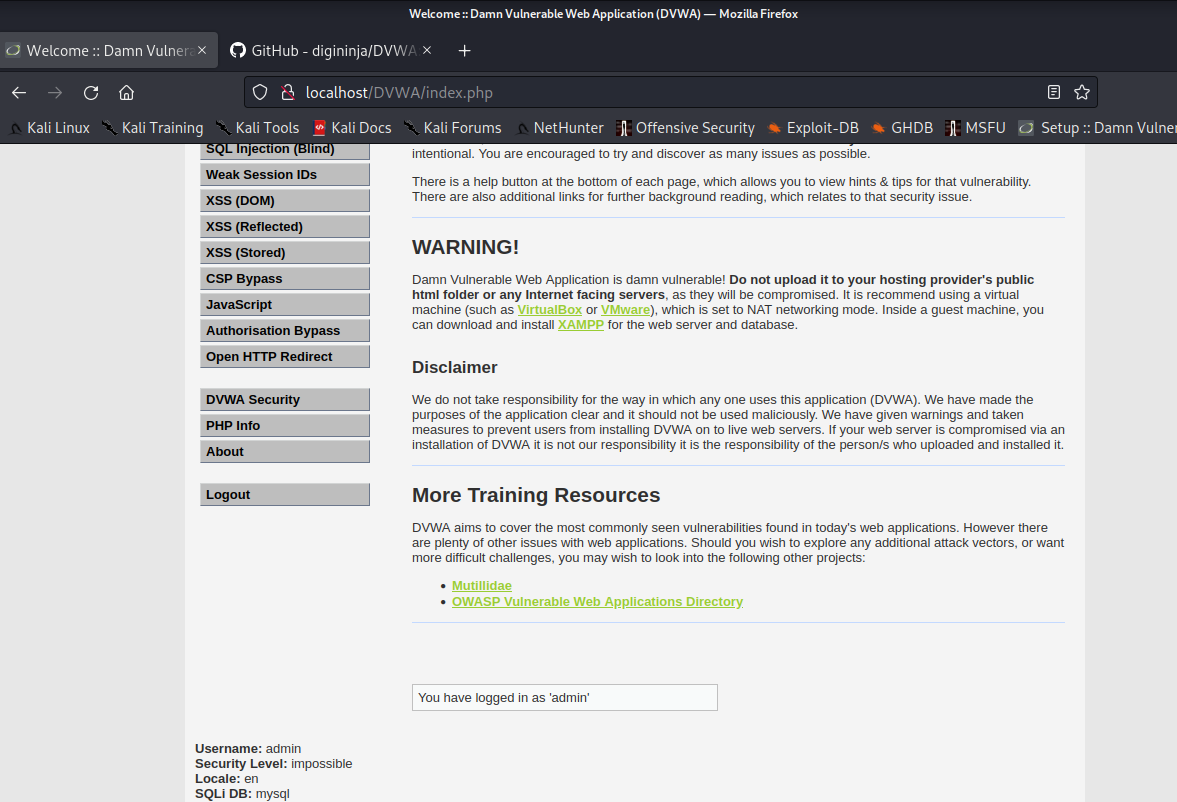
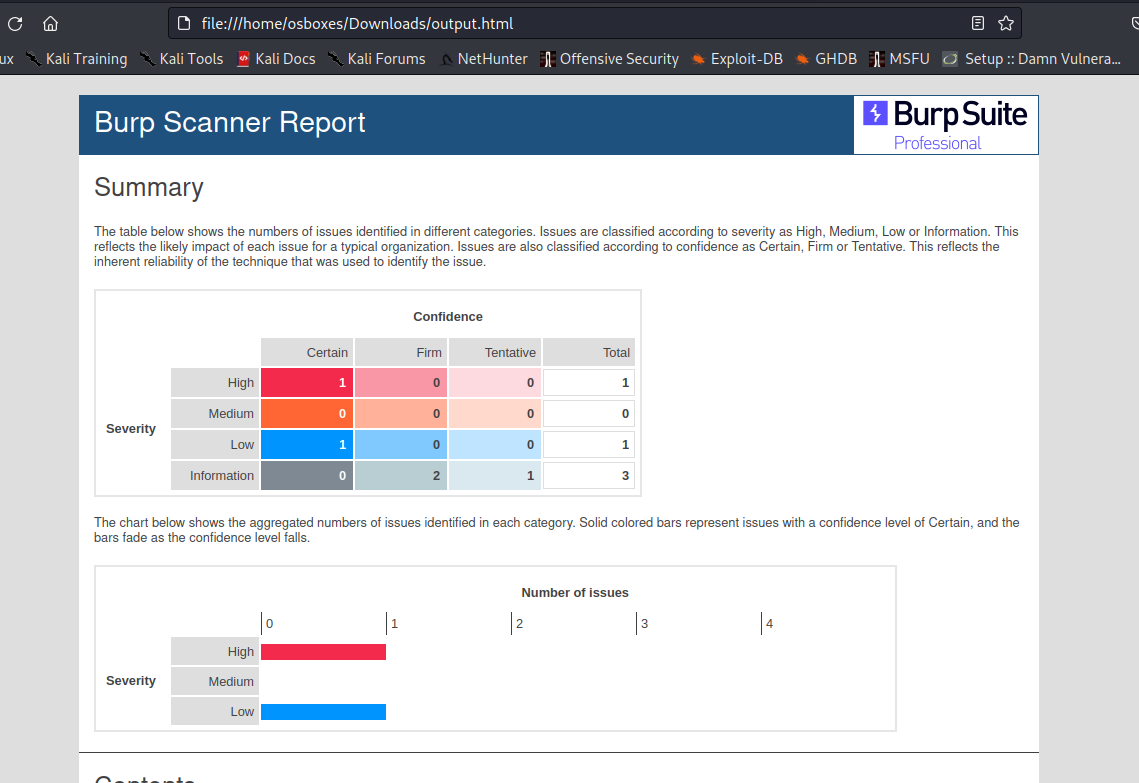
1.



2.



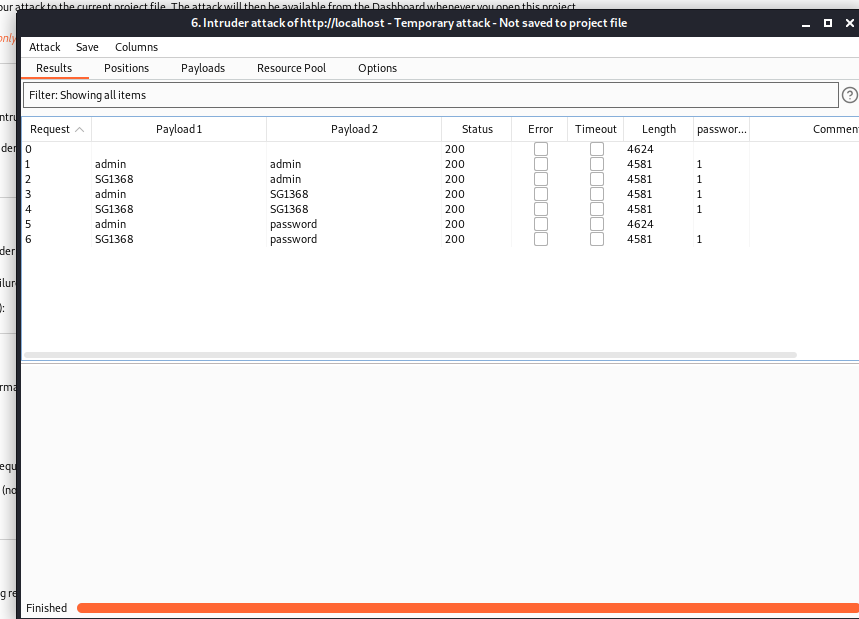
3. 

4. The Burp suite scanner report found multiple flaws with the DVWA that could constitute a serious risk to the web application's security. The flaws are listed in the report, along with their severity rating and the scanner's level of confidence in recognizing them. Clear text password submission, unencrypted communications, path-relative style sheet import, cross-site request forgery, and Clickjacking.

This tells us how we can use tools like burp suite scanner to identify issues within webapps to automatically find the threats and report them with their appropriate mitigation techniques. Also, the severity ratings would help prioritize the issues and address the most critical threats first. It also contains the mitigations that can be used to address these issues. But it cannot identify all the security issues within the web application like below where they are vulnerable to brute force attack on a login page. The clear text password submission can be easily identifiable by just looking at the HTTP requests that the webserver is using instead of the secure HTTPS (SSL/TLS) to communicate.

ID : SG1368

5.



6.

In the brute force attack, we had used burp suite proxy toolset with the intercept on for POST login request. After intercepting the message we transferred it to the burp suite intruder to perform cluster bomb from the payload and next provided payload with lists for each of them. To distinguish the successful login attempts with others we added grep-matching for the output response where login failed. And below is the output where we can see the successful attempt which doesn’t contain that value.

A successful brute force attack can be performed using burp suite and using common login usernames and passwords like admin-admin can be brute forced easily.