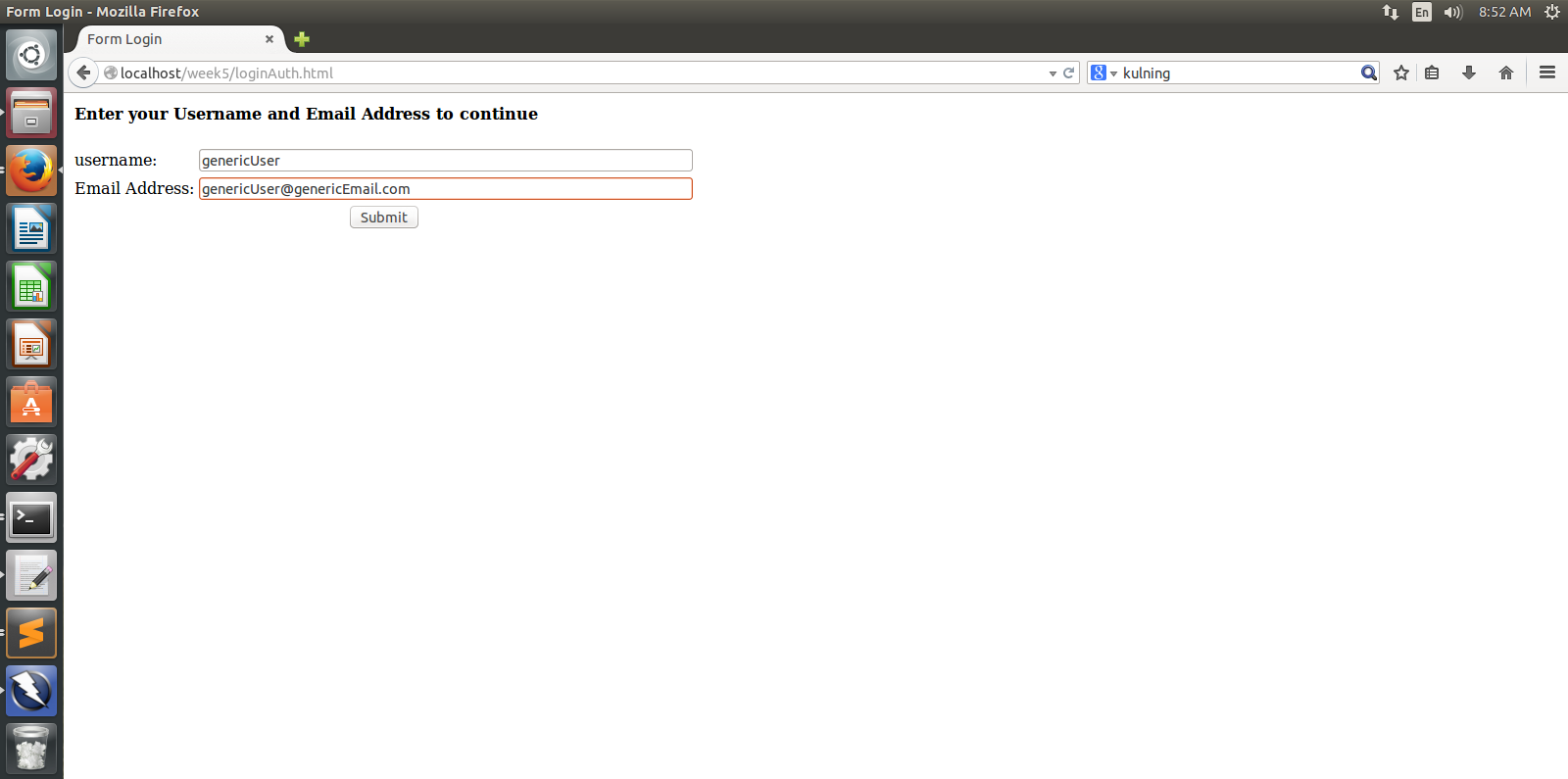
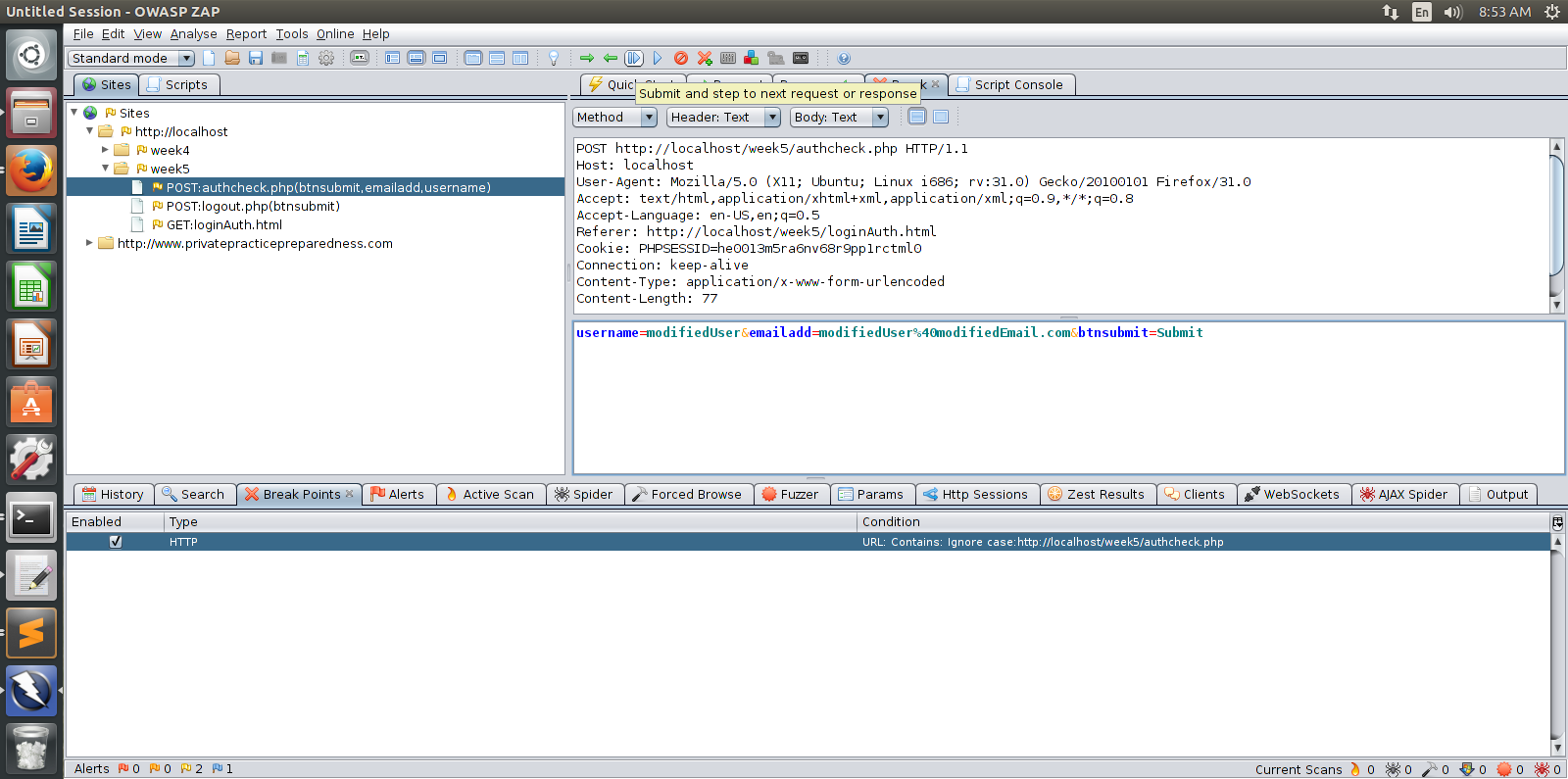
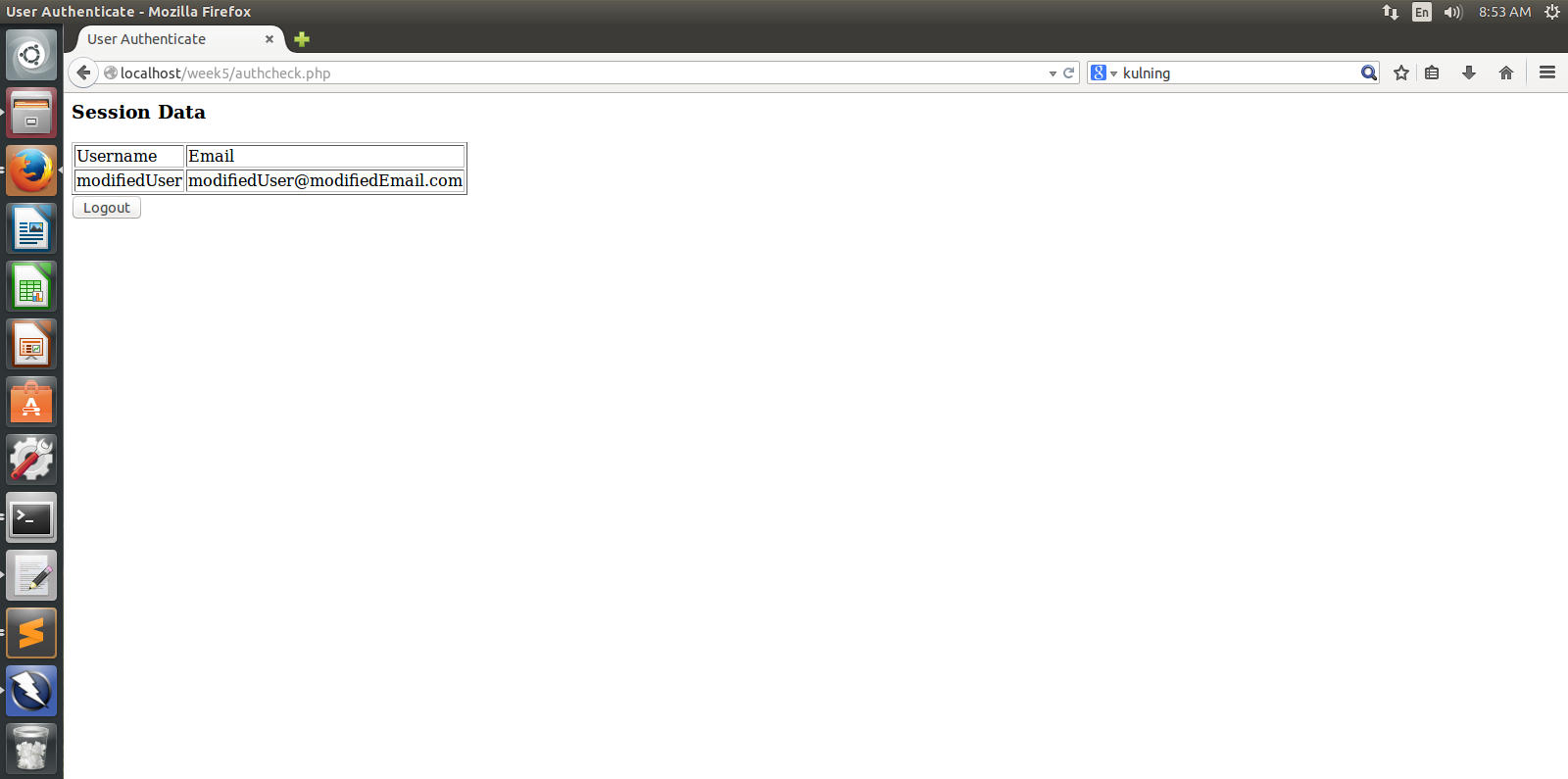
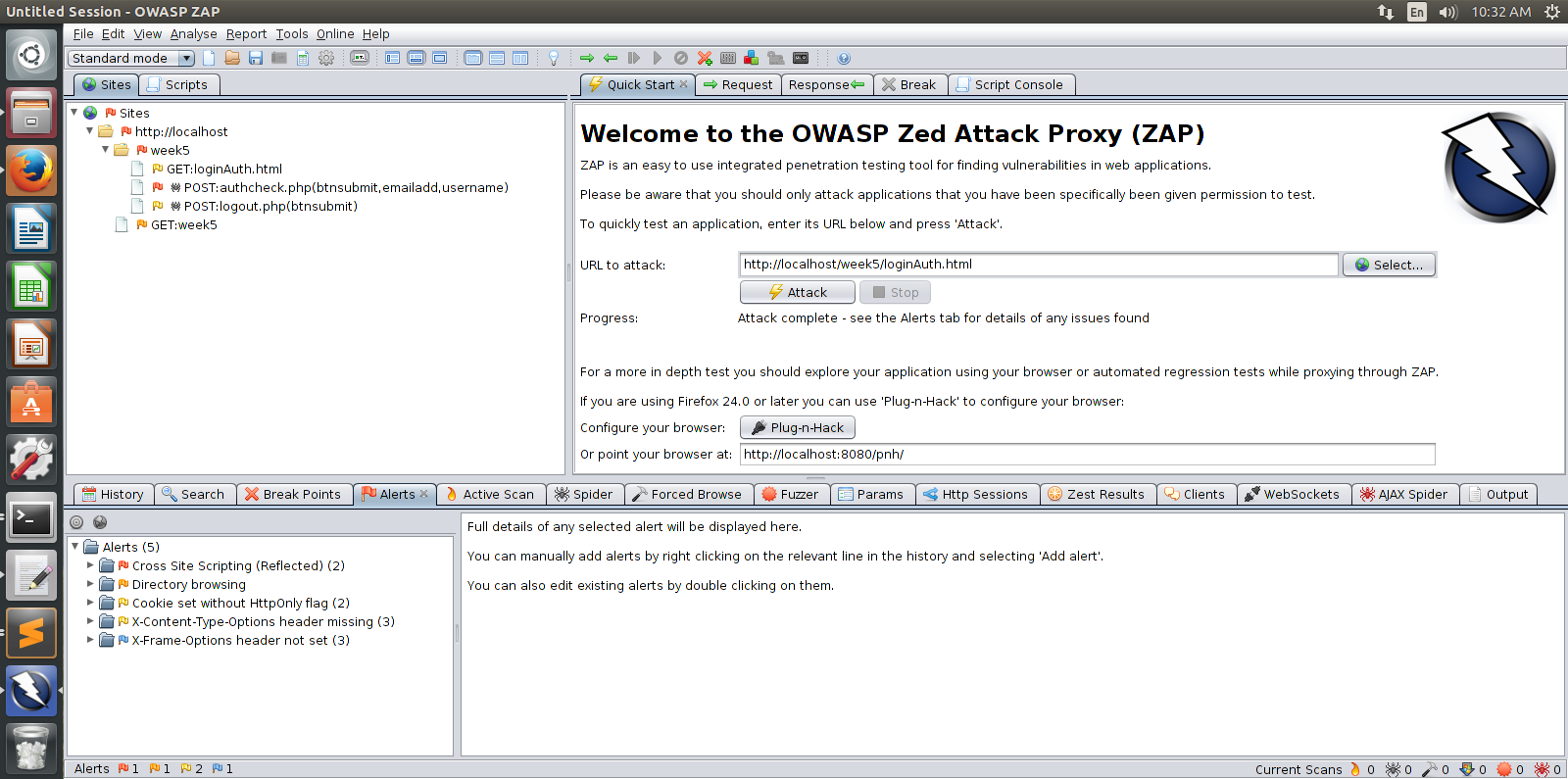
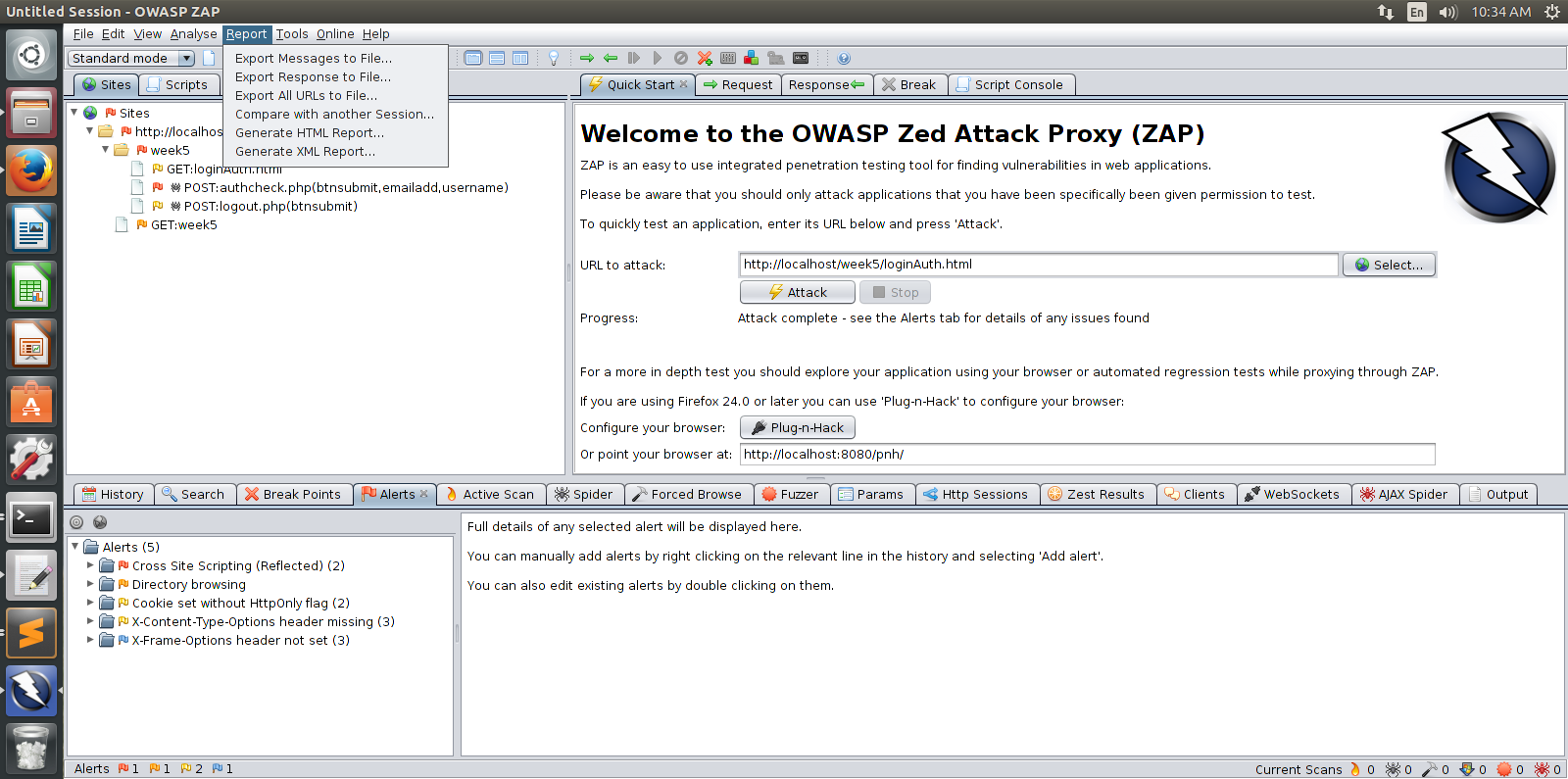
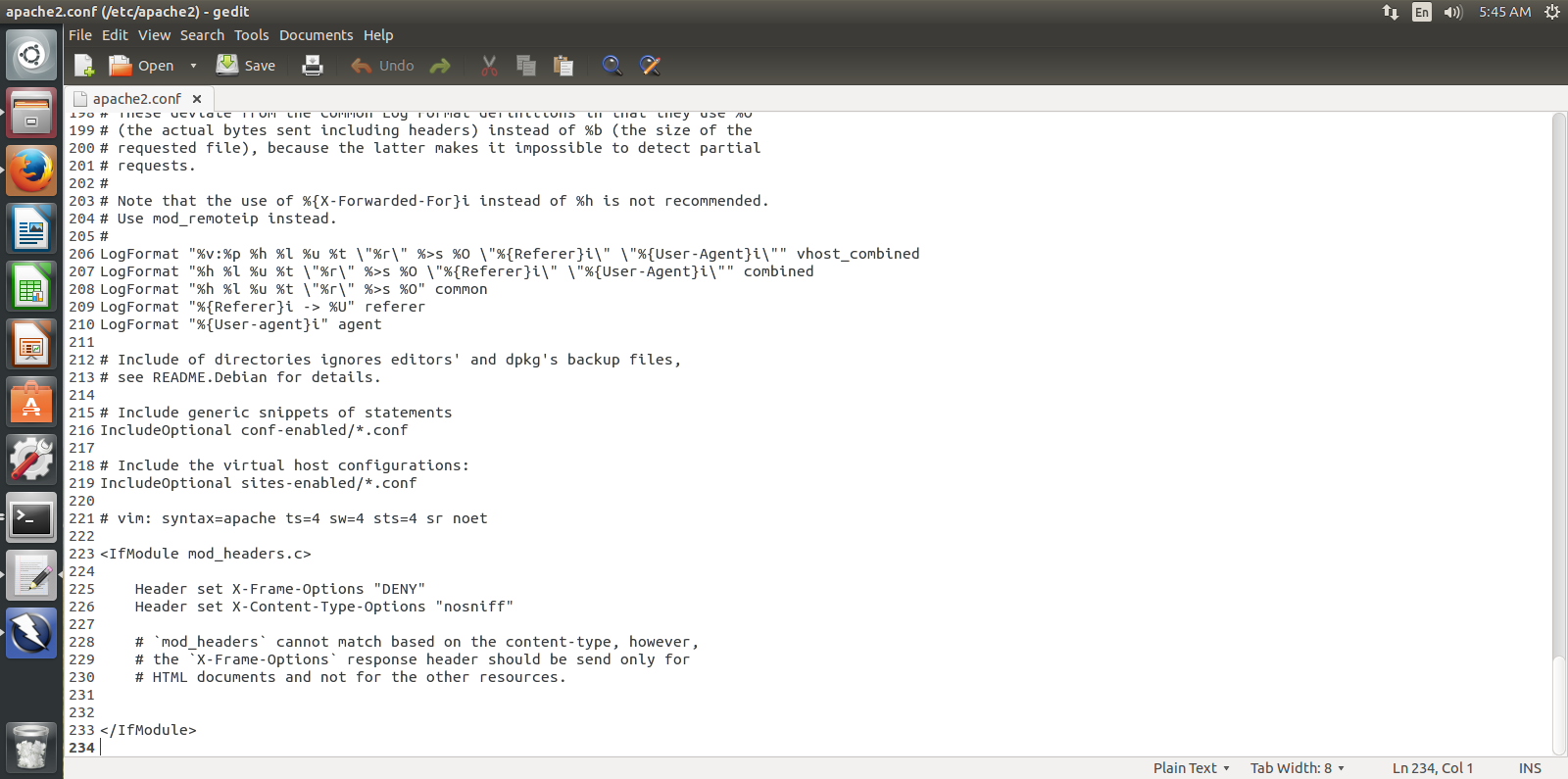
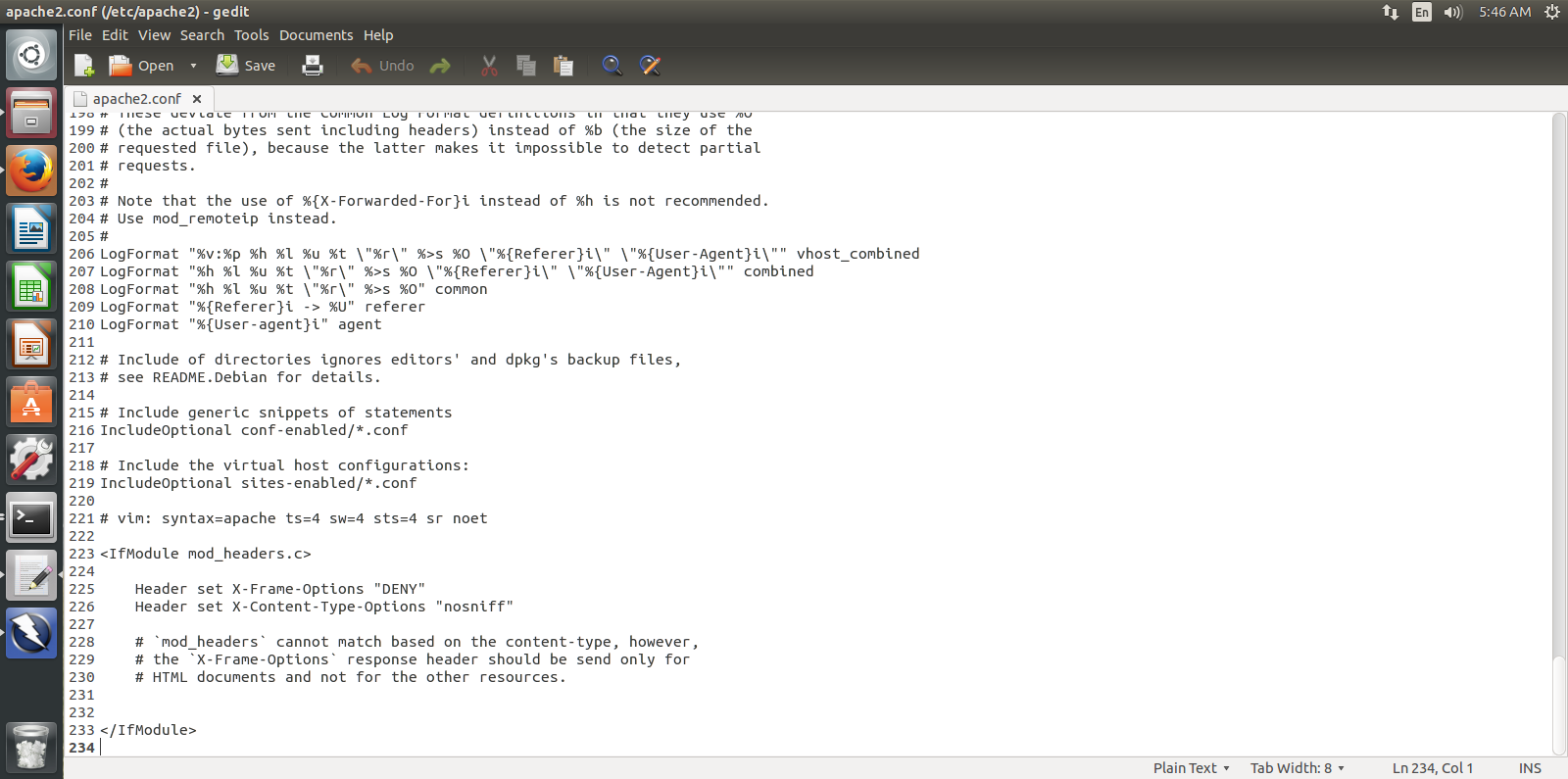
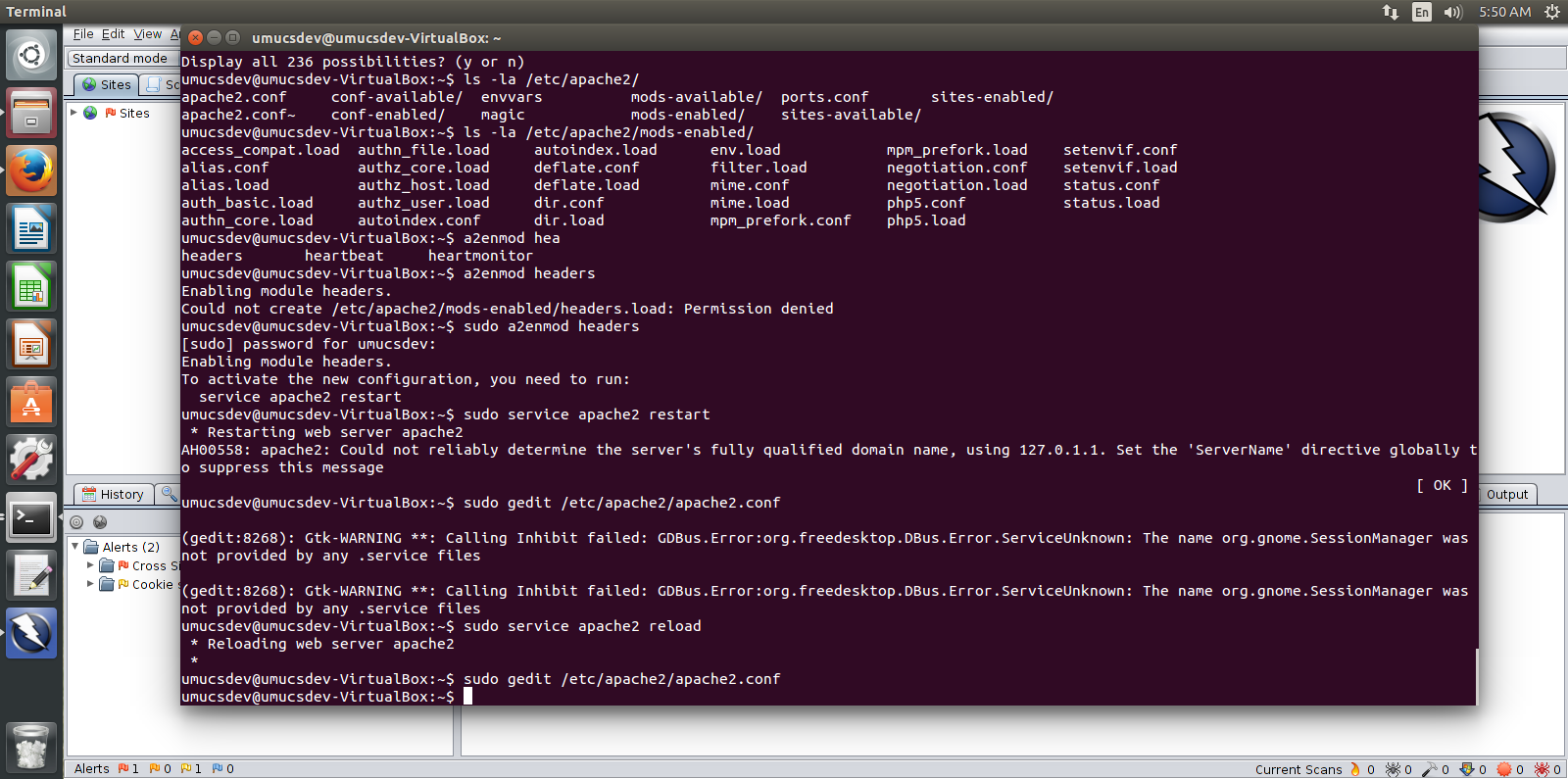
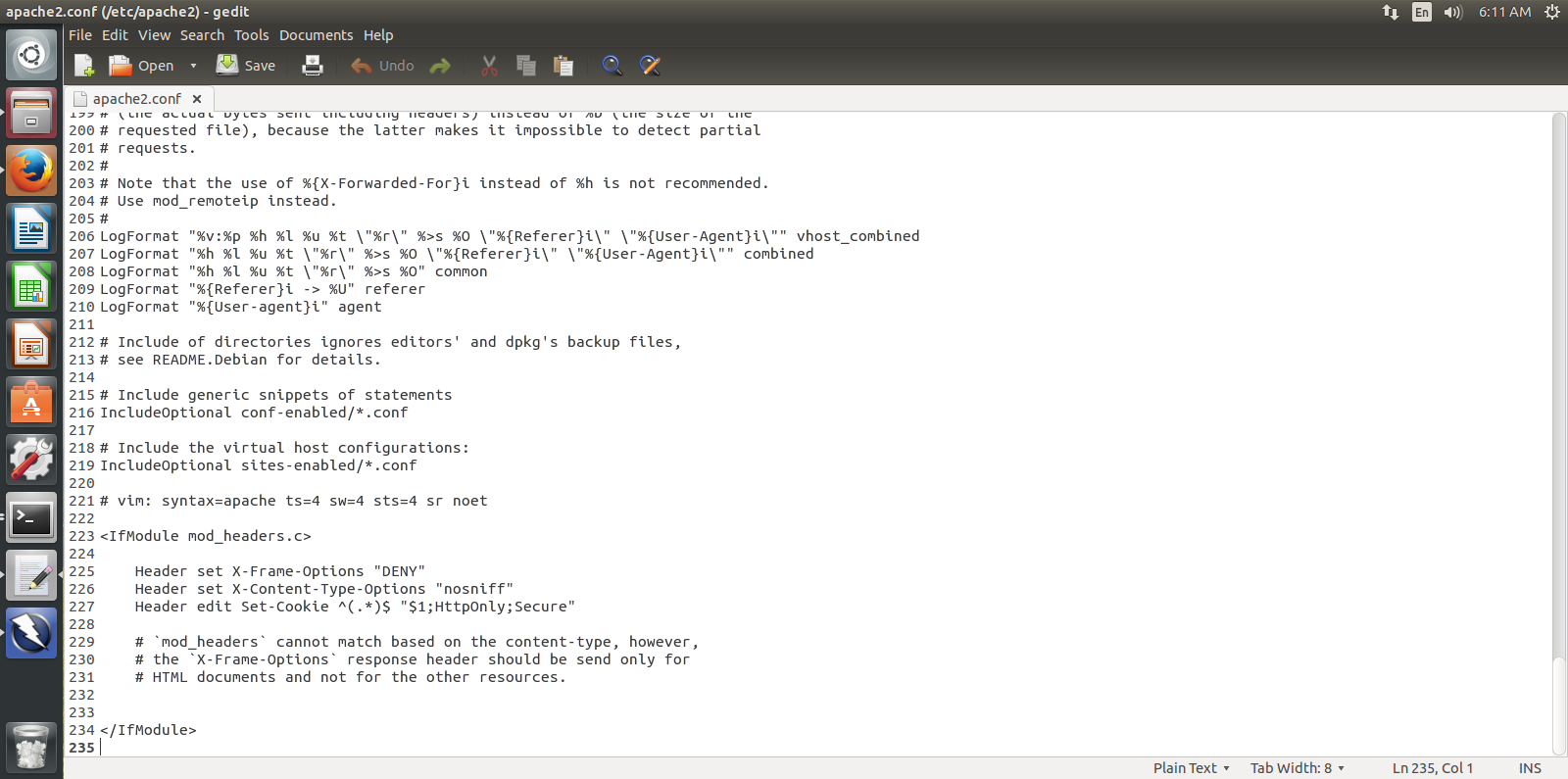
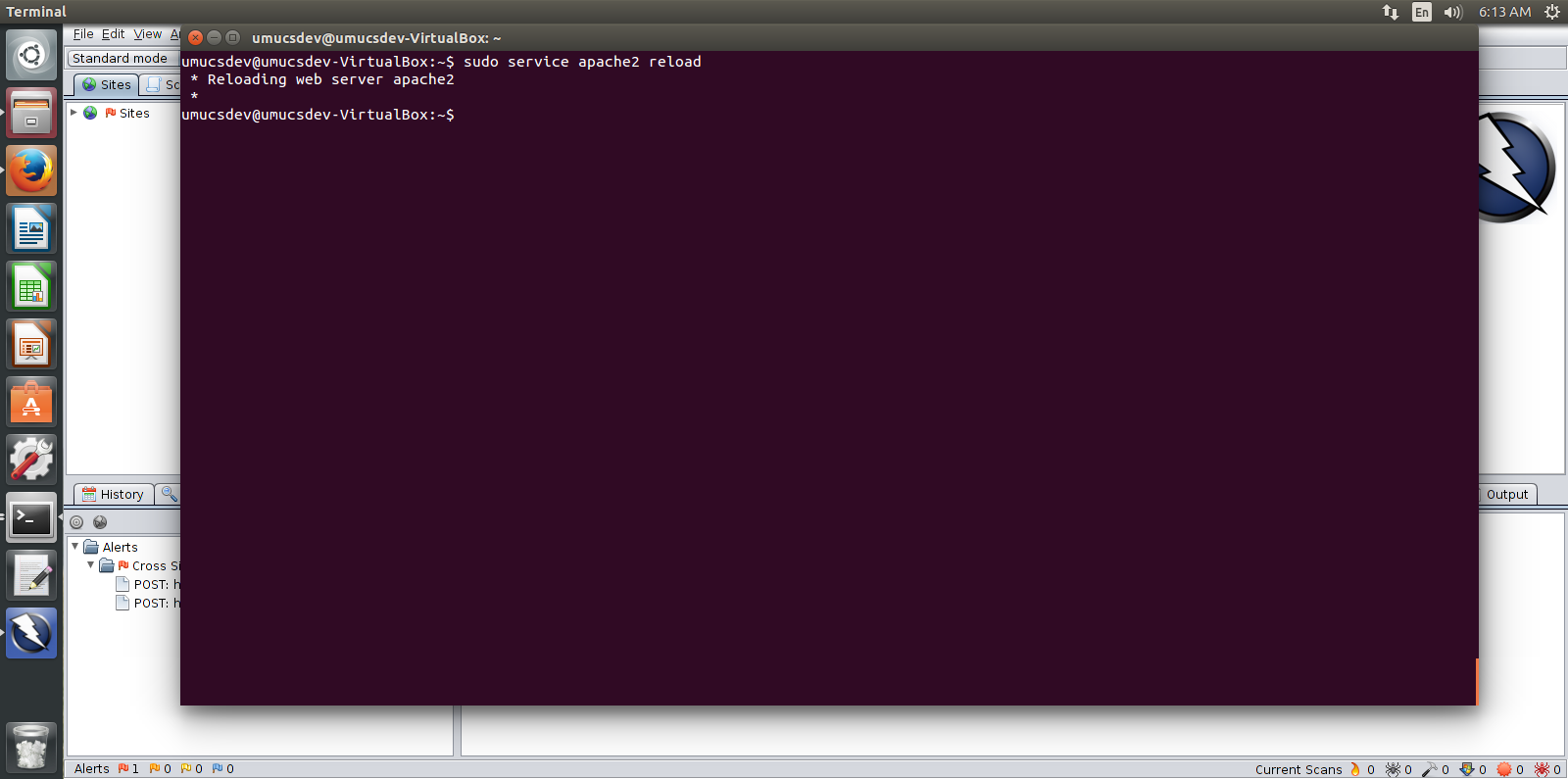
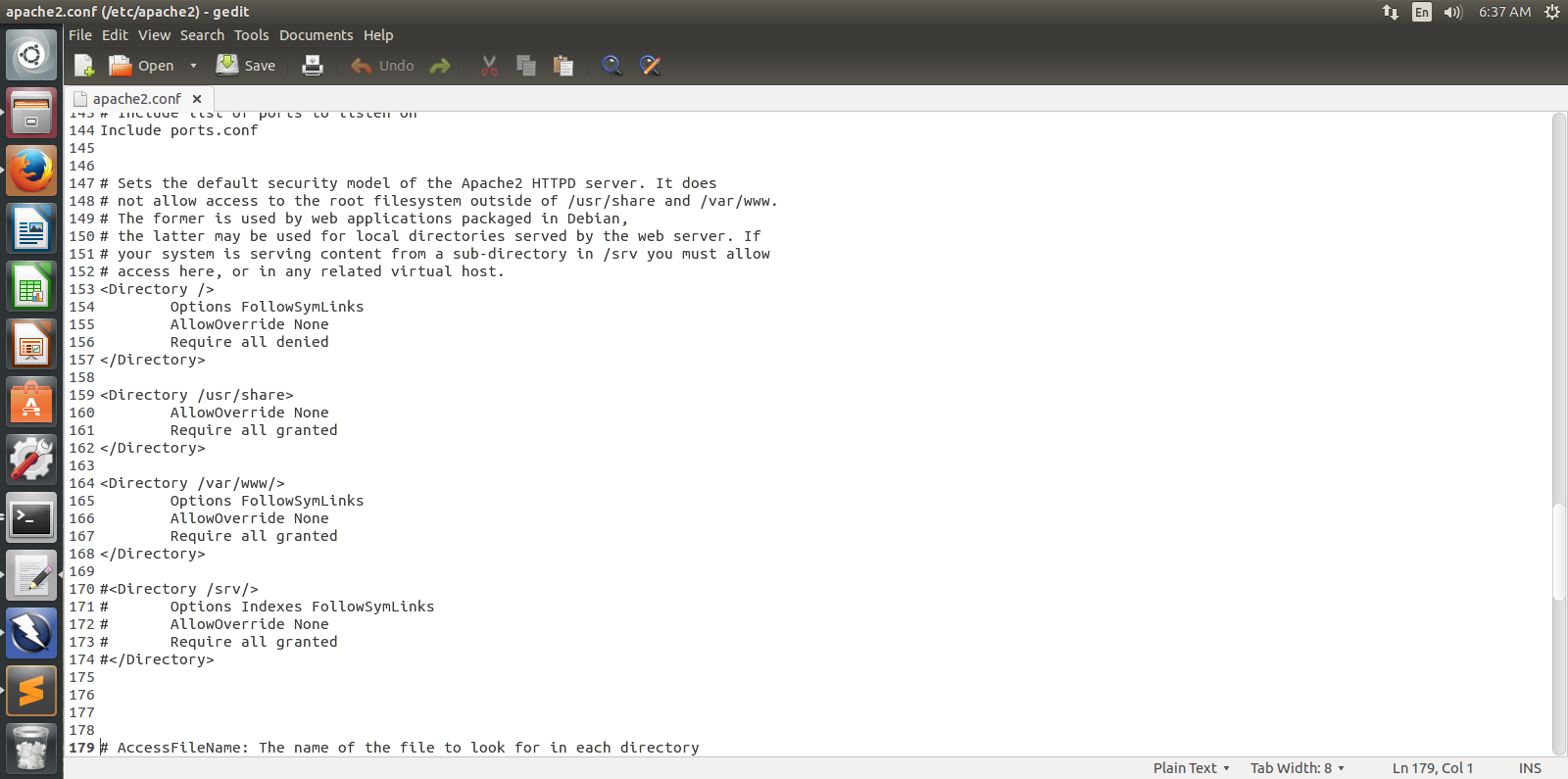
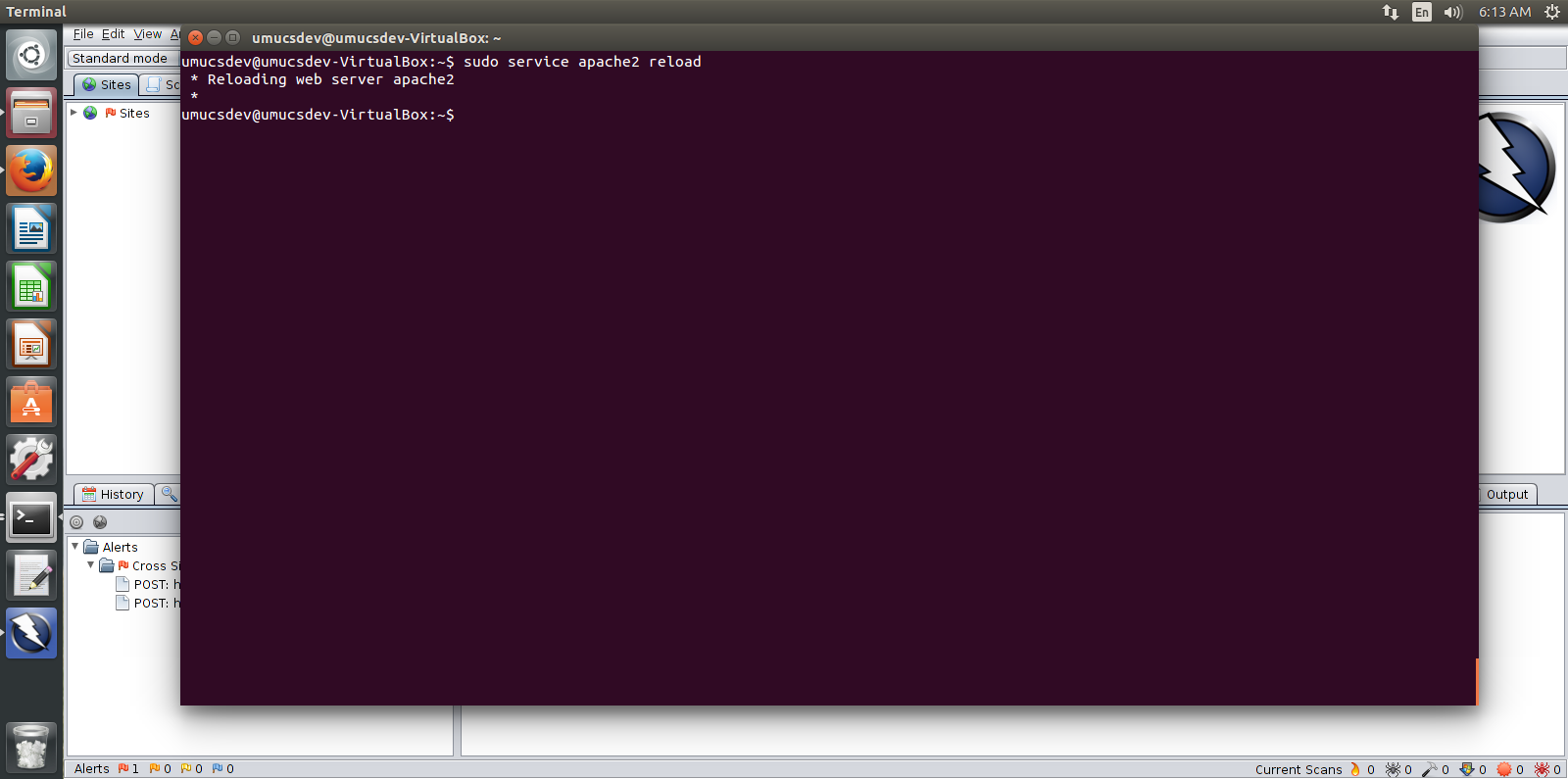
Malachi woodlee

SDEV 300 7981 Building Secure Web Applications

(2178)

November 26, 2017

1. I start with the manual interception test. I have entered a generic user and generic user email address. 
2. After submitting the login info, the login is paused by ZAP at the break point set to the URL http//localhost/…/authcheck.php. The login data is changed. Username is now modifiedUser and the email is modifiedUser@modifiedEmail.com.
3. The data is resent, and the break point released. The modified data is passed through because there is no data verification set up.
4. Next, I started the automatic scanner from the quick start tab. 
5. The automatic scan completed, and I generated an HTML report using the report generator. There were a total of 11 alerts returned.
6. I started by fixing the X-Frame-Options header setting. I can prevent cross-site hijacking by setting the X-Frame-Options header. I am going to set it Deny so that the server will refuse to provide the page to any page using frames.
7. While I am editing the apache2.conf file I will also address the X-Type-Content-Options setting. This setting will prevent scripts from discovering the types of data contained. Thereby stopping any misuse by switching the data for a malicious insertion.
8. I then configured and reloaded the apache2 server. I did this by using the command a2enmod headers, which creates a symlink between the mod\_available and mod\_enable files. The I reloaded the server.
9. Now, it’s time to set the header so that Apache will set all cookies to HttpOnly and Secure. This will prevent attackers from using javascript to steal cookies. Stolen cookies can be used by the cookie’s thief to falsely identify as the cookie’s owner.
10. Reloading the apache2 server to update the new configuration. 
11. Continuing, I now prevent access to the directory index. I edit the apache2.conf file and set the options to only allow access through FollowSymLinks. This prevents accidental discovery of data, or files, by attacker traversing the directory hierarchy rather than through the links provided.
12. Again, reload the server.
13. Finally to fix the final and the most critical alert.