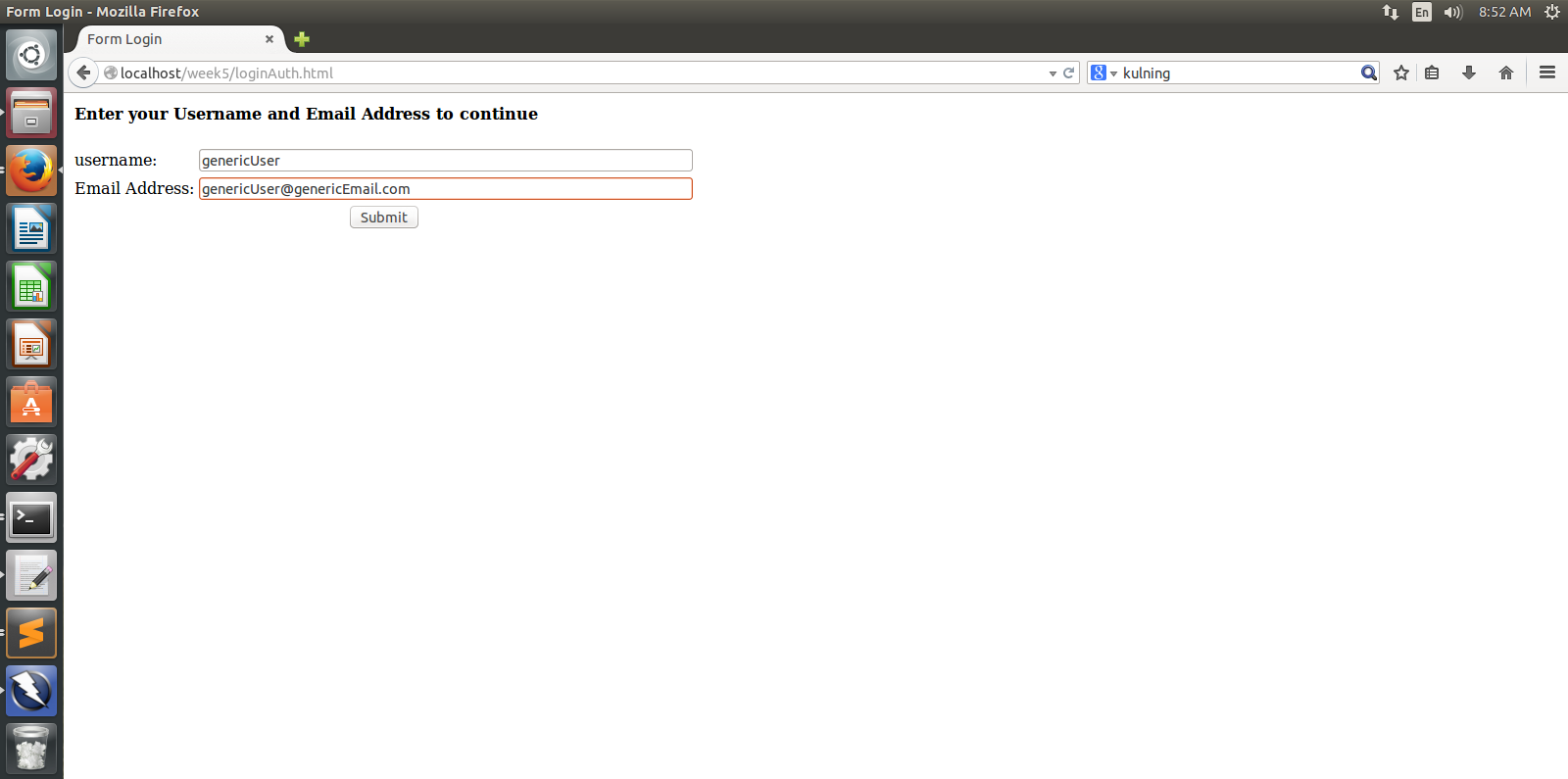
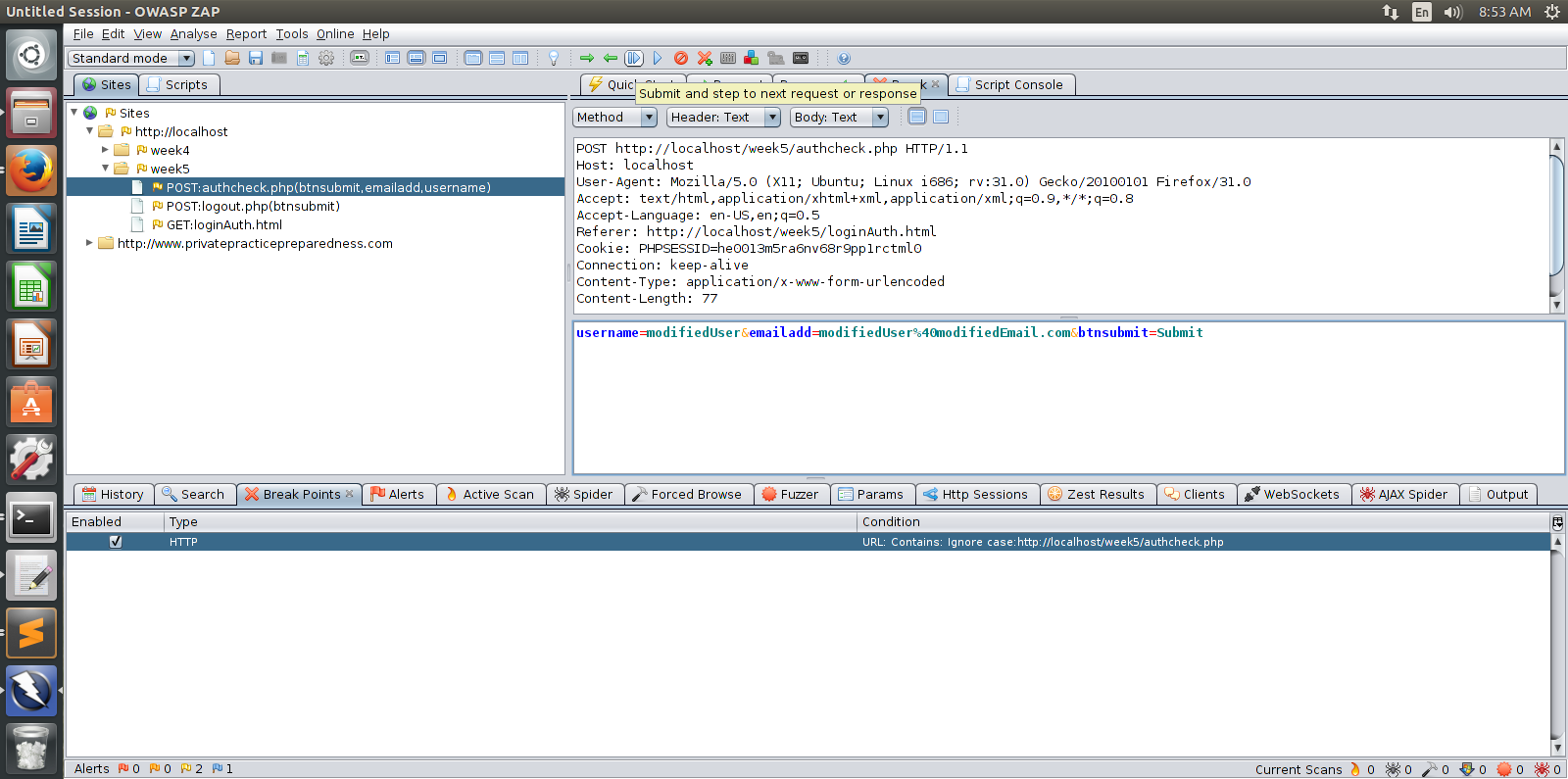
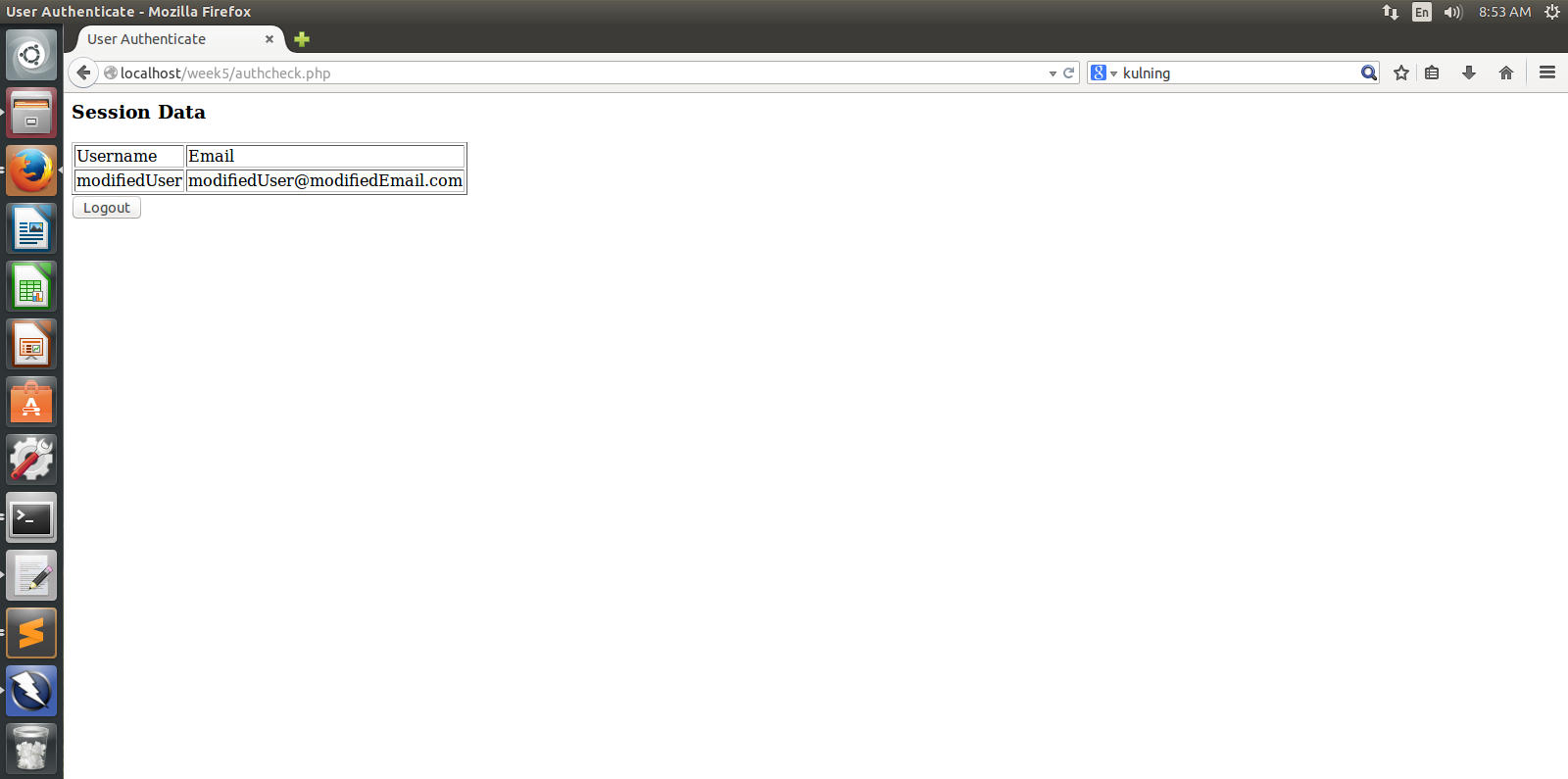
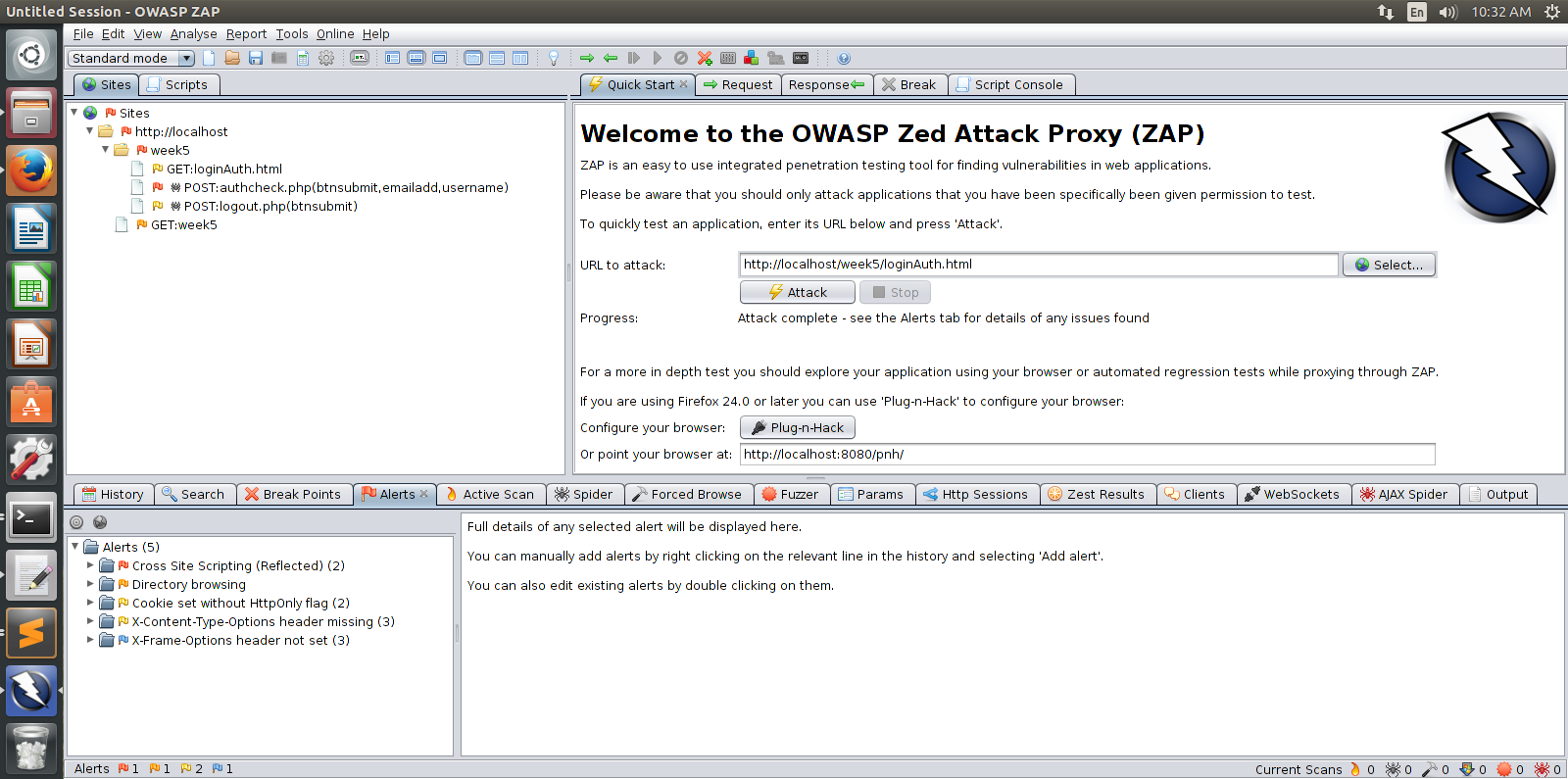
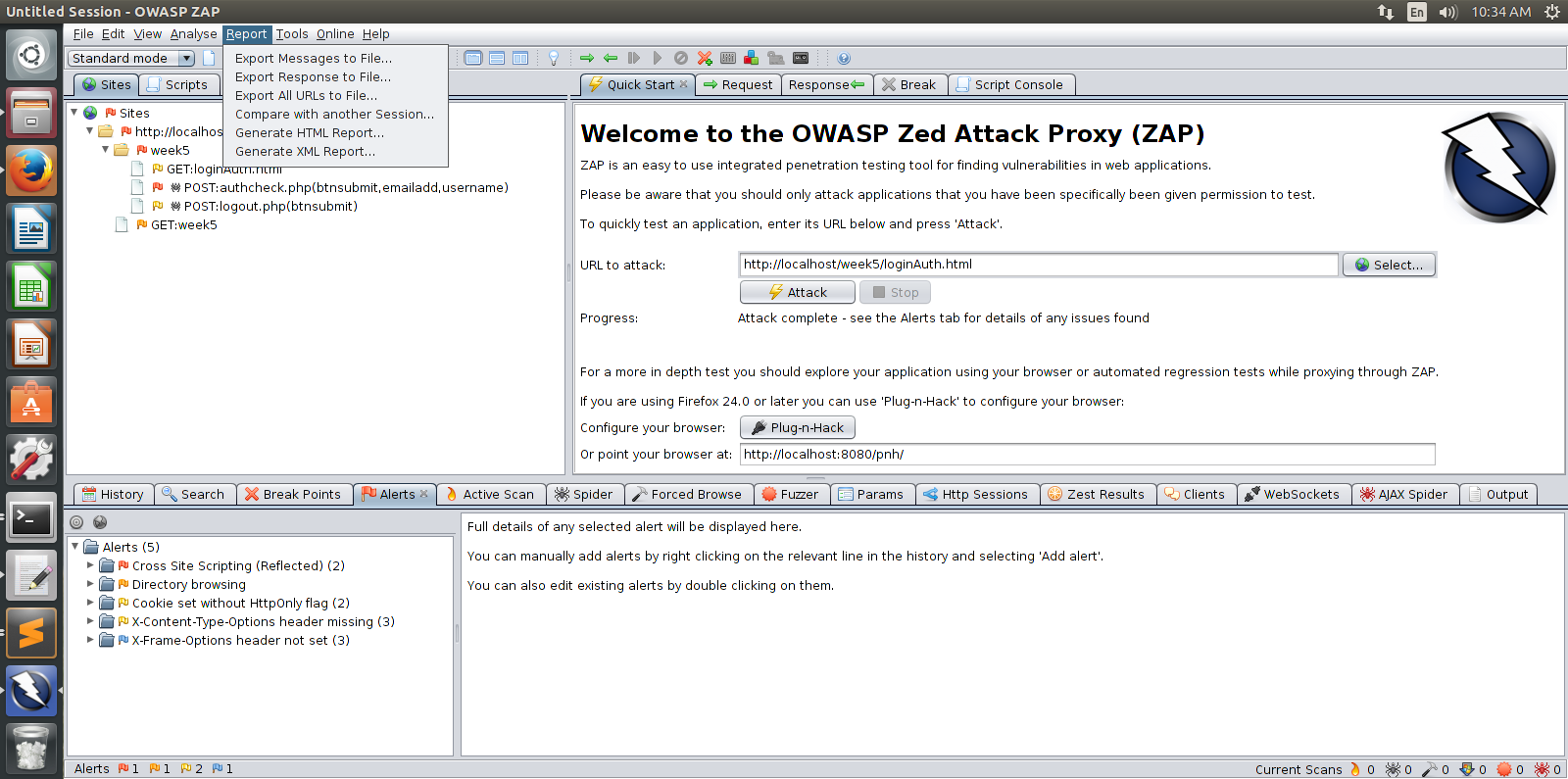
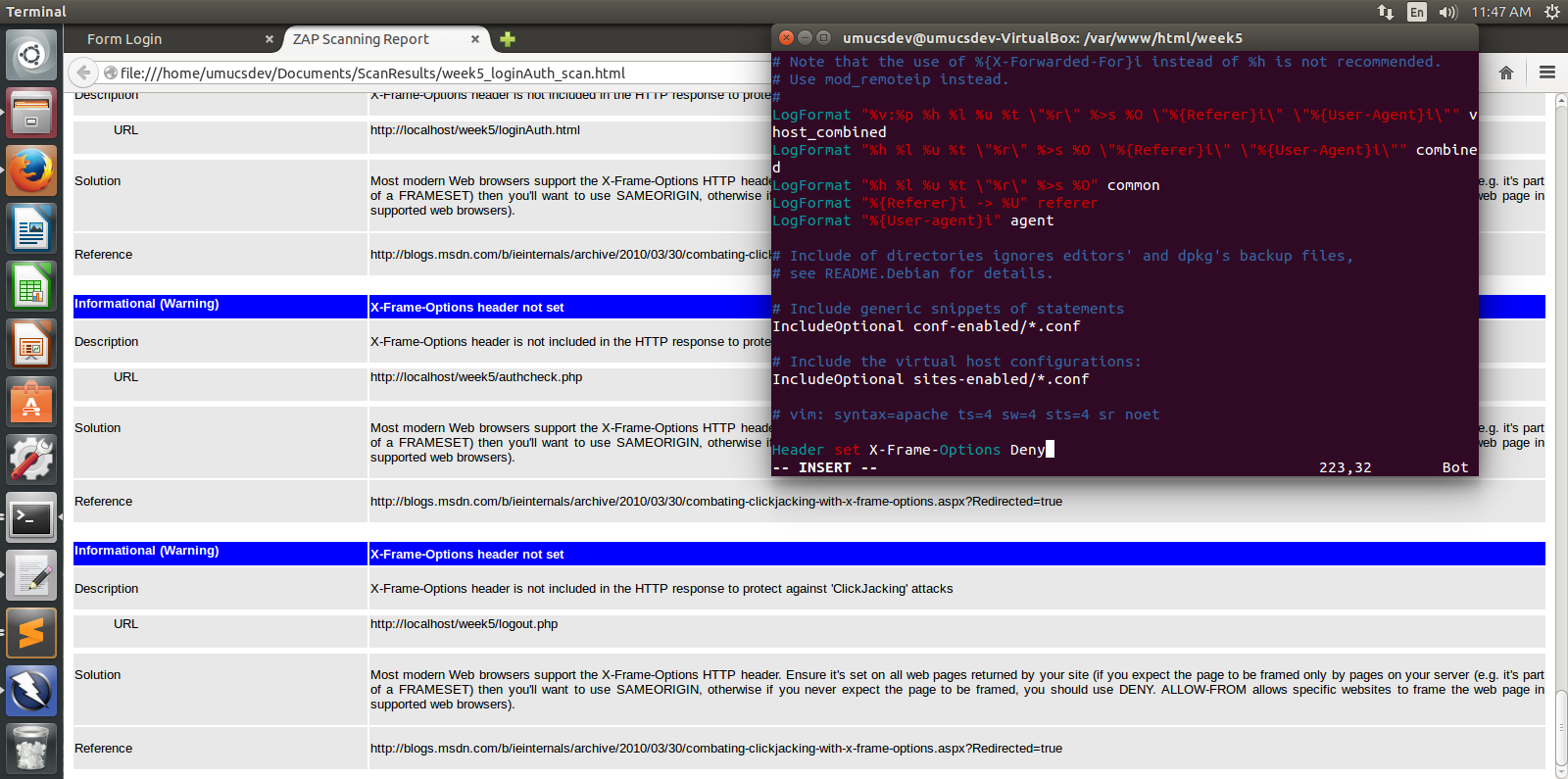
Malachi woodlee

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. Then I will move up the alert level and 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.