Fabio Saurez

Timothy Nguyen

Jessica Yu

Ajay Patel

CIS4930: Mini Project 1 Report

<https://youtu.be/PaA9l9Vfu_c> --> XSS

<https://youtu.be/9ARgHZCu52c> --> Idor

<https://youtu.be/CqTqKnYDftA> --> Cookie

<https://youtu.be/NtoD1xf6PiQ> --> SQL Vul

Our mini-project was compromised of a site that is comprisable by four vulnerabilities which are: XSS, IDOR, Cookie Manipulation and SQL.

The first exploit that we used was our XSS attack, in which a notification allows the site to have a vulnerability due to the possibility of a hacker having the ability to execute arbitrary commands and display arbitrary content in a victim user’s browser. Our XSS attack was accomplished through parsing; in the screencast one can see the hardened site that doesn’t allow a notification would be the site that was not vulnerable.

The second exploit that we used for our site was IDOR; in the text that one user could use their information/access to access another user’s information simply by adjusting the URL. This vulnerability was possible due to the use of sessions as the user is stored in the session rather than passed into the URL. In our screencast, the exploit isn’t possible in the hardened site which is a defense against IDOR related attacks.

The third exploit used for the site was the use of cookie manipulation in which the mitigations were applied through sessions; as sessions have user information stored in that particular session versus passing it to the URL. Cookie manipulation was possible through the inspect element on the webpage and simply changing the username information, this is incredibly dangerous as one could simply change their username to another user’s and have all the information ready.

Our final exploit used for our website was an SQL Injection, that was applied through parsing as well. This exploit allowed for the a specific user to gain access to all other user’s information by using the entry field for execution to dump all the database contents out. In our screencast available, one can see using regular login information will only allow that specific user’s information but once an SQL Injection was applied in the entry field represented through 1 which is true, all the database contents were dumped.