Vulnerability Report for Michael Handlin’s Team:

For the vulnerability analysis of the other team’s server, Craig decided to primarily target the weakness of PHP and SQL as a result. Craig decided to start by looking for tools on how to target SQL injection, to which he didn’t find much in the way of help. He then used NMAP to perform a port scan on the box, to which he found that only port 80 and 22 were available to connect from. He then found some other tools that could help, the most helpful of which was a browser extension (and penetration testing kit) named ‘Penetration Testing Kit’. It is developed by OWASP (Open Web Application Security Project) and has a variety of tools within it to help penetration testers create more secure web apps. He decided to use that tool because of how expansive the options are and because it was relatively easy to learn. While using it, he found that the website ran on an old version of Javascript, which allowed cross-site scripting. Craig also attempted some SQL injection, which also proved unsuccessful. He was pleasantly surprised as to the state of the server’s security. Craig found it hard to do a successful SQL injection attack and the XSS vulnerabilities do not require any urgent changes to prevent the box from being compromised and thankfully they made it impossible to exploit outdated protocols and connections such as Telnet.

Phuc also made an attempt with NMAP to ping any vulnerabilities but none were to be found. He also tried the Hydra tool to attack by brute force but came to a dead end with that as well. Jessica made an attempt at a type of social engineering/phishing attack by using the netcat command which would allow us to enter their box without being detected by the firewall. Netcat essentially requires a remote administration tool to be installed into the other user’s server so as to provide a connection that is being requested by the other server to ours. Therefore, since this is a server we had to use a VPN for, she wasn't able to find a way to get the remote admin tool on the other server. Due to this, netcat wasn’t a successful tool either.