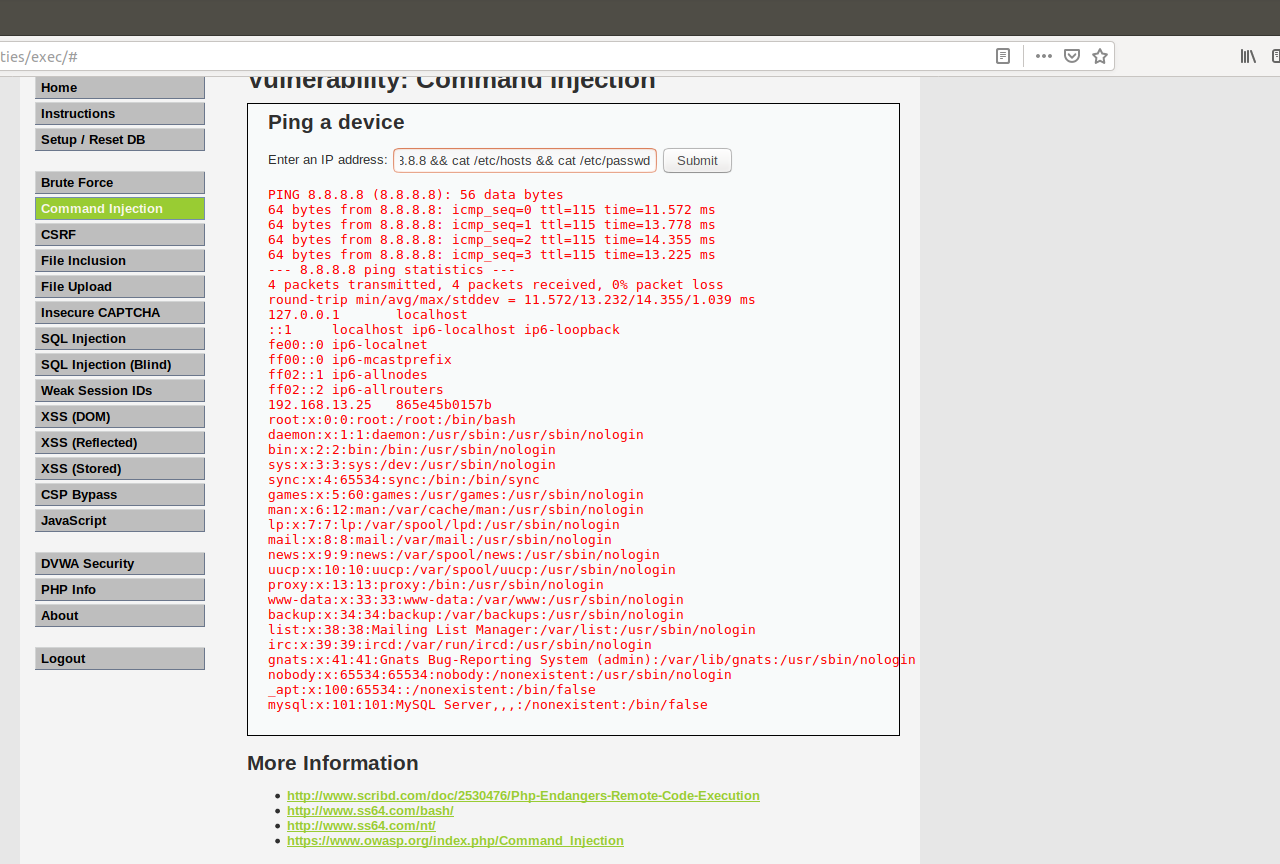
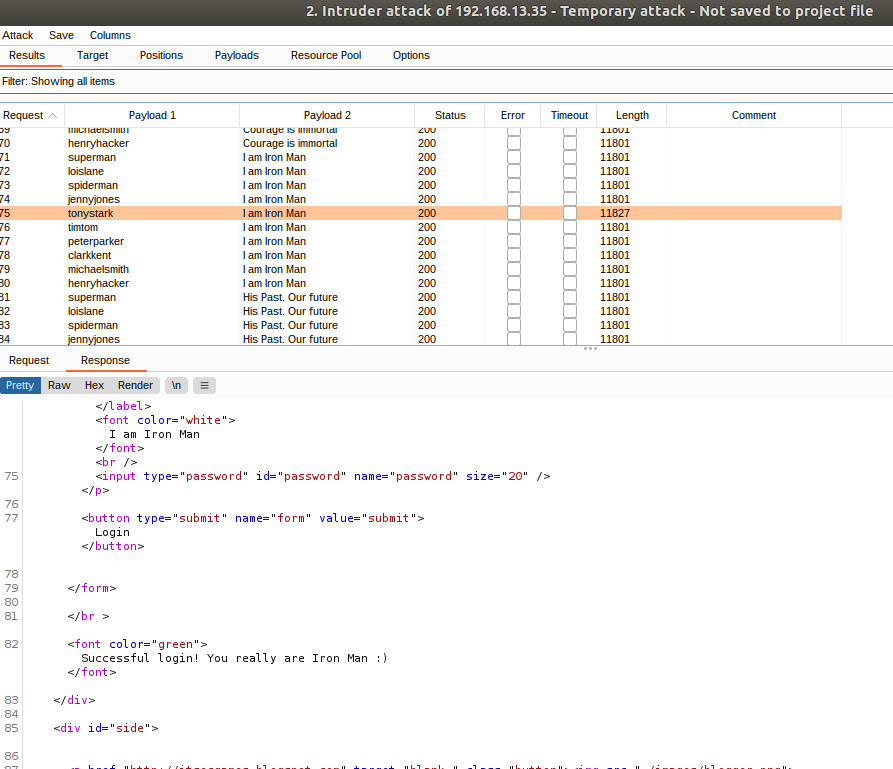
Task #1



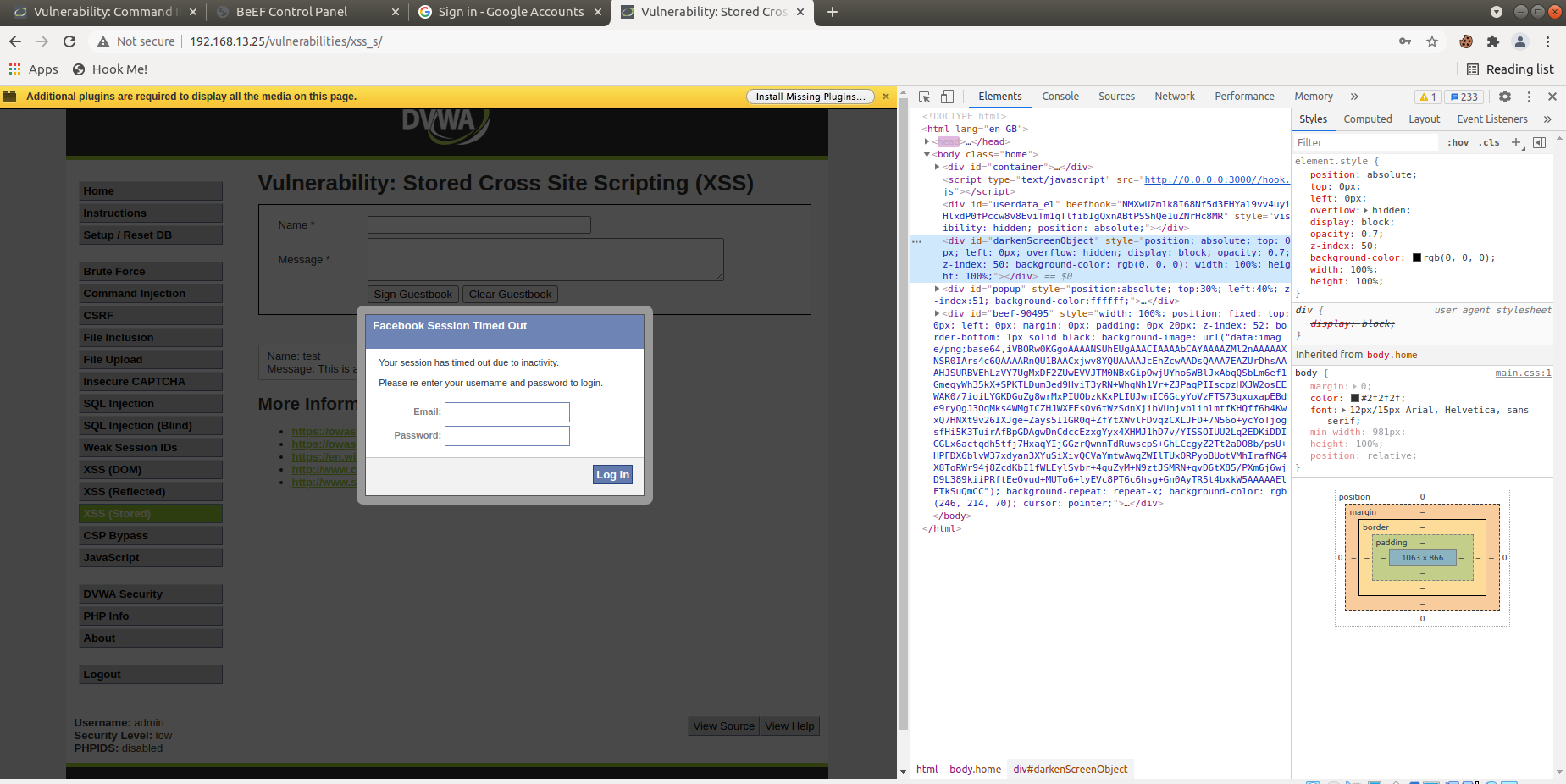
Some ways to mitigate cross site scripting is to not allow HTML code inputs, sanitize your data and to use a web app firewall. With those, another strategy would be to regularly pen test your network to find the holes and to patch them.

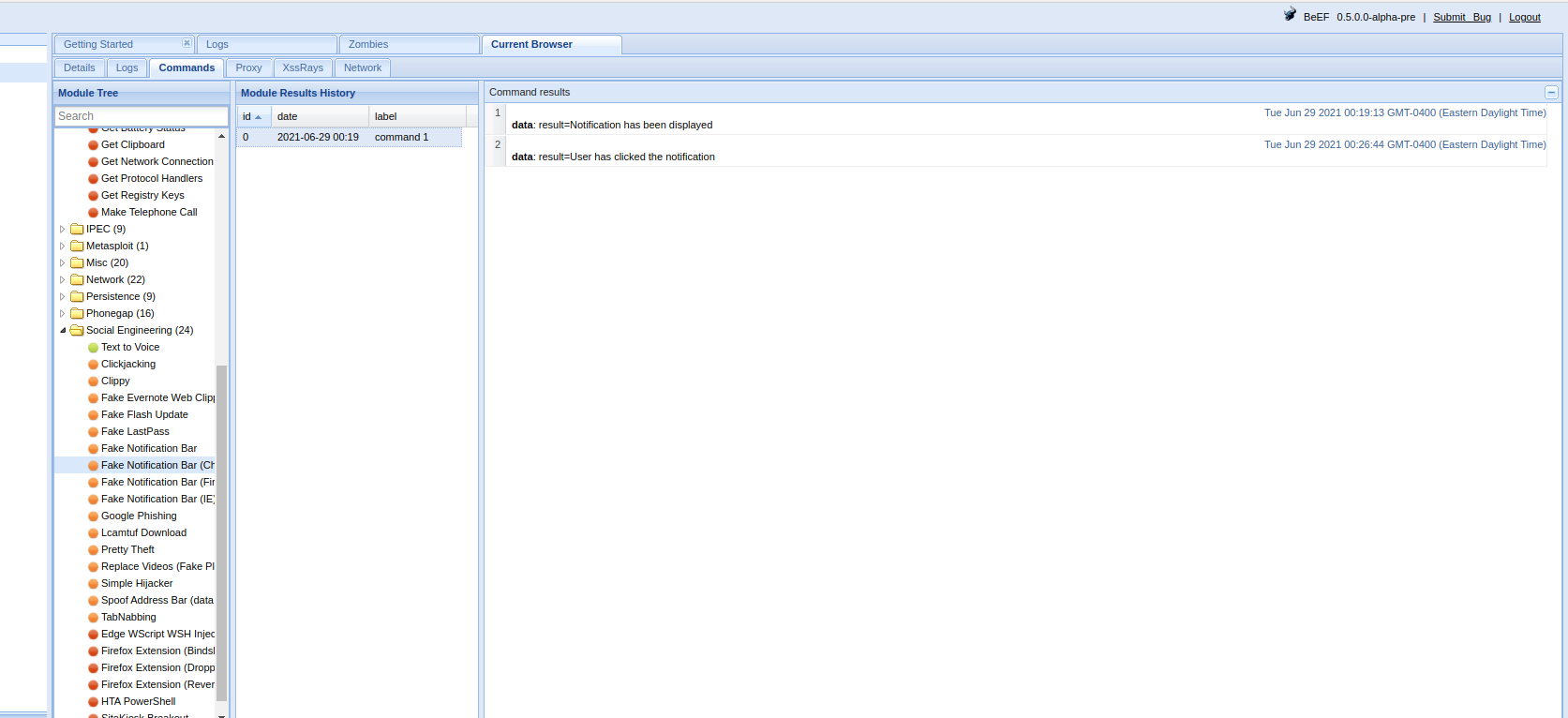
Task #2



For an attack like this there are a few different mitigation strategies including locking out the account after so many attempts or multi-factor authentication. This exercise did not use a huge pool to pull from but each username was tried 10 different times in a couple of seconds which is typically not normal so things like getting locked out after 3-5 failed attempts would help mitigate this threat. Another is multi-factor authentication, so having a secondary account to “ok” the sign in would help alert people of an attempted hack.

Task #3





Some mitigation strategies for an attack like this is to try to keep up on phishing training, having a strong and up to date firewall, or only allowing employees onto trusted and predetermined sites while on the company network. This type of attack can happen anytime an employee clicks on a bad link or goes to a hooked/zombie site so stopping them from going to said sites or keeping up on training to not click on links should help deter attacks like this.