Cybersecurity

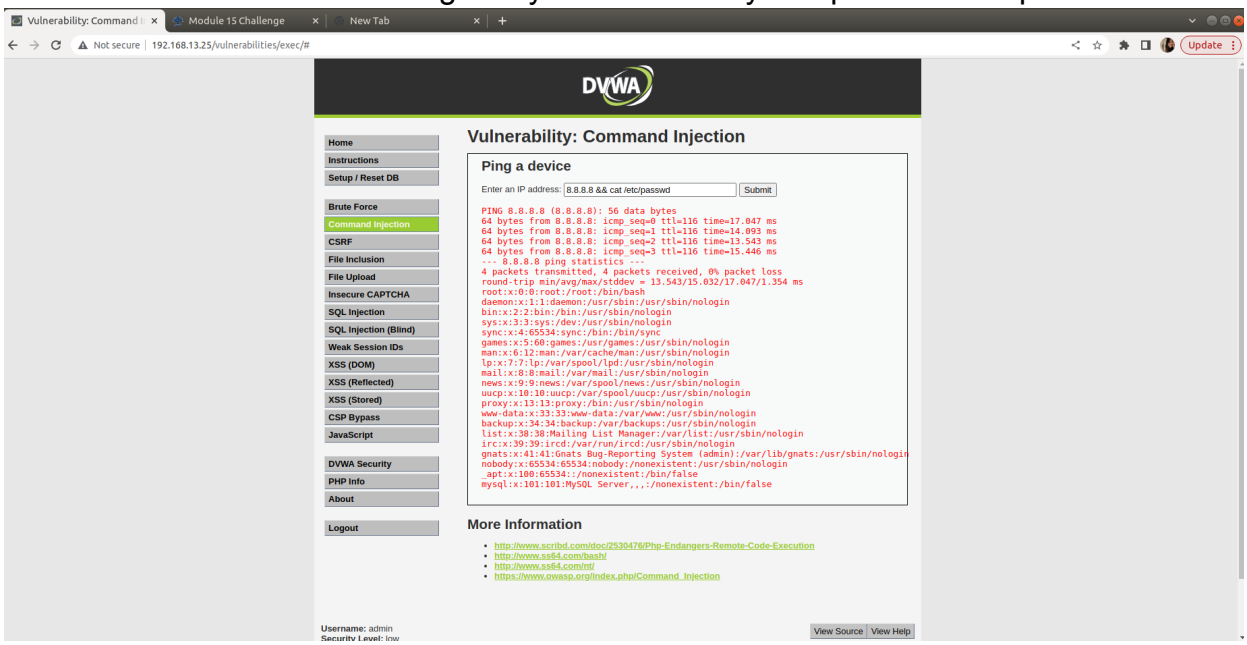
Module 15 Challenge Submission File

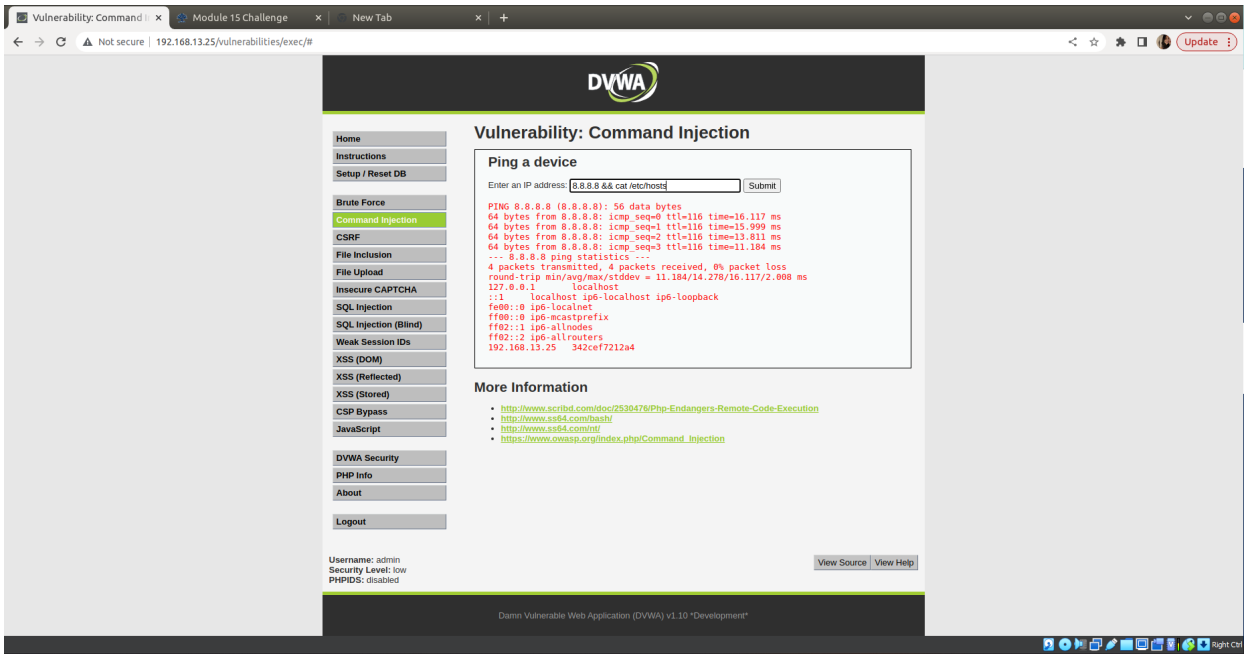
Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:



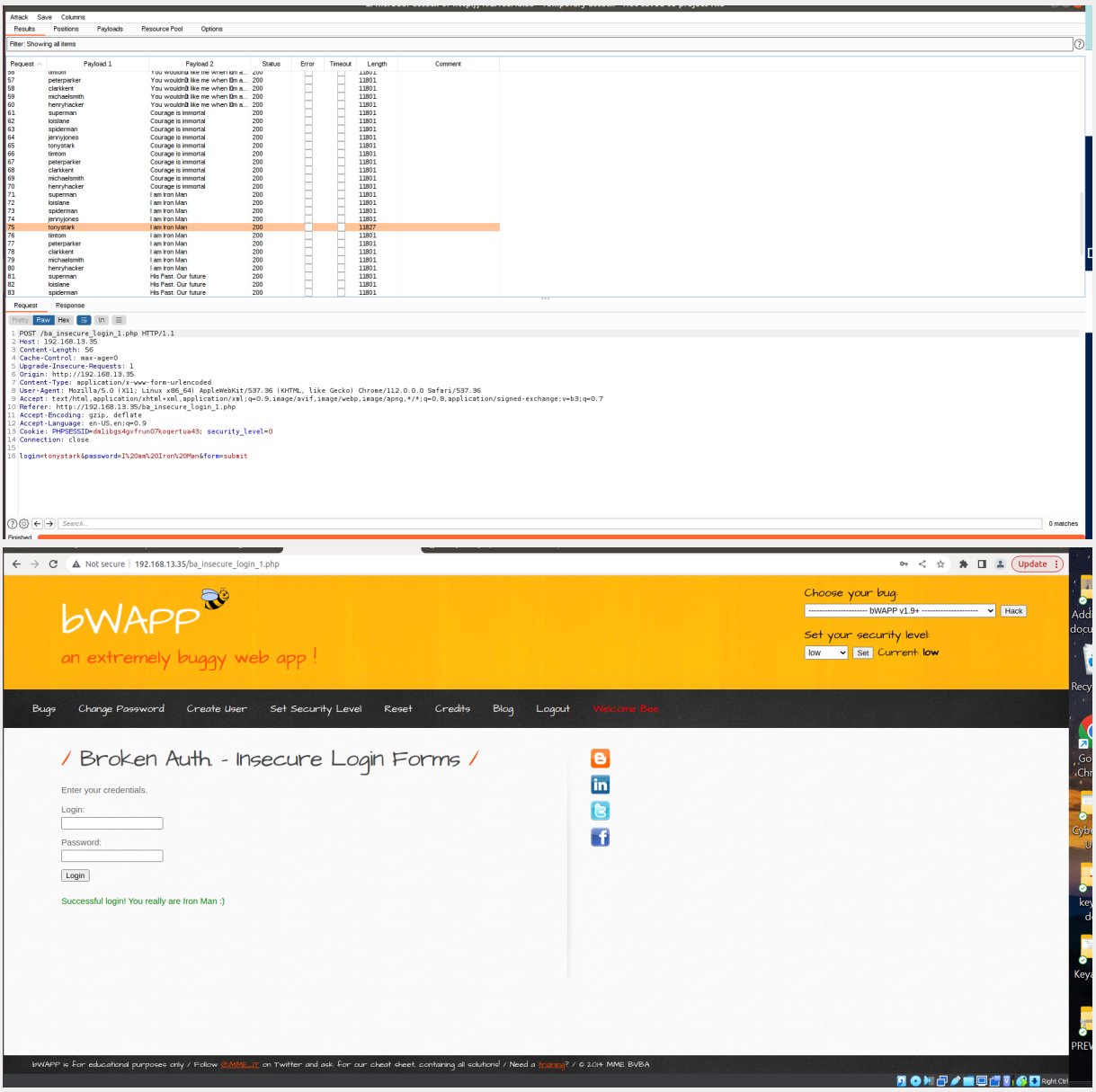


Write two or three sentences outlining mitigation strategies for this vulnerability:

This vulnerability of Command Injection can be mitigated by avoiding to run the system Commands with User-Supplied Input.Additionally, it is viable to use strong Commands that will validate the passed input data and to make sure that we test our applications and patch any errors and vulnerabilities on a daily basis.

Web Application 2: *A Brute Force to Be Reckoned With*

Provide a screenshot confirming that you successfully completed this exploit:

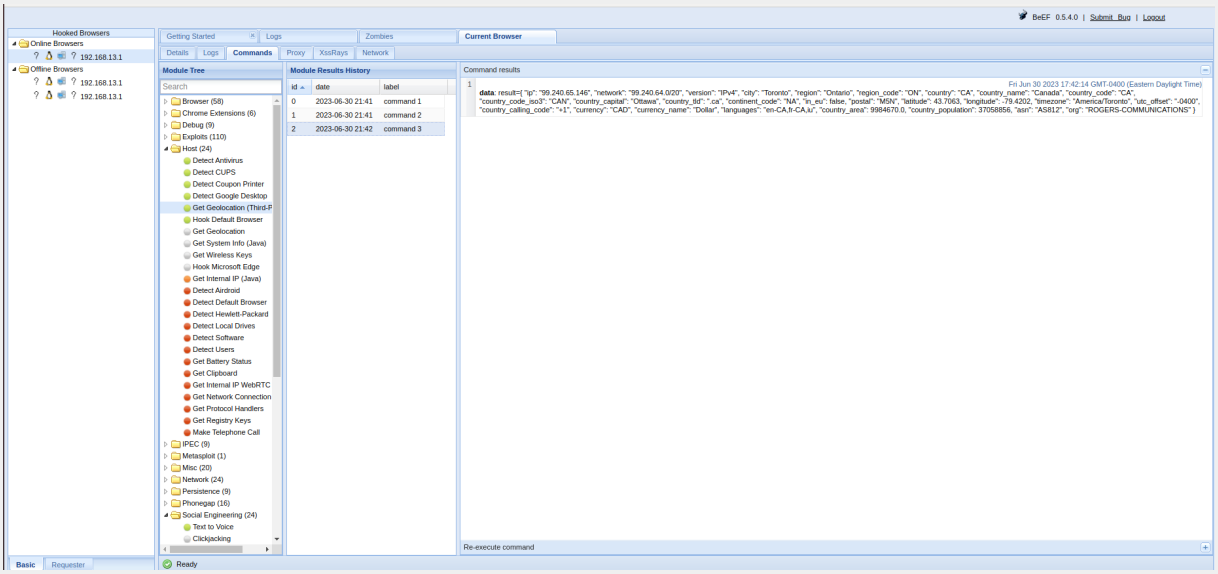


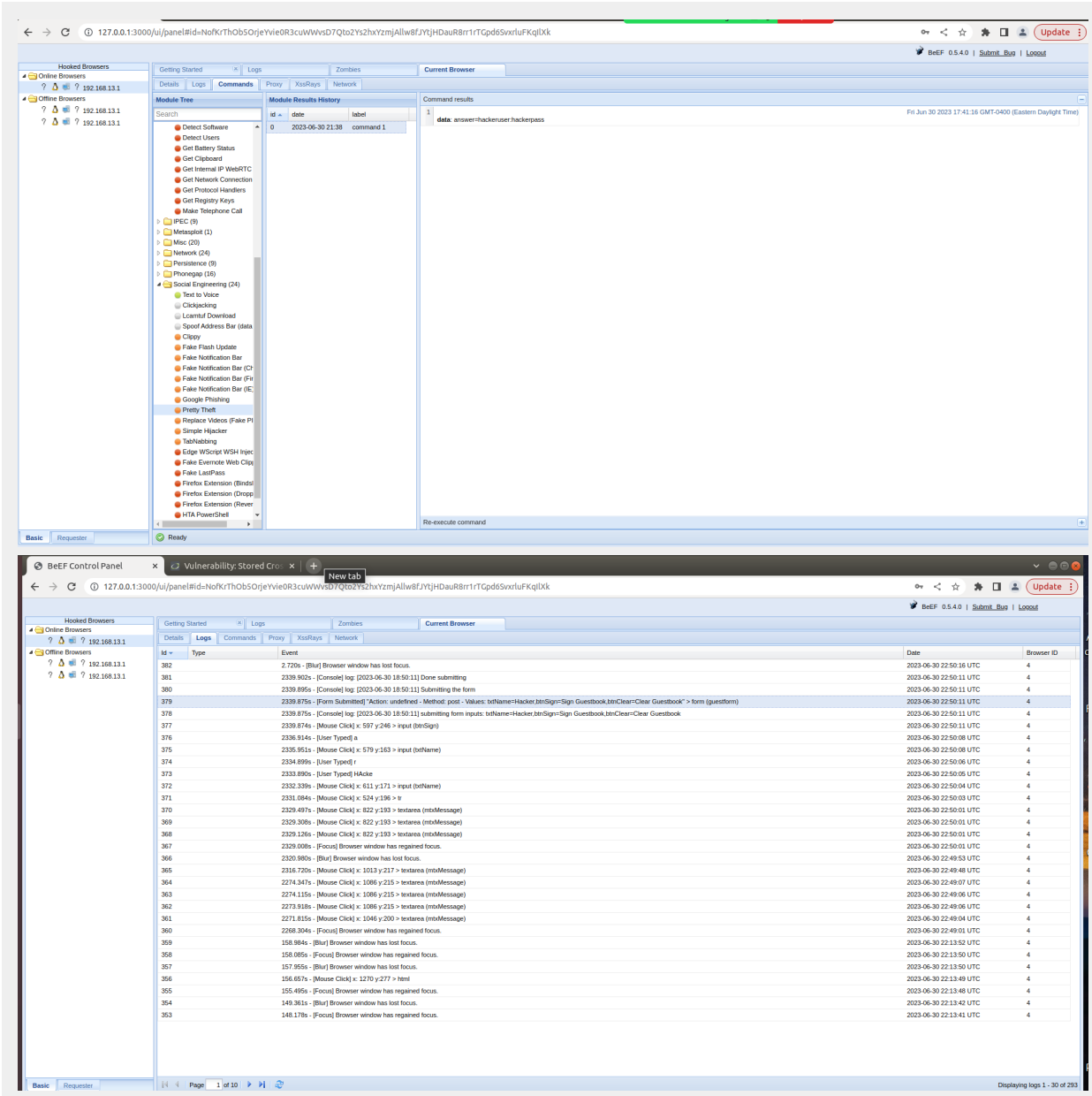
Write two or three sentences outlining mitigation strategies for this vulnerability:

The Brute Force attacks are the most common and harmful types of attacks. One of the most commonly used methods of mitigation is to lock out accounts after a defined number of incorrect password attempts and another is to Employ CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), this will prevent from brute force attack and will make sure that it is a human/user attempting to login.

Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:





Write two or three sentences outlining mitigation strategies for this vulnerability:

To prevent this XSS attacks,it is extremely recommended to make sure that the application validates all and any kind of data imputed, making sure that the data which is being processed is amongst the allowlisted data. This will also make sure that all variable output in a page which has been returned to the user is encoded.