| 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:

| In order to mitigate the risk, we need to whitelist acceptable characters and reject special characters. In this particular case we could limit possible input length. |
| --- |

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

Provide a screenshot confirming that you successfully completed this exploit:

|  |
| --- |

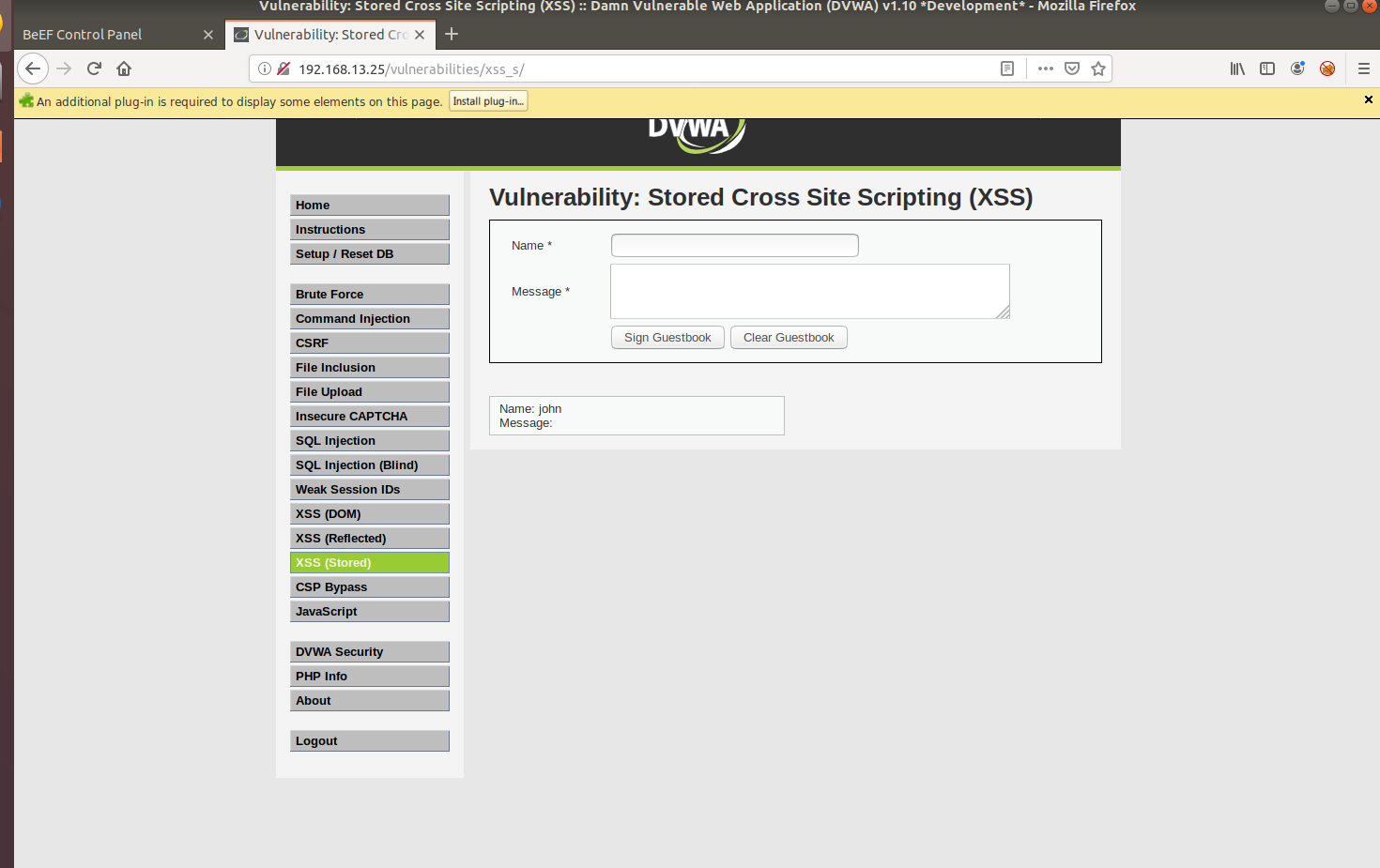
Write two or three sentences outlining mitigation strategies for this vulnerability:

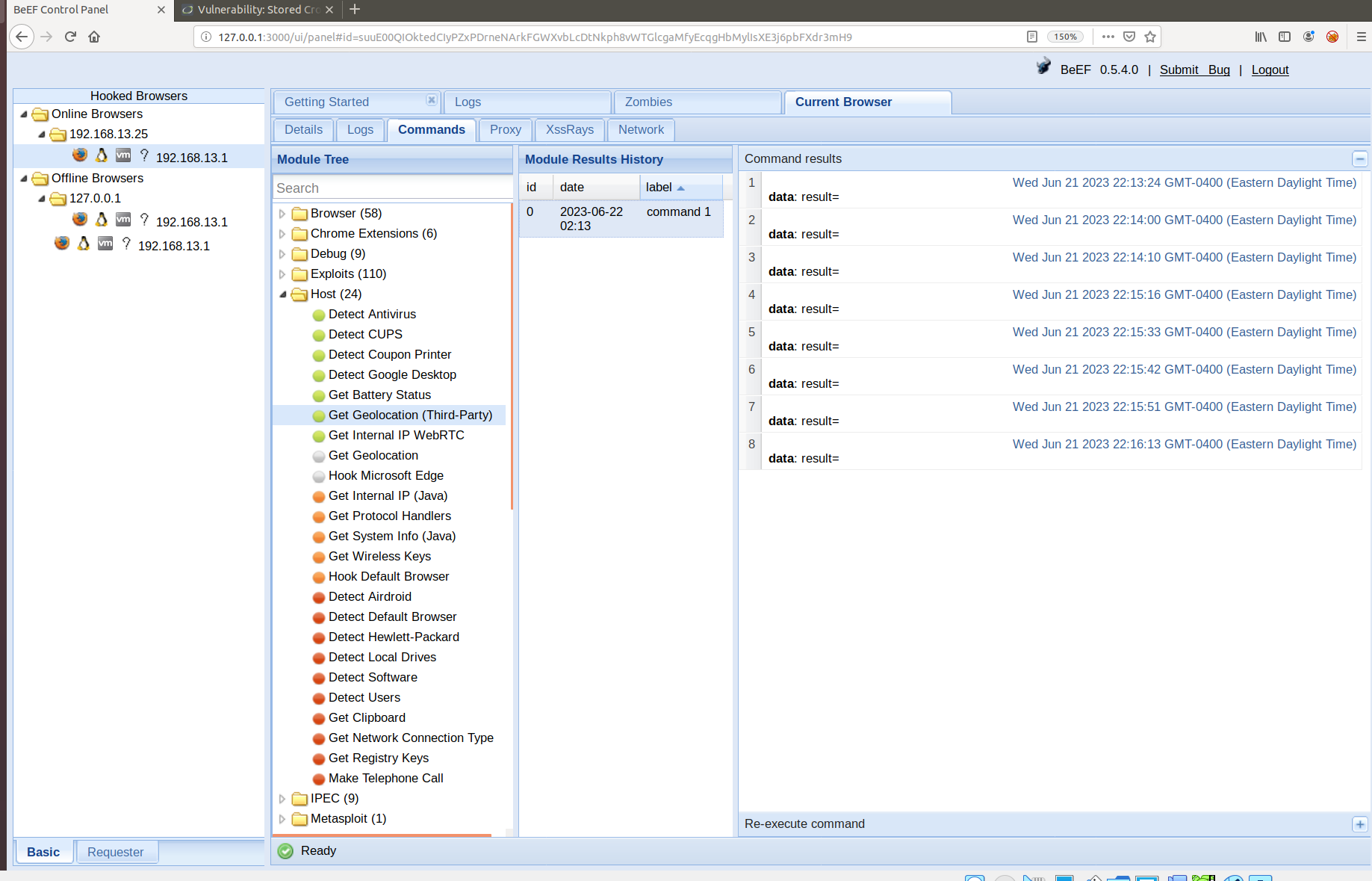
| To mitigate brute-force attack we could implement captcha or time-out period between attempts. |
| --- |

### 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 mitigate risk of XSS attack developers need to implement character validation and filtering, white-list acceptable characters. Also Output encoding may help. From the user-side the best way may be script execution disabling, HTTP-only cookies. Pop-up blocking and site redirecting may help while hooked. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.