| 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 completed this exploit:

| **127.0.0.1 && cat ../../../../../etc/hosts**    **127.0.0.1 && cat ../../../../../etc/passwd** |
| --- |

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

| To mitigate command injections a company or a person can implement input validation, allowing the rejection of any characters or sequences that could be interpreted as part of a command. You could also limit the permissions of the application’s executing environment. |
| --- |

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

Provide a screenshot confirming that you successfully completed this exploit:

| **User:tonystark passwd:I am Iron Man** |
| --- |

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

| To mitigate potential brute force attacks, you could implement strategies such as account lockout mechanisms which would temporarily lock the ussr account after a few failed attempts, and adding double factor authentication would also make preceding with a brute force attack harder. |
| --- |

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

Provide a screenshot confirming that you completed this exploit:

| **1.Pretty theft**      **2. Fake Notification Bar**      **3. Geolocation:** |
| --- |

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

| Mitigation strategies for this vulnerability include implementing a WAF-web application firewall, which helps detect and block any malicious activity. Managing the input validation also seems beneficial for this vulnerability |
| --- |

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