| 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:

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

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

| -Implement strict input validation and sanitization mechanisms to ensure that user-supplied data is within the expected range and format.  -Use whitelists to only allow specific characters or patterns in input data, rejecting anything that falls outside those constraints.  -Segregation of confidential files from the web server and accessible directories. |
| --- |

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

Provide a screenshot confirming that you successfully completed this exploit:

| ◦ User: tonystark  ◦ Password: I am Iron Man |
| --- |

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

| -Requiring complex usernames and passwords  -Using multi-factored authentication  -Enabling a lockout after a certain amount of failed login attempts. |
| --- |

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

Provide a screenshot confirming that you successfully completed this exploit:

| Changed the max length of the payload to 100 from 50. |
| --- |

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

| -Implement strict input validation and sanitization mechanisms on the Replicants web application.  -Validate and sanitize all user-supplied data, especially those that are used in dynamic content generation. |
| --- |

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