| 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:

| Separate confidential information from the main server in order to lessen the likelihood of leaks. Deny access to command line calling by Avoiding system calls and setup input validation to prevent XSS and SQL injection attacks. |
| --- |

### 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:

| Utilize various prevention techniques such as enforcing complex password requirements, password reset every 90 days, account lockout with multiple failed attempts, captcha authentication. |
| --- |

### 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:

| A few ways to mitigate getting a BeEF hook is to not visit vulnerable web apps. Constantly clearing your cookies/cache history can help prevent getting hooked. Updating software and patching if necessary. Periodic password changes. Increase security training for employees with focuses on vulnerabilities such as phishing. |
| --- |

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