| 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:

| Mitigation strategies for a ping command injection vulnerability in a web application include input validation and sanitization to ensure only expected values (e.g., IP addresses) are accepted, effectively preventing malicious input. Use parameterized functions instead of directly executing user input within system commands. Additionally, implement secure coding practices such as escaping shell metacharacters and using restricted user permissions for executing commands to minimize the impact of potential exploits. |
| --- |

### 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:

| Mitigation strategies for broken authentication and insecure login forms include implementing strong password policies, such as requiring complex passwords and limiting failed login attempts to prevent brute force attacks. Use multi-factor authentication (MFA) to add an extra layer of security beyond just usernames and passwords. Additionally, ensure that login forms use secure transmission protocols like HTTPS, protect against credential stuffing attacks with rate limiting, and securely store passwords using hashing algorithms |
| --- |

### 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:

| Mitigation strategies against Browser Exploitation Framework (BeEF) attacks include implementing Content Security Policy (CSP) headers to restrict the execution of malicious scripts and limit browser communication with untrusted sources. Regularly update and patch browsers and browser extensions to protect against known vulnerabilities exploited by BeEF. Additionally, educate users on the risks of phishing and encourage cautious browsing behavior, such as avoiding suspicious links and disabling unnecessary browser plugins that could be exploited. |
| --- |

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