| 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:

| Some good mitigation strategies can include, Server-side validation that does not allow selection of unintended files.​Segregation of confidential files from the web server and accessible directories.Permissions to restrict web server account accessibility. |
| --- |

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

Provide a screenshot confirming that you successfully completed this exploit:

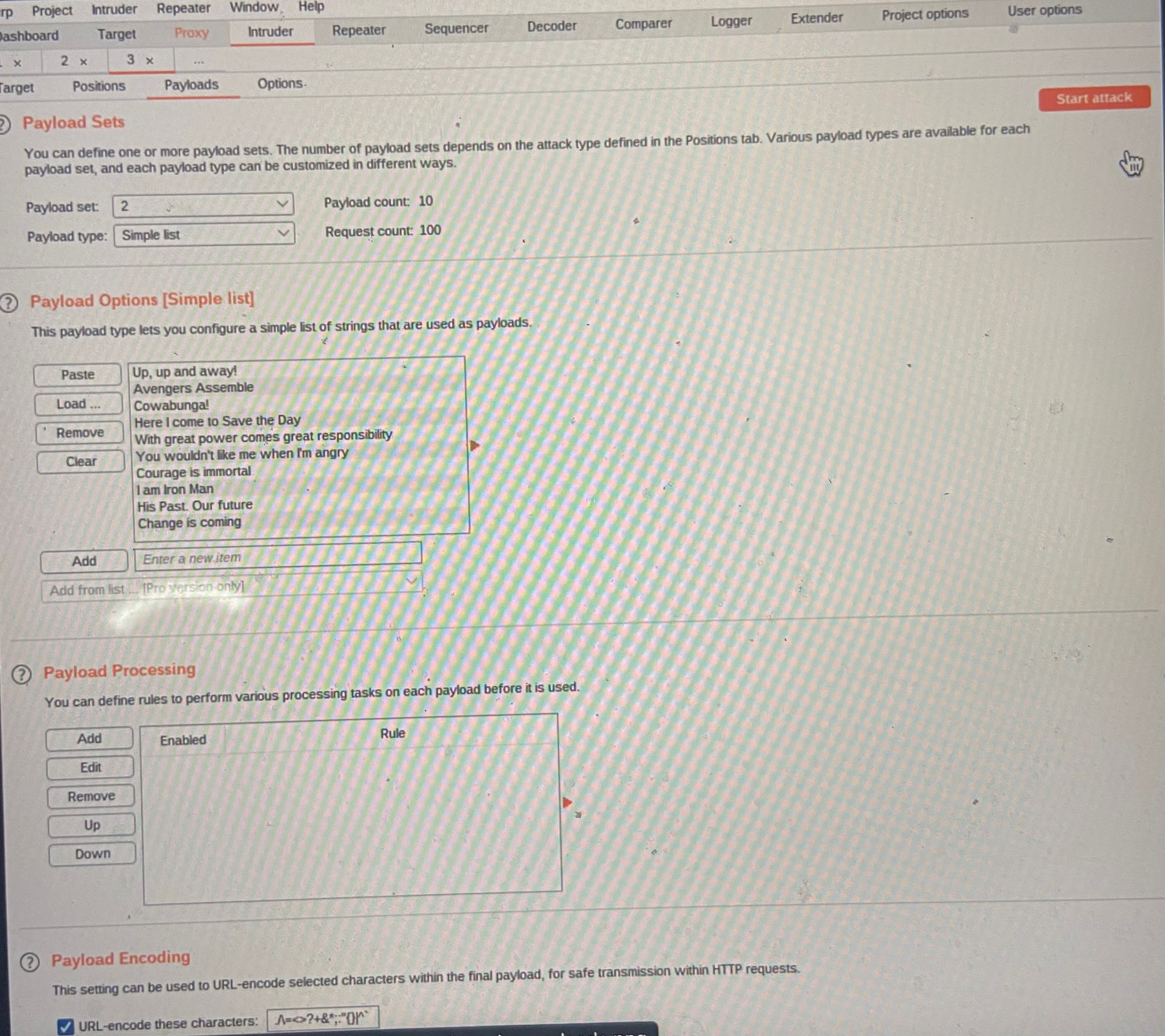
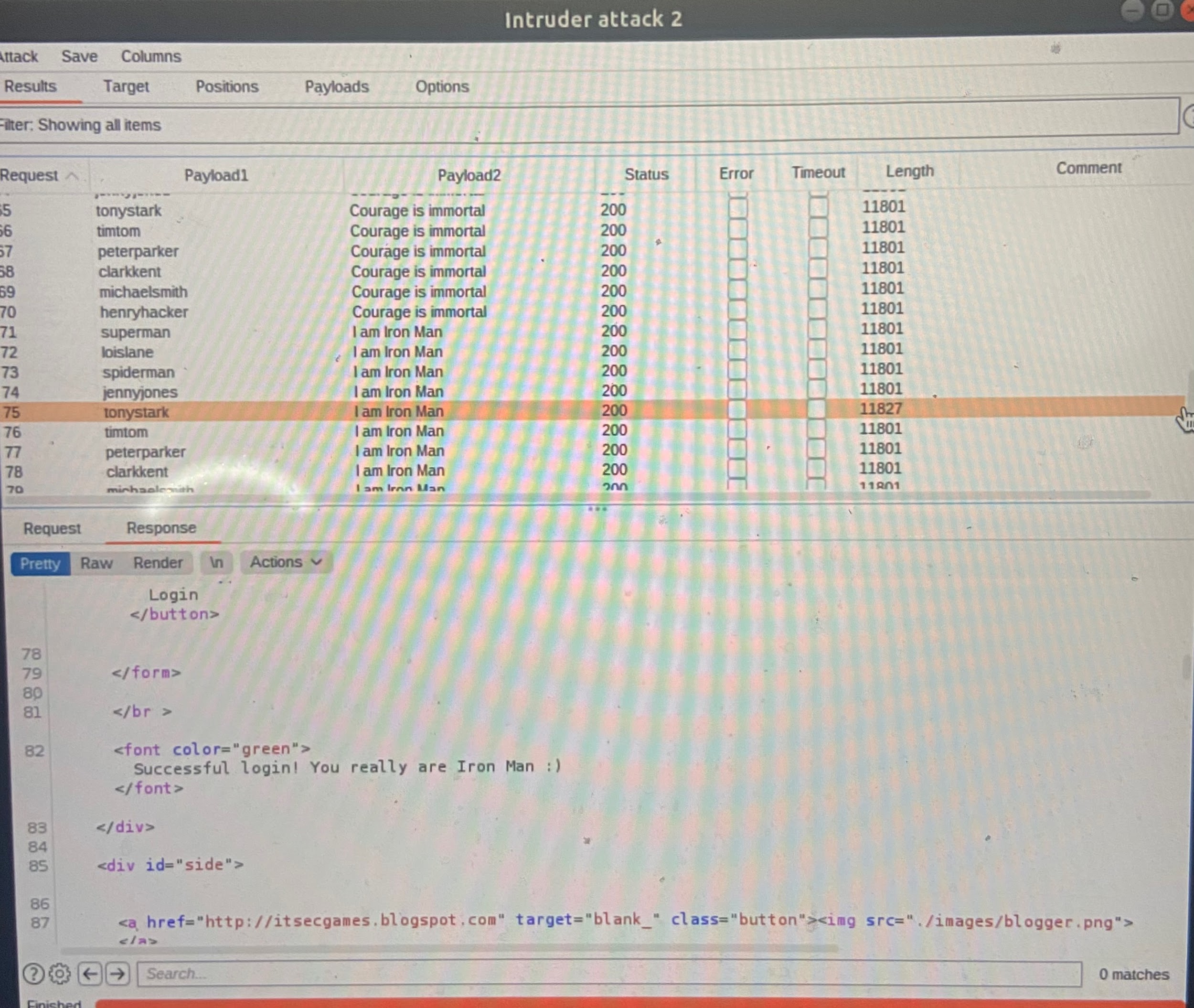
|  |
| --- |

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

| Mitigations can include requiring complex usernames and passwords, using multi-factored authentication, and 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:



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

| Input validation is a common method used to mitigate cross-site scripting. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.