| Box | Type | Challenge | Notes | Burp | Nessus | Qualsys | Detectify | Total | % |
|---|---|---|---|---|---|---|---|---|---|
| Pentest I | XSS | Example 1 | Basic XSS | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | XSS | Example 2 | Keyword filtering, case sensitive | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | XSS | Example 3 | Removes keywords | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | XSS | Example 4 | Blacklists the word script | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | XSS | Example 5 | rejects some JS functions | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | XSS | Example 6 | Inline JS | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest I | XSS | Example 7 | Inline JS, PHP Special chars | 1 | 0 | 1 | 0 | 2 | 50.0% |
| Pentest I | XSS | Example 8 | XSS in URL path | 1 | 0 | 1 | 0 | 2 | 50.0% |
| Pentest I | XSS | Example 9 | Dom based XSS | 1 | 0 | 1 | 0 | 2 | 50.0% |
| Pentest I | SQLi | Example 1 | Basic SQLi | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | SQLi | Example 2 | Basic SQLi but no spaces | 1 | 0 | 0 | 0 | 1 | 25.0% |
| Pentest I | SQLi | Example 3 | Basic SQLi but no spaces/tabs | 1 | 0 | 0 | 0 | 1 | 25.0% |
| Pentest I | SQLi | Example 4 | Basic SQLi but input is a number not a string | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | SQLi | Example 5 | As above but uses regex to check input starts with number | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | SQLi | Example 6 | As above but uses regex to check input ends with number | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | SQLi | Example 7 | Uses regex to filter but broken using a line break | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | SQLi | Example 8 | SQLi in an Order By (with back tick) | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | SQLi | Example 9 | SQLi in an Order By (no back tick) | 1 | 0 | 1 | 0 | 2 | 50.0% |
| Pentest I | Directory Traversal | Example 1 | Basic LFI | 0 | 0 | 0 | 1 | 1 | 25.0% |
| Pentest I | Directory Traversal | Example 2 | LFI but ensures start of string matches expected pattern | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | Directory Traversal | Example 3 | Basic LFI but has to have %00 on the end to stop extension | 0 | 0 | 1 | 1 | 2 | 50.0% |
| Pentest I | File Include | Example 1 | Basic file include | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest I | File Include | Example 2 | File include with null byte termination | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | Code Injection | Example 1 | Basic PHP code injection | 1 | 0 | 1 | 0 | 2 | 50.0% |
| Pentest I | Code Injection | Example 2 | usort create function injection | 1 | 0 | 0 | 1 | 2 | 50.0% |
| Pentest I | Code Injection | Example 3 | PCRE_REPLACE_EVAL /e modifier | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | Code Injection | Example 4 | assert function injection | 1 | 0 | 0 | 0 | 1 | 25.0% |
| Pentest I | Commands Injection | Example 1 | Use ; or && to add own command | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest I | Commands Injection | Example 2 | Use multiline character to add own command | 0 | 1 | 0 | 1 | 2 | 50.0% |
| Pentest I | Commands Injection | Example 3 | Similar to the previous example but with a redirect | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest I | LDAP Injection | Example 1 | Null binds | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | LDAP Injection | Example 2 | LDAP injection | 1 | 0 | 0 | 0 | 1 | 25.0% |
| Pentest I | File Upload | Example 1 | Simple file upload | 0 | 0 | 1 | 0 | 1 | 25.0% |
| Pentest I | File Upload | Example 2 | File upload with some extension filtering | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest I | XML Attacks | Example 1 | XXE | 1 | 0 | 0 | 1 | 2 | 50.0% |
| Pentest I | XML Attacks | Example 2 | XPATH injection | 1 | 0 | 0 | 0 | 1 | 25.0% |
| Pentest II | SQLi | Example 1 | Basic SQLi | 1 | 1 | 1 | 0 | 3 | 75.0% |
| Pentest II | SQLi | Example 2 | Ensures that only 1 row is returned | 1 | 1 | 0 | 0 | 2 | 50.0% |
| Pentest II | SQLi | Example 3 | Blocks single qoutes but escaping works | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | SQLi | Example 4 | part of the query in parameter | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest II | SQLi | Example 5 | Injecting on the keyword LIMIT | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest II | SQLi | Example 6 | Injecting on the "GROUP BY" keyword | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest II | SQLi | Example 7 | Error based injection | 1 | 1 | 1 | 1 | 4 | 100.0% |
| Pentest II | SQLi | Example 8 | Second order SQL Injection | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | SQLi | Example 9 | Uses GBK charset | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authentication | Example 1 | Common password | 0 | 1 | 1 | 0 | 2 | 50.0% |
| Pentest II | Authentication | Example 2 | string comparison vulnerability (time) | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authentication | Example 3 | Cookie modification after logging in | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authentication | Example 4 | Similar to above but hashed | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authentication | Example 5 | Case insensitive registration | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authentication | Example 6 | space check registration | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 1 | Remove captcha parameter | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 2 | Answer is leaked in HTML | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 3 | Answer leaked in cookie | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 4 | Can reuse correct value | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 5 | Limited number of words | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 6 | Easily scripted | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 7 | Scripted but remove blue hatch fill | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 8 | Unimplode the image | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Captcha | Example 9 | Simple arithmetic captcha | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authorization | Example 1 | Forced browsing, needs to be able to login | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authorization | Example 2 | IDOR: increment number in URL | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Authorization | Example 3 | IDOR: increment number in URL | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Mass Assignment | Example 1 | Basic mass assignment | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Mass Assignment | Example 2 | Mass assignment in update profile | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Mass Assignment | Example 3 | Mass assignment after logging in | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Randomness Issues | Example 1 | Seed of 0 | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Randomness Issues | Example 2 | Seeded with current time | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Randomness Issues | Example 3 | Seed of 0 just random length | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | Randomness Issues | Example 4 | Bruteforce the value | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | MongoDB Injection | Example 1 | Basic MongoDB injection | 0 | 0 | 0 | 0 | 0 | 0.0% |
| Pentest II | MongoDB Injection | Example 2 | Blind MongoDB injection | 0 | 0 | 0 | 0 | 0 | 0.0% |
| | | | 72 | 32 | 22 | 27 | 12 | | |
| | | | | 44.4% | 30.6% | 37.5% | 16.7% | | |