SECURDE

Penetration Test Template

Instructions:

The tasks provided below are just examples, they are not necessarily applicable to the securing group’s website. The attacking group can replace it with a different attack vector or even add more. The lower limit of tasks is 20. Groups will be decided in class (lottery).

Securing Group Members: FERNANDEZ, Ryan Austin

HADE, Alden Luc

POBLETE, Clarisse Felicia

SYFU, Jonah

Attacking Group Members: COTE, Christian

ERIVE, Winona

SEO, Dong Seong

|  |  |  |
| --- | --- | --- |
| **GENERAL** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Be able to run the program in http (should not work since it should only run in https) | Secured |  |
| Be able to click the back button and ruin the site. | Secured |  |
| Be able to tamper with the url | Secured |  |

|  |  |  |
| --- | --- | --- |
| **LOG-IN (AUTHENTICATION)** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Role-based | | |
| Be able to access customer page while not logged in | Secured |  |
| Be able to access administrator page while not logged in | Secured |  |
| Be able to access product manager while not logged in | Secured |  |
| Be able to access accounting manager while not logged in | Secured |  |
| Be able to access customer page as a different user | Secured |  |
| Be able to access administrator page as a different user | Secured |  |
| Be able to access product manager page as a different user | Secured |  |
| Be able to access accounting manager page as a different user | Secured |  |
| User specific | | |
| Be able to try to guess user password even after 3 failed attempts | Secured |  |
| Be able to still be logged in even if the account has been locked out due to failed attempts | Secured |  |
| Be able to login the system with a user that is not created. | Secured |  |
| Injections | | |
| Be able to do SQL Injection on username field | Secured |  |
| Be able to do SQL Injection on password field | Secured |  |
| Be able to do XSS on username field | Secured |  |
| Be able to do XSS on password field | Secured |  |
| CSRF | | |
| Be able to perform CSRF attack on the page | Secured |  |

|  |  |  |
| --- | --- | --- |
| **SIGN-UP (AUTHENTICATION)** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Data Validation | | |
| Be able to sign up with a username that is less than 6 characters | Secured |  |
| Be able to sign up with a username that already exists in the database | Secured |  |
| Be able to sign up with a password less than 8 characters | Secured |  |
| Be able to sign up with a password that is only all letters | Secured |  |
| Be able to sign up with a password that is only all numbers | Secured |  |
| Be able to sign up with a password that does not match with the confirmation password | Secured |  |
| Be able to sign up with an email that already exists in the database | Secured |  |
| Be able to sign up with an email that does not comply with the email format | Secured |  |
| Be able to sign up with a personal information that does not comply with the necessary rule/pattern (ex. ZIP code that is in numbers) | Secured |  |
| Injections | | |
| Be able to do SQL Injections on any field | Secured |  |
| Be able to do XSS on any field | Secured |  |

|  |  |  |
| --- | --- | --- |
| **CUSTOMER PAGE (INDEX)** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Injections | | |
| Search Field | | |
| Be able to perform SQL injection to the search field | Secured |  |
| Be able to perform XSS to the search field | Secured |  |
| Checkout Fields | | |
| Be able to perform SQL injection to any field | Secured |  |
| Be able to perform XSS to any field | Secured |  |
| Edit Account Fields | | |
| Be able to perform SQL injection to any field | Secured |  |
| Be able to perform XSS to any field | Secured |  |
| Data Validation | | |
| Checkout Fields | | |
| Be able to enter an invalid format for a credit card number | Secured |  |
| Be able to enter an expired date | Secured |  |
| Be able to enter an invalid format for a card verification code | Secured |  |
| CSRF | | |
| Be able to perform CSRF attack on the page | Secured |  |
| Add to cart | | |
| Be able to add an item to cart that is not in the items | Secured |  |

|  |  |  |
| --- | --- | --- |
| **PRODUCT MANAGER PAGE (Products List)** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Injections | | |
| Search Field | | |
| Be able to perform SQL injection to the search field | Secured |  |
| Be able to perform XSS to the search field | Secured |  |
| Edit Fields | | |
| Be able to perform SQL injection to any edit field | Secured |  |
| Be able to perform XSS to any edit field | Secured |  |
| Table data (Reports and information) | | |
| Be able to delete an item immediately without prior notice. | Breached | * Clicked delete on a product * Product was immediately deleted without * NOTE: What if delete product was accidentally clicked? This means the product was accidentally deleted? That means it isn’t recoverable anymore? |
| Be able to edit an item and affect the sales record gravely. | Breached | * Clicked delete on a product * Product was immediately deleted * Accounting Manager logged in * Previous sales information was lost |
| Be able to edit an item immediately without prior notice. | Breached | * Clicked edit on a product * Product was immediately edited without confirmation |
| Be able to edit an item and affect the sales record gravely. | Breached | * Clicked edit on a product * Product was immediately edited without confirmation * Previous sales prices were affected |

|  |  |  |
| --- | --- | --- |
| **ADMIN PAGE** | | |
| Task | Status (Breached/Secured) | How to replicate(if breached) |
| Injections | | |
| Search Field | | |
| Be able to perform SQL injection to the search field | Secured |  |
| Be able to perform XSS to the search field | Secured |  |
| Create Account Fields | | |
| Be able to perform SQL injection to any field | Secured |  |
| Be able to perform XSS to any field | Secured |  |
| Data Validation | | |
| Be able to perform SQL injection to the old password field | Secured |  |
| Be able to perform XSS to the old password field | Secured |  |
| Be able to perform SQL injection to the new password field | Secured |  |
| Be able to perform XSS to the new password field | Secured |  |
| Be able to perform SQL injection to the confirm new password field | Secured |  |
| Be able to perform XSS to the confirm new password field | Secured |  |
| CSRF | | |
| Be able to perform CSRF attack on the page | Secured |  |