[STEA-23] Test for HTTP Verb tampering Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000dz:
Sprint:	STEA Sprint 1

Description

1. Manually try modifying the HTTP method of POST request of any sensitive transaction to GET and analyze whether the request is successful.

[STEA-22] Test for Insecure Direct Object Reference Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000dr:
Sprint:	STEA Sprint 1

Description

1. Identify the points where the Object reference may occur.
2. Test by modifying the value of parameter used directly to retrieve a database record or to Perform an Operation in the System or used Directly to Retrieve a File System Resource or Used Directly to Access Application Functionality,

[STEA-21] Test for XSS Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000dj:
Sprint:	STEA Sprint 1

[STEA-20] Test for SQL Injection Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000db:
Sprint:	STEA Sprint 1

Description

1. Identify SQL injection points like form fields.
2. Assess the severity of the injection and the level of access that can be achieved through it.
3. Using Proxy tools to run a scan to identify the requests that are vulnerable to SQL injection and testing them manually.

[STEA-19] Check for CSRF Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000d3:
Sprint:	STEA Sprint 1

Description

1. Test for CSRF when there is a valid action, session based cookie handling and there is no unpredictable request parameters.

[STEA-18] Check for the effectiveness of session termination

Created: 05/Nov/23 Updated: 05/Nov/23

Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000cv:
Sprint:	STEA Sprint 1

Description

1. Check session termination after a maximum lifetime
2. Check session termination after relative timeout
3. Check session termination after logout
4. Test to see if users can have multiple simultaneous sessions

[STEA-17] Test for Session cookie attributes in HTTP headers

Created: 05/Nov/23 Updated: 05/Nov/23

Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000cn:
Sprint:	STEA Sprint 1

Description

1. Check session tokens for cookie is set with attributes of httpOnly and secure in HTTP Response headers.
2. Check session cookie scope (path and domain) and session cookie duration (expires and max-age)
3. Test session cookies for randomness

[STEA-16] Test for Logout Functionality Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000cf:
Sprint:	STEA Sprint 1

Description

1. Test for Server side session termination.
2. Test for Session timeout

Reference:

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/06-Testing_for_Logout_Functionality

[STEA-14] Test for Brute Force attacks in Login Page Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000bz:
Sprint:	STEA Sprint 1

Description

1. Using the dictionary of words and Repeater tab of Burp Proxy tool automate the supply of credentials to Login page.
2. If the system is securely designed the IP address from which the Brute forcing happens should be blocked after 5 failed attempts.

[STEA-13] Test for User Enumeration Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000br:
Sprint:	STEA Sprint 1

Description

1. Using the Repeater option of Burp Proxy tool and a dictionary of wordlists attacker can enumerate the user names of the target application.
2. Verify the *information retrieved from successful authentication (HTTP 200 Response, length of the response) by providing valid credentials. Look at the server response for the following scenarios:*
    1. Testing for valid user with wrong password
    2. Testing for Nonexistent user.

Reference:

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account

[STEA-12] Checks for details over HTTPS Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000bj:
Sprint:	STEA Sprint 1

Description

From the Active scan results of the Proxy tool (OWASP ZAP or BurpSuite) check the folowing:

1. Check SSL Version, Algorithms, Key length, Check for Digital Certificate Validity (Duration, Signature and CN)
2. Check whether the credentials, login form, session tokens are delivered over HTTPS
3. Check if HTTP Strict Transport Security (HSTS) header in use.

[STEA-11] Test for HTTP methods and HTTP Headers Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000b3:
Sprint:	STEA Sprint 1

Description

1. Discover the supported HTTP methods.
2. Test for arbitrary HTTP methods.
3. Test for Head Access Control Bypass.

Reference:

https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/06-Test_HTTP_Methods

[STEA-10] Directory listing using Wfuzz or Dirbuster Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000av:
Sprint:	STEA Sprint 1

Description

1. Use Fuzzing tools to list the directories of the target application.
2. Check whether there are any administrative URLs. If so try to access this URL form the browser as attacker does.

[STEA-9] Perform Web Application Fingerprinting Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Security Testing of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Rank:	0|i000bb:
Sprint:	STEA Sprint 1

Description

1. Spider/crawl or peform an active scan of the target application which is ecommerce application using proxy tools like OWASP-ZAP/ Burp suite.
2. Check for files such as robots.txt, sitemap.xml, .DS_Store. Check for “Disallow” values.
3. From the scan results (if possible) Identify technologies used, Identify application entry points, Identify all hostnames and ports and Identify third-party hosted content(if any).

Generated at Sun Nov 05 17:13:59 UTC 2023 by Aishwarya Selvarajan using Jira 1001.0.0-SNAPSHOT#100240-sha1:341642299face3a73787b1ff0621c4c5fa6e6142.