[SSDEA-31] Protecting the Logs against Log Forging Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Logging of Security related errors
Sprint:	Security Sprint 1

Description

As an administrator

I want to Protect the Logs from Unauthorised disclosure, modification or deletion

so that it could be used for investigations during attack.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 7.3.1

Verify that all logging components appropriately encode data to prevent log injection.

OWASP Application Security Verification Standard v4.0.3 - 7.3.3

Verify that security logs are protected from unauthorized access and modification.

[SSDEA-30] Login Fails, Access Control failures, Server Side Input Validation failures must be logged. Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Logging of Security related errors
Sprint:	Security Sprint 1

Description

As an administrator

I want to Log the failed authentication events, access control failures, deserialization failures and input validation failures

so that when an attack happens it will be helpful for investigation.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 7.1.3

Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.

[SSDEA-27] Reset Passwords using a URL Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Forgot Password Functionality
Sprint:	Security Sprint 1

Description

As a system developer

I want to ensure that when the user uses Forgot Password functionality, passwords are reset by sending a unique URL to system users that takes them to a password reset page

so that the users could reset their passwords in a secure way.

Reference :

https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html

[SSDEA-26] Ensuring unsafe Parameter Assignment while checking out the Product Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Checkout Functionality
Sprint:	Security Sprint 1

Description

As a system developer

I want the user to Check out on only the products that have been added to cart

so that attacker does not intercept and manipulate the parameters like quantity or price associated with the Check out of the product

Reference:

OWASP Application Security Verification Standard v4.0.3 - 5.1.1

Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).

OWASP Application Security Verification Standard v4.0.3 - 5.1.2

Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.

[SSDEA-25] Handle the unconventional input successfully Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Adding Product to Cart Functionality
Sprint:	Security Sprint 1

Description

As an user

I want to allow only conventional inputs when adding a required number of Product

so that I am ensuring that there are no business logic Vulnerabilities.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 5.4.3

Verify that sign, range, and input validation techniques are used to prevent integer overflows.

OWASP Application Security Verification Standard v4.0.3 - 11.1.1

Verify that the application will only process business logic flows for the same user in sequential step order and without skipping steps.

OWASP Application Security Verification Standard v4.0.3 - 4.2.1

Verify that sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.

OWASP Application Security Verification Standard v4.0.3 - 4.2.2

Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.

[SSDEA-24] Search for a product securely Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Product Searching Functionality
Sprint:	Security Sprint 1

Description

As a system developer

I want to let the user search for the intended product alone in the search field and reflect the result with correct Product name

so that the attacker does not take advantage of injecting malicious scripts or values to the search field or exceute the malicious scripts in the enduser’s browser session.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 5.1.1

Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).

OWASP Application Security Verification Standard v4.0.3 - 5.1.3

Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).

[SSDEA-23] Invalidate the session token during Session timeout and Logout

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Logout Functionality for an ecommerce application
Sprint:	Security Sprint 1

Description

As a user

I want to my session to be terminated when I click on the Logout Button or when the session timeout

so that the session the attackers does not use the session tokens to do malicious activites.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 3.3.1

Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.

[SSDEA-22] Display a generic error message when the credentials are not valid Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development of Ecommerce application
Components:	None
Affects versions:	None
Fix versions:	None

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

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system user

I want generic error message to be displayed when the Login fails

so that the attacker is not provided a chance with enumeration of either username or password.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 7.4.1

Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.

[SSDEA-19] Enable two factor authentication Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Comments

Comment by Aishwarya Selvarajan [04/Nov/23]

As a system developer

I want to enable 2FA using Google authenticator

so that I secure my user accounts from Brute forcing or session hijacking.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 2.7.1

Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.

[SSDEA-18] Rate limit brute force attempts. Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to limit the number of failed attempts during Login

so that the attacker does not Brute force to find the valid credentials.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 2.2.1

Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

[SSDEA-16] Validate the user inputs in the Login page

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to make sure that the user login fields are intended to have the right structured data

so that the attacker fails to exploit the system by injecting malicious user inputs.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 5.1.3

Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (allow lists).

[SSDEA-15] Ensure secure data in transit during Login Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to make sure that all the communications are made through secure channel (over HTTPS)

so that the attacker does not have the chance for MITM like session Hijacking.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 9.1.1

Verify that TLS is used for all client connectivity, and does not fall back to insecure or unencrypted communications.

[SSDEA-14] Validate the inputs in the HTML form fields of the user registration page

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure User Registration Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to make sure that the user inputs from the registration page are validated against the allowed characters, length and pattern

so that the malicious inputs from the attacker are blocked.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 5.1.4

Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers, e-mail addresses, telephone numbers, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).

[SSDEA-13] Encourage highly entropic password and discourage common password

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure User Registration Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to have the users create their passwords in the system with high entropy

so that passwords are strong enough to be cracked.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 2.1.8 : Verify that a password strength meter is provided to help users set a stronger password.

[SSDEA-12] Hash user passwords from user registration using unique salt

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure User Registration Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I want to create a system where the user passwords from the registration page are hashed with unique salt

so that the system is resistant to Offline attacks by an attacker.

Reference:

OWASP Application Security Verification Standard v4.0.3 - 2.4.1 : Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.

[SSDEA-11] Gather only the information needed in the user registration page

Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure User Registration Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system developer

I have to create a user registration page with limited information from the user, preferably username, email id, password and confirm password fields

so that I can gather the information that is needed thereby not leading to unnecessary liability.

[SSDEA-10] System should let the users use password managers Created: 04/Nov/23 Updated: 04/Nov/23

Status:	To Do
Project:	Secure Software Development 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		

Epic Link:	Create a Secure Login Page for an ecommerce application
Sprint:	Security Sprint 1

Description

As a system user

I want to have secure connection during Login

so that my credentials are not intercepted by MITM.

Reference :

OWASP Application Security Verification Standard v4.0.3 - 9.2.2

Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.