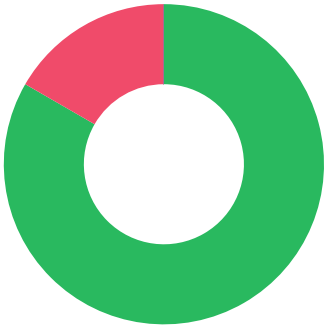
TR6 Express run 2024/11/17

Identifying vulnerabilities and ensuring the Prestashop demo website is safeguarded against potential threats. Testing includes simulated attacks like SQL injection, cross-site scripting (XSS), and unauthorized access attempts to validate the robustness of security mechanisms. The focus is on verifying data protection, secure session management, and input sanitization.

Completion chart



Completion stats

- Untested (0)
- Passed (5)
- Failed (1)
- Blocked (0)
- Retest (0)
- Skipped (0)
- Invalid (0)

Completion rate

100%

Started by	Start time	Estimated	Time spent
Radosław Waszak	2024-11-17 20:57:54	00:00:00	00:16:43.296

Environment

Prestashop Demo Environment - - Security testing

Milestone

-

Operating System

Mac OS

SQL Injection

Status	Time spent	Assignee
Passed	00:03:31.213	Radosław Waszak

Results

Result 1

Status	Time spent	User	Defects
Passed	00:03:31.213	Radosław Waszak	-

Finish time

2024-11-17 21:01:34

Steps

Step	1
Action	Identify a form or input field (e.g., login form, search bar, contact form).
Expected result	Input field is accessible and functional.
Actual result	Input field is accessible and functional.
Status	Passed

Step	2
Action	Enter a malicious SQL query into the field (e.g.,\'; DROP TABLE users; --).
Expected result	The application should display an error or handle the input gracefully without breaking or exposing data.
Actual result	The server rejects the connection.  error.JPG
Status	Passed

Step	3
Action	Monitor the application’s behavior (e.g., error messages or unexpected results).
Expected result	No sensitive data is exposed (e.g., "SQL syntax error") or unauthorized actions performed.
Actual result	No sensitive data is exposed or unauthorized actions performed.
Status	Passed

Cross-Site Scripting (XSS)

Status	Time spent	Assignee
Passed	00:02:59.619	Radosław Waszak

Results

Result 1

Status	Time spent	User	Defects
Passed	00:02:59.619	Radosław Waszak	-

Finish time

2024-11-17 21:04:37

Steps

Step	1
Action	Identify any input fields or content sections (e.g., order tracking).
Expected result	Input fields are functional.
Actual result	Input fields are functional.
Status	Passed

Step	2
Action	Input a script tag (e.g.,).
Expected result	The input should be sanitized or rejected.
Actual result	Input is rejected.  error.JPG
Status	Passed

Step	3
Action	Submit the input and observe the behavior of the page.
Expected result	The script should not execute, and no unauthorized actions (e.g., pop-ups or alerts) should occur.
Actual result	The script doesn\'t execute, and no unauthorized actions (e.g., pop-ups or alerts) occur.
Status	Passed

User Authentication Security

Status	Time spent	Assignee
Failed	00:02:39	Radosław Waszak

Results

Result 1

Status	Time spent	User	Defects
Failed	00:02:39	Radosław Waszak	D-14 (Open)

Finish time

2024-11-17 21:07:42

Actual result

Account doesn\'t lock or display a CAPTCHA after 5 failed attempts.

Steps

Step	1
Action	Log in to Prestashop with valid credentials.
Expected result	Login is successful and redirects to the appropriate user dashboard.
Actual result	Login is successful and redirects to the appropriate user dashboard.
Status	Passed

Step	2
Action	Attempt to log in with incorrect credentials multiple times.
Expected result	Account should lock or display a CAPTCHA after 5 failed attempts.
Status	Failed

Step	3
Action	Observe error messages for failed logins.
Expected result	Generic error message "Authentication failed." is displayed without revealing specific details.
Actual result	Generic error message "Authentication failed." is displayed without revealing specific details.
Status	Passed

Session Management

Status	Time spent	Assignee
Passed	00:01:55.111	Radosław Waszak

Results

Result 1

Status	Time spent	User	Defects
Passed	00:01:55.111	Radosław Waszak	-

Finish time

2024-11-17 21:10:06

Steps

Step	1
Action	Log in to the application and perform standard actions.
Expected result	Actions are executed without session issues.
Actual result	Actions are executed without session issues.
Status	Passed

Step	2
Action	Log out and attempt to use the browser’s back button to access a restricted page.
Expected result	Access is denied or redirected to the login page.
Actual result	Redirected to the login page.
Status	Passed

Step	3
Action	Inspect cookies using browser tools (e.g., Chrome DevTools) and note their attributes (e.g.,Secure, HttpOnly).
Expected result	Cookies are flagged as Secure and HttpOnly, and sensitive data is not exposed.
Actual result	Cookies are flagged as Secure and HttpOnly, and sensitive data is not exposed.
Status	Passed

Sensitive Data Exposure

Status	Time spent	Assignee
Passed	00:00:40.953	Radosław Waszak

Results

Result 1

Status	Time spent	User	Defects
Passed	00:00:40.953	Radosław Waszak	-

Finish time

2024-11-17 21:10:48

Steps

Step	1
Action	Log in and navigate through the application, performing standard actions (e.g., checkout, viewing user details).
Expected result	Application behaves as expected without exposing sensitive information.
Actual result	Application behaves as expected without exposing sensitive information.
Status	Passed

Step	2
Action	Use DevTools to inspect network requests during actions.
Expected result	Sensitive data (e.g., passwords, payment details) is not visible in plaintext.
Actual result	Sensitive data (e.g., passwords, payment details) is not visible in plaintext.
Status	Passed

Step	3
Action	Inspect page source and console logs for any sensitive data.
Expected result	No sensitive data is exposed in HTML or JavaScript logs.
Actual result	No sensitive data is exposed in HTML or JavaScript logs.
Status	Passed

Password Security

Status	Time spent	Assignee
Passed	00:04:57.400	Radosław Waszak

Results

Result 1

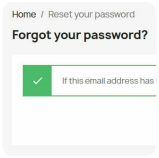
Status	Time spent	User	Defects
Passed	00:04:57.400	Radosław Waszak	-

Finish time

2024-11-17 21:15:46

Steps

Step	1
Action	Attempt to register a new account using a weak password (e.g., "12345").
Expected result	Registration is denied with a message requiring stronger passwords.
Actual result	Registration is denied with a message requiring stronger passwords.
Status	Passed

Step	2
Action	Attempt to reset a password using the "Forgot Password" feature.
Expected result	A password reset link is sent to the registered email; the password is never exposed.
Actual result	A password reset link is sent to the registered email; the password is never exposed.  restoring2.JPG
Status	Passed

Step	3
Action	Inspect password change requests using browser tools to ensure data is transmitted securely.
Expected result	Passwords are never transmitted in plaintext over the network.
Actual result	Passwords are never transmitted in plaintext over the network.
Status	Passed