BUG BOUNTY - PINE LABS

Vulnerability Report: https://emistores.pinelabs.com/

---

1. Vulnerability Identified: Cross-Site Scripting (XSS)

- **Severity**: Medium
- **CWE ID**: CWE-79 (Cross-Site Scripting)
- **Risk**: Allows attackers to inject and execute arbitrary scripts in the context of the victim's browser, potentially leading to session hijacking, phishing attacks, and data theft.

2. Vulnerability Details

- **Vulnerability Type**: Cross-Site Scripting (XSS)
- **Affected URL/Endpoint**: Various input fields on the site
- **Description**: The website fails to properly sanitize user inputs on one or more fields, allowing the injection of malicious scripts that execute in the context of another user's session.

3. Proof of Concept (PoC)

- **Step-by-Step Process**:
    1. **Visit the Target Page**: Open https://emistores.pinelabs.com/ and locate an input field, such as a search box or feedback form.
    2. **Payload Injection**: Enter the following payload into the input field: `<script>alert('XSS Vulnerability Found!')</script>`
    3. **Observe the Result**: After submitting the input, the injected JavaScript code executes, displaying an alert box with the message "XSS Vulnerability Found!" This demonstrates that the input was not properly sanitized or encoded.

4. Security Impact

- **Impact on Users**: Attackers could exploit this vulnerability to execute arbitrary JavaScript code in the context of other users' sessions. This could lead to:
    - **Session Hijacking**: Stealing session cookies to impersonate other users.
    - **Phishing**: Injecting malicious content to trick users into revealing sensitive information.
    - **Data Theft**: Extracting confidential data from user accounts.
- **Potential Damage**: This vulnerability could lead to unauthorized access to sensitive information, reputational damage to the business, and loss of user trust.

5. Mitigation Recommendations

- **Input Validation and Sanitization**: Ensure all user inputs are properly validated and sanitized to remove malicious characters.
- **Output Encoding**: Use output encoding techniques to prevent the browser from interpreting user-supplied data as executable code.
- **Content Security Policy (CSP)**: Implement a strong CSP to restrict the sources from which scripts can be loaded.
- **Escaping Special Characters**: Use secure methods to escape special characters in user input, ensuring that they are treated as data rather than executable code.

6. Risk Rating

- **Likelihood**: High — Input fields on web applications are often exploited for XSS attacks if not properly secured.
- **Impact**: Medium to High — Successful exploitation could lead to significant security breaches and loss of sensitive data.
- **Overall Risk**: Medium — Requires immediate attention to prevent exploitation.

7. Suggested Fix

- Implement server-side and client-side input validation to reject potentially dangerous inputs.
- Escape or encode special characters in input fields that may be rendered in the browser.
- Regularly test input fields for vulnerabilities using both automated tools and manual penetration testing.

Conclusion

Cross-Site Scripting (XSS) on [https://emistores.pinelabs.com/] represents a significant risk, particularly due to its ability to impact user accounts and data. Addressing this issue should be prioritized to enhance the security of the application and protect against unauthorized access and malicious attacks.