**Reflected Cross-Site Scripting (XSS) in MODX CMS**

**Vulnerability Overview**

* Product Name: - MODX CMS
* Product URL: - https://modx.com
* Affected Versions: - modx 3.1.0
* Vulnerability Type: - ReflectedCross-Site Scripting (XSS)
* Component: Profile Image Upload Feature
* Severity: - High

**Vulnerability Description**

A cross-site scripting (XSS) vulnerability has been identified in modx versions prior to 3.1.0. The vulnerability allows authenticated users to upload SVG files containing malicious JavaScript code as profile images, which gets executed in victims' browsers when viewing the profile image**.**

**Problem Description**

The application allows users to upload SVG files as profile images without proper sanitization. SVG files can contain embedded JavaScript code that executes when the image is rendered in a browser. This creates an XSS vulnerability where malicious code can be executed in the context of other users' sessions.

**Technical Impact**

* Allows execution of arbitrary JavaScript code in victims' browsers
* Potential theft of session tokens and sensitive data
* Ability to perform unauthorized actions on behalf of the victim
* Possible escalation to more severe attacks through initial JavaScript execution

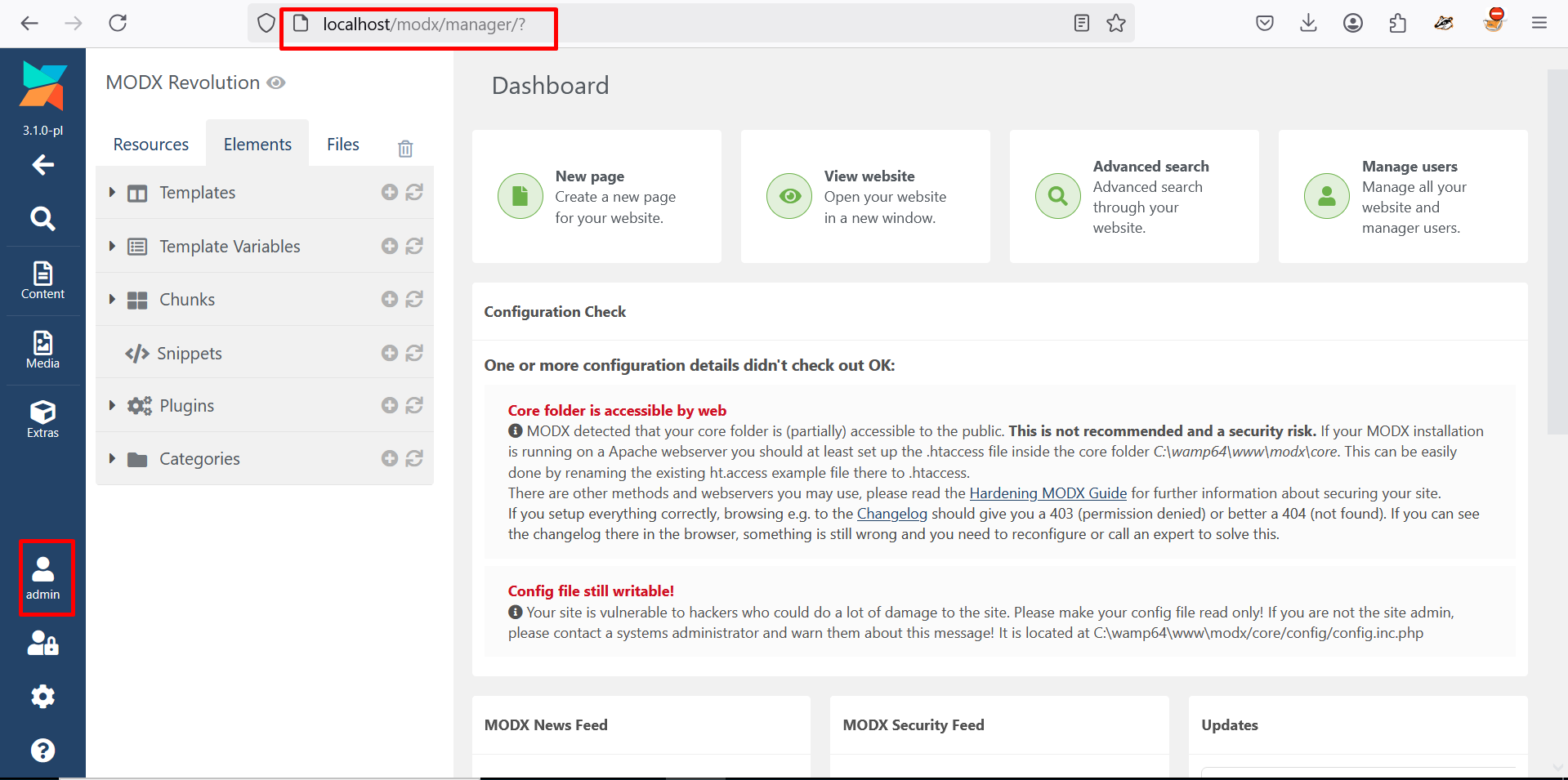
**Attack Vectors**

* Attackers upload a specially crafted SVG file as their profile image
* The SVG file contains embedded JavaScript code
* When other users view the attacker's profile or any page displaying the profile image, the malicious code executes

**Proof of Concept: -**

**Step to Reproduce**

1. **Access the Admin Panel.**
   * Navigate to: <http://localhos/modx/manager/>?
   * Log in with **valid credentials**.



1. **Upload a Malicious svg: -**

* Click the on the upload button Choose files option.
* Select and upload a malicious svg file.

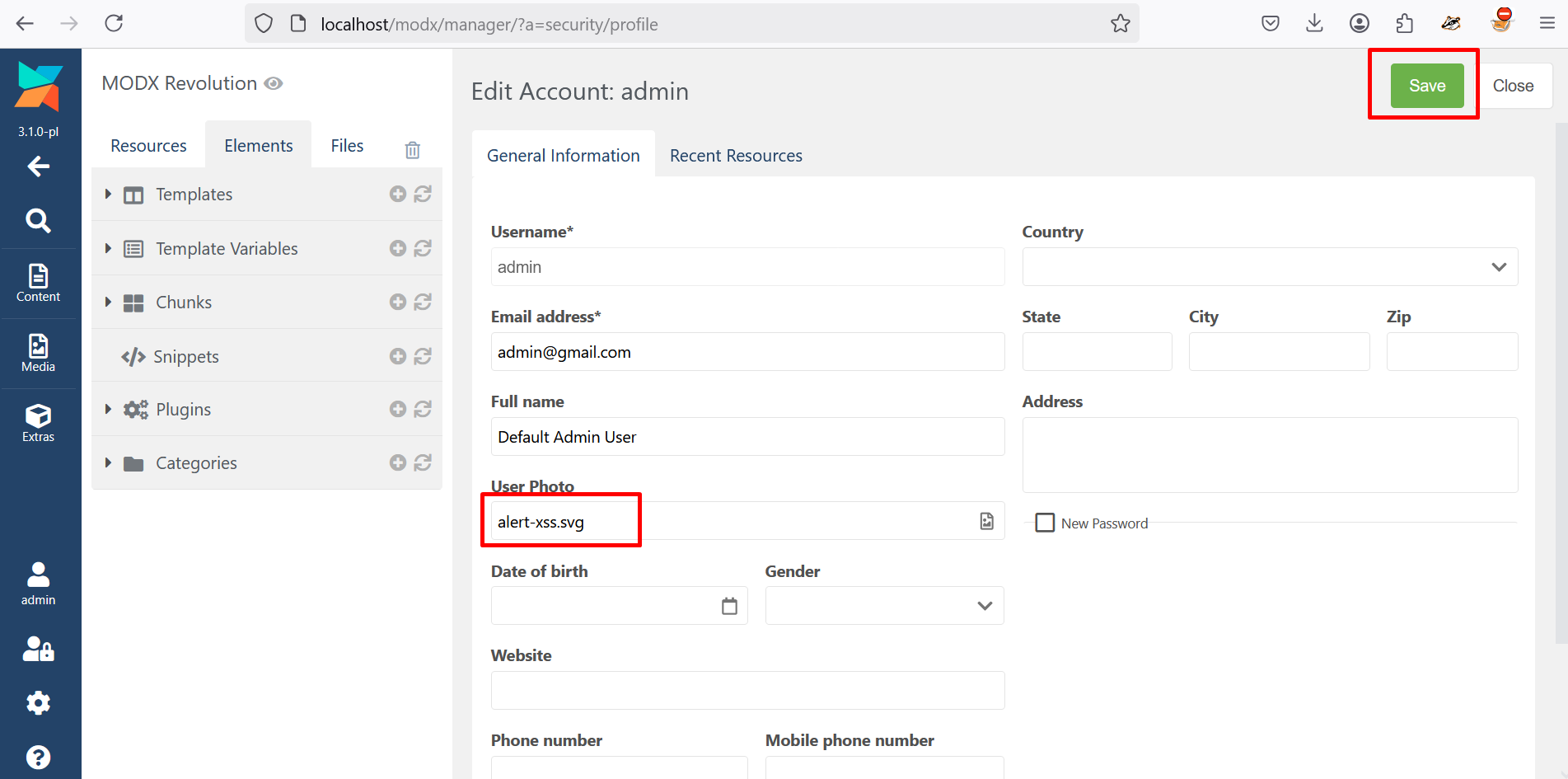
A screenshot of a computer

AI-generated content may be incorrect.

* Click the upload button. The file is uploaded successfully without detection.

A screenshot of a computer

AI-generated content may be incorrect.



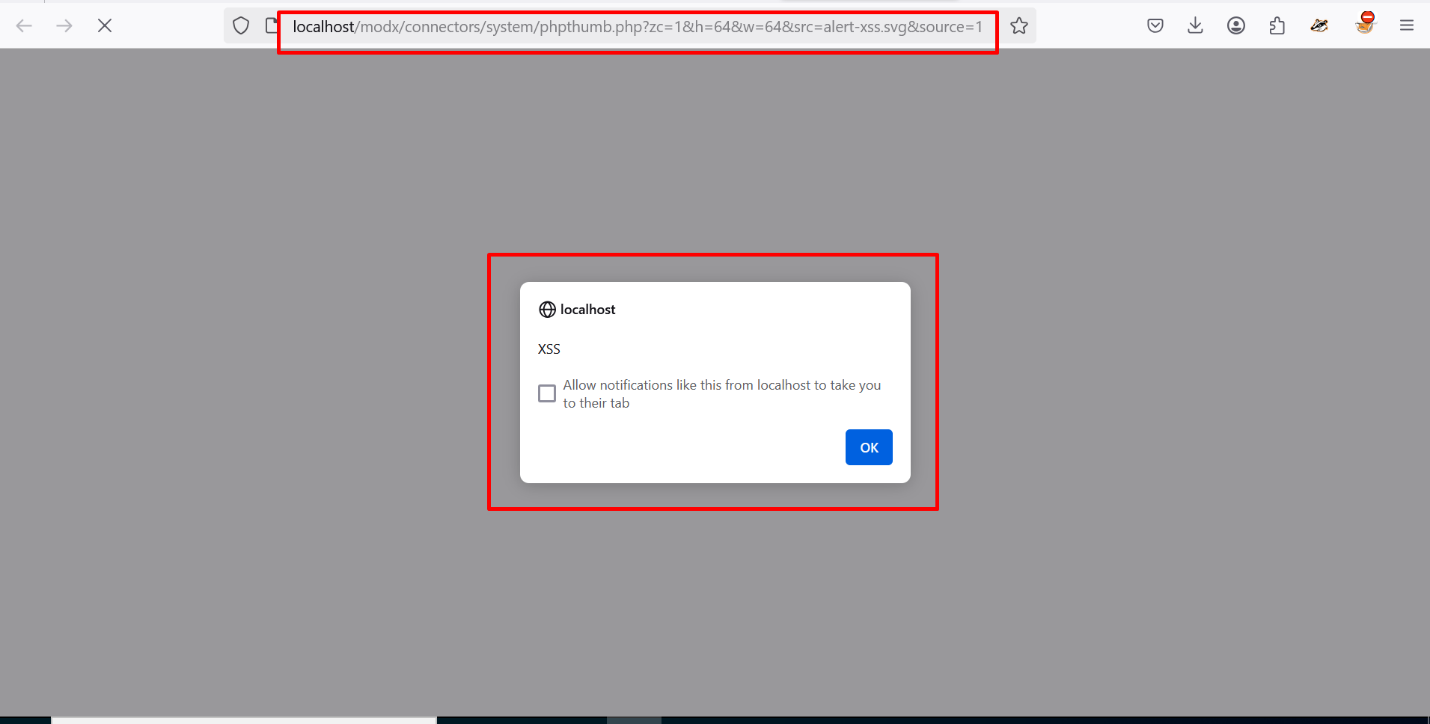
1. Click on the profile icon and open it in **Open Images in New Tab**.

A screenshot of a computer

AI-generated content may be incorrect.



1. **Observe the execution of the injected JavaScript payload.**



**Impact**

* Execution of arbitrary JavaScript in the context of the admin's browser.
* Potential to steal admin cookies, hijack sessions, or perform actions on behalf of the admin.

**Recommended Actions**

1. Input Validation: Enforce strict validation to block harmful scripts or tags.
2. Output Encoding: Encode user inputs before rendering.
3. Content Security Policy (CSP): Use a strong CSP to block unauthorized scripts.
4. Upgrade: Update Modx CMS to a patched version if available.

**References**

* OWASP XSS Prevention Cheat Sheet: <https://owasp.org>