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

0

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

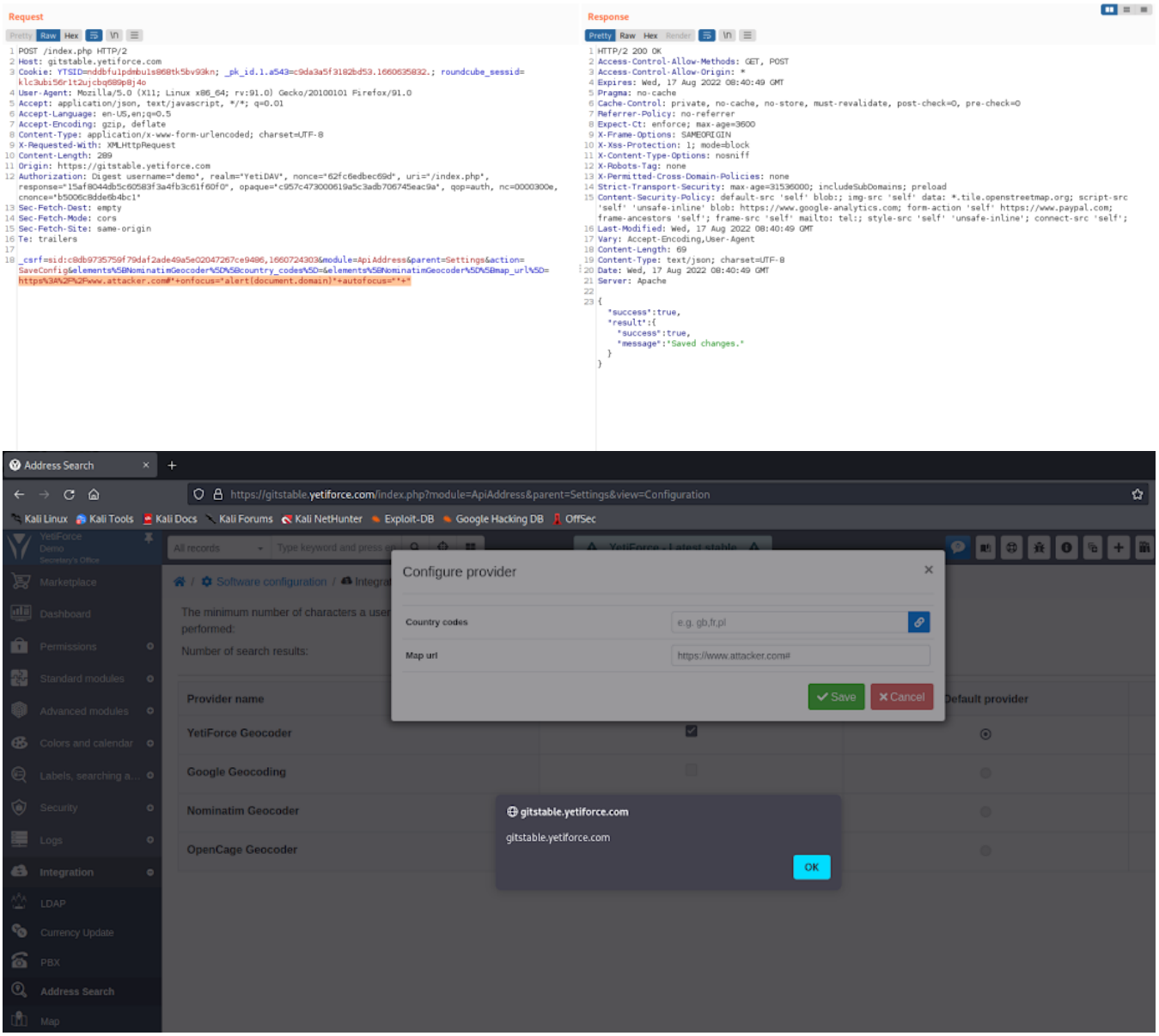
1- Login to the application
2- Access the ApiAddress Module via the following URL:
`https://gitstable.yetiforce.com/index.php?module=ApiAddress&parent=Settings&view=Configuration`
3- Click to the button "Configure provider",
Change the value of "map_url" parameter with the following payload:

```
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

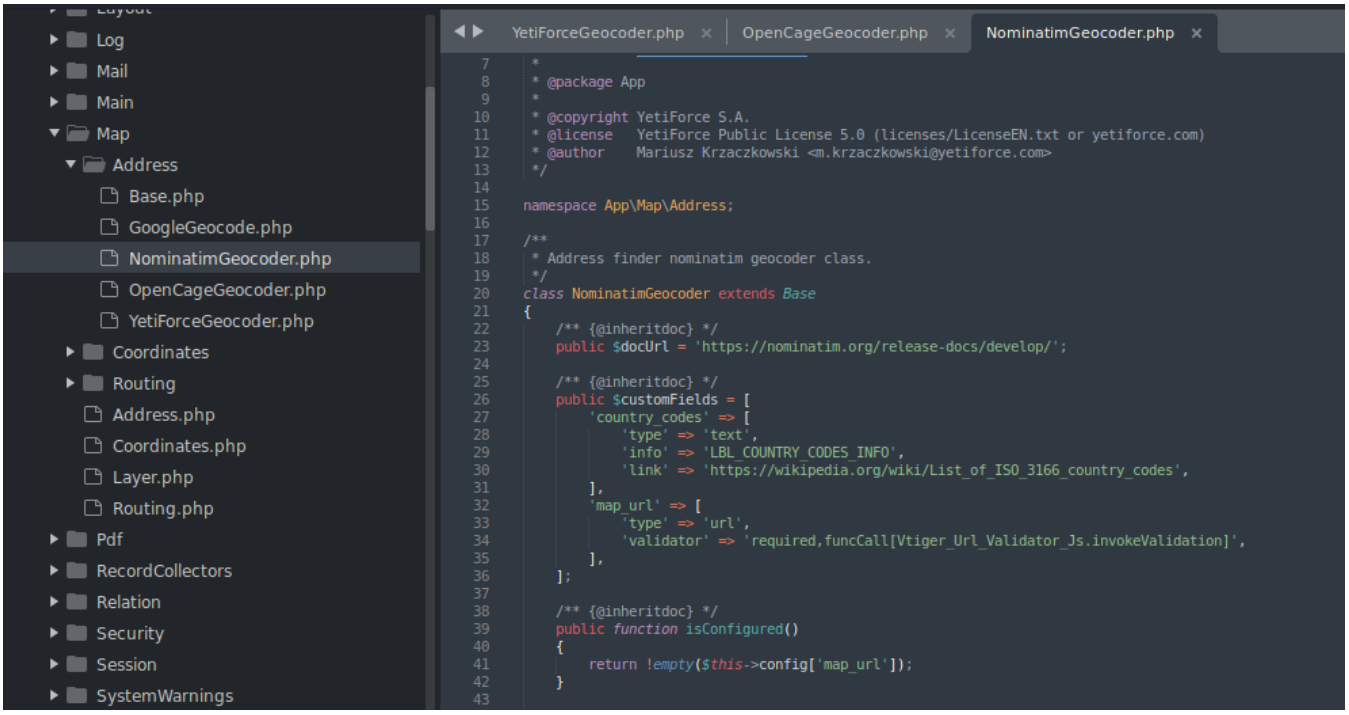


PoC Video

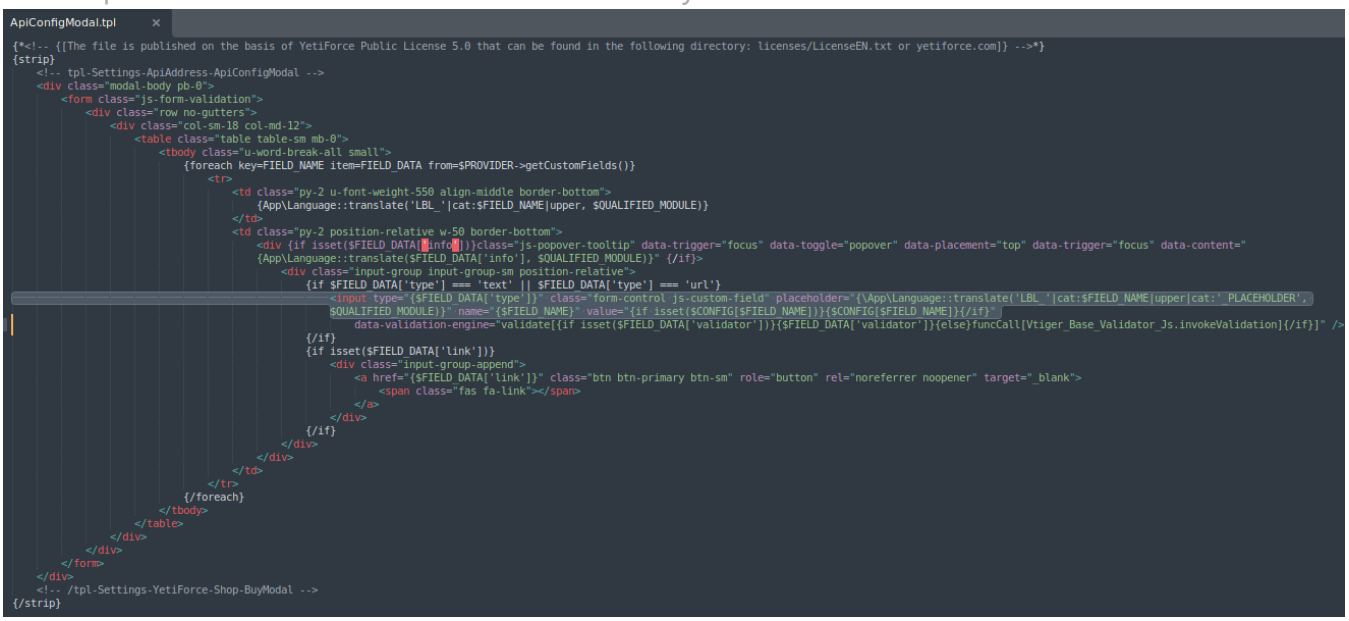
https://drive.google.com/file/d/1Bb_-s_2ELyR87vfkhVjb0U0VThb7eOzZ/view?usp=sharing

Vulnerable Code

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



2- The parameter is not encoded and use directly:



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

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

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