信息收集

主机发现

124

端口扫描

22,80

服务识别

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5c:8e:2c:cc:c1:b0:3e:7c:0e:22:34:d8:60:31:4e:62 (RSA)
|   256 81:fd:c6:4c:5a:50:0a:27:ea:83:38:64:b9:8b:bd:c1 (ECDSA)
|_  256 c1:8f:87:c1:52:09:27:60:5f:2e:2d:e0:08:03:72:c8 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Momentum | Index
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

子域名发现

敏感目录遍历

```
2022/02/05 10:03:30 Starting gobuster in directory enumeration mode
===============================================================
/css                  (Status: 301) [Size: 314] [--> http://192.168.56.124/css/]
/index.html           (Status: 200) [Size: 2001]
/manual               (Status: 301) [Size: 317] [--> http://192.168.56.124/manual/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.56.124/js/]
/img                  (Status: 301) [Size: 314] [--> http://192.168.56.124/img/]
```

web信息搜集

index.html:

4张图片没啥收获

点击进去图片发现有个隐藏页面opus-details.php,<-----遗漏的flag

/opus-details.php:

参数id存在xss

漏洞发现

威胁建模

apache2.4.38:cve-2019-0211本地提权

openssh7.9p1:无

网页:

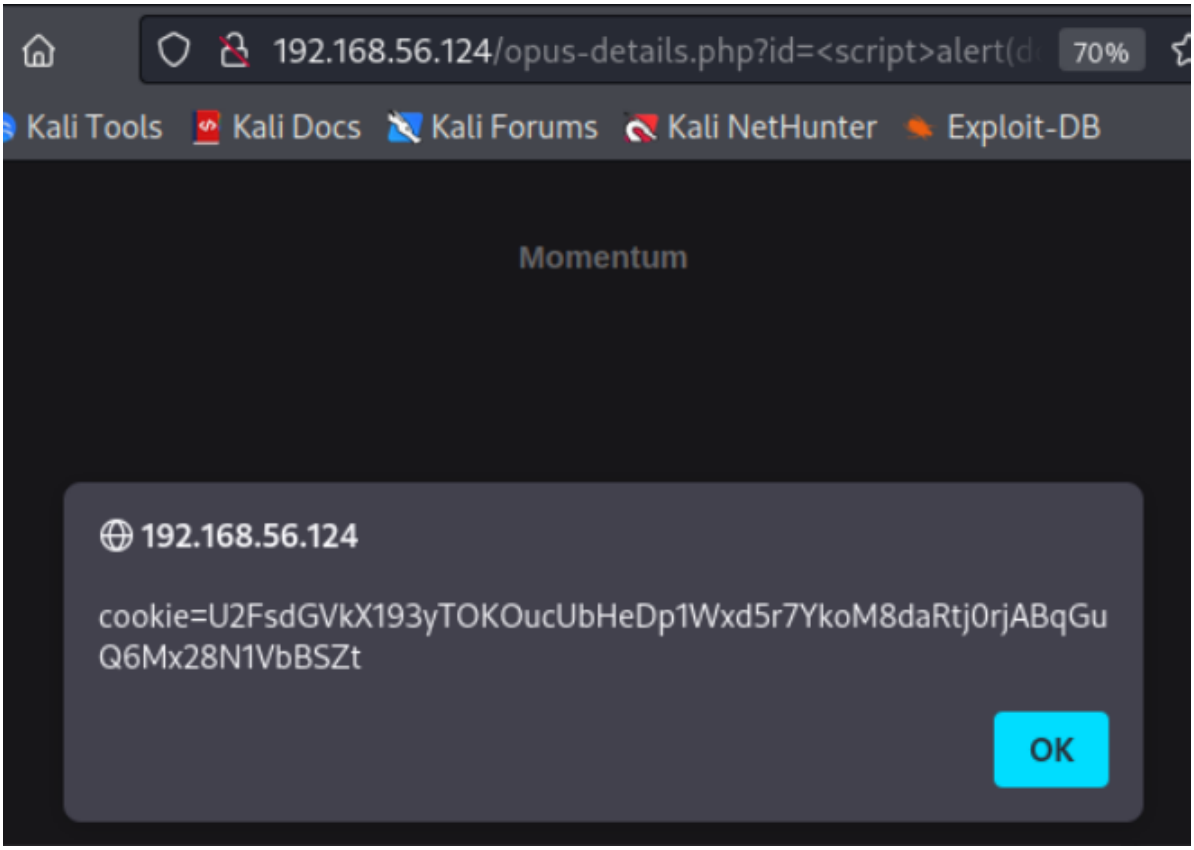
index.html:隐写术

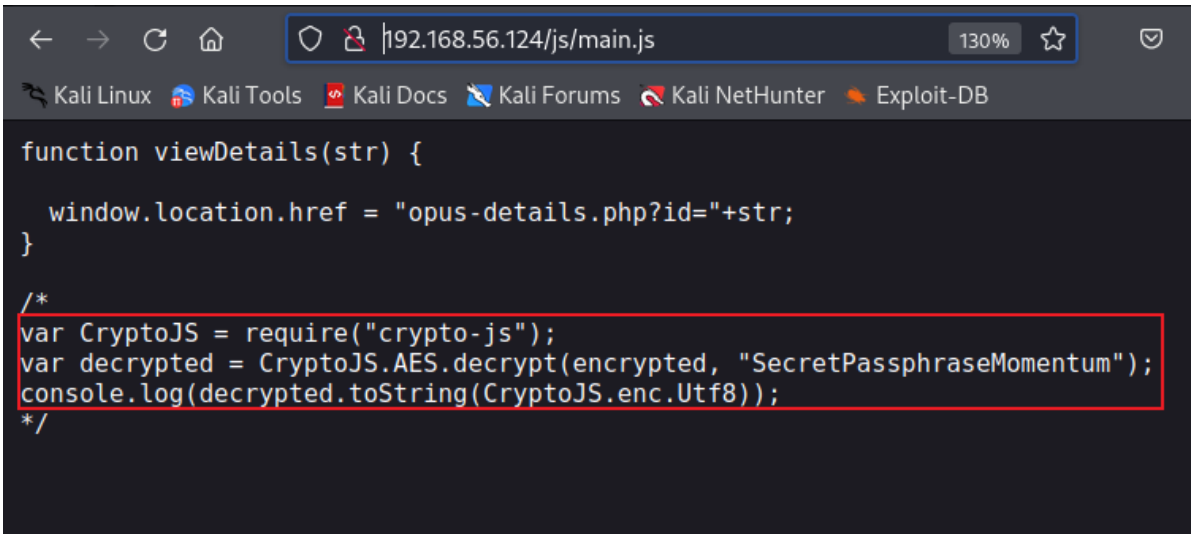
漏洞利用

边界突破

JS脚本分析

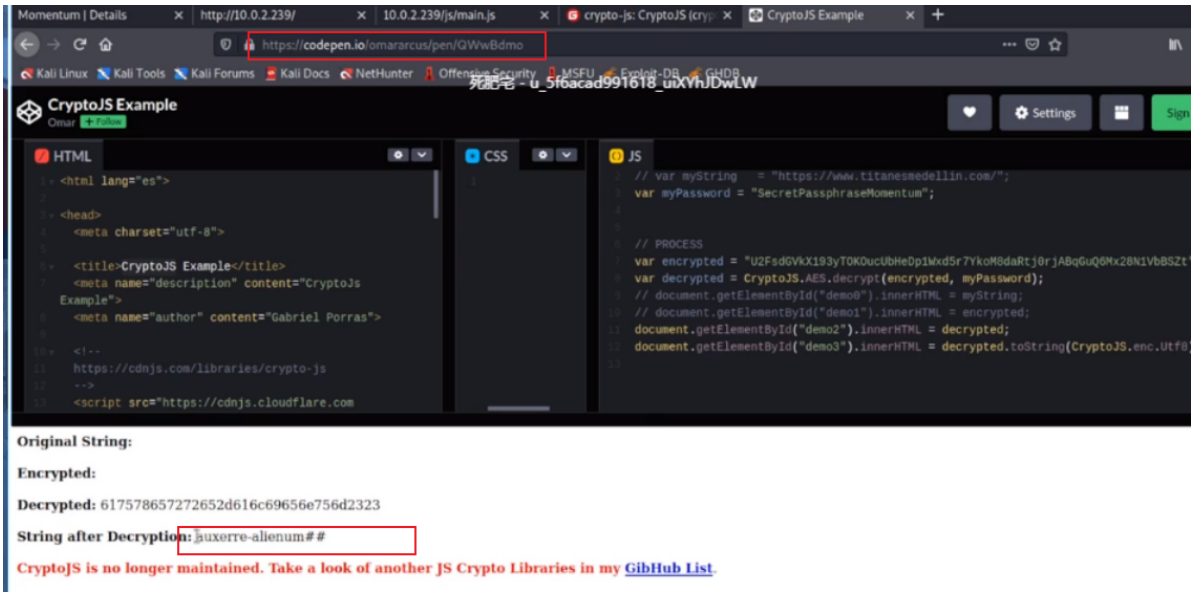
获取到本地cooie,尝试解密,找到脚本





发现这里用的时AES加密算法,自行查看加密和解密的过程

AES解密



权限提升

目标没有netstat,用ss查看端口,发现有redis

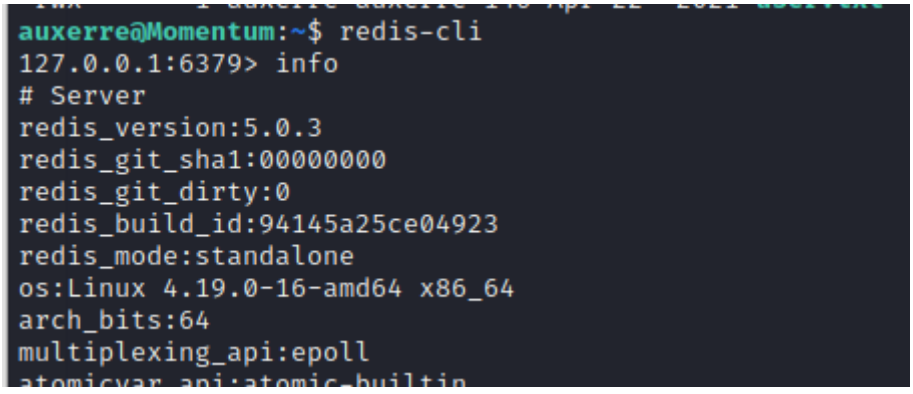
```
ss -pantu
```

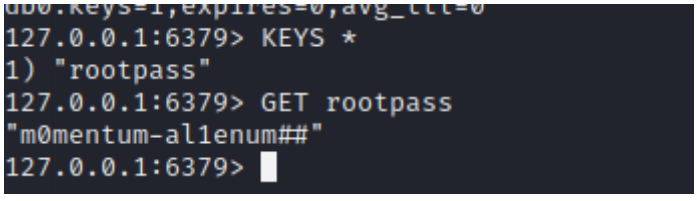
redis认证漏洞

redis默认开放在0.0.0.0:6379且没有认证

尝试不用密码登录redis

```
redis-cli #登录成功
#redis
info #查看是有权限
KEYS * #查看所有的key
GET rootpass #获取rootpass的值
```





再次su,提权成功

总结