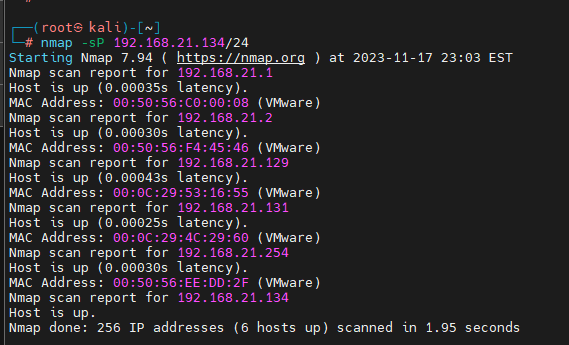
Momentum

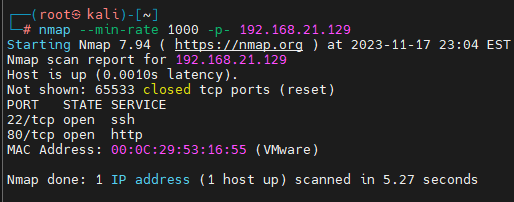
下载地址：<https://download.vulnhub.com/momentum/Momentum.ova>

主机发现

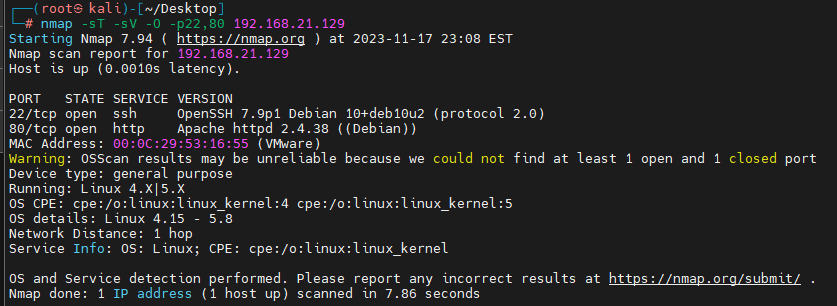


目标192.168.21.129

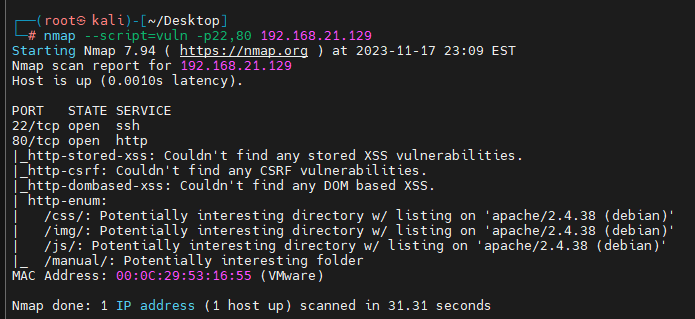
端口扫描



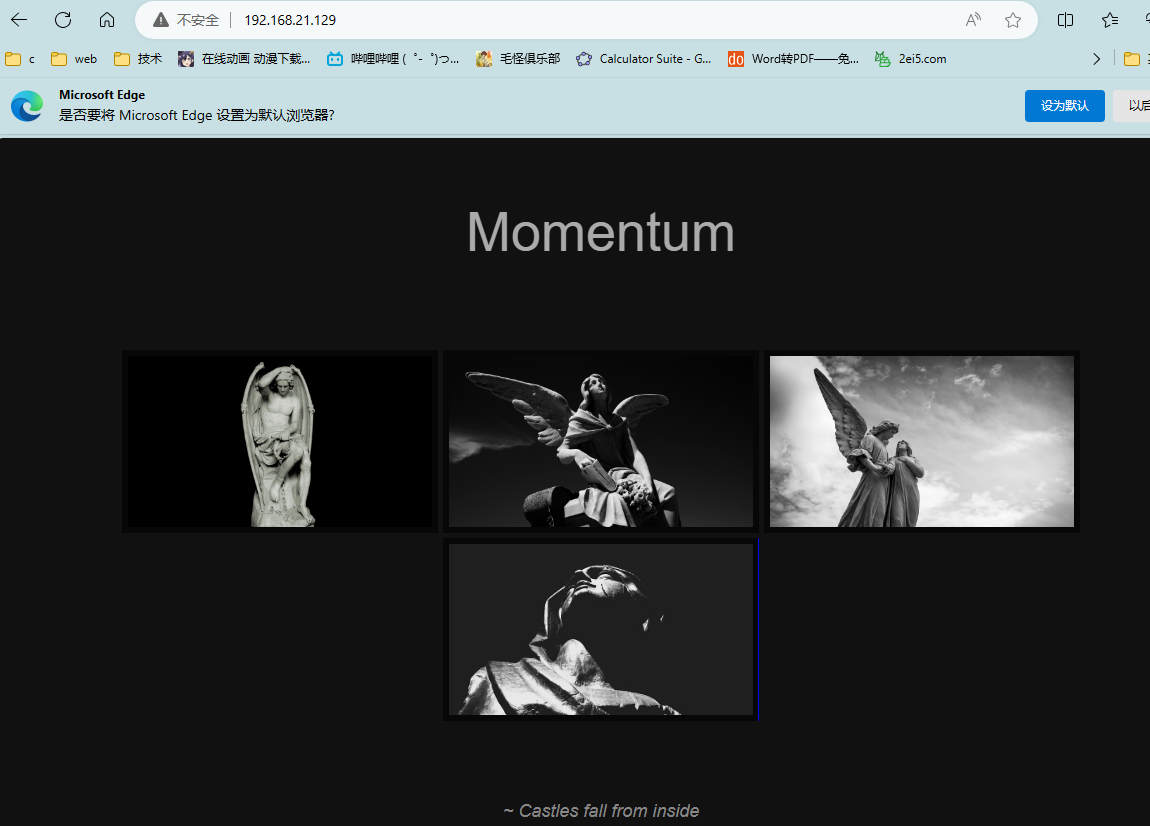
端口版本扫描



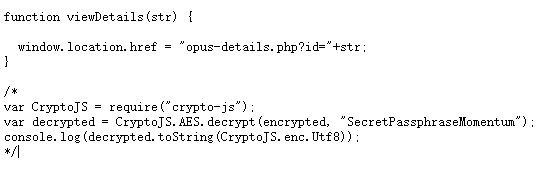
漏洞扫描



扫出来点目录简单看看



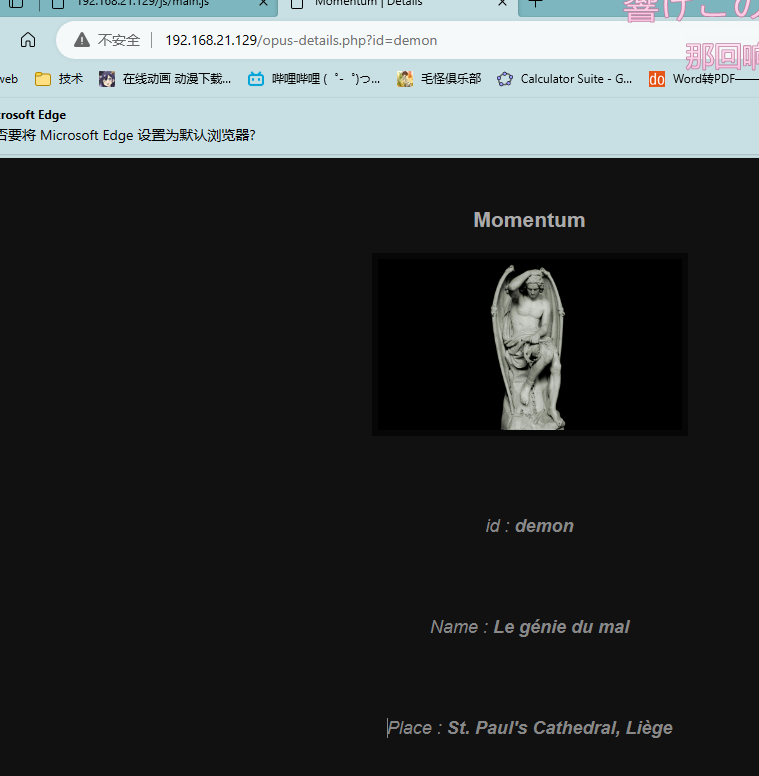
发现js里面有一点东西



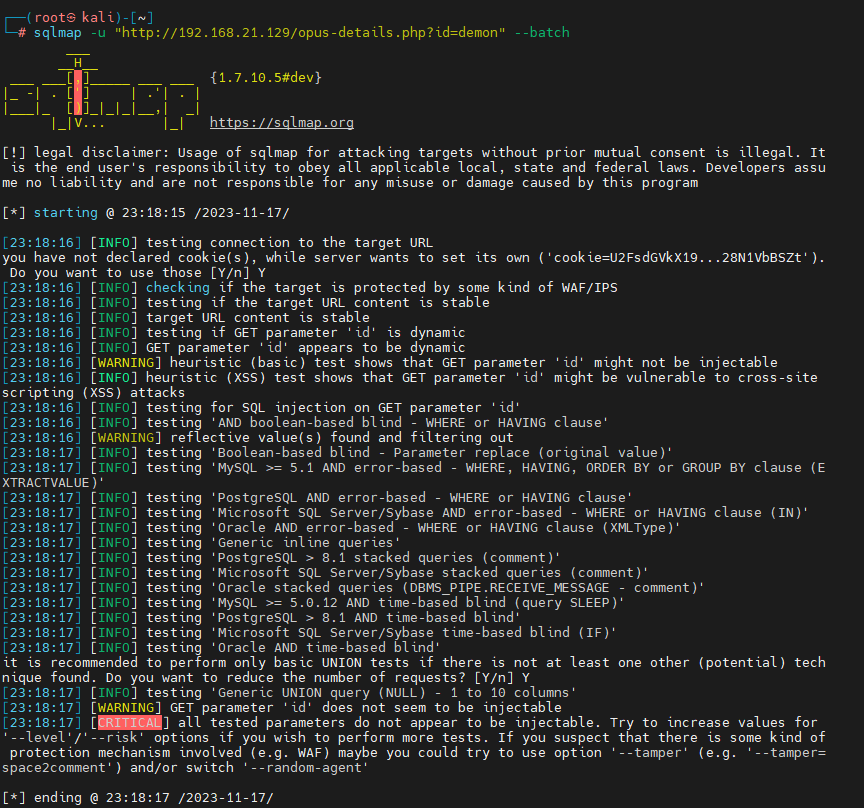
这里面告诉了我们了web文件有id传值，而且有aes加密还有密钥

跟二没有啥区别，还是要扫目录

发现点进去有点东西

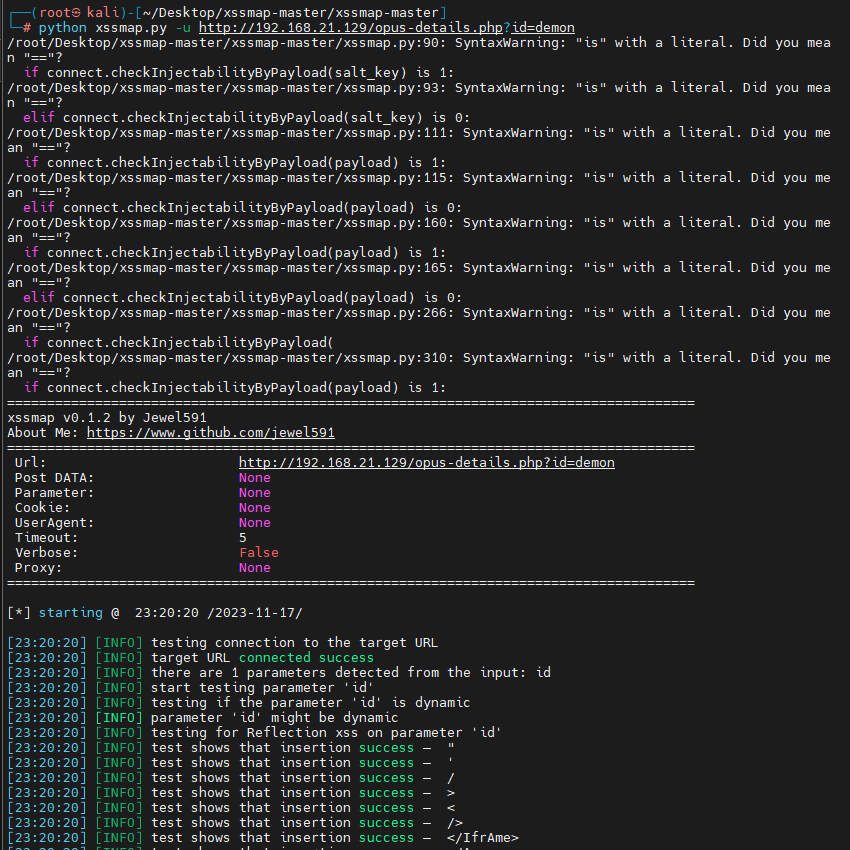


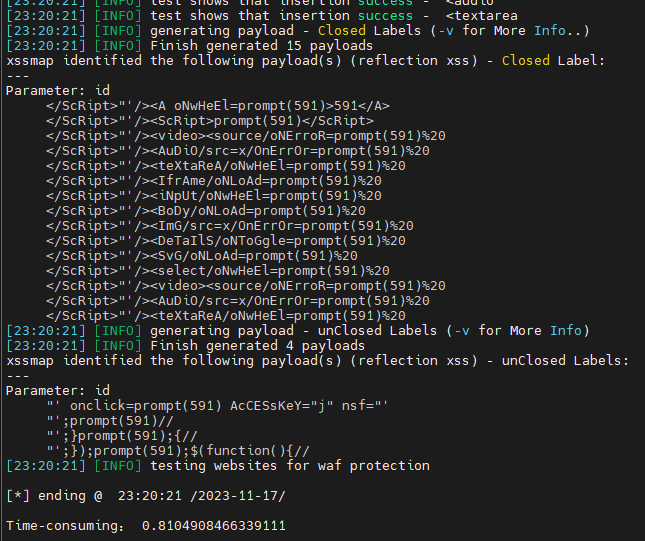
此处的url及时我们js看到的东西，看到传值就直接从sql注入开始（sqlmap直接梭哈）



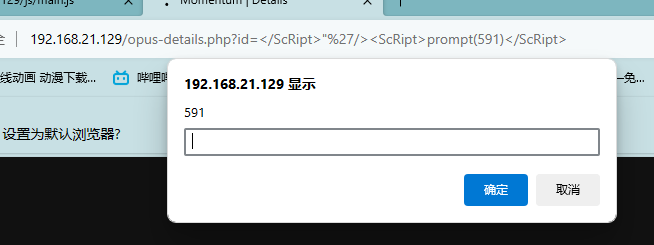
好直接寄

接下来试试xss（xssmap直接梭哈）

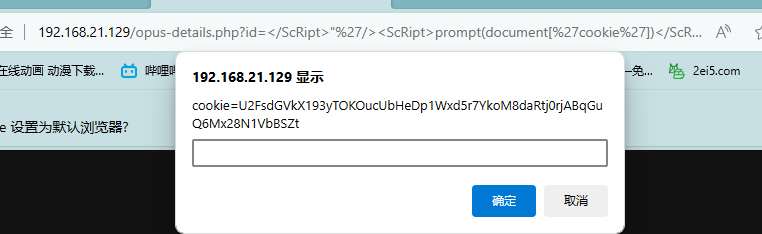




Payload直接出来，试一下就好了



这里直接获取cookie（注意替换591为document[%27cookie%27]就可以）



cookie=U2FsdGVkX193yTOKOucUbHeDp1Wxd5r7YkoM8daRtj0rjABqGuQ6Mx28N1VbBSZt

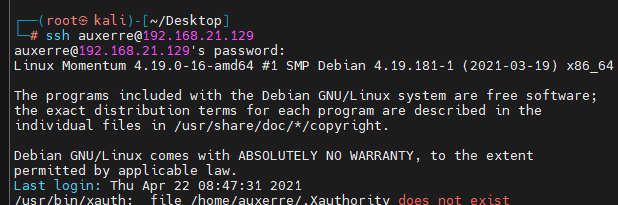
好js说了要aes解码（密钥在js里面）

这玩意网上多[AES加密-AES解密-在线AES加密解密工具 (jsons.cn)](http://www.jsons.cn/aesencrypt/)

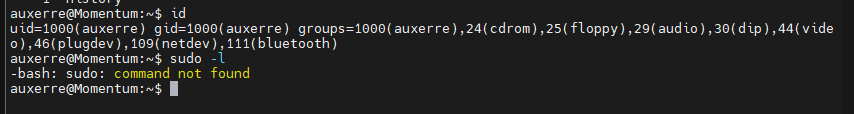


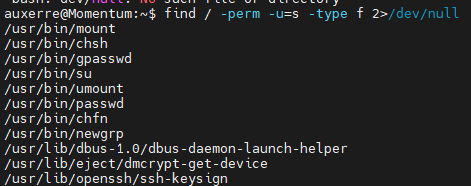
auxerre-alienum##

账号密码大概率就是这（账号是前面的，密码是一整个）

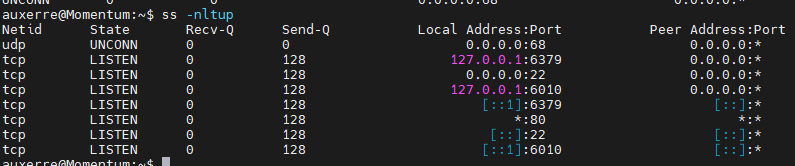


信息收集

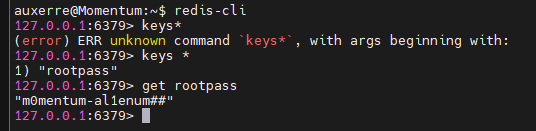




排查一下端口



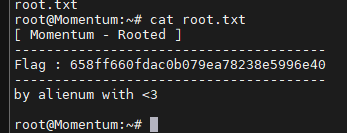
映入眼帘的127.0.0.1还是6379redis实锤



就是passwd



成功



结束