登录

【PHP代码审计】入门之路——第一篇

phpoop / 2017-12-04 13:51:00 / 浏览数 4295 新手 入门资料 顶(2) 踩(0)

0x01 前言

虽然市面上的代码审计的文章已经一大把了，但是还是决定重复造轮子，打算作为一个系列来写的，近年越来越多的安全研究人员投入到php应用的漏洞挖掘，相对应的代码

0x02 准备

技术准备：PHP基础，MySql

```
■■■■■Visual Studio
■■■■■■xampp
■■■■■phpStudy
■■■■■sql■■■■http://pan.baidu.com/s/1bId1eQ ■■■otrh
```

0x03 脑图

脑图主要总结了sql注入、xss跨站脚本攻击、csrf、xsrf、文件操作相关得漏洞、代码&&命令执行、设计缺陷以及SSRF七种常见漏洞，每种漏洞都有很多种的情况与案例，

0x04 SQL注入入门

注入的主要原因是程序员在写sql语句的时候没有根据使用的场景进行过滤导致的外部可以任意操作执行的sql，另外SQL语句有Select、Insert、Update和Delete四种类型，

浏览器输入：

```
http://127.0.0.1/test/test.php?id=1
```

然后在浏览器输入：

```
http://127.0.0.1/test/test.php?id=1'
```

可以从红色的方框中看到多了一个 '导致了 sql 错误爆错了
接着在浏览器输入：

```
http://127.0.0.1/test/test.php?id=1' and '1'='1
```

发现与图1中返回了一样的结果。
在次在浏览器输入：

```
http://127.0.0.1/test/test.php?id=1' and '1'='2
```

这次可以发现没有数据输出了 因为我们执行的语句中 goods_id 不止需要 等于1 并且还需要 `string(1) = string(2)` 才返回真 但是
`string(1)`永远不可能等于`string(2)` 所以条件不满足不返回数据，
从这里我们可以知道，我们外部带入的语句被成功的带入数据库并且查询了，所以可以判断有sql注入。

Mysql注释：
从--序列到行尾。请注意--的后面有个空格,注释风格要求第2个破折号后面至少跟一个字符(例如空格、tab、换行符、字符串等等)。
从#字符从行尾。
从/*序列到后面的*/序列。结束序列不一定在同一行中，因此该语法允许注释跨越多行。

下面的例子显示了3种风格的注释：

```
mysql>SELECT 1+1;     #
mysql>SELECT 1+1;     --
mysql>SELECT 1 /* xxxxxx */ + 1;■■■■■■■
```

可以看到页面现在返回的是 正常的说明这表列数大于1，自己加大直到爆错

一直输到8页面爆错了，说明我们这个表的字段数小于8，那么就是说此表的字段为7

页面输出了1,2,3,4,5,6,7 这些都是输出点

分别输出了当前连接的用户，数据， 服务器版本

获取全部的库

获取test库的所有表
获取16进制：
SELECT hex('test');
结果74657374
加上0x+74657374
16进制：0x74657374

```
http://127.0.0.1/test/test.php?id=-1 union select 1,2,group_concat(table_name) from information_schema.tables where table_sche
```

table_schema === 库名16进制编码
table_name === 表名16进制编码

获取 tdb_admin 表的所有字段

获取 tdb_admin 表数据

0x05 修复方法

```
$id=@intval($_GET['id']);
```

本文是这博客的第一篇文章，希望能够帮助刚入门的萌新学习：）

上一篇：Meterpreter载荷执行原理分析 下一篇：Linux奇技y巧之类的探讨
1. 3 条回复


大先知 2017-12-04 16:24:43

围观大佬

0 回复Ta


r00tuser 2017-12-04 17:20:40

第一眼看到，使用工具:visual studio，被吓到了。后来发现是vs code，想起了被微软神器统治的日子。。

期待系列文章~

0 回复Ta


piglet 2017-12-05 09:42:46

期待后续文章

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板