审计笔记

奇怪的文件:

inc/checklogin.php

代码:

<?php

$user=$\_COOKIE['user'];

if ($user==""){

header("Location: ?r=login");

exit;

}

?>

意思：验证是否有user这个cookie 如果无

此cookie转到 当前地址加?r=login

然后执行exit;

conn.php文件：

设置数据库编码为UTF-8无宽字节注入

代码:

mysql\_query('SET NAMES UTF8') or die('字符集设置错误'.mysql\_error());

设置$llink=addslashes($\_GET['r']);

接奇怪的文件:

Admin/index.php 导入模板 地址为

Admin/files 主页为index.php

主页导入:

Checklogin.php

Conn.php

地址为:

../Inc/checklogin.php

..inc/conn.php';

回到之前奇怪的文件

代码并不奇怪

如果cookie的内容没有user或者没有user这个cookie

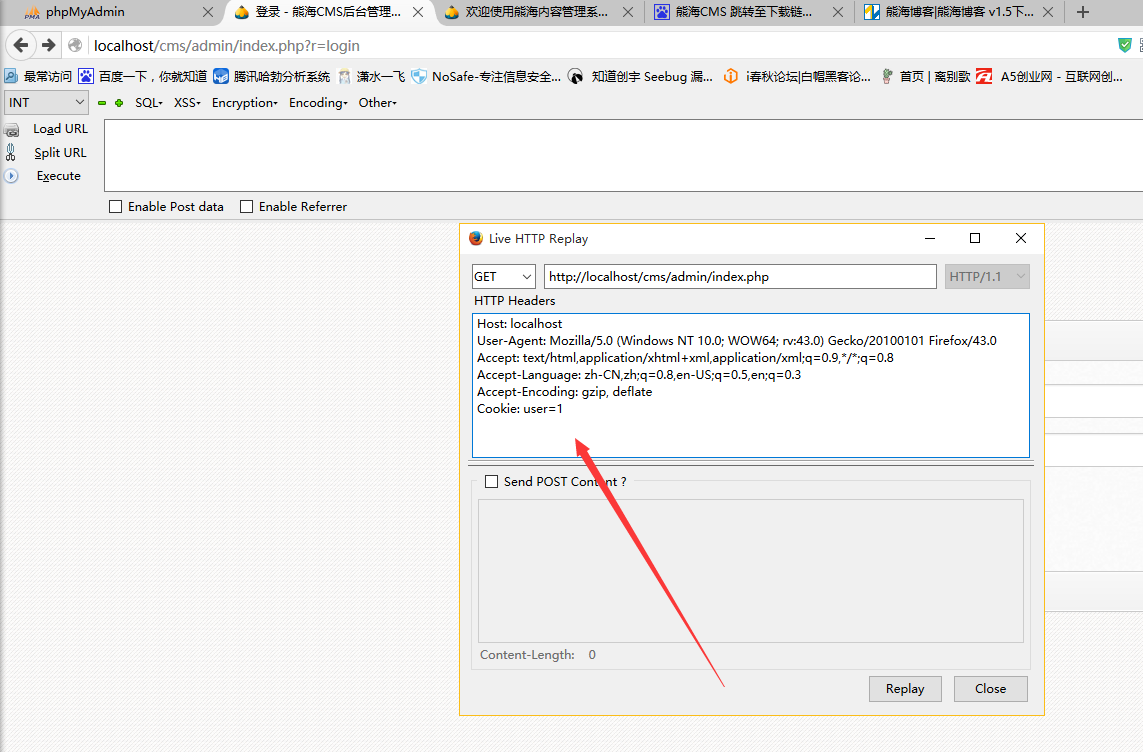
即跳转到?r=login

配合主页文件即为login.php

漏洞利用:

1.登陆抓包

2.设置cookie内容 User= 什么都可以 不能为空



放包 即进入后台页面：

