华金安全性测试报告（管理后台）

1. 安全测试用例执行结果

1、代码注入(高)

1.1 测试描述：跨站点脚本编制（参数对特殊字符过滤不完善，导致可用插入前端脚本代码）

注入成功截图如下：



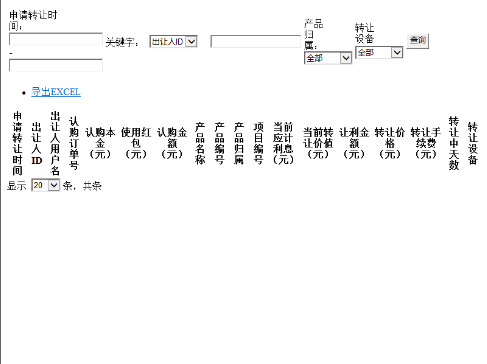
存在问题的url如下

|  |  |
| --- | --- |
| URL | 参数 |
| http://admintest.hrjk-p2p.com/accountSystem/accountBackendRecharge | accountBackendRecharge |
| http://admintest.hrjk-p2p.com/bankcard/bankcardManageEnterprise | bankcardManageEnterprise |
| http://admintest.hrjk-p2p.com/order/assignIng | stime |
| product\_sourceid |
| platform |
| etime |
| assignIng |
| http://admintest.hrjk-p2p.com/order/assignSuccess | assignSuccess |
| http://admintest.hrjk-p2p.com/order/labelHaveAlready | scomplete\_time |
| numPerPage |
| labelHaveAlready |
| ecomplete\_time |
| http://admintest.hrjk-p2p.com/order/labelHaveAlready | scomplete\_time |
| http://admintest.hrjk-p2p.com/order/payOff | payOff |
| http://admintest.hrjk-p2p.com/order/repayIng | repayIng |
| http://admintest.hrjk-p2p.com/order/subscriptionFail | subscriptionFail |
| stime |
| product\_sourceid |
| keyword\_type |
| keyword |
| etime |
| http://admintest.hrjk-p2p.com/order/subscriptionIng | subscriptionIng |
| stime |
| product\_sourceid |
| etime |
| http://admintest.hrjk-p2p.com/others/article | article |
| http://admintest.hrjk-p2p.com/others/banner | banner |
| http://admintest.hrjk-p2p.com/others/bannerPosition | bannerPosition |
| http://admintest.hrjk-p2p.com/others/help | help |
| http://admintest.hrjk-p2p.com/others/payBank | payBank |
| http://admintest.hrjk-p2p.com/others/paySetting | paySetting |
| http://admintest.hrjk-p2p.com/others/userRisk | userRisk |
| http://admintest.hrjk-p2p.com/product/checkPending | user\_name |
| real\_name |
| product\_sourceid |
| numPerPage |
| mobile |
| issuer\_name |
| currentIndex |
| branchcompany\_id |
| http://admintest.hrjk-p2p.com/product/contract | numPerPage |
| contract |
| http://admintest.hrjk-p2p.com/user/borrowFirm | userid |
| stime |
| select |
| platform |
| etime |
| borrowFirm |
| http://admintest.hrjk-p2p.com/recharge/listBorrowerRechargeFail | listBorrowerRechargeFail |
| http://admintest.hrjk-p2p.com/recharge/listBorrowerRechargeSuccess |  |
| http://admintest.hrjk-p2p.com/recharge/listInvestorRechargeSuccess | stime |
| recharge\_way |
| platform |
| pageNum |
| listInvestorRechargeSuccess |
| keyword\_type |
| keyword |
| http://admintest.hrjk-p2p.com/repayment/listManagePayment | listManagePayment |
| http://admintest.hrjk-p2p.com/repayment/projectListNormal | projectListNormal |
| http://admintest.hrjk-p2p.com/user/borrowUser | userid |
| stime |
| platform |
| numPerPage |
| keywords |
| is\_borrow\_buy |
| http://admintest.hrjk-p2p.com/user/list | userid |
| select |
| platform |
| pageNum |
| numPerPage |

1.2 测试描述：跨站点请求伪造（钓鱼站点可伪造请求）（中）

测试截图如下:

1、正常请求



2、修改头信息**Referer:** http://bogus.referer.ibm.com，发去请求，得到了正常响应



|  |
| --- |
| 存在问题的URL |
| http://admintest.hrjk-p2p.com/order/assignIng |
| http://admintest.hrjk-p2p.com/order/assignSuccess |
| http://admintest.hrjk-p2p.com/order/payOff |
| http://admintest.hrjk-p2p.com/others/banner |
| http://admintest.hrjk-p2p.com/product/checkPending |
| http://admintest.hrjk-p2p.com/product/contract |
| http://admintest.hrjk-p2p.com/product/releasePending |
| http://admintest.hrjk-p2p.com/product/repayIng |
| http://admintest.hrjk-p2p.com/recharge/listBorrowerRechargeFail |
| http://admintest.hrjk-p2p.com/recharge/listBorrowerRechargeSuccess |
| http://admintest.hrjk-p2p.com/recharge/listInvestorRechargeFail |
| http://admintest.hrjk-p2p.com/repayment/projectListNormal |
| http://admintest.hrjk-p2p.com/withdraw/applyExamine |
| http://admintest.hrjk-p2p.com/withdraw/applyExamineBorrower |
| http://admintest.hrjk-p2p.com/withdraw/examineFail |
| http://admintest.hrjk-p2p.com/withdraw/examineFailBorrower |
| http://admintest.hrjk-p2p.com/withdraw/listOfFailBorrower |
| http://admintest.hrjk-p2p.com/withdraw/listOfSuccessBorrower |

1. 系统安全机制测试结果
2. 银行存管交互安全机制（高）

安全机制描述：

使用接口前，每个平台生成公/私密钥对，所有请求和返回报文都包含签名参数，接收方务必检查签名的正确性，以保证业务数据合法安全。  
签名使用标准签名算法”SHA1withRSA” 。

1. 接口重复调用
2. 数据传输加密