文档编号：LH-20161118SKY

密　　级：【限制级-仅对最终用户查阅】

渗透测试报告

北京江南天安科技有限公司

网络安全攻防实验室

2016 年 11 月 18 日

文档信息

项目名称		石科院渗透测试服务	
文档名称		渗透测试报告	
文档编号		2016-11	
版本号	日期	参与人员	更新说明
1.0	2016-11	于林涛	建立文档，初始化

分发控制

编号	读者	文档权限	与文档的主要关系
1	攻防实验室	编写，修改	负责编制、修改
2			
3			

版权说明

本文件中出现的全部内容，除另有特别注明，均遵守双方签署的保密条款。

目录

一、渗透测试概述

渗透测试（Penetration Test）是为了测试企业网络抵御攻击的能力而设计的一种测试方法，是信息与系统安全运行保障的重要手段之一，是风险评估工作重要安全结论的辅助验证手段之一。渗透测试是在可控条件下，采取可控的、不造成不可弥补损失的黑客入侵手法，对目标网络和系统完全模拟黑客可能使用的攻击技术和漏洞发现技术发起真正攻击，对目标系统的安全做深入的探测，发现系统最脆弱的环节。渗透测试能够直观的让管理人员知道网络所面临的问题。

实际上渗透测试并没有严格的分类方式，普遍认同的几种分类方法如下。

根据渗透方法分类：

- **黑箱测试：**黑箱测试又被称为所谓的“Zero-Knowledge Testing”，渗透者完全处于对系统一无所知的状态，通常这类型测试，最初的信息获取来自于 DNS、Web、Email 及各种公开对外的服务器。
- **白盒测试：**白盒测试与黑箱测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通。这类测试的目的是模拟企业内部雇员的越权操作。

- **隐秘测试：** 隐秘测试是对被测单位而言的，通常情况下，接受渗透测试的单位网络管理部门会收到通知：在某些时段进行测试。因此能够监测网络中出现的变化。但隐秘测试则被测单位也仅有极少数人知晓测试的存在，因此能够有效地检验单位中的信息安全事件监控、响应、恢复做得是否到位。

- **本次渗透测试采取黑盒测试方法完成测试工作。**

二、测试对象和目标

渗透测试利用网络安全扫描器、专用安全测试工具和富有经验的安全工程师的人工经验，通过互联网对网络进行非破坏性质的模拟黑客攻击，目的是侵入系统并获取敏感信息，将入侵的过程和细节产生报告给用户。

序号	IP 或域名	时间	支持方式	备注
1	www.sylzyhg.com www.syxbsyjg.com www.chinarefining.com	2016-11	在线	石科院

三、测试组织

1.1 测试方法

1.1.1 信息收集

信息收集分析几乎是所有入侵攻击的前提/前奏/基础。“知己知彼，百战不殆”，信息收集分析就是完成的这个任务。通过信息收集分析，攻击者（测试者）可以相应地、有针对性地制定入侵攻击的计划，提高入侵的成功率、减小暴露或被发现的几率。

信息收集的方法包括主机网络扫描、端口扫描、操作类型判别、应用判别、账号扫描、配置判别等等。入侵攻击常用的工具包括 nmap、nessus、X-SCAN 等，有时，操作系统中内置的许多工具（例如 telnet）也可以成为非常有效的攻击入侵武器。

1.1.2 权限提升

通过收集信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试者可以直接控制目标系统，这时测试者可以直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程重大弱点，但是可以获得远程普通权限，这时测试者可以通过该普通权限进一步收集目标系统信息。接下来，尽最大努力获取本地权限，收集本地资料信息，寻求本地权限升级的机会。这些不停的信息收集分析、权限升级的结果构成了整个渗透测试过程的输出。

1.1.3 溢出测试

当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。

1.1.4 SQL 注入攻击

SQL 注入常见于那些应用了 SQL 数据库后端的网站服务器，黑客通过向提交某些特殊 SQL 语句，最终可能获取、篡改、控制网站 服务器端数据库中的内容。此类漏洞是黑客最常用的入侵方式之一。

1.1.5 检测页面隐藏字段

网站应用系统常采用隐藏字段存储信息。许多基于网站的电子商务应用程序用隐藏字段来存储商品价格、用户名、密码等敏感内容。心存恶意的用户，通过操作隐藏字段内容，达到恶意交易和窃取信息等行为，是一种非常危险的漏洞。

1.1.6 跨站攻击

攻击者可以借助网站来攻击访问此网站的终端用户，来获得用户口令或使用站点挂马来控制客户端。

1.1.7 第三方软件误配置

第三方软件的错误设置可能导致黑客利用该漏洞构造不同类型

的入侵攻击。

1.1.8 Cookie 利用

网站应用系统常使用 cookies 机制在客户端主机上保存某些信息，例如用户 ID、口令、时间戳等。黑客可能通过篡改 cookies 内容，获取用户的账号，导致严重的后果。

1.1.9 后门程序检查

系统开发过程中遗留的后门和调试选项可能被黑客所利用，导致黑客轻易地从捷径实施攻击。

1.1.10 其他测试

在渗透测试中还需要借助暴力破解、网络嗅探等其他方法，目的也是为获取用户名及密码。

1.2 测试流程

本次测试工作流程如图 2 所示，1）进行信息收集，2）进行制定攻击方案。3）高低级风险利用。4）提升权限等级。

另外，信息的收集和分析伴随着每一个渗透测试步骤，每一个步骤又有三个组成部分：操作、响应和结果分析。

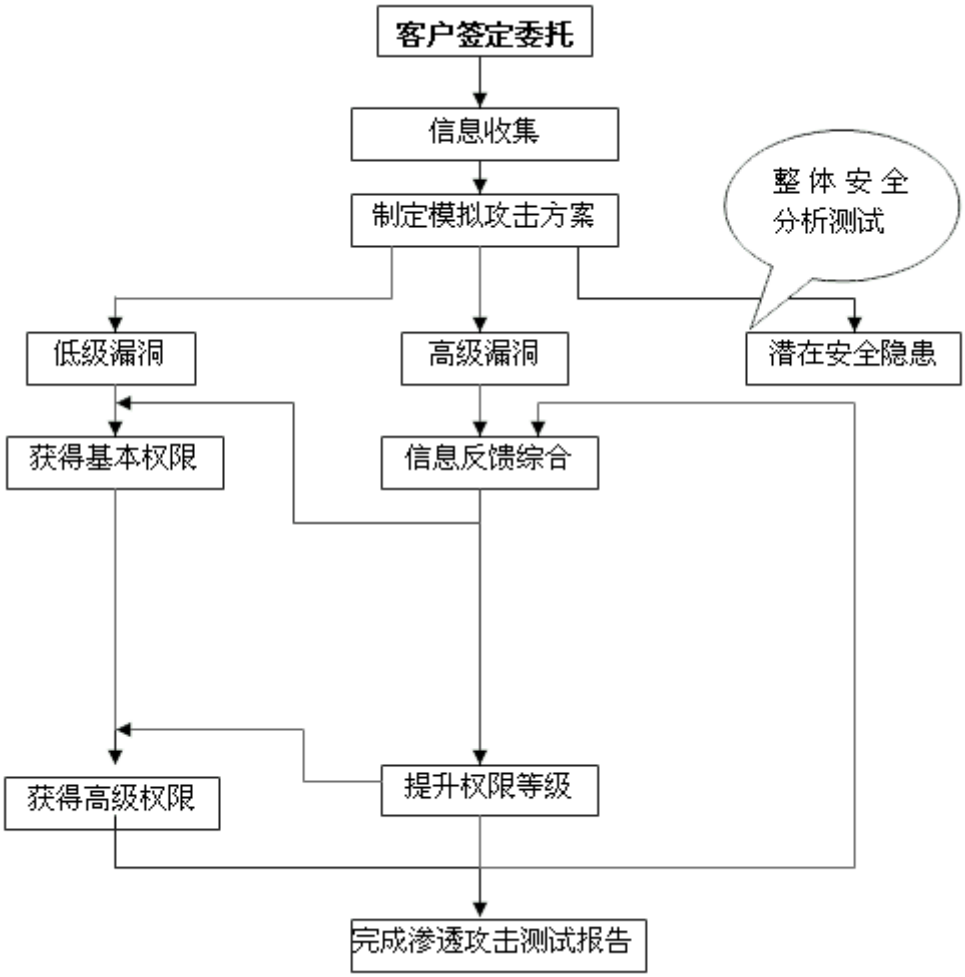


图 1 测试工作流程

四、测试中所用工具

1.3 应用层工具

1.3.1 IBM Appscan Scanner

IBM Rational® AppScan® 是一款自动进行漏洞评估的 Web 应用程序安全性测试工具。

AppScan 通过自动化的安全性分析检测易受攻击的漏洞，降低与

手动漏洞测试相关的成本并帮助防护网络攻击的威胁。

- 支持全面和自动化的 Web 应用程序漏洞测试
- 全面集成的恶意软件扫描：扫描 Web 站点上的嵌入式恶意软件和链接到恶意或不良网站的链接。
- 提供自定义和可扩展的功能：AppScan eXtension Framework 让用户社区能够构建和共享开源插件。
- 自动化渗透测试的功能：先进的测试实用工具和 Pyscan 框架为手动测试提供了补充，提供了更强大的功能和效率。
- 支持安全性测试以检测新出现的 Web 漏洞：目前包含检测 RSS 订阅源注入、易受攻击的 ActiveX、文件上传、Flash 源代码泄露等。
- 法规遵从性报表：40 款开箱即用的遵从性报表，包括 PCI 数据安全标准、支付应用程序数据安全（PA-DSS）（新）、ISO 27001 和 ISO 27002（新）和 Basel II。
- 对 Web 应用程序对组织造成的安全性和法规遵从性风险进行可视化管理。
- 让信息安全工具能够扩展审计活动，并且确保 Web 应用程序都是经过测试的。
- 支持组织邀请其开发和质量保证团队参与并对其进行培训，在整个软件开发生命周期中实施控制，以降低风险和成本。
- 结合使用各种测试技术以提供尽可能彻底的自动化评估。
- 提供适合每一个参与的利益相关人的协作功能和工具 - 信息安

全、开发、质量保证和管理。

- Acunetix 开创了 web 应用程序安全扫描技术：早在 1997 年 Acunetix 工程师就已关注网络安全并成为网络站点分析和漏洞检测方面的编程领导者。
- Acunetix Web Vulnerability Scanner 包含多种创新功能：
- AcuSensor 技术
- 自动的客户端脚本分析器，允许对 Ajax 和 Web 2.0 应用程序进行安全性测试。
- 业内最先进且深入的 SQL 注入和跨站脚本测试
- 高级渗透测试工具，例如 HTTP Editor 和 HTTP Fuzzer
- 可视化宏记录器帮助您轻松测试 web 表格和受密码保护的区域
- 支持含有 CAPTHCA 的页面，单个开始指令和 Two Factor（双因素）验证机制
- 丰富的报告功能，包括 VISA PCI 依从性报告
- 高速的多线程扫描器轻松检索成千上万个页面
- 智能爬行程序检测 web 服务器类型和应用程序语言
- Acunetix 检索并分析网站，包括 flash 内容、SOAP 和 AJAX
- 端口扫描 web 服务器并对在服务器上运行的网络服务执行安全检查

1.4 其他方法和工具

端口扫描程序——专用的对网络端口进行扫描的工具，定义好 IP 地址范围和端口后就可以开始扫描。

网络侦查和服务器侦查程序——通过该种程序可以侦查出网络上已经开启的端口。如 PingPro 的工作是通过监控远程工程调用服务。

以及测试人员自行编译的渗透测试工具等等。

1.6 手工方法测试

利用熟悉的 web 攻击手法进行实战测试

五、测试结论

www.sylzyhg.com，www.syxbsyjg.com,和 www.chinarefining.com 三个网站同属 JournalX 期刊稿件处理系统，具有相同的技术架构，所以有共同的脆弱性特征，下面将统一说明。

1.1 后台管理地址泄露

漏洞等级： 中危

漏洞地址： http://www.sylzyhg.com/ht-login.jsp

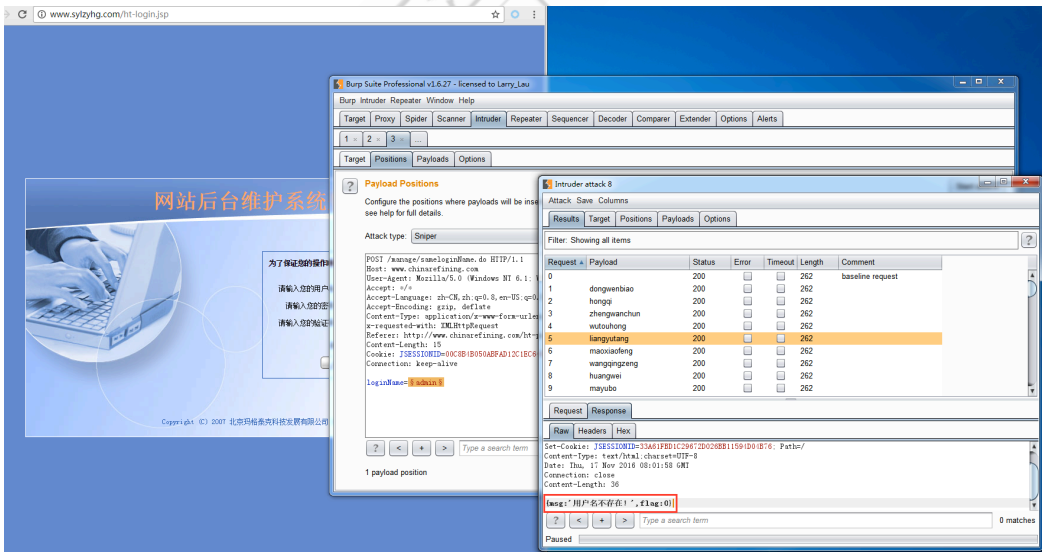
http://www. syxbsyjg.com/ht-login.jsp

http://www. chinarefining.com/ht-login.jsp

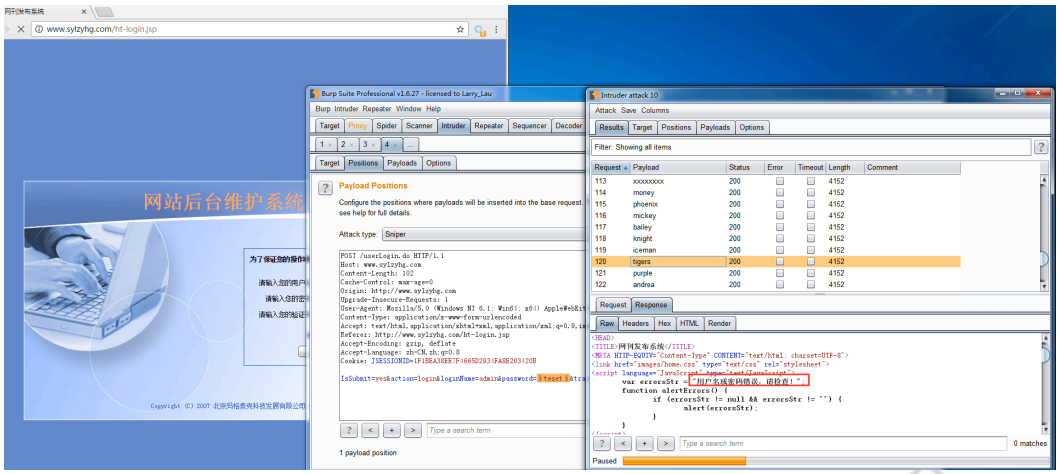
漏洞说明：

通过探测，发现这三个系统都存在公网可以访问的管理后台，并且可以暴力破解用户名和密码，如下图：

通过“找回密码”功能，探测系统存在的管理用户：



然后利用得到的用户名探测密码：



1.2 得到后台管理用户

漏洞等级： 高危

漏洞地址： http://www.sylzyhg.com/ht-login.jsp

漏洞说明：

利用社工技术，与北京玛格泰克科技发展有限公司的技术支持人员交谈，骗取信任，拿到账号密码。


www.sylzyhg.com/userLogin.do
功能菜单
管理首页
权限管理
权限组管理
功能权限管理
后台用户管理
网刊管理
年卷期列表
文章信息列表
被删除文章列表
热点文章列表
学科分类列表
专业分类列表
栏目分类列表
Email Alert
RSS列表
文章反馈列表
生成作者索引
过刊页面检查
文章查缺
生成索引
稿件检索
会员管理
会员信息列表
欢迎进入网站后台维护系统
版本号：2013-07-17
当前位置：网站后台维护 → 系统管理中心
版权所有：北京玛格泰克科技发展有限公司 2008, All Rights Reserved.


模块维护
添加模块
序号 名称 说明 地址 权限组分组 操作
1 文章点击数统计 文章点击数统计 manage/browse/listBrowseArticle.do 点击分析 编辑 删除
2 文章下载数统计 文章下载数统计 manage/download/listDownloadArticle.do 点击分析 编辑 删除
3 栏目统计更新 栏目统计更新 manage/updateChannelStat.do 点击分析 编辑 删除
4 订单信息列表 订单信息列表 manage/order/listOrderInfo.do 发行管理 编辑 删除
5 订阅详细列表 订阅详细列表 manage/order/listOrderDetail.do 发行管理 编辑 删除
6 产品信息列表 产品信息列表 manage/order/listProductInfo.do 发行管理 编辑 删除
7 订阅信息统计 订阅信息统计 manage/order/statOrderDetail.do 发行管理 编辑 删除
8 订户类型 订户类型 manage/subscribersort/listSubscriberSortInfo.do 发行管理 编辑 删除
9 图书信息列表 图书信息列表 manage/order/listBooksInfo.do 发行管理 编辑 删除
10 邮签模板列表 邮签模板列表 manage/order/printFormatTemplateList.do 发行管理 编辑 删除
11 浮动广告管理 浮动广告列表 manage/adInfo/listAdInfo.do 广告管理 编辑 删除
12 广告位信息 广告位信息 manage/location/listLocationInfo.do 广告管理 编辑 删除
13 广告信息查询 广告信息查询 manage/location/listAdvInfo.do 广告管理 编辑 删除
14 参会人员导出 参会人员导出 manage/canhuirenyuan/listCanhuirenyuanInfo.do 会议管理 编辑 删除
15 会议报名 会议报名 manage/conference/listConferences.do 会议管理 编辑 删除
16 已到款项记录 商品信息管理 manage/money/providerFeeList.do?moneyStatus=T 会员管理 编辑 删除
17 未到款项记录 商品信息管理 manage/money/providerFeeList.do?moneyStatus=F 会员管理 编辑 删除
18 已到款项记录 已到款项记录 manage/money/userFeeList.do?moneyStatus=T 会员管理 编辑 删除
19 继续教育 继续教育 manage/kaojuan/listKaoJuanInfo.do 会员管理 编辑 删除
20 下载文件列表 下载文件列表 manage/down/listDownInfo.do 会员管理 编辑 删除
21 会员信息列表 会员信息列表 manage/user/listUserInfo.do 会员管理 编辑 删除
22 会员缴费列表 会员缴费列表 manage/finance/userFeeList.do 会员管理 编辑 删除
23 免费IP地址段 免费IP地址段 manage/ipaddr/listIpAddrInfo.do?IpType 会员管理 编辑 删除

1.3 弱口令漏洞

漏洞等级： 高危

漏洞地址： http://www.sylzyhg.com/ht-login.jsp

http://www. syxbsyjg.com/ht-login.jsp

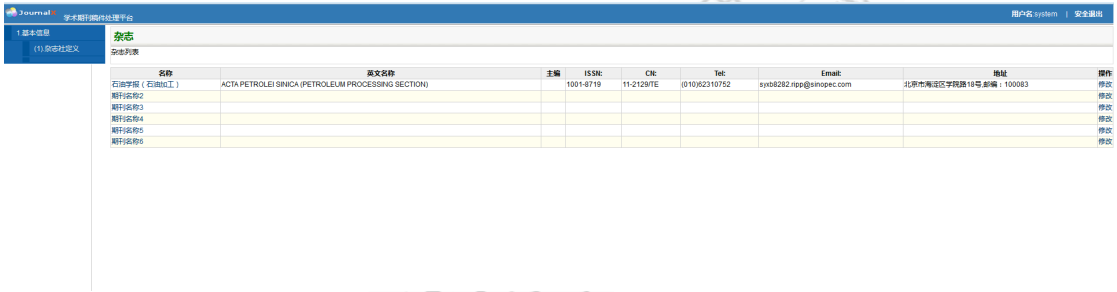
http://www. chinarefining.com/ht-login.jsp

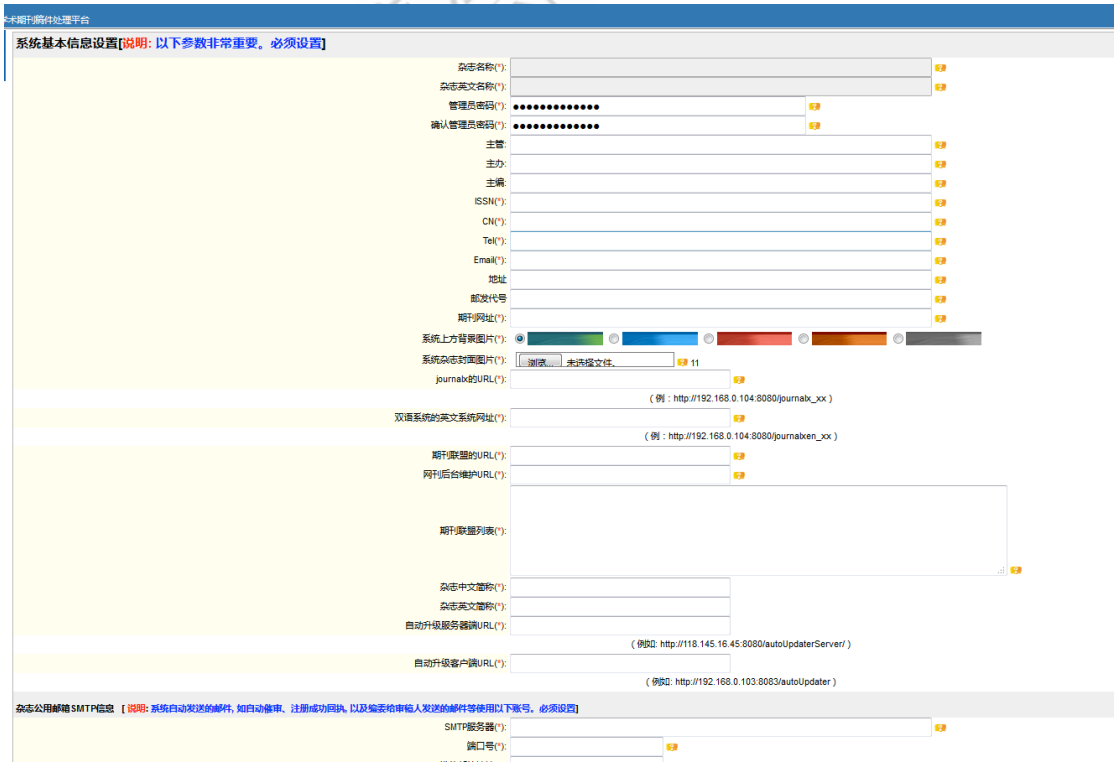
漏洞说明：

弱口令：system：system

点击“主编办公”功能，用弱口令账号登录，如下图：


www.syxbsyjg.com/CN/volumn/current.shtml
该版本插件存在安全隐患，应当更新。
激活 Adobe Flash。
检查更新...
首 页 | 期刊介绍 | 编委会 | 获奖情况 | 评价指标 | 期刊订阅 | 留言板 | 联系我们 | English
读者中心
最新录用
过刊浏览
文章检索
会员注册和服务
作者中心
作者投稿
作者查稿
下载区
修改说明
编审中心
专家审稿
编辑办公
主编办公
审稿专家自荐
文章快速检索
GO
高级检索
石油学报（石油加工）
2016年 32卷 5期
刊出日期 2016-10-25
研究报告
研究报道
上一期
下一期
合并选中摘要
研究报告
选择合并摘要 | 引用本文
龚剑洪1，龙军1，毛安国1，张久顺1，蒋东红1，杨晴2
LCO加氢-催化组合生产高辛烷值汽油或轻质芳烃技术(LTAG)的开发
2016 Vol. 32 (5): 867-874 [摘要] (135) [HTML 0KB] [PDF 823KB] (463)
选择合并摘要 | 引用本文
王红，王子军，王攀红，余玉成，王威
加氢渣油中沥青质的加氢再转化性能
2016 Vol. 32 (5): 875-882 [摘要] (94) [HTML 0KB] [PDF 709KB] (119)
选择合并摘要 | 引用本文
陈颖1，乔腾飞1，姬生伦1，苗双1，张宏宇2
混合胺改性SBA-15的制备及其吸附脱硫特性
2016 Vol. 32 (5): 883-890 [摘要] (110) [HTML 0KB] [PDF 2256KB] (374)
新闻公告
"十一"期间服务器关闭通知
2016中国化工产学研高峰论
更多>>
其它刊物
石油炼制与化工
Petroleum Processing and Petrochemicals
友情链接
中国科学技术协会
中国石油学会
石油化工科学研究院
中国科学院
中国知网(CNKI)
万方数据库
中国石化
中国石油
中国海洋石油
更多>>
该版本插件存在安全隐患，应当更新。
激活 Adobe Flash。
检查更新...


杂志
杂志列表
名称
英文名称
主编
ISSN:
CN:
Tel:
Email:
地址
操作
石油学报（石油加工）
ACTA PETROLEI SINICA (PETROLEUM PROCESSING SECTION)
1001-8719
11-2129/TE
(010)62310752
sybs8282.ripp@sinopec.com
北京市海淀区学院路18号 邮编：100083
修改


系统基本信息设置[说明: 以下参数非常重要。必须设置]
杂志名称(*):
杂志英文名称(*):
管理员密码(*):
确认管理员密码(*):
主管:
主办:
主编:
ISSN(*):
CN(*):
Tel(*):
Email(*):
地址
邮发代号
期刊网址(*):
系统上方背景图片(*):
系统杂志封面图片(*):
浏览...
未选择文件。
journalx的URL(*):
（例：http://192.168.0.104:8080/journalx_xx）
双语系统的英文系统网址(*):
（例：http://192.168.0.104:8080/journalxen_xx）
期刊联盟的URL(*):
网刊后台维护URL(*):
期刊联盟列表(*):
杂志中文简称(*):
杂志英文简称(*):
自动升级服务器端URL(*):
（例如: http://118.145.16.45:8080/autoUpdaterServer/）
自动升级客户端URL(*):
（例如: http://192.168.0.103:8083/autoUpdater）
杂志公用邮箱SMTP信息 [说明: 系统自动发送的邮件, 如自动催审、注册成功回执, 以及编委给审稿人发送的邮件等使用以下账号。必须设置]
SMTP服务器(*):
端口号(*):

六、结论：

通过本次测试发现了被测试系统服务器及应用系统整体安全性较高，服务器部署了 WAF、溯源攻击系统阻断并记录了黑客对网站的攻击行为及记录。渗透测试人员在使用技术能力对网站进行入侵的过程中， 并未发现网站存在严重的安全隐患，但发现有个别管理员存在弱口令等问题。通过弱口令，从后台发现有石化人员名单， 再通过组合弱口令获取了其中一个邮箱信息， 得到了中国石化所有的员工信息、所在单位及电话等等。建议重视弱口令的问题，加强口令的复杂度，设定口令生命周期，同时也可考虑通过建设 OTP 等弱口令解决方案来解决。

另外，本次渗透测试，还通过社会工程学的方法，获取到了软件开发商的信任，我们最终获取到了目标权限，从而从新制定了密码，从而登录后台，控制了目标权限，通过该权限可以进入石化内网。但根据贵单位的授权范围，我方未做深入渗透。目前。在渗透测试攻击中， 社会工程学是最常用的一种攻击手段。建议加强自身及相关服务人员的信息安全意识及权限管理机制。