NSFOCUS

思迈特大数据分析软件

[简称：Smartbi Insight] V8

（Windows 版）

渗透测试报告

■ 文档编号		■ 密级	商业机密
■ 版本编号	1.3	■ 日期	2019-01-17

NSFOCUS

目录

一. 摘要

1.1 基本信息

经思迈特软件的授权，绿盟科技渗透测试小组对其思迈特大数据分析软件[简称：Smartbi Insight] V8（Windows 版）进行了渗透测试。本次测试基本信息如下：

测试对象	域名、URL	账号
思迈特大数据分析软件 [简称：Smartbi Insight] V8 （Windows 版）	https://192.168.4.161:18443/smartbi/vision/index.jsp http://192.168.4.161:18080/smartbi/vision/index.jsp	admin/admin demo/demo

测试工作时间段			
起始时间	2018-11-01	结束时间	2018-11-02

参测人员名单			
测试人员	李建豪	联系方式	13580569483

1.2 测试方法

在不知道目标网络环境的情况下，模拟黑客攻击，使用各种主流测评工具及自主开发的内部测试工具，参照相应安全性能指标标准进行安全检查。

1.3 漏洞概要

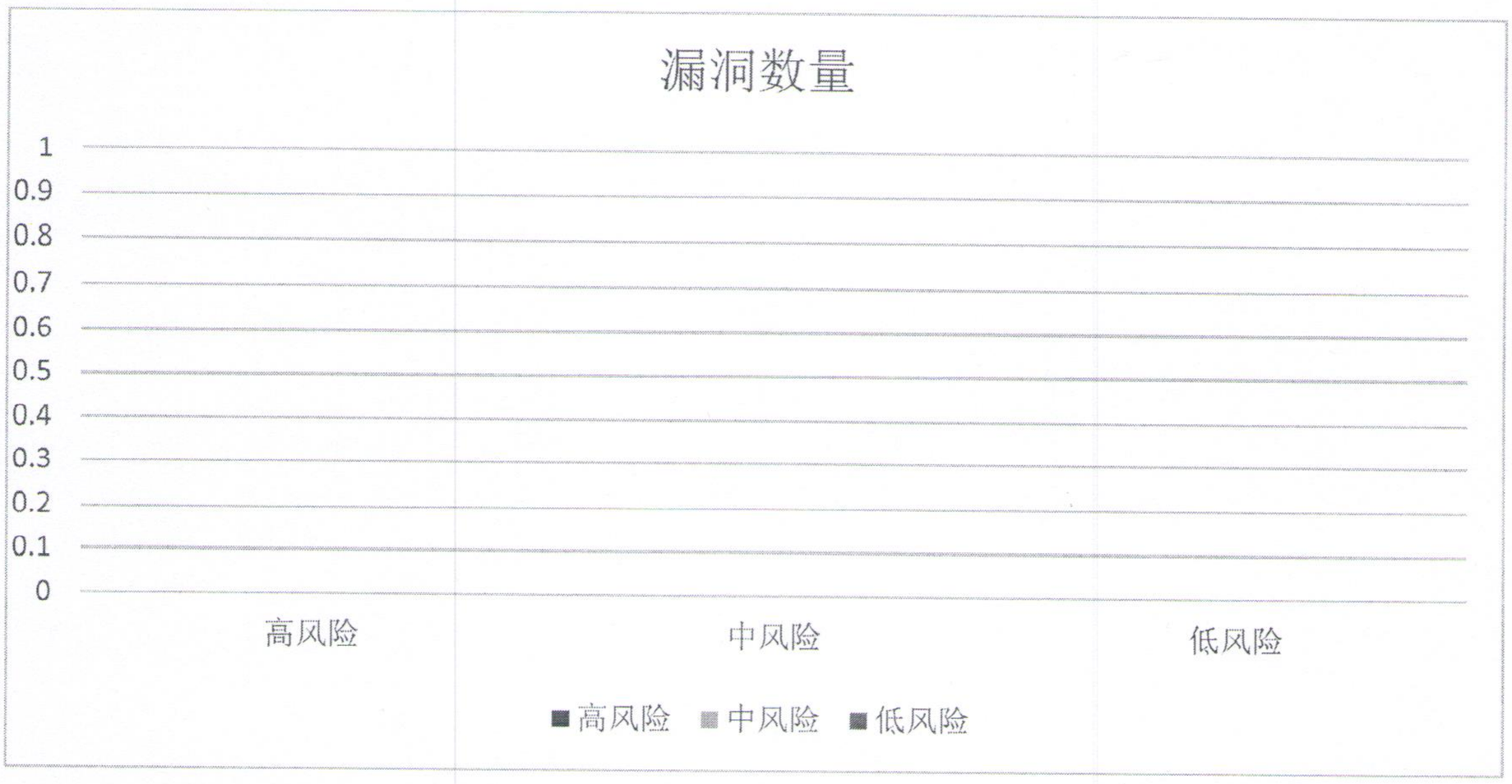
漏洞名称	风险等级	漏洞数	备注
Mysql 弱口令	高	1	已修复
SQL 注入	高	1	已修复
任意 SQL 语句执行	高	1	已修复
跨站脚本一	高	1	已修复

跨站脚本二	高	1	已修复
下载信息泄露	高	1	已修复
RC4 弱加密算法	中	1	已修复
POODLE 攻击漏洞	中	1	已修复
会话固定	中	1	已修复
信息泄露	低	1	已修复

表 1.1 问题列表

漏洞数量：

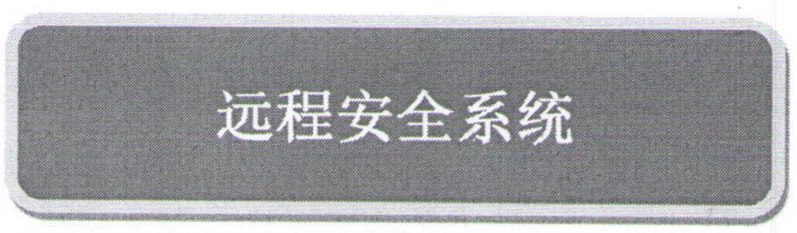
- ☑ 高风险：0 个
- ☑ 中风险：0 个
- ☑ 低风险：0 个



安全风险分布图

1.4 系统当前安全状况

经绿盟安全评估小组进行全面安全评估后，绿盟安全评估小组认为当前系统安全状况如下图。级别为：



二. 渗透测试概述

2.1 概述

对于已经部署了安全防护措施（安全产品、安全服务）或者即将部署安全防护措施的用户而言，明确网络当前的安全现状对下一步的安全建设有重大的指导意义。渗透测试服务用于验证在当前的安全防护措施下网络、系统抵抗黑客攻击的能力。

透测试小组利用各种主流的攻击技术对网络、系统做模拟攻击测试，以发现网络、系统中存在的安全漏洞和风险点。企业、组织根据测试的结果遵循安全策略制定适合的、不同优先级别的安全防护措施、流程。

渗透测试流程定义为如下阶段：

信息收集

此阶段中，渗透测试小组进行必要的信息收集，如操作系统类型、开放的端口和服务、web服务应用系统版本、后台数据库类型、web 开发语言等。

渗透测试

此阶段中，渗透测试小组根据第一阶段获得的信息对网络、系统进行渗透测试。此阶段如果成功的话，可能获得普通权限或系统权限。

本地信息收集

此阶段中，渗透测试小组进行本地信息收集，用于下一阶段的权限提升。

权限提升

此阶段中，渗透测试小组尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

清除

此阶段中，渗透测试小组清除日志记录等数据。

输出报告

此阶段中，渗透测试小组根据测试的结果编写直观的渗透测试服务报告。

2.2 风险管理

相对其他服务而言，渗透测试是一种需要相当技术深度的高端服务，要求渗透测试人员有丰富的经验及新颖的思路。

在渗透测试过程中，虽然我们尽量避免影响正常业务的运行，也会采取适当的风险规避、风险降低的方法，但是由于测试的不确定性，渗透测试服务仍然有可能对网络、系统运行造成一定不同程度的影响，可能造成服务停止，甚至是宕机。

另外，对于安全防护措施严密的网络、系统，在有限的时间内进行渗透测试可能不会获得成功结果。这在一定程度也证明了网络、系统能够在一定程度上抵抗黑客的攻击。

2.3 收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，特别是在进行安全项目之前进行渗透测试，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设。

在进行了安全项目之后进行渗透测试，则可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

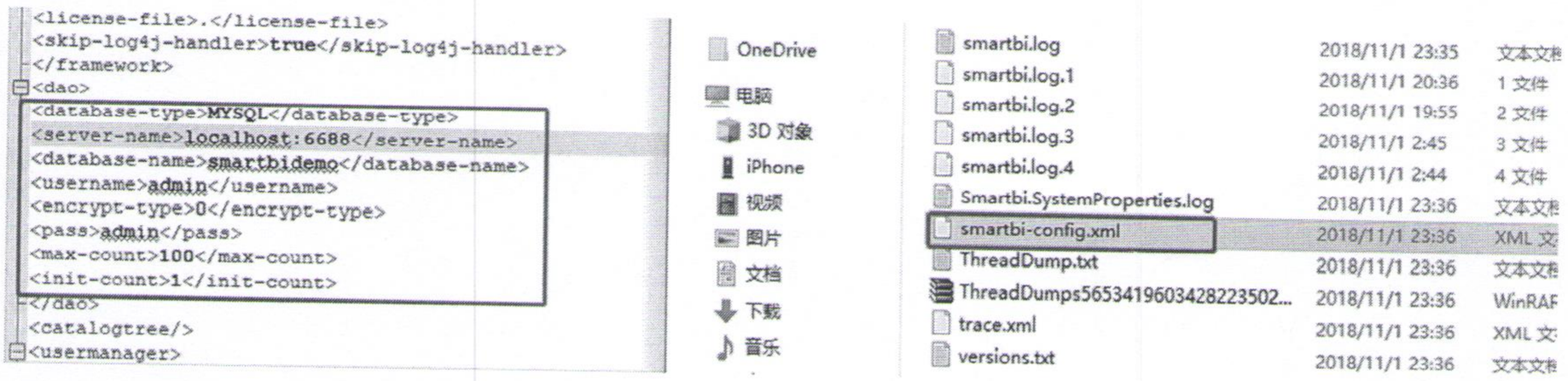
三. 安全测试

3.1 漏洞详情

3.1.1 Mysql 弱口令（高风险）（已修复）

【问题说明】

根据配置文件可知，MYSQL 账号密码为 admin/admin，属弱口令，容易被攻击者猜测出来。



【修复建议】

1、 密码长度要求 6 位以上，至少包含字母+数字。

2、 进行密码强度限制，避免使用 111111、123456、admin、password、admin123 等常见弱口令。

【复测情况】

已修复，未使用弱口令。

```
<database-type>MYSQL</database-type>
<server-name>localhost:6688</server-name>
<database-name>smartbidemo</database-name>
<username>admin</username>
<encrypt-type>1</encrypt-type>
<pass>9aaacae0b0f235e388d4e28e766e38cc</pass>
<max-count>100</max-count>
<init-count>1</init-count>
<mysql-cluster>false</mysql-cluster>
<validation-query-method>0</validation-query-method>
```

3.1.2 SQL 注入（高风险）（已修复）

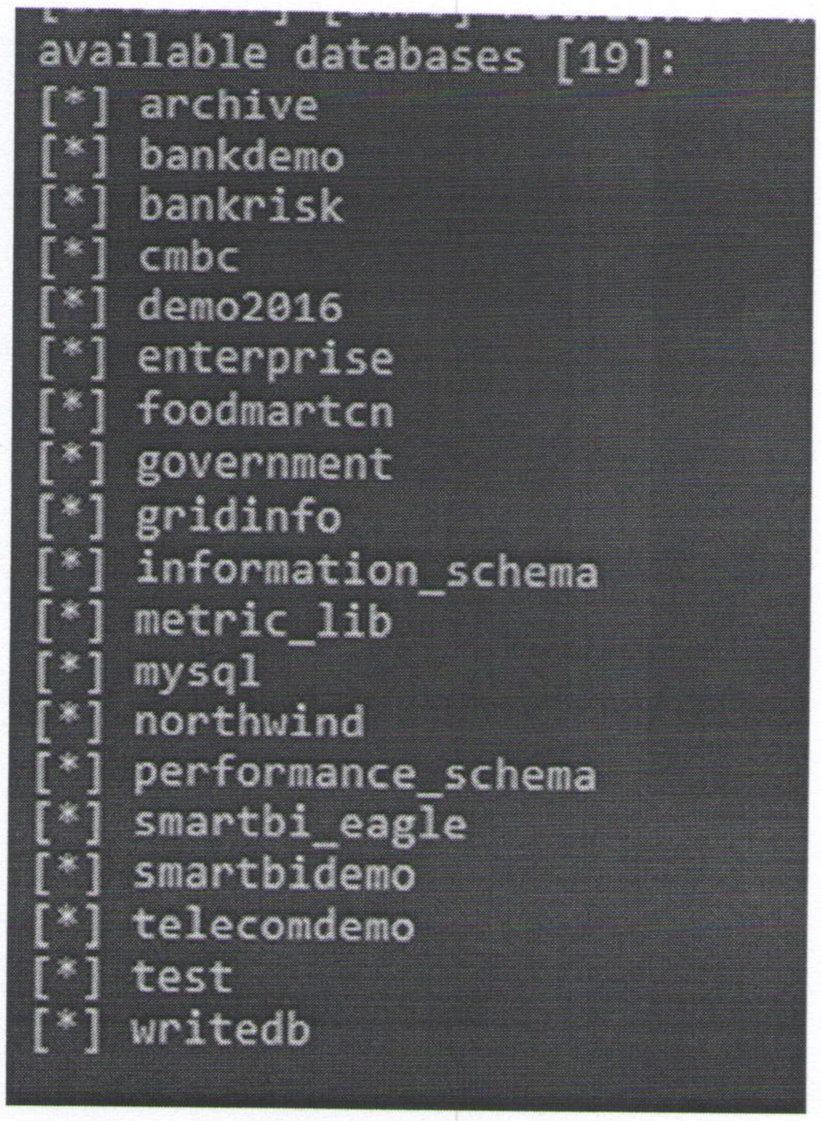
【问题说明】

Sql 注入（SQL injection）是指攻击者在服务器端构造数据库执行代码可以在服务器中数据库得到执行。由于攻击代码在数据库中执行，根据连接用户的权限，可以读、修改数据库资料甚至执行数据库外部命令，典型的攻击方法为窃取数据库资料、控制操作系统等。

问题链接：

192.168.4.161:18080/smartbi/vision/FileResource;jsession=?resId=l2c9410bc274b0e4901274c27aa790a92&op=OPEN&rd=0.06982386072208568

resId 参数存在注入，可获取数据库详细信息



【修复建议】

1、增加全局防注入功能，从客户端获取到的参数都必须通过安全校验，防范以下常见攻击字符：

'|"|>|..|and|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare|script|frame|;|or|-|+|,|)|etc|style|expression

注：对获取的参数进行安全检测之前应首先统一字符编码和大小写，避免攻击者通过编码和大小写混用绕过安全检查。

2、摒弃 SQL 动态拼接的查询方式，使用参数化查询。

【复测情况】

已修复，已对危险字符进行过滤。

Request

Raw | Params | Headers | Hex

```
GET
/smartbi/vision/FileResource;jsession=?resId=I2c9410bc274b0e4901274c27aa790a92'&op=OPEN&rd=0.06982386072208568 HTTP/1.1
Host: proj.smartbi.com.cn:18860
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0)
Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: LOGIN_CREDENTIALS=I8a8a4c2001684c094c094ac501684c1ac6c90038;
JSESSIONID=5FAE429A59B9ADCB2B24AE0A948F176A
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Length: 0
Date: Mon, 14 Jan 2019 11:26:50 GMT
Connection: close
```

3.1.3 任意 SQL 语句执行（高风险）（已修复）

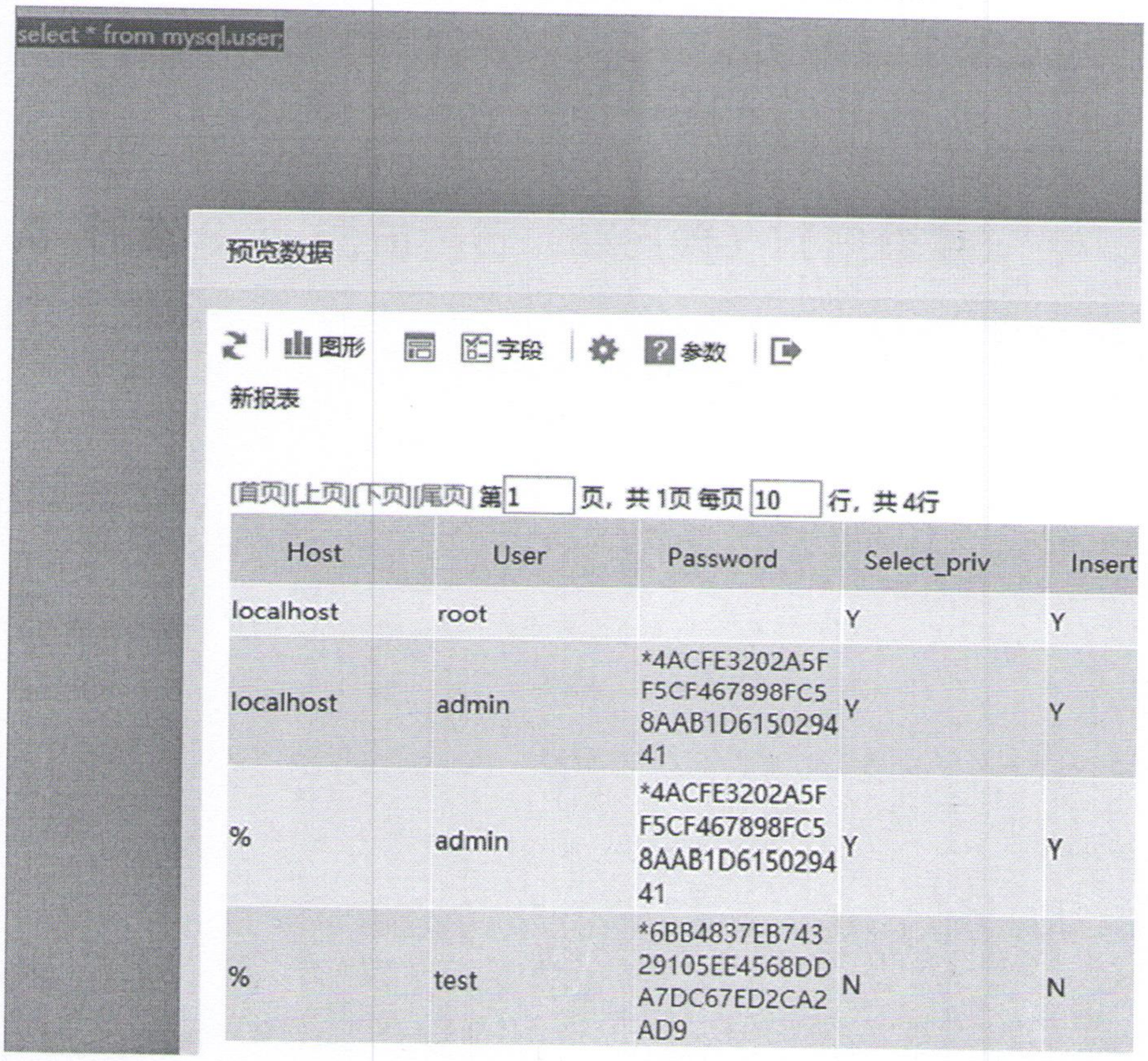
【问题说明】

定制管理>数据集>原生 SQL 查询

该模块可允许客户执行任意 SQL 语句，如可创建新用户等高风险操作，未对用户的输入进行安全防范。

执行 create user test identified by '123456'; 创建一个新用户

执行 select * from mysql.user; 查询现有用户，显示已创建成功。



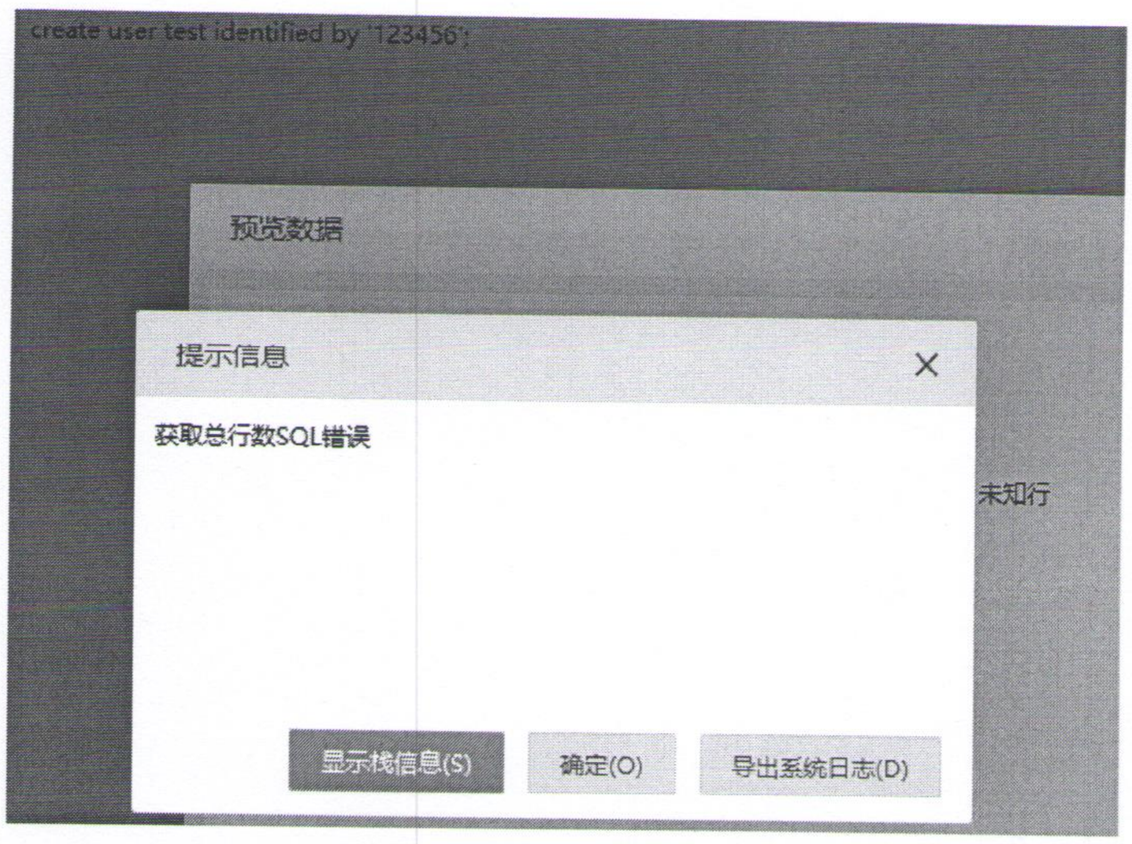
Host	User	Password	Select_priv	Insert
localhost	root		Y	Y
localhost	admin	*4ACFE3202A5FF5CF467898FC58AAB1D615029441	Y	Y
%	admin	*4ACFE3202A5FF5CF467898FC58AAB1D615029441	Y	Y
%	test	*6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9	N	N

【修复建议】

限制用户输入，禁止用户输入 SQL 语句。

【复测情况】

已修复，已限制执行恶意操作。



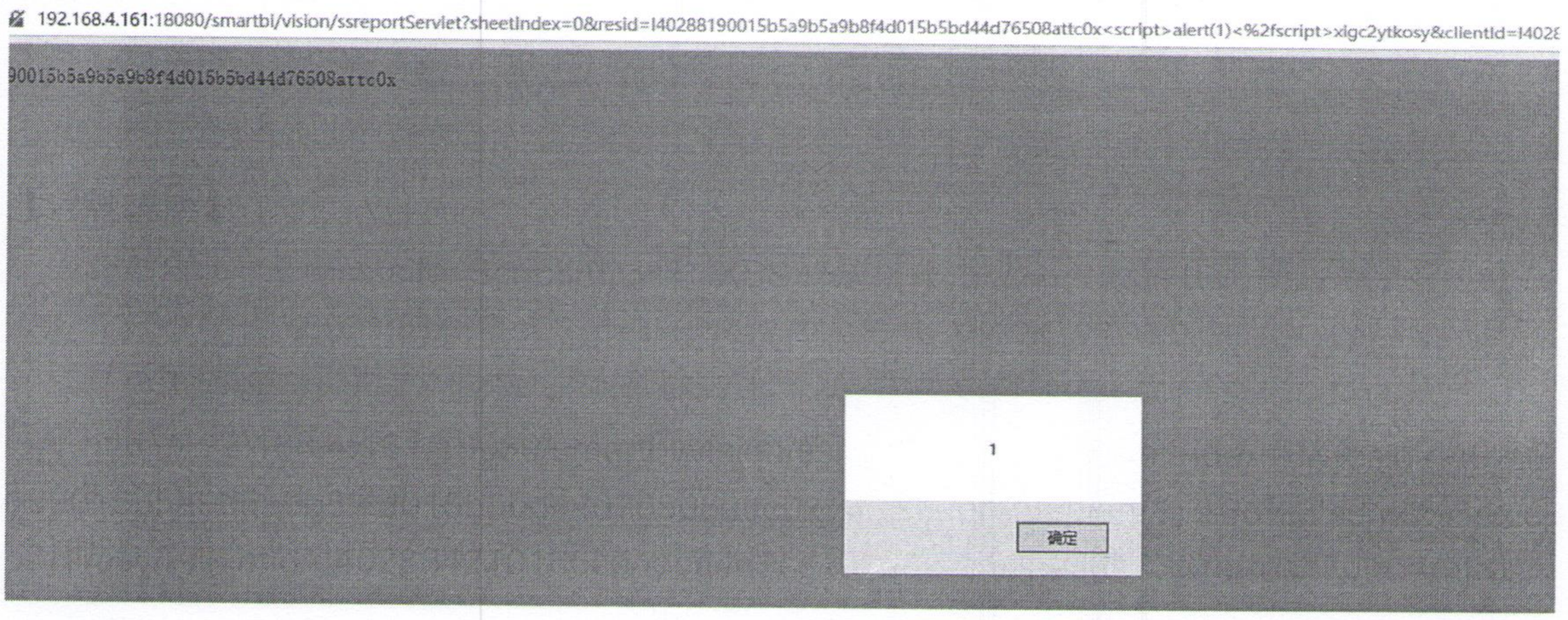
3.1.4 跨站脚本一（高风险）（已修复）

【问题说明】

跨站脚本（Cross-site Scripting 简称 XSS）是指攻击者输入攻击代码到服务器端，代码在其它用户的浏览器中得到执行。由于攻击代码在受害者的浏览器中执行，可以读、修改和传输任何浏览器可以读取的资料，典型的攻击方法为窃取 Cookie、网页重定向等。

http://192.168.4.161:18080/smartbi/vision/ssreportServlet?sheetIndex=0&resid=I40288190015b5a9b5a9b8f4d015b5bd44d76508attc0x%3cscript%3ealert(1)%3c%2fscript%3exigc2ytkosy&clientId=I402884210166cd4dcd4d9cdc0166cea59aa50b33&refreshType=refresh&paramsInfo=&pageId=0&writeBackData=&exportSheetIndexes=&exportId=

在参数 resid 中插入%3cscript%3ealert(1)%3c%2fscript%3e，成功执行



【修复建议】

1、增加全局防护功能，从客户端获取到的参数都必须通过安全校验，防范以下常见攻击字符：

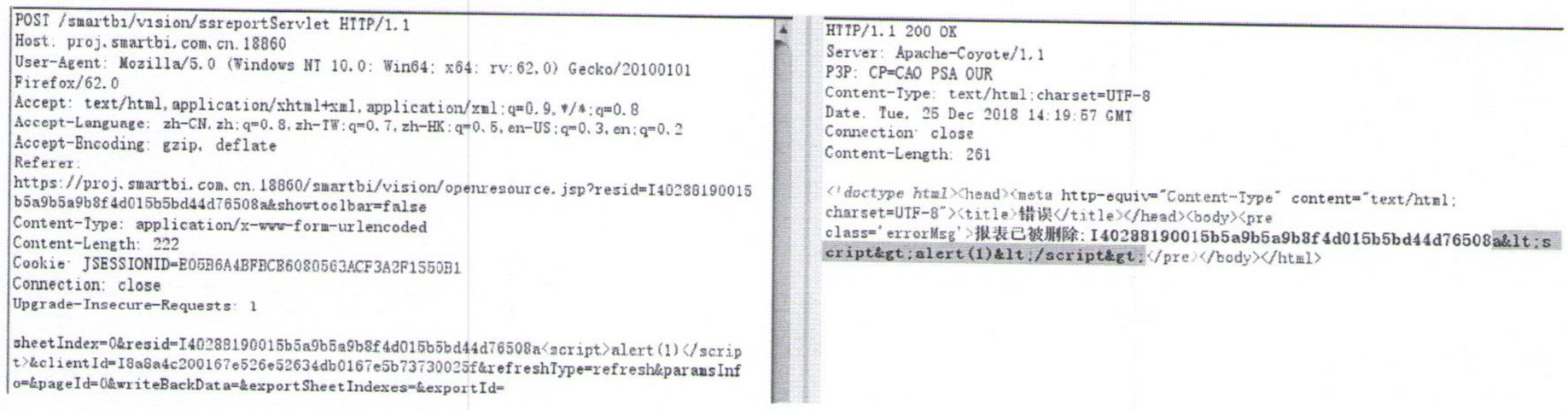
```
'|"|>|..|and|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare|script|frame|;|or|-|+|,|)|etc|style|expression
```

注：对获取的参数进行安全检测之前应首先统一字符编码和大小写，避免攻击者通过编码和大小写混用绕过安全检查。

2、将获取到的数据进行 HTML 转码再存入数据库或输出。

【复测情况】

已对敏感字符进行 HTML 转码输出。



```
POST /smartbi/vision/ssreportServlet HTTP/1.1
Host: proj.smartbi.com.cn:18860
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101
Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://proj.smartbi.com.cn:18860/smartbi/vision/openresource.jsp?resid=I40288190015
b5a9b5a9b8f4d015b5bd44d76508a&showtoolbar=false
Content-Type: application/x-www-form-urlencoded
Content-Length: 222
Cookie: JSESSIONID=E05B6A4BFBCB6080563ACF3A2F1550B1
Connection: close
Upgrade-Insecure-Requests: 1

sheetIndex=0&resid=I40288190015b5a9b5a9b8f4d015b5bd44d76508a<script>alert(1)</scrip
t>&clientId=I8a8a4c200167e526e52634db0167e5b73730025f&refreshType=refresh&paramsInf
o=&pageId=0&writeBackData=&exportSheetIndexes=&exportId=
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
P3P: CP=CAO PSA OUR
Content-Type: text/html;charset=UTF-8
Date: Tue, 25 Dec 2018 14:19:57 GMT
Connection: close
Content-Length: 261

<!doctype html><head><meta http-equiv="Content-Type" content="text/html;
charset=UTF-8"><title>错误</title></head><body><pre
class='errorMsg'>报表已被删除:I40288190015b5a9b5a9b8f4d015b5bd44d76508a&lt;s
cript&gt;alert(1)&lt;/script&gt;</pre></body></html>
```

3.1.5 跨站脚本二（高风险）（已修复）

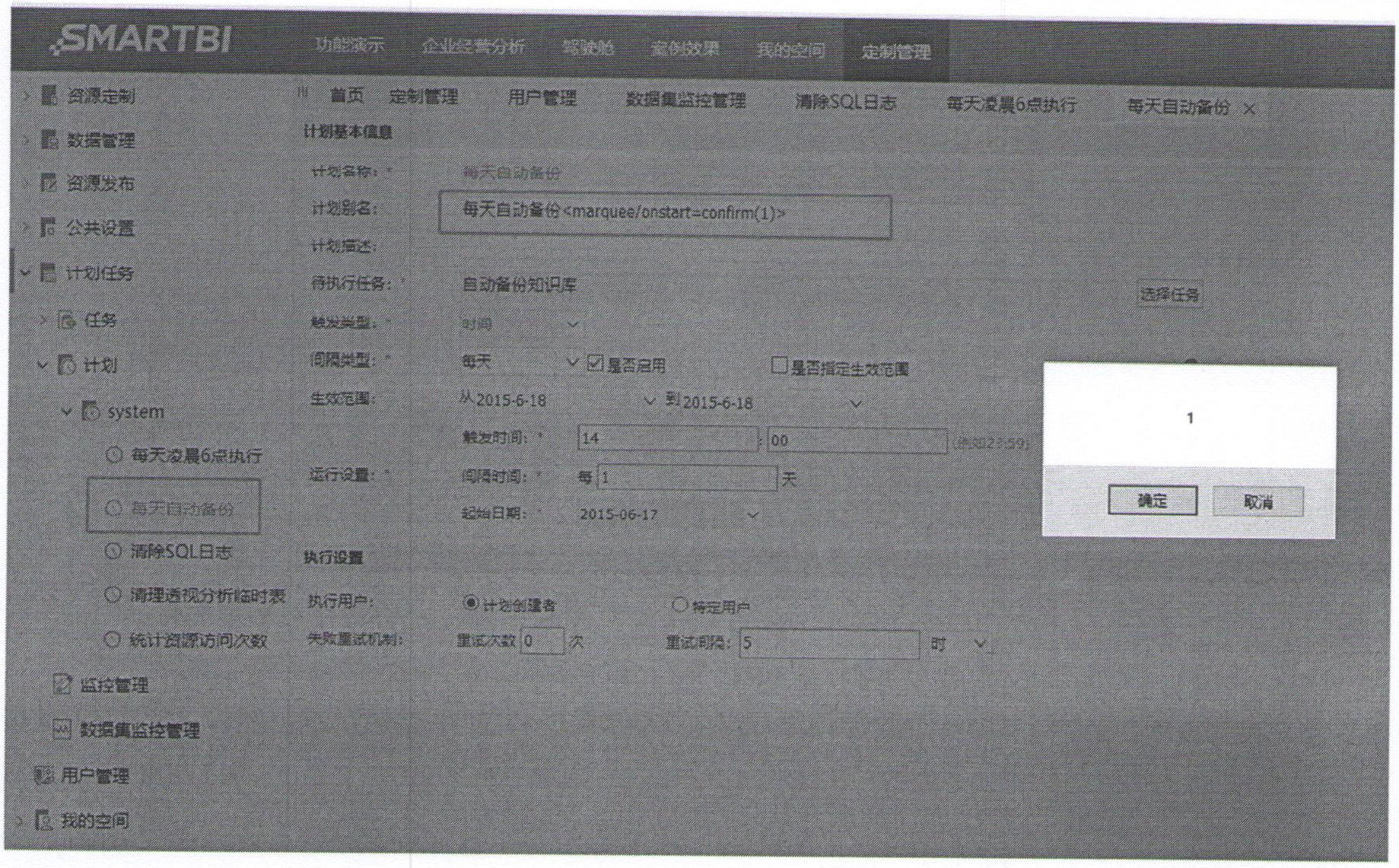
【问题说明】

跨站脚本（Cross-site Scripting 简称 XSS）是指攻击者输入攻击代码到服务器端，代码在其它用户的浏览器中得到执行。由于攻击代码在受害者的浏览器中执行，可以读、修改和传输任何浏览器可以读取的资料，典型的攻击方法为窃取 Cookie、网页重定向等。

定置管理>多个可修改的功能模块

举例：定置管理>计划任务>system>每天自动备份

在计划别名处添加<marquee/onstart=confirm(1)>，点击保存后成功执行代码。



【修复建议】

1、增加全局防护功能，从客户端获取到的参数都必须通过安全校验，防范以下常见攻击字符：

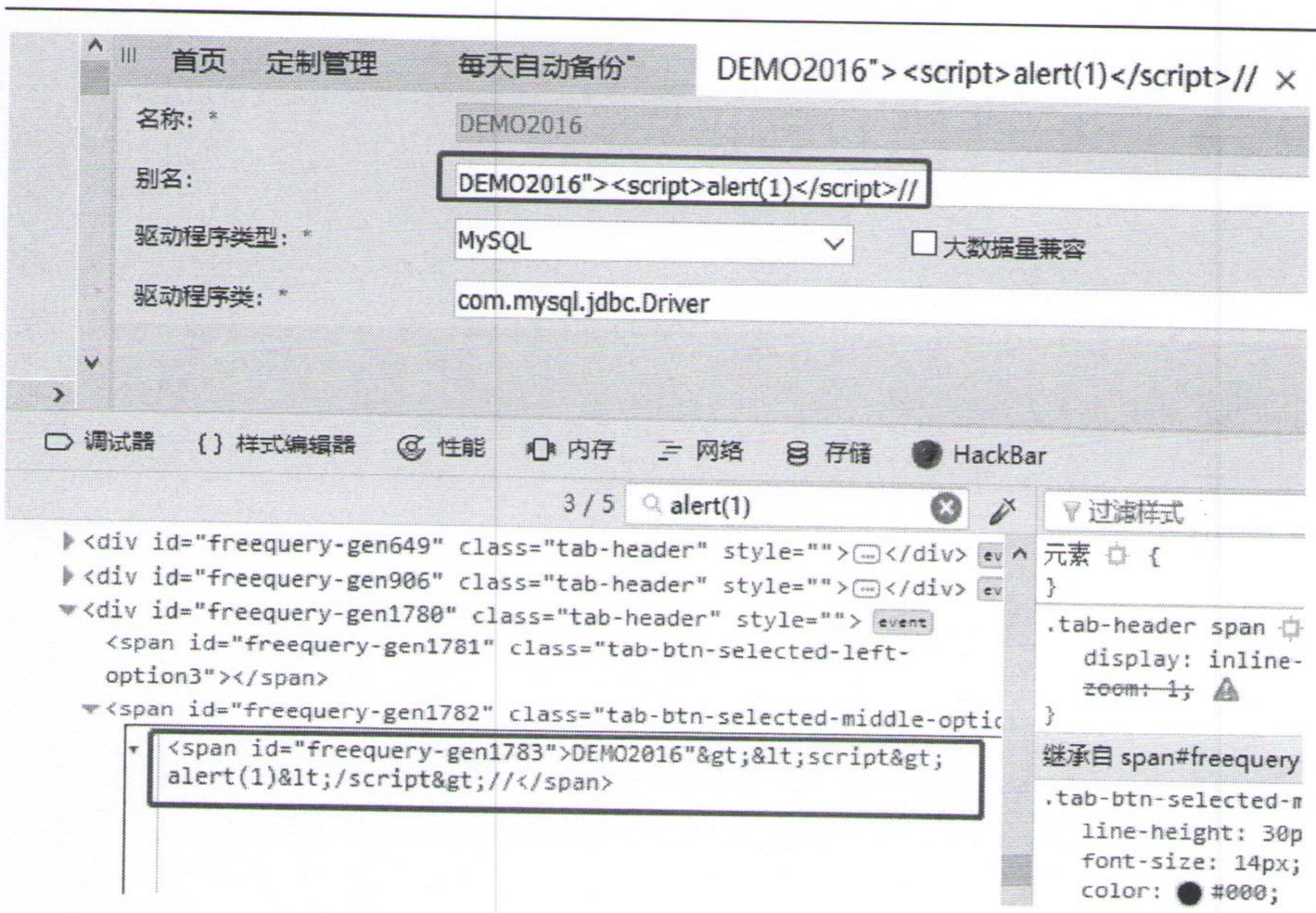
'|"|>|..|and|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare|script|frame|;|or|-|+|,|)|etc|style|expression

注：对获取的参数进行安全检测之前应首先统一字符编码和大小写，避免攻击者通过编码和大小写混用绕过安全检查。

2、将获取到的数据进行 HTML 转码再存入数据库或输出。

【复测情况】

已对敏感字符进行 HTML 转码输出。



3.1.6 下载信息泄露（高风险）（已修复）

【问题说明】

定制管理>系统日志

http://192.168.4.161:18080/smartbi/vision/MigrateServlet;jsessionid=01633036515E2FB33AC8E9081E6CEEAC?type=download&filename=FILE_DOWNLOAD_Smartbi-logs.zip_l402884200166cd30cd3053940166d43ba5b44f1d

点击可下载系统日志，其中包含了部分带有敏感信息的配置文件，如 smartbi-config.xml 中使用明文记录了 MYSQL 的端口以及账号密码，攻击者可借此入侵数据库。

【修复建议】

系统日志压缩包中不应带有泄露账号密码等敏感信息的文件，只提供用户下载脱敏文件。

【复测情况】

已修复，对敏感信息进行了加密。

```
<database-type>MYSQL</database-type>
<server-name>localhost:6688</server-name>
<database-name>smartbidemo</database-name>
<username>admin</username>
<encrypt-type>1</encrypt-type>
<pass>9aaacae0b0f235e388d4e28e766e38cc</pass>
<max-count>100</max-count>
<init-count>1</init-count>
<mysql-cluster>false</mysql-cluster>
<validation-query-method>0</validation-query-method>
```

3.1.7 弱加密算法（中风险）（已修复）

【问题说明】

测试发现 https 加密中 ssl 加密中使用了弱加密算法。

如下图所示，sslv3 使用了 40、56 位和 RC4 等弱算法：

```
SSLv3
--------------------------------------------------------------------
AES256-SHA                    - 256 Bits - Supported - HTTP/1.1 404 Not Found
CAMELLIA256-SHA               - 256 Bits - Supported - HTTP/1.1 404 Not Found
DHE-DSS-AES256-SHA            - 256 Bits - Unsupported
DHE-DSS-CAMELLIA256-SHA       - 256 Bits - Unsupported
DHE-RSA-AES256-SHA            - 256 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-CAMELLIA256-SHA       - 256 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-AES256-SHA         - 256 Bits - Unsupported
ECDHE-ECDSA-AES256-SHA        - 256 Bits - Unsupported
ECDHE-RSA-AES256-SHA          - 256 Bits - Unsupported
ECDH-RSA-AES256-SHA           - 256 Bits - Unsupported
PSK-AES256-CBC-SHA            - 256 Bits - Unsupported
DES-CBC3-SHA                  - 168 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-DES-CBC3-SHA       - 168 Bits - Unsupported
ECDHE-ECDSA-DES-CBC3-SHA      - 168 Bits - Unsupported
ECDHE-RSA-DES-CBC3-SHA        - 168 Bits - Unsupported
ECDH-RSA-DES-CBC3-SHA         - 168 Bits - Unsupported
EDH-DSS-DES-CBC3-SHA          - 168 Bits - Unsupported
EDH-RSA-DES-CBC3-SHA          - 168 Bits - Supported - HTTP/1.1 404 Not Found
PSK-3DES-EDE-CBC-SHA          - 168 Bits - Unsupported
AES128-SHA                    - 128 Bits - Supported - HTTP/1.1 404 Not Found
CAMELLIA128-SHA               - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-DSS-AES128-SHA            - 128 Bits - Unsupported
DHE-DSS-CAMELLIA128-SHA       - 128 Bits - Unsupported
DHE-DSS-SEED-SHA              - 128 Bits - Unsupported
DHE-RSA-AES128-SHA            - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-CAMELLIA128-SHA       - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-SEED-SHA              - 128 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-AES128-SHA         - 128 Bits - Unsupported
ECDH-ECDSA-RC4-SHA            - 128 Bits - Unsupported
ECDHE-ECDSA-AES128-SHA        - 128 Bits - Unsupported
ECDHE-ECDSA-RC4-SHA           - 128 Bits - Unsupported
ECDHE-RSA-AES128-SHA          - 128 Bits - Unsupported
ECDHE-RSA-RC4-SHA             - 128 Bits - Unsupported
ECDH-RSA-AES128-SHA           - 128 Bits - Unsupported
ECDH-RSA-RC4-SHA              - 128 Bits - Unsupported
IDEA-CBC-SHA                  - 128 Bits - Supported - HTTP/1.1 404 Not Found
PSK-AES128-CBC-SHA            - 128 Bits - Unsupported
PSK-RC4-SHA                   - 128 Bits - Unsupported
RC4-MD5                       - 128 Bits - Supported - HTTP/1.1 404 Not Found
RC4-SHA                       - 128 Bits - Supported - HTTP/1.1 404 Not Found
SEED-SHA                      - 128 Bits - Supported - HTTP/1.1 404 Not Found
DES-CBC-SHA                   -  56 Bits - Supported - HTTP/1.1 404 Not Found
EDH-DSS-DES-CBC-SHA           -  56 Bits - Unsupported
EDH-RSA-DES-CBC-SHA           -  56 Bits - Supported - HTTP/1.1 404 Not Found
EXP-DES-CBC-SHA               -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-EDH-DSS-DES-CBC-SHA       -  40 Bits - Unsupported
EXP-EDH-RSA-DES-CBC-SHA       -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-RC2-CBC-MD5               -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-RC4-MD5                   -  40 Bits - Supported - HTTP/1.1 404 Not Found
```

【修复建议】

在服务器上禁用弱加密的算法。

【复测情况】

已禁用弱加密算法。

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.1  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.1  128 bits  DHE-RSA-CAMELLIA128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-CAMELLIA128-SHA
```

3.1.8 POODLE 攻击（中风险）（已修复）

【问题说明】

该漏洞它能够在某些情况下泄露 SSL/TLS 加密流量中的密文，从而将账户用户名密码、信用卡数据和其他敏感信息泄露给黑客。

经测试确认支持 sslv3 且存在该漏洞：

```
SSLv3
-----------------------------------------------------------------
AES256-SHA                  - 256 Bits - Supported - HTTP/1.1 404 Not Found
CAMELLIA256-SHA             - 256 Bits - Supported - HTTP/1.1 404 Not Found
DHE-DSS-AES256-SHA          - 256 Bits - Unsupported
DHE-DSS-CAMELLIA256-SHA     - 256 Bits - Unsupported
DHE-RSA-AES256-SHA          - 256 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-CAMELLIA256-SHA     - 256 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-AES256-SHA       - 256 Bits - Unsupported
ECDHE-ECDSA-AES256-SHA      - 256 Bits - Unsupported
ECDHE-RSA-AES256-SHA        - 256 Bits - Unsupported
ECDH-RSA-AES256-SHA         - 256 Bits - Unsupported
PSK-AES256-CBC-SHA          - 256 Bits - Unsupported
DES-CBC3-SHA                - 168 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-DES-CBC3-SHA     - 168 Bits - Unsupported
ECDHE-ECDSA-DES-CBC3-SHA    - 168 Bits - Unsupported
ECDHE-RSA-DES-CBC3-SHA      - 168 Bits - Unsupported
ECDH-RSA-DES-CBC3-SHA       - 168 Bits - Unsupported
EDH-DSS-DES-CBC3-SHA        - 168 Bits - Unsupported
EDH-RSA-DES-CBC3-SHA        - 168 Bits - Supported - HTTP/1.1 404 Not Found
PSK-3DES-EDE-CBC-SHA        - 168 Bits - Unsupported
AES128-SHA                  - 128 Bits - Supported - HTTP/1.1 404 Not Found
CAMELLIA128-SHA             - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-DSS-AES128-SHA          - 128 Bits - Unsupported
DHE-DSS-CAMELLIA128-SHA     - 128 Bits - Unsupported
DHE-DSS-SEED-SHA            - 128 Bits - Unsupported
DHE-RSA-AES128-SHA          - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-CAMELLIA128-SHA     - 128 Bits - Supported - HTTP/1.1 404 Not Found
DHE-RSA-SEED-SHA            - 128 Bits - Supported - HTTP/1.1 404 Not Found
ECDH-ECDSA-AES128-SHA       - 128 Bits - Unsupported
ECDH-ECDSA-RC4-SHA          - 128 Bits - Unsupported
ECDHE-ECDSA-AES128-SHA      - 128 Bits - Unsupported
ECDHE-ECDSA-RC4-SHA         - 128 Bits - Unsupported
ECDHE-RSA-AES128-SHA        - 128 Bits - Unsupported
ECDHE-RSA-RC4-SHA           - 128 Bits - Unsupported
ECDH-RSA-AES128-SHA         - 128 Bits - Unsupported
ECDH-RSA-RC4-SHA            - 128 Bits - Unsupported
IDEA-CBC-SHA                - 128 Bits - Supported - HTTP/1.1 404 Not Found
PSK-AES128-CBC-SHA          - 128 Bits - Unsupported
PSK-RC4-SHA                 - 128 Bits - Unsupported
RC4-MD5                     - 128 Bits - Supported - HTTP/1.1 404 Not Found
RC4-SHA                     - 128 Bits - Supported - HTTP/1.1 404 Not Found
SEED-SHA                    - 128 Bits - Supported - HTTP/1.1 404 Not Found
DES-CBC-SHA                 -  56 Bits - Supported - HTTP/1.1 404 Not Found
EDH-DSS-DES-CBC-SHA         -  56 Bits - Unsupported
EDH-RSA-DES-CBC-SHA         -  56 Bits - Supported - HTTP/1.1 404 Not Found
EXP-DES-CBC-SHA             -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-EDH-DSS-DES-CBC-SHA     -  40 Bits - Unsupported
EXP-EDH-RSA-DES-CBC-SHA     -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-RC2-CBC-MD5             -  40 Bits - Supported - HTTP/1.1 404 Not Found
EXP-RC4-MD5                 -  40 Bits - Supported - HTTP/1.1 404 Not Found
```

```
ssl-poodle:
  VULNERABLE:
  SSL POODLE information leak
    State: VULNERABLE
    IDs:  CVE:CVE-2014-3566  OSVDB:113251
          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
          products, uses nondeterministic CBC padding, which makes it easier
          for man-in-the-middle attackers to obtain cleartext data via a
          padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
```

【修复建议】

禁止使用 SSLv3 协议。

【复测情况】

已禁用 SSLv3 协议。

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.1  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.1  128 bits  DHE-RSA-CAMELLIA128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA
Accepted  TLSv1.0  256 bits  DHE-RSA-CAMELLIA256-SHA
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA
Accepted  TLSv1.0  128 bits  DHE-RSA-CAMELLIA128-SHA
```

3.1.9 会话固定（中风险）（已修复）

【问题说明】

如图，系统登录前后 cookie 值保持一致，存在被攻击者盗用会话的风险。

登录前

```
GET /smartbi/vision/index.jsp HTTP/1.1
Host: 192.168.4.161:18080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.4.161:18080/smartbi/vision/
Cookie: FQConfigLogined=; FQPassword=; JSESSIONID=939ECDD10C7FDC54E8EDB83A06531C76
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

登录后

```
GET
/smartbi/vision/gbk.jsp?names=freequery.tree.SuperviseTreePopupMenuHandler,smartbi.smartbix.Smartb:
y.tree.CatalogTreePopupMenuBaseHandler&l=zh_CN HTTP/1.1
Host: 192.168.4.161:18080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.4.161:18080/smartbi/vision/index.jsp
Cookie: FQConfigLogined=; FQPassword=; JSESSIONID=939ECDD10C7FDC54E8EDB83A06531C76
Connection: close
If-None-Match: ""15655--1173953288""
```

【修复建议】

登录成功后重新分配一个新的会话凭证。

【复测情况】

登录后已重新分配一个新的会话凭证。

登录前

```
GET /smartbi/vision/loginbg.jsp HTTP/1.1
Host: proj.smartbi.com.cn:18860
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://proj.smartbi.com.cn:18860/smartbi/vision/index.jsp
Cookie: JSESSIONID=5FAE429A59B9ADCB2B24AE0A948F176A
Connection: close
If-None-Match: 2019-01-11 13:57:15_DEFAULT
Cache-Control: max-age=0
```

登录后

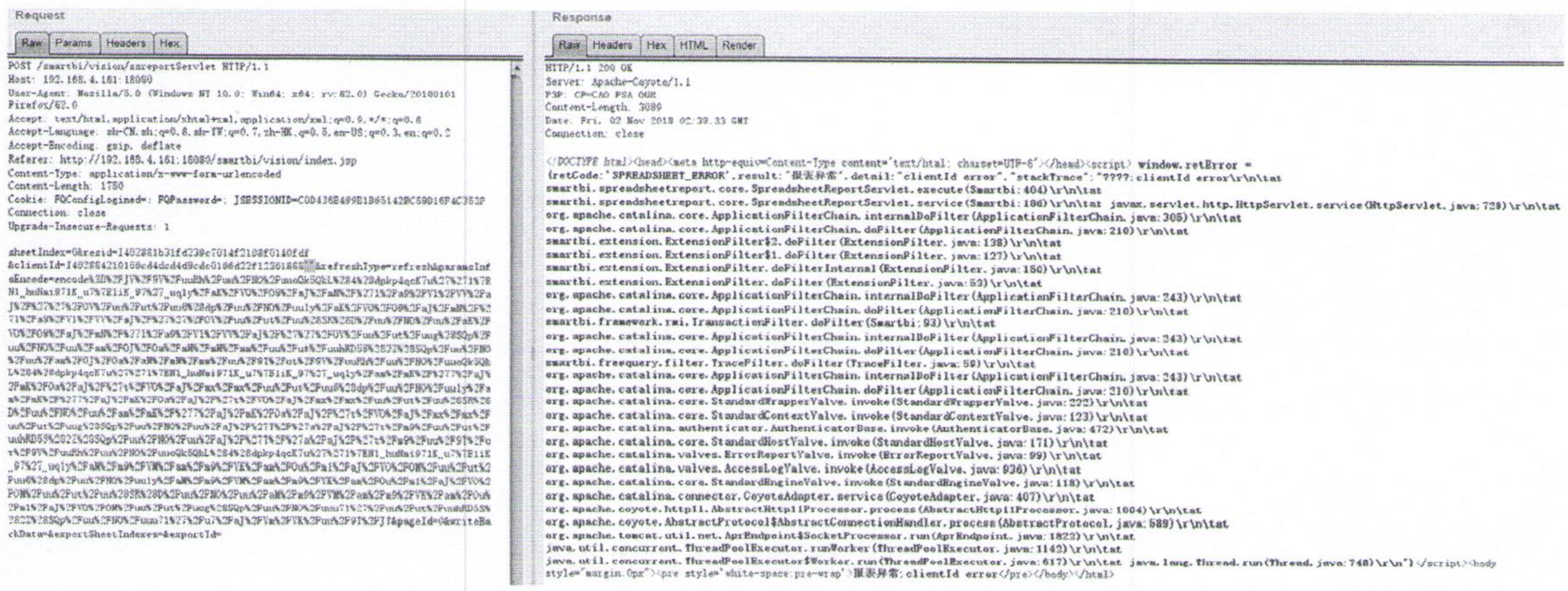
```
POST /smartbi/vision/RMIServlet HTTP/1.1
Host: proj.smartbi.com.cn:18860
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://proj.smartbi.com.cn:18860/smartbi/vision/index.jsp
If-Modified-Since: 0
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 42
Cookie: LOGIN_CREDENTIALS=I8a8a4c2001684c094c094ac501684c1ac6c90038; JSESSIONID=5FAE429A59B9ADCB2B24AE0A948F176A
Connection: close

encode=zDp4Wp4gRip+-pkF2OiiwQ6kc6_w+/JV/JT
```

3.1.10 信息泄露（低风险）（已修复）

【问题说明】

程序错误信息可帮助程序员发现程序缺陷，也可以将程序弱点暴露给攻击者，利用已知漏洞进行攻击。

如图，当请求参数异常时，服务器返回报错信息。

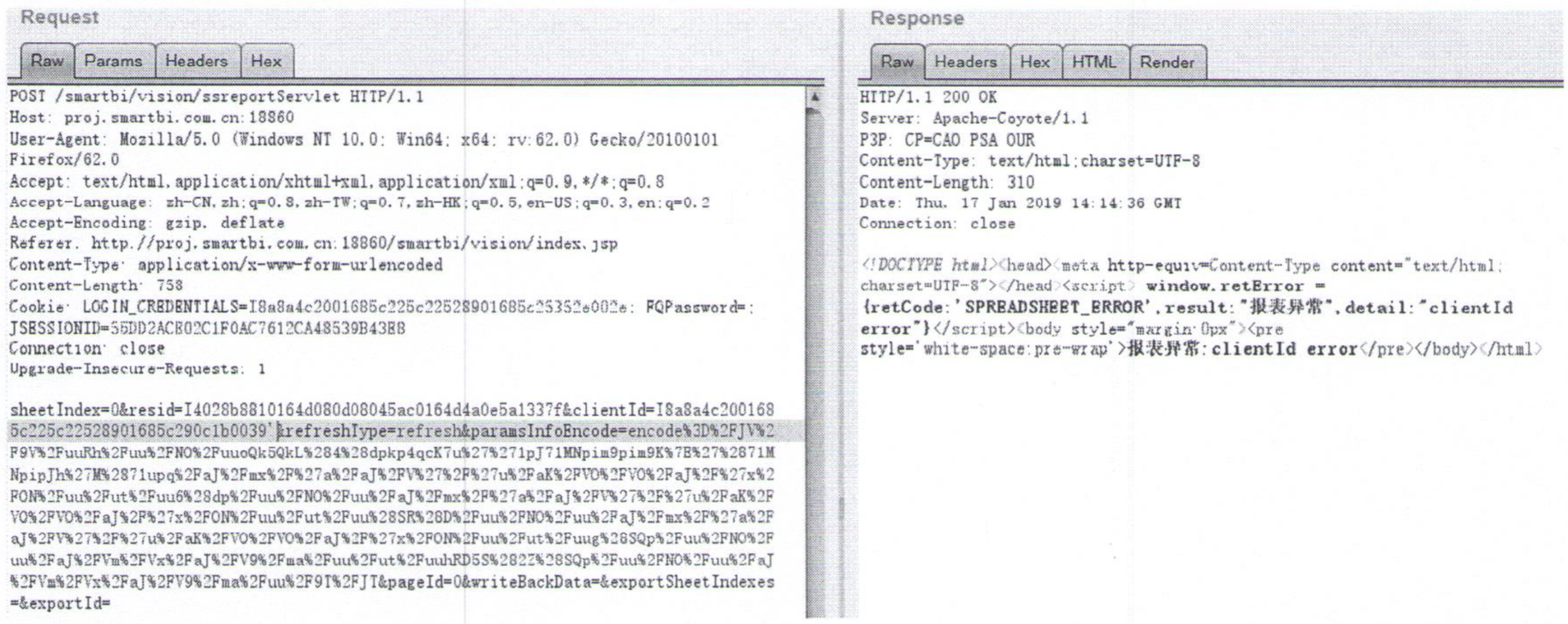


【修复建议】

使用自定义的错误响应页面，程序出错时统一转向该错误处理页，屏蔽具体的错误信息。

【复测情况】

已修复，已屏蔽了报错信息。



四. 参考与建议

4.1 安全等级评定参考

4.1.1 应用系统单一漏洞风险等级评定参考

应用系统单一漏洞风险等级评定参考如下：

严重风险	1、直接获取系统权限的漏洞（服务器权限、客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传获取 Webshell、SQL 注入获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。
	2、直接导致业务拒绝服务的漏洞。包括但不仅限于直接导致移动网关业务 API 业务拒绝服务、网站应用拒绝服务等造成严重影响的远程拒绝服务漏洞。
	3、严重的敏感信息泄漏。包括但不仅限于核心 DB（资金、身份、交易相关） 的 SQL 注入，上万级别的敏感信息泄露。
	4、严重的逻辑设计缺陷和流程缺陷。包括但不仅限于伪造任意号码发送消息、任意账号资金消费、任意帐号密码修改漏洞。
高风险	1、敏感信息泄漏。包括但不仅限于非核心 DB SQL 注入、源代码压缩包泄漏、可获取大量用户交易信息的接口、服务器应用加密可逆或明文、移动 API 访问摘要、硬编码等问题引起的敏感信息泄露。
	2、敏感信息越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码、任意订单查看、任意用户敏感信息访问、获取大量内网敏感信息的 SSRF，影响业务运行的 Broadcast 消息伪造等 Android 组件权限漏洞等。
	3、越权敏感操作。包括但不仅限于账号越权修改重要信息、进行订单普通操作、重要业务配置修改等较为重要的越权行为。
	4、大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的存储型 XSS（包括存储型 DOM-XSS）和涉及交易、资金、密码、店铺的 CSRF。
	5、影响到服务器的本地提权漏洞。
中风险	1、需交互方可影响用户的漏洞。包括但不仅限于反射型 XSS（包括反射型 DOM-XSS）、普通 CSRF、URL 跳转漏洞。
	2、本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等。

	3、普通越权操作。包括但不仅限于不正确的直接对象引用。
	4、普通信息泄漏。包括但不仅限于客户端明文存储密码、客户端密码明文传输以及 web 路径遍历、系统路径遍历。
	5、普通的逻辑设计缺陷和流程缺陷。
低风险	1、轻微信息泄漏。包括但不仅限于路径信息泄漏、SVN 信息泄漏、PHPinfo、异常信息泄露，以及客户端应用本地 SQL 注入（仅泄漏数据库名称、字段名、cache 内容）、日志打印、配置信息、异常信息等。
	2、难以利用但存在安全隐患的漏洞。包括但不仅限于难以利用的 SQL 注入点、可引起传播和利用的 Self-XSS、需构造部分参数且有一定影响的 CSRF。

4.1.2 应用系统安全等级评定参考

应用系统安全等级评定参考如下：

远程严重风险系统 （符合任何一个条件）	1、存在 1 个以上严重风险安全问题，可直接导致系统受到破坏；
	2、与其他严重风险系统连接，同时存在相互信任关系（或帐号互通）的主机；
	3、发现已经被人入侵且留下远程后门的主机；
	4、存在 3 个或以上高风险安全问题的主机；
	5、与其他非安全系统在一个共享网络中，同时远程维护明文传输口令；
	6、完全不能抵抗小规模的拒绝服务攻击
远程高风险系统 （符合任何一个条件）	1、存在 1 个或以上高风险安全问题的主机；
	2、与其他非安全系统直接连接，但暂时不存在直接信任(或帐号互通)关系；
	3、远程维护通过明文的方式传递信息；
	4、存在三个以上中风险问题的主机；
	5、只能抵御小规则的拒绝服务攻击；
远程中风险系统 （符合全部条件）	1、存在 1 个或以上中等安全问题的主机；
	2、存在 3 个以上低风险问题，通过多个低风险问题可以构成中风险漏洞的。
	3、远程维护通过编码的方式传递信息；
	4、能抵挡小规模的拒绝服务攻击。
远程低风险系统 （符合全部条件）	1. 最多存在 1-2 个轻度安全问题；
	2. 远程维护方式安全；
	3. 与不安全或一般安全系统相对独立；
	4. 能抵挡一定规模的拒绝服务攻击。

4.2 安全意见

经过本次远程渗透测试，我们发现被检测系统中存在一些安全问题或者隐患，因此我们在本节中，建议采用如下方式修补这些问题。对于无法马上得到解决的问题，我们也将提出相应的解决建议供您参考。

4.2.1 传输安全

敏感数据传输采用 HTTPS 传输，并进行内容加密，可以保障网站数据和账户信息的安全性。

4.2.2 Web 安全编程

即使有客户端验证，也不要相信客户端的输入！

- 请求 URL 的参数部分
- HTML 表单通过 POST 或 GET 请求提交的数据
- 在客户端临时保存的数据（也就是 Cookie）
- 数据库查询。

4.2.3 安全复检

针对此次检查发现一些安全问题，相信相关管理人员能够尽快解决。不过，有限的时间和随时变化的漏洞库无法保证网站没有其他的安全隐患。建议再次进行安全检测，以校验评估安全状态，并确保无其他安全问题存在。

4.2.4 定期进行安全审计

虽然我们在本次检测中发现了这些问题，并且相信这些安全隐患能够在短时间内解决。我们仍然建议您定期进行类似的安全审计，保障不断发展的动态网络的持续安全。