

主测人：

XXXX管理系统网站渗透测试报告

2017年01月 05日

[文档编号：xxxx-ST-20170105]

版本说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 修订人 | 修订内容 | 修订时间 | 版本号 | 审阅人 |
| 张凯 | 编写文档 | 2017.01.05 | V1.0 | 李鑫 |

文档信息

|  |  |  |  |
| --- | --- | --- | --- |
| 文档名称 | 文档版本号 | 文档编号 | 保密级别 |
| XXXX管理系统网站安全渗透测试报告 | V1.0 | 【xxxx-ST-20170105】 | 项目组公开 |

版权声明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京知道创宇信息技术有限公司所有，受到有关产权及版权法保护。任何个人、机构未经北京知道创宇信息技术有限公司的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

目录

[1. 综述 1](#_Toc474917049)

[2. 网站漏洞分布 1](#_Toc474917050)

[2.1. 漏洞等级分布 1](#_Toc474917051)

[2.2. 漏洞类型分布 2](#_Toc474917052)

[2.3. 渗透测试汇总 3](#_Toc474917053)

[3. 渗透测试结果分析 4](#_Toc474917054)

[3.1. b2c-prelaunch.xx.com 4](#_Toc474917055)

[3.1.1. Mysql数据库弱口令 4](#_Toc474917056)

[3.1.2. Apache Solr未授权访问 5](#_Toc474917057)

[3.1.3. HashiCorp未授权访问 6](#_Toc474917058)

[3.1.4. 存储型XSS 7](#_Toc474917059)

[3.1.5. 存储型XSS 9](#_Toc474917060)

[3.1.6. SQL注入 11](#_Toc474917061)

[危险等级：高 11](#_Toc474917062)

[3.1.7. 登陆密码明文提交 13](#_Toc474917063)

[4. 漏洞修复方案 14](#_Toc474917064)

[4.1. SQL注入修复建议 14](#_Toc474917065)

[4.2. 跨站脚本攻击(XSS) 14](#_Toc474917066)

[4.3. 用户凭证明文传输 15](#_Toc474917067)

[4.4. 应用程序错误信息 15](#_Toc474917068)

[5. 附录A：漏洞风险评级标准 16](#_Toc474917069)

[6. 附录B：应用系统风险评级标准 16](#_Toc474917070)

[7. 附录C：典型Web安全风险简介 17](#_Toc474917071)

[7.1. SQL注入简介 17](#_Toc474917072)

[7.2. LDAP 注入漏洞简介 17](#_Toc474917073)

[7.3. XPath注入漏洞简介 18](#_Toc474917074)

[7.4. SSI注入漏洞简介 18](#_Toc474917075)

[7.5. 跨站（XSS）简介 19](#_Toc474917076)

[7.6. 操作系统命令执行漏洞简介 19](#_Toc474917077)

[7.7. 格式字符串远程命令执行漏洞简介 20](#_Toc474917078)

[7.8. 路径遍历漏洞简介 20](#_Toc474917079)

[8. 附录D：漏洞测试工具简介 20](#_Toc474917080)

[8.1. Sqlmap注入工具 20](#_Toc474917081)

[8.2. BurpSuite代理工具 21](#_Toc474917082)

[8.3. Firefox hackbar插件 21](#_Toc474917083)

[8.4. WebSOC网站安全立体监控系统 21](#_Toc474917084)

[8.5. 知道创宇Pocsuite开源远程漏洞测试框架 21](#_Toc474917085)

[8.6. 知道创宇渗透测试人员专用工具包 21](#_Toc474917086)

[9. 附录E 知道创宇研发技能表v3.0 22](#_Toc474917087)

1. 综述

本次报告有效测试时间是从2017年01月04日开始到2017年01月06日结束，在此期间针对**xxxx管理系统网站**网站的安全性和完整性进行测试并以此作为报告统计依据。

本次对**xxxx管理系统网站**网站进行Web安全测试，共检测域名1个，漏洞总数7个，整体安全风险总评级为**严重**。其中高风险网站1个，中风险网站0个，安全网站0个。总共发现严重漏洞**1**个，高危漏洞**5**个，中危漏洞**0**个，低危漏洞**1**个。

由于本次测试过程中采用保守测试方法，生产环境评估为高风险操作的的功能，均与**xxxx管理系统网站**相关接口人进行沟通，并在操作风险可控的情况下进行相关测试操作，以规避测试过程中的生产运营风险。

**本次测试的目标系统如下：**

|  |  |
| --- | --- |
| 网站域名 | 目标IP地址 |
| b2c-prelaunch.xx.com | xxx.xx.xx.xx |

**使用账号信息如下：**

|  |  |
| --- | --- |
| 账号 | 密码 |
| cexxxx | xxxxxxx |
| Cexxxx | xxxxxxx |

1. 网站漏洞分布
   1. 漏洞等级分布

本次漏洞风险按等级统计：

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞风险等级个数统计表 | | | |
| 严重 | **高危** | **中危** | **低危** |
| 1 | 5 | **0** | **1** |

* 1. 漏洞类型分布

本次漏洞按类型统计：

|  |  |  |  |
| --- | --- | --- | --- |
| 风险等级 | 数量 | 安全问题名称 | 域名 |
| 严重风险 | 1 | Mysql数据库弱口令 | b2c-prelaunch.xxcom |
| 高风险 | 1 | SQL注入 | b2c-prelaunch.xx.com |
| 高风险 | 2 | 存储型XSS | b2c-prelaunch.xx.com |
| 高风险 | 1 | Apache solr未授权访问 | b2c-prelaunch.xx.com |
| 高风险 | 1 | HashiCorp未授权访问 | b2c-prelaunch.xx.com |
| 低风险 | 1 | 登录密码明文提交 | b2c-prelaunch.xx.com |

* 1. 渗透测试汇总

**漏洞结果列表:**

|  |  |
| --- | --- |
| 漏洞名称 | 漏洞URL |
| 严重漏洞 |  |
| Mysql数据库弱口令 | 地址：xxx.xx.xx.xx 端口：55222 |
| 高危漏洞 |  |
| 存储型XSS | http://b2c-prelaunch.xx.com/b2c/storegallery/touchScreen/update/82 |
| 存储型XSS | http://b2c-prelaunch.xx.com/b2c/cms/category/updateView/12 |
| SQL注入 | http://b2c-prelaunch.xx.com/b2c/payment/list?page=0&size=10&sortType=createTime&sortDirection=desc&orderId=1680617010387931 |
| Apache Solr未授权访问 | http://b2c-prelaunch.xx.com:8983/solr/#/ |
| HashiCorp未授权访问 | http://b2c-prelaunch.xx.com:8500/ui/#/dc1/services/b2chub\_app |
| 低危漏洞 |  |
| 登录密码明文提交 | http://b2c-prelaunch.xx.com/b2c/login |

1. 渗透测试结果分析

通过本次对**XX管理系统**网站进行Web安全测试，知道创宇工程师发现目标网站存在多个漏洞，属于**严重不安全系统**。

* 1. b2c-prelaunch.xx.com
     1. Mysql数据库弱口令

**漏洞地址：**xxx.xx.xx.xx

**端口：**xxxxx

**危险等级：严重**

**漏洞说明：**Mysql数据库Root用户，密码过于简单。容易被攻击者猜解并进入数据库，会给数据库中的数据带来极大影响。

**漏洞截图**：

在针对xxx.xx.xx.xx进行端口扫描时，发现开放了xxxxx端口为mysql数据库端口。于是便对数据库root用户密码进行简单猜解。最后猜解出root用户密码为：123



此数据库中保存数据众多，包括了许多管理员的账号密码。

**漏洞危害：**攻击者可以对数据库中的数据进行增删改查以及导出数据库等危险操作，另外由于root用户权限比较大甚至可能会影响到mysql数据库服务器的安全。

**修复方案：**修改Mysql数据库密码为高强度且复杂不容易被猜解的密码。

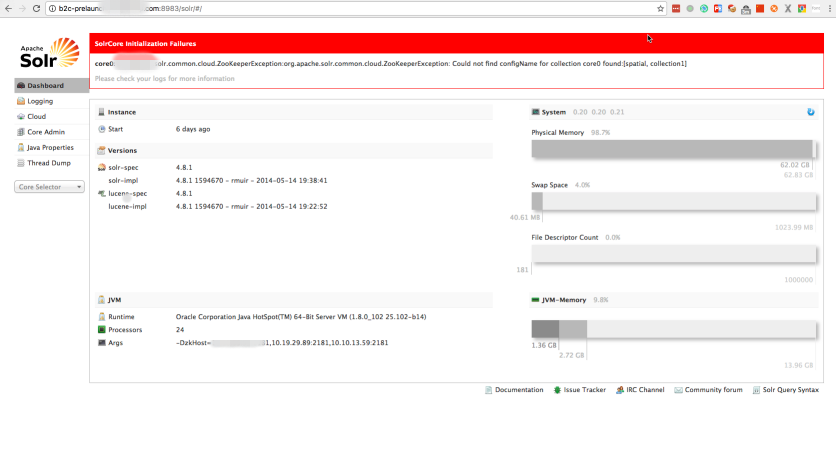
* + 1. Apache Solr未授权访问

**漏洞地址：**http://b2c-prelaunch.xx.com:8983/solr/#/

**危险等级：高**

**漏洞说明：**攻击者可以未经授权便可以访问查看solr系统上的敏感信息，包括数据库地址啊，代码错误信息等。

**漏洞截图**：



**漏洞危害：**会造成严重的信息泄露。攻击者可以未经授权便可以访问查看solr系统上的敏感信息，包括数据库地址啊，代码错误信息查看，以及查看文件内容等。

**修复方案：**对服务器上的solr进行正确配置，对Apache solr进行访问控制，禁止公网无需认证即可访问solr。

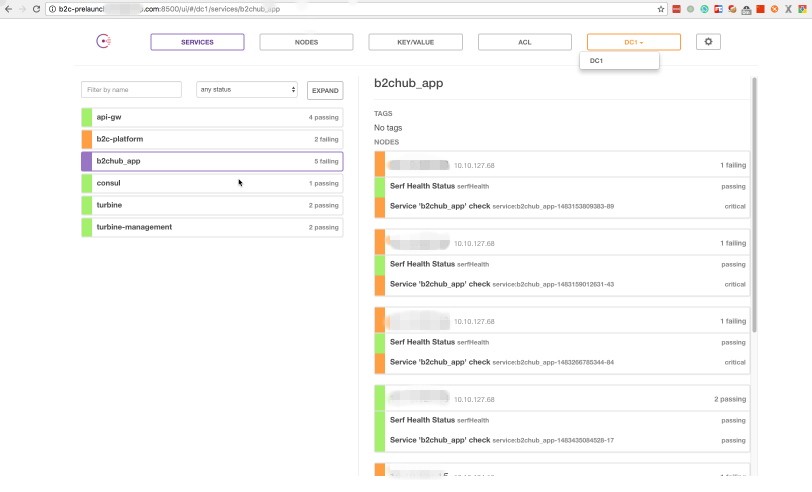
* + 1. HashiCorp未授权访问

**漏洞地址：**http://b2c-prelaunch.xx.com:8500/ui/#/dc1/services/b2chub\_app

**危险等级：高**

**漏洞说明：**攻击者可以未经授权便可以访问查看HashiCorp系统上的敏感信息，可以添加以及删除信息，节点。

**漏洞截图**：



**漏洞危害：**攻击者可以未经授权便可以访问查看HashiCorp系统上的敏感信息。可以查看节点以外还可以添加以及删除信息跟节点。会给网站正常运营带来影响。

**修复方案：**对HashiCorp系统进行正常配置，要求输入账号密码。或者公网不允许访问HashiCorp系统。

* + 1. 存储型XSS

**漏洞地址：**http://b2c-prelaunch.xx.com/b2c/storegallery/touchScreen/update/82

**漏洞存在点：**场次名称

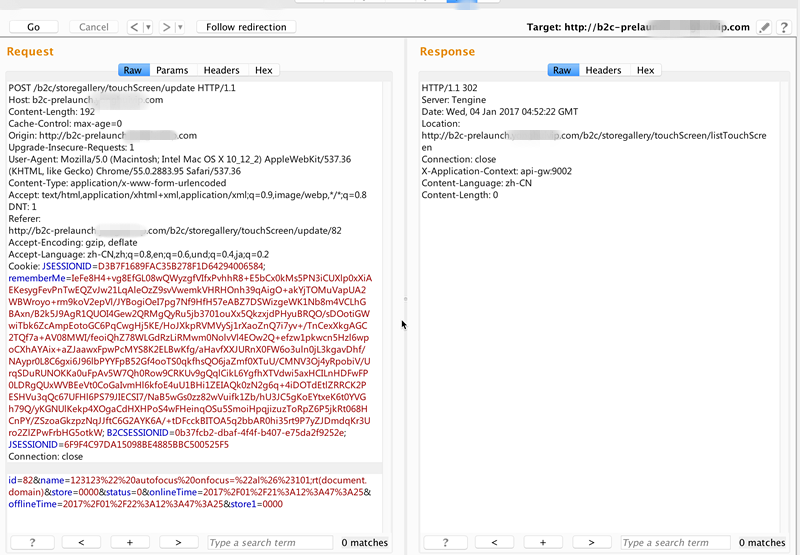
**危险等级：高**

**漏洞说明：**虽然使用了XSEC WAF来从提交的数据包中来拦截关键字，但是未对关键字符进行过滤所以稍加处理即可绕过XSEC WAF的防护。

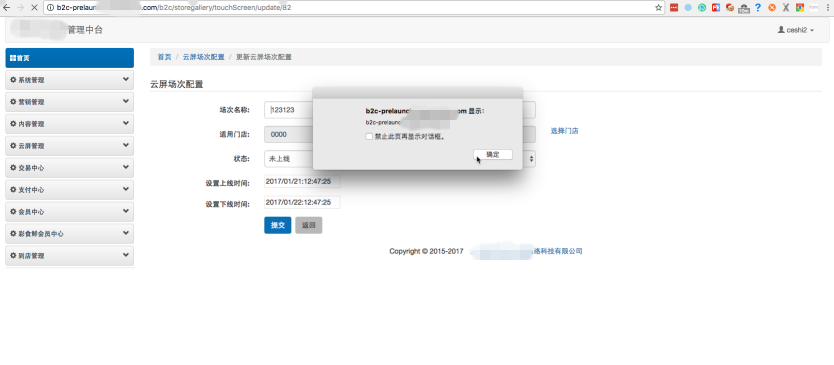
比如拦截了alert 只需要对其中一个字符进行编码即可绕过拦截。导致该模块出现跨站漏洞。攻击者可以利用该漏洞任意修改页面内容，实施钓鱼攻击、窃取用户登陆凭证、csrf攻击、挂马攻击等。

**漏洞截图**：

提交包含payload的数据包



正常浏览时，触发XSS漏洞。



**漏洞危害：**攻击者可以利用该漏洞任意修改页面内容，实施钓鱼攻击、窃取用户登陆凭证、csrf攻击、挂马攻击等

**修复方案：**从代码层面先过滤以及转义一些危险字符 比如 单引号 双引号 尖括号等，然后再拦截一些html标签的时间以及js危险函数的关键字比如:document alert**。**

* + 1. 存储型XSS

**漏洞地址：**http://b2c-prelaunch.xx.com/b2c/cms/category/updateView/12

**漏洞存在点：**跳转链接

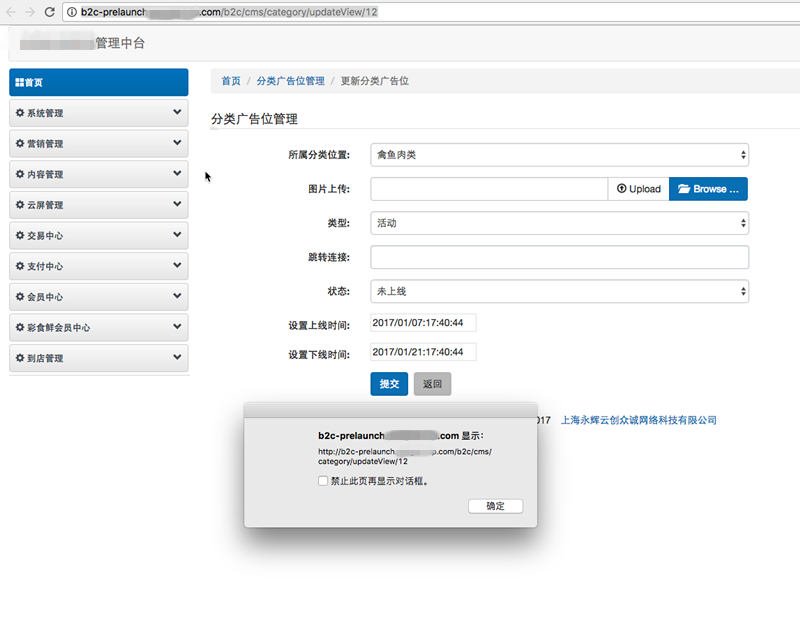
**危险等级：高**

**漏洞说明：**虽然使用了XSEC WAF来从提交的数据包中来拦截关键字，但是未对关键字符进行过滤所以稍加处理即可绕过XSEC WAF的防护。

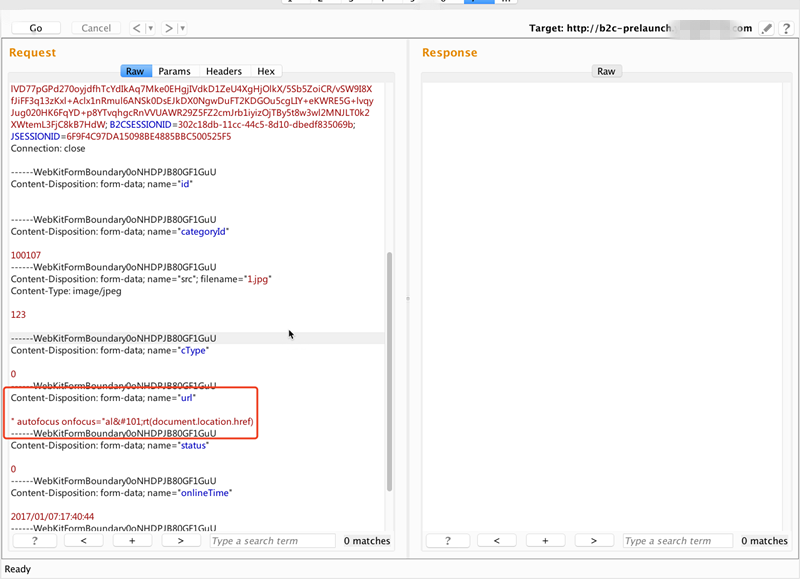
比如拦截了alert 只需要对其中一个字符进行编码即可绕过拦截。导致该模块出现跨站漏洞。攻击者可以利用该漏洞任意修改页面内容，实施钓鱼攻击、窃取用户登陆凭证、csrf攻击、挂马攻击等。

**漏洞截图**：

漏洞存在证明



提交包含payload的数据包



漏洞页面源代码



**漏洞危害：**攻击者可以利用该漏洞任意修改页面内容，实施钓鱼攻击、窃取用户登陆凭证、csrf攻击、挂马攻击等

**修复方案：**从代码层面先过滤以及转义一些危险字符 比如 单引号 双引号 尖括号等，然后再拦截一些html标签的时间以及js危险函数的关键字比如:document alert**。**

* + 1. SQL注入

**漏洞地址：**http://b2c-prelaunch.xx.com/b2c/payment/list?page=0&size=10&sortType=createTime&sortDirection=desc&orderId=1680617010387931

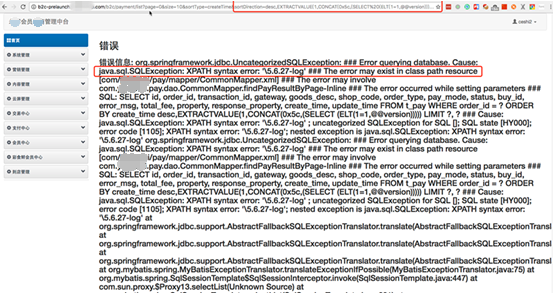
**漏洞参数：**sortDirection

**危险等级**：高

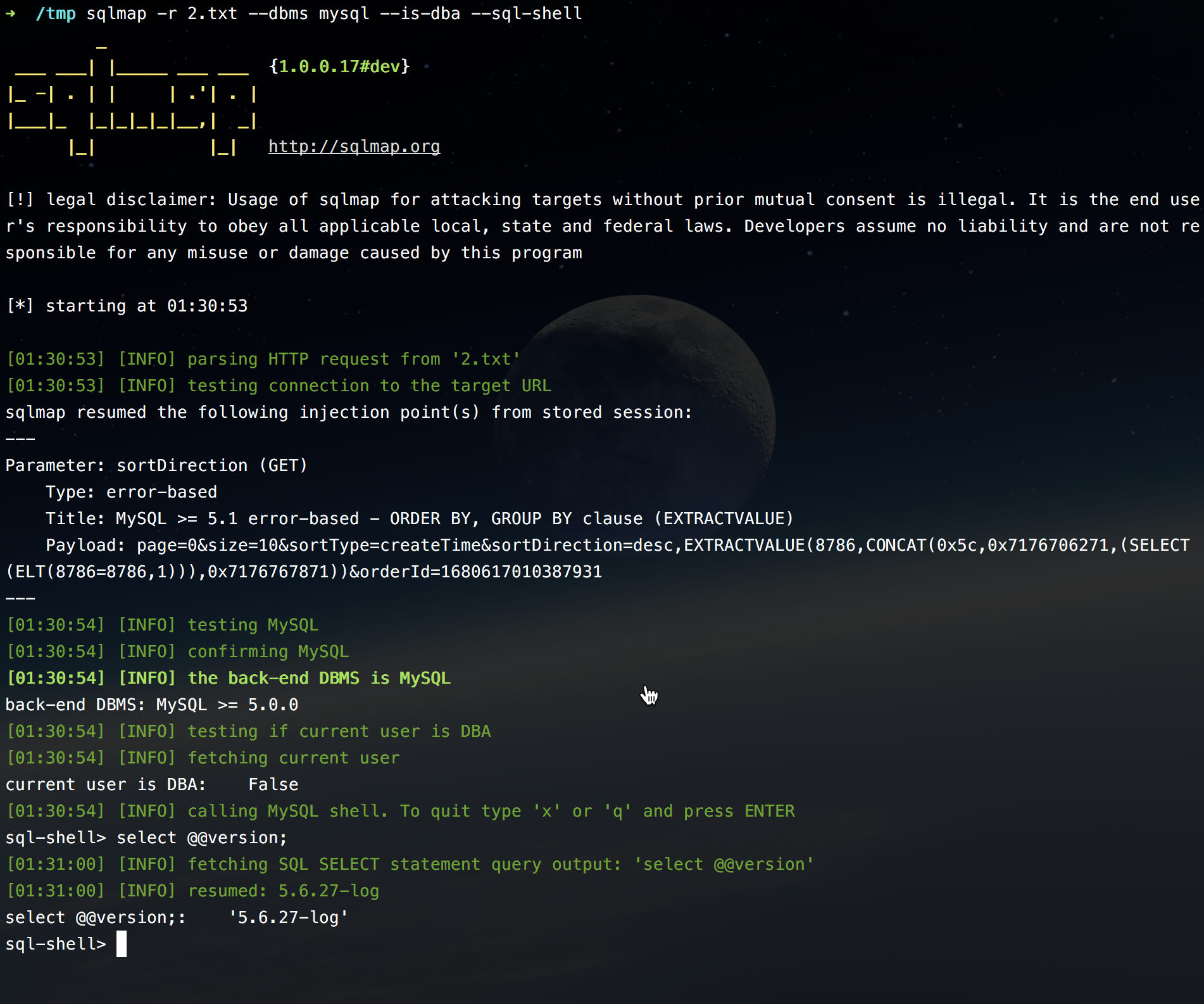
**漏洞说明：**sortDirection参数处接受的数据未经过滤便带入到了sql语句中执行，从而造成了SQL注入漏洞的产生。

**漏洞截图**：

显错注入，查询mysql版本号 select @@version;



使用sqlmap工具利用SQL注入



**漏洞危害:** sql注入对数据库造成威胁非常大，攻击者可以对数据库中的数据进行查询，导出数据库中的数据。如果被攻击者恶意攻击会给业务带来极大影响。

**修复方案：**使用框架封装的sql函数，或者对传入参数进行转义或者过滤。

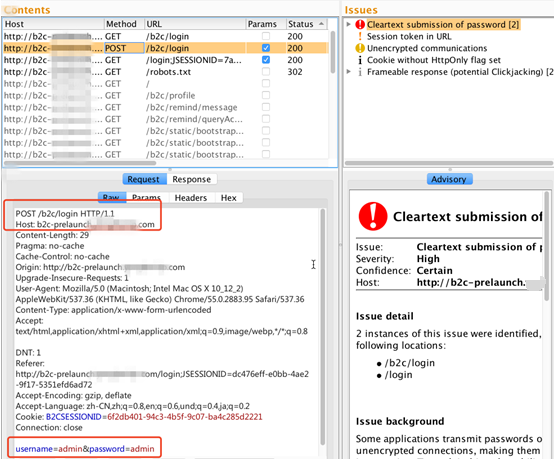
* + 1. 登陆密码明文提交

**漏洞地址：**http://b2c-prelaunch.xx.com/b2c/login

**危险等级：低**

**漏洞说明：**账号密码未加密，如果存在dns欺诈，内网嗅探等攻击，可直接泄露用户账户密码。

**漏洞截图**：



**漏洞危害：**账号密码未加密，如果存在dns欺诈，内网嗅探等攻击，可直接泄露用户账户密码

**修复方案：**敏感信息采用https传输，对用户名密码进行加密

1. 漏洞修复方案
   1. SQL注入修复建议

**修复建议：**

1. 过滤用户输入的内容，检查用户输入的内容中是否有非法内容。如，|（竖线符号）、 & （& 符号）、;（分号）、$（美元符号）、%（百分比符号）、@（at 符号）、'（单引号）、"（引号）、\'（反斜杠转义单引号）、\"（反斜杠转义引号）、<>（尖括号）、()（括号）、+（加号）、 CR（回车符，ASCII 0x0d）、 LF（换行，ASCII 0x0a）、,（逗号）、\（反斜杠）、)（结束括号）等符号。

2. 过滤危险的SQL语句关键字，如select,from,update,insert,delete等。

3. 利用存储过程，将数据访问抽象化，让用户不直接访问表或视图。当使用存储过程时，请利用 ADO 命令对象来实施它们，以强化变量类型。

4. 使用防注入系统。

* 1. 跨站脚本攻击(XSS)

**描述：**Web程序代码中把用户提交的参数未做过滤就直接输出到页面，参数中的特殊字符打破了HTML页面的原有逻辑，攻击者可以利用该漏洞执行恶意HTML/JS代码、构造蠕虫传播、篡改页面实施钓鱼攻击等。

**修复方案：**

(1) 判断参数的合法性，不合法不返回任何内容。

(2) 严格限制URL参数输入值的格式，不能包含不必要的特殊字符（%0d、%0a、%0D、%0A等）。

(3) 针对Cookie设置HttpOnly策略。

(4) 针对ASP.NET的防XSS库，Microsoft有提供统一的库，具体可以参见如下链接微软官网：

http://xx.xx.com/en-us/library/aa973813.aspx

* 1. 用户凭证明文传输

**描述：**用户凭据通过未加密的通道传输。第三方可以通过拦截未加密的HTTP连接读取用户的凭据。

**修复方案：**用户凭据被认为是敏感的信息，要通过加密连接传送到服务器（HTTPS）。

* 1. 应用程序错误信息

**描述：**

页面包含可披露敏感信息的错误/警告消息。该消息还可以包含产生异常的文件的位置。攻击者可以从错误消息中获取有利信息从而用于进一步的攻击。

**修复方案：**

（1）仔细分析该请求行为，在编码中给予足够的错误检查、过滤、白名单，增强系统稳定性。

（2）设置禁止错误信息输出。

1. 附录A：漏洞风险评级标准

|  |  |
| --- | --- |
| *公网系统漏洞风险评级标准* | |
| 漏洞评级 | **漏洞评级说明** |
| 严重漏洞 | 直接获取业务服务器权限的漏洞以及获取重要数据的漏洞，包括但不限于任意命令执行、上传webshell、任意代码执行、SQL注入获得大量数据；  严重影响系统业务安全的逻辑漏洞，包括但不限于任意帐号密码重置或更改漏洞，大量获取用户身份认证信息的漏洞，越权访问漏洞，未授权访问后台管理系统等；  可通过一定手段严重影响业务运行，可能给客户带来巨大损失的，如关键业务操作可被Dos，登录接口可被撞库，业务系统可被轻易薅羊毛等；  当前阶段正在大规模爆发应引起足够重视的安全漏洞等。 |
| 高危漏洞 | 需要强烈的用户交互才能获取用户身份信息的漏洞，包常规存储型／反射型XSS漏洞，核心关键业务操作的CSRF漏洞等；  任意文件读取、修改、覆盖、删除、下载；  绕过限制修改用户个人资料、个人信息、强制用户执行某些操作；  能够对目标系统带来危害的严重信息泄漏，敏感信息文件备份或源码泄露等（如存储密钥泄露，数据看连接密码泄露，SVN／Git帐号泄露，VPN帐号泄露等）。 |
| 中危漏洞 | 能够对目标系统的安全造成影响但无法直接证实可被利用的；  能够获取目标网络设备权限但确定无法进一步利用的；  非重要信息泄露、开放的URL跳转漏洞、有一定限制且确定较难利用的XSS漏洞、非核心关键业务操作的CSRF漏洞等。 |
| 低危漏洞 | 无法确定是否能够对目标系统的安全造成影响的，如目标系统管理端口向公网开放但无法直接利用，目标系统Banner信息可被识别，以及其他渗透测试人员认定，较难利用但可能会存在潜在安全威胁的漏洞。 |

1. 附录B：应用系统风险评级标准

|  |  |
| --- | --- |
| *公网应用系统风险评级标准* | |
| 系统风险评级 | **漏洞评级说明** |
| 严重不安全系统 | 存在1个及以上严重漏洞，或2个以上高危漏洞的系统 |
| 高危不安全系统 | 存在1个及以上高危漏洞，或3个以上中危漏洞的系统 |
| 中危不安全系统 | 存在1个及以上中危漏洞，或5个以上低危漏洞的系统 |
| 安全系统 | 存在5个以内低危漏洞，或不存在漏洞的系统 |

1. 附录C：典型Web安全风险简介
   1. SQL注入简介

SQL注入（SQL Injection），简称注入攻击、SQL注入，被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。Web 应用程序通常在后端使用数据库，以与企业数据仓库交互。查询数据库事实上的标准语言是 SQL（各大数据库供应商都有自己的不同版本）。Web 应用程序通常会获取用户输入（取自 HTTP 请求），将它并入 SQL 查询中，然后发送到后端数据库。接着应用程序便处理查询结果，有时会向用户显示结果。

如果应用程序对用户（攻击者）的输入处理不够小心，攻击者便可以利用这种操作方式。在此情况下，攻击者可以注入恶意的数据，当该数据并入 SQL 查询中时，就将查询的原始语法更改得面目全非。例如，如果应用程序使用用户的输入（如用户名和密码）来查询用户帐户的数据库表，以认证用户，而攻击者能够将恶意数据注入查询的用户名部分（和/或密码部分），查询便可能更改成完全不同的数据复制查询，可能是修改数据库的查询，或在数据库服务器上运行 Shell 命令的查询。

* 1. LDAP 注入漏洞简介

LDAP 注入是一个可供利用 Web 站点的攻击技术，它利用用户提供的输入来构造 LDAP 语句。

轻量级目录访问协议（LDAP）是用来查询及操作 X.500 目录服务的开发标准协议。LDAP 协议是通过 TCP 之类的因特网传输协议来运行。Web 应用程序可以利用用户提供的输入来创建动态 Web 页面请求的定制 LDAP 语句。

当 Web 应用程序未将用户提供的输入适当清理时，攻击者便有可能改变 LDAP 语句的结构，使过程得以利用执行命令的组件（例如：数据库服务器、Web 应用程序服务器、Web 服务器）的相同许可权来运行。这有可能造成很严重的安全问题，许可权可能会授予查询、修改或除去 LDAP 树状构造内任何条目的权利。

在LDAP 注入中，也能够依照类似方式来应用SQL 注入中所能使用的相同的清理利用技术。”

* 1. XPath注入漏洞简介

XPath 是用来引用一部分 XML 文档的语言。它可以直接供应用程序用来查询 XML 文档，或用作较大操作的一部分（例如，将 XSLT 变换应用于 XML 文档，或将 XQuery应用于XML文档，等等）。

XPath的语法有些类似 SQL查询，而且利用XPath也确实有可能在XML 文档上形成类似SQL的查询。例如，假定XML文档包含“user”名称的元素，每个元素各包含3个子元素 －“name”、“password”和 “account”。这时下列 XPath 表达式会产生名称为“jsmith”、密码为“Demo1234”的用户的帐号（如果没有这样的用户，便是空字符串）：string(//user[name/text()='jsmith' and password/text()='Demo1234']/account/text())

因此，如果Web应用程序利用XPath来查询XML文档，且检索了从客户端接收其名称和密码的用户的账号，这类应用程序可能将这些值直接嵌入在XPath查询中，从而创建安全漏洞。

* 1. SSI注入漏洞简介

当符合下列条件时，攻击者可以在 Web 服务器上运行任意命令：

A. Web 服务器已开启SSI支持（服务器端包含）。

B. Web应用程序在返回 HTML 页面时，嵌入用户输入的内容。

C. 参数值未进行输入清理。

例如，如果脚本接收文本输入，供 Web 服务器稍后处理，下列由 SSI 命令组成的输入便会侵害服务器的安全：

<!--#include file=""...""-->（会显示给定的文件）

<!--#exec cmd=""...""-->（会执行给定的 shell 命令）

* 1. 跨站（XSS）简介

跨站脚本攻击（Cross-site scripting，通常简称为XSS）发生在客户端，可被用于进行窃取隐私、钓鱼欺骗、偷取密码、传播恶意代码等攻击行为。 恶意的攻击者将对客户端有危害的代码放到服务器上作为一个网页内容， 使得其他网站用户在观看此网页时，这些代码注入到了用户的浏览器中执行，使用户受到攻击。一般而言，利用跨站脚本攻击，攻击者可窃会话COOKIE从而窃取网站用户的隐私，包括密码。

XSS攻击使用到的技术主要为HTML和Javascript，也包括VBScript和ActionScript等。XSS攻击对WEB服务器虽无直接危害，但是它借助网站进行传播，使网站的使用用户受到攻击，导致网站用户帐号被窃取，从而对网站也产生了较严重的危害。

* 1. 操作系统命令执行漏洞简介

在Web应用中，有些程序或脚本是通过操作系统调用来执行命令。有时，URL 参数会用来作为命令的一部分。在这种情况下，有可能注入将在操作系统上运行的代码。这类代码注入可以使用各种语法：

cmd1|cmd2 （利用cmd1的输出作为cmd2的输入）

cmd1&&cmd2 （如果cmd1的返回码是 true，便运行cmd2）

cmd1||cmd2 （如果cmd1的返回码是false，便运行cmd2）

有时候，会用单引号（'）或双引号（"）括住第一个命令，因此，如果要运行第二个命令，必须先转义引号。

攻击者可以利用这些变体，尝试在主机上执行任意代码。

* 1. 格式字符串远程命令执行漏洞简介

“格式字符串问题”是在 C/C++ 的 sprintf 及其他语言类似函数或特定逻辑中，以客户端输入作为格式化字符串输入所造成。如果恶意的用户将由 printf() 转换字符（%f, %p、%n 等）组成的“格式化字符串”作为参数传递，Web 应用程序可能会遭受破坏而执行任意代码。

示例： 应用程序使用由用户发送的参数“Email\_address”。应用程序使用 printf 来打印该变量：

printf(Email\_address);

在这种情况下，会对客户端输入进行解析（由 printf 进行）。

打印地址的正确方式如下：

printf("%s",Email\_address);

在这种情况下，不会对 Email\_address 变量进行解析。

* 1. 路径遍历漏洞简介

路径遍历漏洞允许恶意攻击者突破Web应用程序的安全控制，直接访问攻击者想要的敏感数据，包括配置文件、日志、源代码等，配合其它漏洞的综合利用，攻击者可以轻易的获取更高的权限，并且这样的漏洞在发掘上也是很容易的，只要对Web应用程序的读写功能块直接手工测试，通过返回的页面内容来判断，是很直观的，利用起来也相对简单。

1. 附录D：漏洞测试工具简介
   1. Sqlmap注入工具

Sqlmap是国外的一个免费的注入工具，基于python开发，支持现在几乎所有的数据库，支持get、post、cookie注入，可以添加cookie和user-agent，支持盲注，报错回显注入，DNS回显注入等，还有其他多种注入方法，支持代理，优化算法，更高效，可通过指纹识别技术判断数据库。

* 1. BurpSuite代理工具

Burp Suite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

* 1. Firefox hackbar插件

简单的安全审计、渗透测试小工具包，包含一些常用的工具。(SQL injection，XSS，编码，加密、解密等)。

* 1. WebSOC网站安全立体监控系统

知道创宇网站安全立体监控系统（WebSOC）是高性能、周期性网站集中安全监测硬件产品，支持单设备和集群部署。能够从网站基本信息、网站可用性、网站安全事件、网站漏洞四个维度对大批量的网站进行全方位安全监控，对网站安全事件和漏洞情况及时告警，并可提供全部监测目标的全局统计报表和趋势分析，为监管层改进组织的网站安全情况提供有价值的参考数据。

* 1. 知道创宇Pocsuite开源远程漏洞测试框架

Pocsuite 是由知道创宇安全研究团队打造的一款开源的远程漏洞测试框架。它是知道创宇安全研究团队发展的基石，是团队发展至今一直维护的一个项目，保障了我们的 Web 安全研究能力的领先。

Pocsuite 采用 Python 编写，支持验证与利用两种插件模式，你可以指定单个目标或者从文件导入多个目标，使用单个 PoC 或者 PoC 集合进行漏洞的验证或利用。可以使用命令行模式进行调用，也支持类似 Metasploit 的交互模式进行处理，除此之外，还包含了一些基本的如输出结果报告等功能。

* 1. 知道创宇渗透测试人员专用工具包

知道创宇渗透测试人员专用工具包，由知道创宇渗透测试工程师研发，收集和使用，包含专用于测试人员的批量自动测试工具，自主研发的工具、脚本或利用工具等。

1. 附录E 知道创宇研发技能表v3.0

http://blog.knownsec.com/Knownsec\_RD\_Checklist/v3.0.html

