密 级:

MatriXay Web应用安全评估报告

本报告： 项目采用web安全检测后得出的评估报告。由于报告内容属于机密资料,请报告拥有者在阅读和发布时妥善进行适当的安全控制

1 . 综述

本报告共包含1个Web安全检测项目， 一共检查了1个网站， 共访问了14个URL，完成了3304次测试，共发现Web安全漏洞6个，其中紧急安全漏洞2个，高危安全漏洞4个。

1.1 . 报告内容

该报告包含以下内容:

评估报告综述

网站详细漏洞

漏洞描述建议

网站评估结论

参考标准

1.2 . 测试策略集

08cms search.php SQL注入,ASP.NET padding oracle,CMS4J JAVA 2005版系统后门,CMSTOP vote.php文件SQL注入,CSII CMS url跳转钓鱼,Ckeditor 4.0.1 跨站脚本漏洞,Cookie SQL注入,Cookie SQL注入（Base64）,Dedeeims wap.php SQL注入,Discuz Flash附件跨站脚本,Discuz v63积分商城插件注入,Discuz! X2.5 521交友插件SQL注入,Discuz!X转换工具Getwebshell漏洞,Discuz图片附件跨站脚本,Ecmall coupon.app.php SQL注入,Ecmall my_goods.app.php SQL注入,Ecmall my_navigation.app.php SQL注入,Ecmall my_payment.app.php文件包含漏洞,Ecmall seller_groupbuy.app.php SQL注入,Ecmall发布商品跨站脚本,Ecmall团购功能跨站脚本,Ecshop 2.6.2版pick_out.php SQL注入,Ecshop 2.7.3官方补丁包存在后门,Ecshop 2.73 lib_transaction.php文件二次SQL注入,Ecshop GBK版user.php宽字节SQL注入,Ecshop flow.php SQL注入（需注册登录）,Ecshop flow.php spec参数SQL注入,Ecshop goods_script.php SQL注入,Ecshop search.php SQL注入,Ecshop 支付插件SQL注入,Ecshop后台任意用户备份整站文件,E时代协同办公系统任意文件下载,FCKeditor 2.4.2 php版本任意文件上传,FCKeditor 2.6.4 php版本任意文件上传,Http响应拆分,JBOSS jmx-console配置错误,JBoss JMX Console弱密码,KingCms门户系统pm.php SQL注入,KingCms门户系统存储型XSS,KingCms企业版本search.php代码执行,LDAP注入,Metinfo getpassword.php SQL注入,Nginx空字节代码执行,Nportal烟草管理系统任意文件上传,OpenSSL HeartBleed漏洞,PHP CGI fix_pathinfo远程代码执行,PHPDisk passport.php SQL注入,PageAdmin CMS 默认数据库下载,Php168 v7后台Getwebshell漏洞,Php168 知道系统user.php SQL注入,Phpcms 2007 Member.php页面SQL注入,Phpcms 2007 onunload.inc.php文件SQL注入,Phpcms 2007 sp6 digg_add.php文件SQL注入,Phpcms 2007 sp6 formid参数SQL注入,Phpcms 2007 sp6 wenba模块SQL注入,Phpcms 2007 web.php文件宽字节SQL注入,Phpcms2008 SQL注入,Phpcms2008 preview.php文件SQL注入,Phpcms2008 referer注入,PhpcmsV9 Apache解析Getwebshell漏洞,PhpcmsV9 attachments.php SQL注入,PhpcmsV9 referer注入,PhpcmsV9 后台adstat注入（需登录后台）,PhpcmsV9 后台oldfield注入（需登录后台）,PhpcmsV9 后台模板功能Getwebshell漏洞,PhpcmsV9 会员系统注入,PhpcmsV9 任意文件读取,PhpcmsV9前台Getwebshell漏洞,Rails框架远程代码执行,SAP NetWeaver系统命令执行,SQL错误信息注入,SQL错误信息注入（Base64）,SQL盲注,SQL盲注（Base64）,ShopEx ctl.tools.php SQL注入,Shopex 4.8.5产品筛选页面盲注漏洞,Shopex search_payment_cfg_list SQL注入,Shopex v4.8.5 SQL注入,Shopex v4.8.5 api.php SQL注入,SiteServer 3.6.3版 SQL注入,SiteServer 3.6.4版 SQL注入,SiteServer CMS cookie欺骗,SiteServer background_log.aspx页面SQL注入,Spring远程代码执行,Struts showConfig跨站脚本,Struts2 URL跳转S2-017,Struts2远程命令执行,Struts2远程命令执行S2-013,Struts2远程命令执行S2-015,Struts2远程命令执行S2-016,Struts错误页面跨站脚本,TRS内容协作平台用户名密码泄露,ThinkPHP框架任意代码执行,Thinksns Getwebshell漏洞,Thinksns本地包含Getwebshell漏洞,Thinksns远程代码执行,Tipask问答系统2.0 ajaxsearch参数SQL注入,Tomcat hello.jsp跨站脚本,Tomcat管理后台弱密码,UNIS-CMS紫光内容管理系统任意文件上传,URL重定向,UTF-7 BOM 字符注入跨站脚本,Ueditor JSP版任意文件上传,Vital Information CMS任意文件下载,Web Service SAX注入,Web Service SQL错误信息注入,Web Service SQL盲注,WebDAV 远程代码执行,WebDAV目录可写（PUT方法）,Weblogic管理后台弱密码

,WordPress Forum插件任意文件泄露,WordPress Woopra插件代码执行,WordPress locator plus插件SQL注入,WordPress reject插件远程文件包含,WordPress缓存插件远程代码执行,XPath注入,ZOPE远程命令执行,Zabbix httpmon.php文件SQL注入,Zimbra本地文件包含,eWebEditor 2.1.6 asp版本注入上传,eWebEditor 默认后台密码,eWebEditor 默认数据库下载,el表达式注入漏洞,jQuery跨站脚本,mhtml协议跨站脚本,phpMyAdmin filename_template远程代码执行,phpMyAdmin visualization跨站脚本漏洞,phpMyAdmin多个主题和库跨站脚本漏洞,umail邮件系统Fileshare.php文件SQL注入,暗链,北方网内容管理系统后台SQL注入（需登录）,北京联银通OA系统平台任意文件上传,北京联银通OA系统平台任意文件下载,本地文件包含,表单绕过,操作系统命令注入,常见数据库文件下载,大汉JCMS jtree.jsp SQL注入,大汉JCMS opr_ajaxusername.jsp SQL注入,大汉JCMS que_chooseusers.jsp SQL盲注,大汉JCMS que_dictionary.jsp SQL盲注,大汉JCMS que_model.jsp SQL盲注,大汉JCMS任意SQL查询,大汉JCMS任意文件读取,大汉JCMS任意文件下载,大汉JCMS数据导入功能Getwebshell,大汉JCMS数据库配置文件读取,大汉JCMS整站数据库重置,大汉JIEP任意文件下载,大汉JIS任意文件上传,大汉JIS任意文件下载,代码注入,帝友P2P借贷系统任意文件读取,动力系统数据库泄露,发现Apache Tomcat examples目录,方维购物分享系统备份文件泄露,方维购物分享系统任意代码执行（需注册登录）,方欣门户管理系统任意文件读取,方欣门户管理系统任意文件上传二,方欣门户管理系统任意文件上传一,访问控制文件内容泄露,国徽CMS管理员用户名密码泄露,国内外多家VPN厂商任意URL跳转,国内外多家VPN厂商任意文件读取,国内外多家VPN厂商任意文件上传二,国内外多家VPN厂商任意文件上传一,国内外多家VPN厂商远程代码执行,灰盒测试跨站脚本,江苏远大放射源安全监控系统权限控制不严,江苏远大环境自动监控系统权限控制不严,江苏远大环境综合业务系统任意文件上传,脚本木马,金百瑞内容管理系统越权遍历目录,金百瑞内容管理系统越权添加管理员,开普互联任意文件上传,开普互联任意文件下载,科创内容管理系统任意文件上传二,科创内容管理系统任意文件上传一,科创内容管理系统任意文件下载,科蓝CSII金融门户内容管理系统j2ee分层架构缺陷,科讯CMS 6.x-7.06 SQL注入,科讯CMS 6.x-8.x Getwebshell漏洞,跨站脚本,跨站脚本（Base64）,宽字符集跨站脚本,框架注入,框架注入（Base64）,力龙内容管理平台任意文件上传,链接注入,良精企业建站系统SQL注入,目录遍历,南方数据用户名密码泄露,骑士cms后台本地包含Getwebshell漏洞,任意文件下载,深喉咙企业建站系统keyword参数SQL注入,太极内容管理系统本地文件包含,通达OA Getwebshell漏洞,通达OA view.php SQL注入（需登录）,通达OA日志功能跨站脚本（需登录）,通元内容管理系统fckeditor目录遍历,通元内容管理系统任意文件下载,网页木马,维维招生网系统任意文件上传,武汉群翔分销系统SQL注入,易思企业网站管理系统SQL注入,易思企业网站管理系统cookie注入,易思企业网站管理系统membermain.php文件SQL注入,易思企业网站管理系统search.php文件SQL注入,易思企业网站管理系统wap模块SQL注入,易思企业网站管理系统会员中心模块注入,易思企业网站管理系统文件包含,易通企业网站系统Getwebshell漏洞,易通企业网站系统后台Getwebshell漏洞,易通企业网站系统跨站脚本,易通企业网站系统任意文件上传,易通企业网站系统注册用户权限提升,易想购物ajax.php SQL注入,易想购物cart.php SQL注入,易想购物link.php SQL注入,易想购物sms.php SQL注入,亿邮邮件系统命令执行,远程文件包含,允许TRACE方法,浙江索思OA系统JSP后门,浙江索思OA系统任意文件上传,织梦ajax_membergroup.php SQL注入,织梦recommend.php SQL注入,织梦v57 download.php SQL注入,织梦安装文件Getwebshell漏洞,织梦安装文件锁定绕过漏洞,织梦后台上传webshell漏洞,织梦内容管理系统本地文件包含,织梦搜索模块SQL注入,逐浪CMS addmis.aspx SQL盲注,逐浪CMS default.aspx SQL注入,孚力采编发系统任意文件上传,

1.3 ． 网站统计列表

本报告包含1个web站点，通过对其进行web安全检测，共发现弱点总数6个，其中紧急漏洞2个，具体列表如下：

网站名称	服务器类型	安全值	漏洞个数	紧急漏洞个数
172.16.80.11	Apache/2.2.15;CentOS;PHP/5.3.3	49	6	2

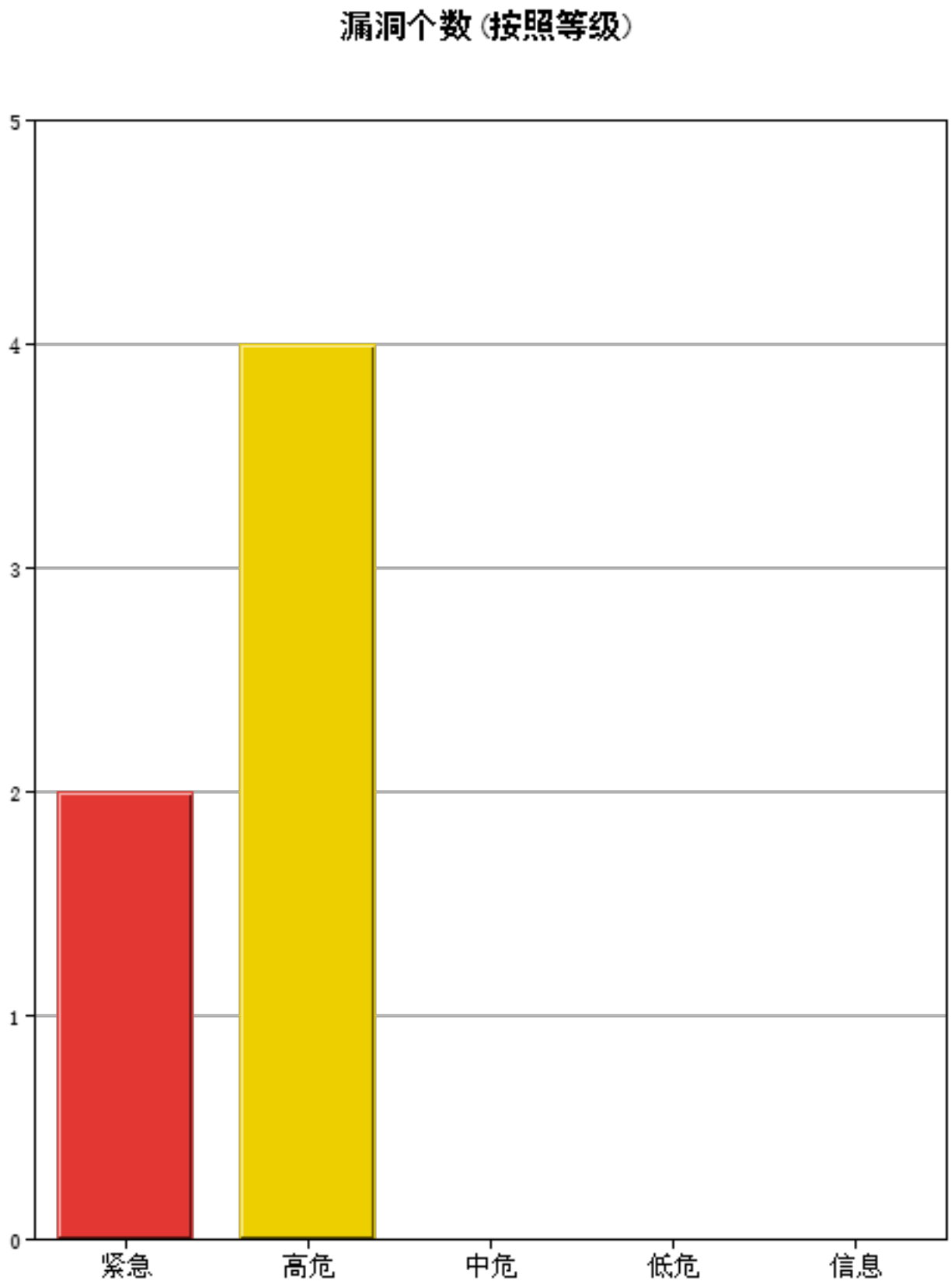
2 . 网站漏洞详细报告

2.1 . 172.16.80.11:80详细报告

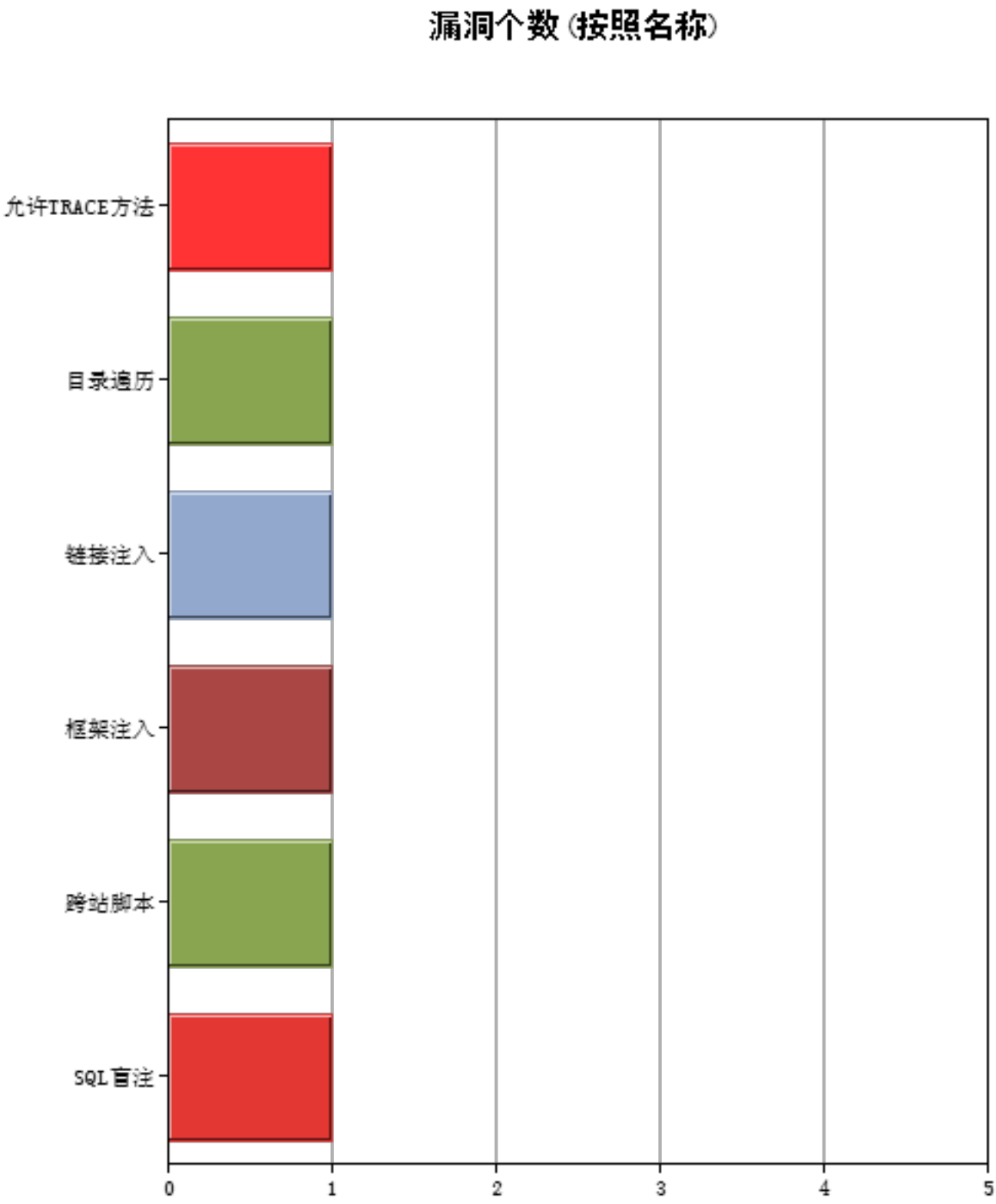
2.1.1 . 扫描信息列表

名称	内容
项目名称	scan_project_47
扫描对象	172.16.80.11
主机端口	80
开始时间	2014-12-19 15:30:16
结束时间	2014-12-19 15:31:49
扫描用时(单位：秒)	93
服务器信息	Apache/2.2.15;CentOS;PHP/5.3.3
服务器时间	2014-12-19 23:28:26
协　议	http
域　名	172.16.80.11
已访问URL	14
URL总数	14
网站安全值	49
漏洞个数	6

2.1.2 . 按照等级统计



2.1.3 . 按照名称统计


漏洞个数(按照名称)
允许TRACE方法
目录遍历
链接注入
框架注入
跨站脚本
SQL盲注
0
1
2
3
4
5

2.1.4 . 漏洞详细信息列表

2.1.4.1 . 紧急漏洞

2.1.4.1.1 . SQL盲注

URL	http://172.16.80.11/index.php?act=news%26id=1
弱点	参数: id=1, 注入类型: 数字型,数据库类型: MySQL,数据库名: ctf,用户名: ctfweb@localhost
等级	紧急

2.1.4.1.1.1 . 漏洞描述：

<bold>可能原因：</bold>

无论是内网环境还是外网环境（互联网），B/S架构的Web应用（以下指网站）都直接或者间接地受到以SQL注入攻击对危害，由于网站服务端语言自身的缺陷与程序员编写代码的安全意识不足，攻击者可以将恶意SQL语句注入到正常的数据库操作指令中去，从而使该恶意SQL语句在后台数据库中被解析执行。在SQL注入攻击之前，首先要找到网站中各类与数据库形成交互的输入点。通常情况下，一个网站的输入点包括：
1、表单提交，主要是POST请求，也包括GET请求。
2、URL参数提交，主要为GET请求参数。
3、Cookie参数提交。
4、HTTP请求头部的一些可修改的值，比如Referer、User_Agent等。
5、一些边缘的输入点，比如.mp3文件的一些文件信息等。
服务端从客户端直接或间接获取数据的过程都是一次输入过程， 无论直接或间接，默认情况下输入的数据都应该认为是不安全的。
上面列举的几类输入点，只要任何一点存在过滤不严，过滤缺陷等问题， 都有可能发生SQL注入攻击。

<bold>技术描述：</bold>

SQL盲注技术就是一些攻击者使用的新技术，其在错误信息被屏蔽的情况下使攻击者仍能获得所需的信息，并继续实施注入攻击。盲注攻击的条件是我们在攻击前对网络应用程序、数据库类型、表结构等等信息都一无所知，这些信息都需要在注入的过程中通过探测获得。

2.1.4.1.1.2 . 修复和改进建议：

<bold>一般性的建议：</bold>

解决SQL注入问题的关键是对所有可能来自用户输入的数据进行严格的检查、对数据库配置使用最小权限原则。

1　　所有的查询语句都使用数据库提供的参数化查询接口，参数化的语句使用参数而不是将用户输入变量嵌入到SQL语句中。当前几乎所有的数据库系统都提供了参数化SQL语句执行接口，使用此接口可以

非常有效的防止SQL注入攻击。
2　　对进入数据库的特殊字符（'"\尖括号&*;等）进行转义处理，或编码转换。
3　　严格限制变量类型，比如整型变量就采用intval()函数过滤，数据库中的存储字段必须对应为int型。
4　　数据长度应该严格规定，能在一定程度上防止比较长的SQL注入语句无法正确执行。
5　　网站每个数据层的编码统一，建议全部使用UTF-8编码，上下层编码不一致有可能导致一些过滤模型被绕过。
6　　严格限制网站用户的数据库的操作权限，给此用户提供仅仅能够满足其工作的权限，从而最大限度的减少注入攻击对数据库的危害。
7　　避免网站显示SQL错误信息，比如类型错误、字段不匹配等，防止攻击者利用这些错误信息进行一些判断。
8　　确认PHP配置文件中的magicquotesgpc选项保持开启。
9　　在部署你的应用前，始终要做安全审评(security review)。建立一个正式的安全过程(formal security process)，在每次你做更新时，对所有的编码做审评。后面一点特别重要。不论是发布部署应用还是更新应用，请始终坚持做安全审评。
10　千万别把敏感性数据在数据库里以明文存放。
11　使用第三方WEB防火墙来加固整个网站系统。

应用程序级别的漏洞，仅仅依靠对服务器的基本设置做一些改动是不能够解决的，必须从提高应用程序的开发人员的安全意识入手，加强对代码安全性的控制，在服务端正式处理之前对每个被提交的参数进行合法性检查，以从根本上解决注入问题。

2.1.4.1.2 ． 跨站脚本

URL	http://172.16.80.11/index.php?act=ver%26msg=1.0
弱点	parameter: msg=1.0, xss: -->'"></iframe></script></style></title></textarea><script >prompt(/Webscan6/)</script>
等级	紧急

2.1.4.1.2.1 ． 漏洞描述：

<bold>可能原因：</bold>

未对用户输入字符正确执行危险字符清理。

<bold>技术描述：</bold>

跨站点脚本（XSS）是针对其他用户的重量级攻击。从某种程度上说，XSS是在Web应用程序中发现的最为普遍的漏洞，困扰着现在绝大多数的应用程序，包括因特网上一些最为注重安全的应用程序，如电子银行使用的应用程序。

如果一个应用程序使用动态页面向用户显示错误消息，就会造成一种常见的XSS漏洞。通常，该页面会使用一个包含消息文本的参数，并在响应中将这个文本返回给用户。对于开发者而言，使用这种机制非常方便，因为它允许他们从应用程序中调用一个定制的错误页面，而不需要对错误页面中的消息分别进行硬编码。

下面的URL将返回错误消息：
https://www.test-dbappsecurity.com/error.php?message=Sorry%2c+an+error+occurred
分析被返回页面的HTML源代码后，我们发现，应用程序只是简单复制URL中message参数的值，并将这个值插入到位于适当位置的错误页面模板中：

```
<p>Sorry, an error occurred.</p>
```

提取用户提交的输入并将其插入到服务器响应的HTML代码中，这是XSS漏洞的一个明显特征；如果应用程序没有实施任何过滤或净化措施，那么它很容易受到攻击。让我们来看看如何实施攻击。
下面的URL经过专门设计，它用一段生成弹出对话框的JavaScript代码代替错误消息：

```
https://wahh-app.com/error.php?message=<script>alert('xss');</script>
```

请求这个URL将会生成一个HTML页面，其中包含以下替代原始消息的脚本：

```
<p><script>alert('xss');</script></p>
```

可以肯定，如果该页面在用户的浏览器中显示，弹出消息就会出现。
进行这个简单的测试有助于澄清两个重要问题：首先，message参数的内容可用任何返回给浏览器的数据替代；其次，无论服务器端应用程序如何处理这些数据（如果有），都无法阻止提交JavaScript代码，一旦错误页面在浏览器中显示，这些代码就会执行。

在现实世界的Web应用程序中存在的XSS漏洞，有近75%的漏洞属于这种简单的XSS bug。在反射型XSS脚本攻击中，要利用一个漏洞，攻击者必须以某种方式诱使受害者访问他专门设计的URL。而保存型XSS脚本攻击则没有这种要求。在应用程序中展开攻击后，攻击者只需要等待受害者浏览已被攻破的页面或功能。通常，这个页面是一个正常用户将会主动访问的常规页面。

其次，如果受害者在遭受攻击时正在使用应用程序，攻击者就更容易实现其利用XSS漏洞的目的。例如，如果用户当前正在进行会话，那么攻击者就可以劫持这个会话。在反射型XSS攻击中，攻击者可能会说服用户登录，然后单击他们提供的一个链接，从而制造这种情况。或者他可能会部署一个永久性的有效载荷并等待用户登录。

主要危害包括：
[1]获取其他用户Cookie中的敏感数据。
[2]屏蔽页面特定信息。
[3]伪造页面信息。
[4]拒绝服务攻击。
[5]突破外网内网不同安全设置。
[6]与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。

2.1.4.1.2.2 ． 修复和改进建议：

<bold>一般性的建议：</bold>

过滤客户端提交的危险字符，客户端提交方式包含GET、POST、COOKIE、User-Agent、Referer、Accept-Language等，其中危险字符如下：

[1] |
[2] &
[3] ;

[4] $
[5] %
[6] @
[7] ’
[8] ″
[9] <>
[10] ()
[11] +
[12] CR
[13] LF
[14] ,
[15] .
[16] script
[17] document
[18] eval

开发语言的建议:

[1]严格控制输入:
Asp:
request
Php:
$_GET、$_POST、$_COOKIE、$_SERVER
Jsp:
request.getParameter、request.getCookies
Asp.net:
Request.QueryString、Form、Cookies、SeverVaiables
客户端提交的变量一般从以上函数获得，严格限制提交的数据长度、类型、字符集。

[2]严格控制输出:
HtmlEncode：对一段指定的字符串应用HTML编码。
UrlEncode：对一段指定的字符串URL编码。
XmlEncode：将在XML中使用的输入字符串编码。
XmlAttributeEncode：将在XML属性中使用的输入字符串编码
escape：函数可对字符串进行编码
decodeURIComponent：返回统一资源标识符的一个已编码组件的非编码形式。
encodeURI：将文本字符串编码为一个有效的统一资源标识符 (URI)。

2.1.4.2 . 高危漏洞

2.1.4.2.1 . 目录遍历

URL	http://172.16.80.11/index.php?act=about%26file=test.txt
弱点	http://172.16.80.11/index.php?act=about&file=/etc/hosts

等级	高危

2.1.4.2.1.1 . 漏洞描述：

<bold>可能原因：</bold>

如果应用程序使用用户可控制的数据、以危险的方式访问位于应用程序服务器或其他后端文件系统中的文件和目录，就会出现路径遍历漏洞。

<bold>技术描述：</bold>
许多功能强迫web应用程序根据用户在请求中提交的参数向文件系统读取或写入数据。如果以不安全的方式执行这些操作，攻击者就可以提交专门设计的输入，使得应用程序访问开发者并不希望它访问的文件。这就是“路径遍历”漏洞，攻击者可以利用这种缺陷读取密码和应用程序日志之类的敏感数据，或者覆写安全性至关重要的数据项，如配置文件和软件代码。在最为严重的情况下，这种漏洞可以使攻击者能够完全攻破应用程序与支撑服务系统。
程序中如果不能正确地过滤客户端提交的../和./之类的目录跳转符,恶意者就可以通过上述符号跳转来访问服务器上的特定的目录或文件。下边PHP代码为例，做简要的分析。

```
/* 实例代码 */
$str = $_GET['name'];
readfile($str);
```

上述代码中变量$str,接受GET方式传递的数据，并未对危险字符做过滤，假如客户端提交“c:/windows/win.ini”或者“/etc/hosts”,那么将在浏览器显示上述文件的内容。

主要危害包括：
[1]读取网站文件、系统文件。
[2]获得敏感信息，例如用户名、密码。
[3]与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等。

2.1.4.2.1.2 . 修复和改进建议：

<bold>一般性的建议：</bold>

在防范遍历路径漏洞的方法中，最有效的是权限的控制，谨慎的处理向文件系统API传递过来的参数路径。主要是因为大多数的目录或者文件权限均没有得到合理的配置，而Web应用程序对文件的读取大多依赖于系统本身的API，在参数传递的过程，如果没有得严谨的控制，则会出现越权现象的出现。在这种情况下，Web应用程序可以采取以下防御方法，最好是组合使用。
(1) 数据净化，对网站用户提交过来的文件名进行硬编码或者统一编码，对文件后缀进行白名单控制，对包含了恶意的符号或者空字节进行拒绝。
(2) Web应用程序可以使用chrooted环境访问包含被访问文件的目录，或者使用绝对路径+参数来控制访问目录，使其即使是越权或者跨越目录也是在指定的目录下。

建议使用WAF防护：应用程序应将其路径遍历共计防御机制与日志和警报机制整合在一起。任何时候，只要收到一个包含路径遍历序列的请求，提出请求的用户就可能心存恶意，应用程序应在日志中进行

纪录，标明该请求企图违反安全机制，并终止该用户的会话；如果有可能，应该冻结该用户帐户并向管理员发出警报。

2.1.4.2.2 ． 框架注入

URL	http://172.16.80.11/index.php?act=ver%26msg=1.0
弱点	parameter: msg=1.0, frame_inj: #*/-- >'");></iframe></script></style></title></textarea><iframe src=http://www.dbappsecurity.com.cn>
等级	高危

2.1.4.2.2.1 ． 漏洞描述：

<bold>可能原因：</bold>

未对用户输入字符正确执行危险字符清理。

<bold>技术描述：</bold>

如果应用程序易于受到框架注入，那么攻击者就可以使用以下步骤利用这种漏洞。
(1)攻击者创建一个看似无害的Web站点，其中包含一段每隔10s就会自动运行的脚本，并尝试使用它覆写main_display框架的内容。新内容保存在攻击者的站点中，其中包含木马功能，它的外观与test.com框架的常规内容完全相同，但可将用户输入的所有数据提交给攻击者。

(2)攻击者或者等待test.com用户浏览他创建的站点，或者使用其他方法诱使他们这样做，如发送电子邮件、购买横幅广告等。

(3)一名用户浏览攻击者创建的看似无害的Web站点。如果用户同时还在使用test.com，或者在另一个浏览器窗口显示攻击者的站点的同时访问test.com，那么攻击者的木马内容就会覆写test.com窗口中的main_display框架。如果用户继续使用貌似为test.com的应用程序，那么他输入的任何数据都将被提交给攻击者。

这种类型的攻击与钓鱼攻击有一定的相似性，因为攻击者必须创建一个克隆的Web站点并诱惑不知情的用户访问它，才能实施有效的攻击。然而，在框架注入中，攻击过程更复杂，也更可信，因为克隆的内容实际上只是替代一个浏览器窗口中的真实内容，但后者的URL仍然指向原来的应用程序。

如果目标应用程序使用HTTPS，攻击依然能够成功，同时浏览器窗口中显示的安全信息还将继续揭示test.com的正确证书。这是因为当浏览器显示一个框架标记时，主窗口的安全信息即与包含框架标记的页面关联起来，这时框架标记仍然源自test.com。因此，即使精明的用户也无法察觉这种攻击。下边PHP代码为例，做简要的分析。

```
/* 实例代码 */
$str = $_GET['name'];
echo $str;
```

上述代码中变量$str,接受GET方式传递的数据，并未对危险字符做过滤，假如客户端提交“<iframe src=http://www.dbappsecurity.com.cn>”,那么将在浏览器内引用“http://www.dbappsecurity.com.cn”。

主要危害包括：
[1]获取其他用户Cookie中的敏感数据。
[2]屏蔽页面特定信息。
[3]伪造页面信息。
[4]拒绝服务攻击。
[5]突破外网内网不同安全设置。

2.1.4.2.2.2 . 修复和改进建议：

<bold>一般性的建议：</bold>

过滤客户端提交的危险字符，客户端提交方式包含GET、POST、COOKIE、User-Agent、Referer、Accept-Language等，其中危险字符如下：

[1] |
[2] &
[3] ;
[4] $
[5] %
[6] @
[7] ’
[8] ″
[9] <>
[10] ()
[11] +
[12] CR
[13] LF
[14] ,
[15] .
[16] script
[17] document
[18] eval

开发语言的建议:

[1]严格控制输入：
Asp:
request

Php:
$_GET、$_POST、$_COOKIE、$_SERVER
Jsp:
request.getParameter、request.getCookies
Asp.net:
Request.QueryString、Form、Cookies、SeverVaiables
客户端提交的变量一般从以上函数获得，严格限制提交的数据长度、类型、字符集。

[2]严格控制输出：
HtmlEncode：对一段指定的字符串应用HTML编码。
UrlEncode：对一段指定的字符串URL编码。
XmlEncode：将在XML中使用的输入字符串编码。
XmlAttributeEncode：将在XML属性中使用的输入字符串编码
escape：函数可对字符串进行编码
decodeURIComponent：返回统一资源标识符的一个已编码组件的非编码形式。
encodeURI：将文本字符串编码为一个有效的统一资源标识符 (URI)。

以下两种方法可用于防止框架注入漏洞。

如果应用程序不要求不同的框架互相通信，就可以通过完全删除框架名称、使用匿名框架防止框架注入。但是，因为应用程序通常都要求框架之间相互通信，因此这种方法并不可行。

使用命名框架，但在每个会话中使用不同的框架，并且使用无法预测的名称。一种可行的方法是在每个基本的框架名称后附加用户的会话令牌，如main_display。

2.1.4.2.3 . 链接注入

URL	http://172.16.80.11/index.php?act=ver%26msg=1.0
弱点	parameter: msg=1.0, link_inj: */-->'");></iframe></script></style></title></textarea>Link_Injecting
等级	高危

2.1.4.2.3.1 . 漏洞描述：

<bold>技术描述：</bold>

链接注入是将某个URL嵌入到被攻击的网站上，进而修改站点页面。被嵌入的URL包含恶意代码，可能窃取正常用户的用户名、密码，也可能窃取或操纵认证会话，以合法用户的身份执行相关操作。下边PHP代码为例，做简要的分析。

```
/* 实例代码 */
$str = $_GET['name'];
echo $str;
```

上述代码中变量$str,接受GET方式传递的数据，并未对危险字符做过滤，假如客户端提交“<a

href='1.htm'>Link_Injecting”,那么将在浏览器内引用“1.htm”。

主要危害包括：
[1]获取其他用户Cookie中的敏感数据。
[2]屏蔽页面特定信息。
[3]伪造页面信息。
[4]拒绝服务攻击。
[5]突破外网内网不同安全设置。

2.1.4.2.3.2 ． 修复和改进建议：

<bold>一般性的建议：</bold>

过滤客户端提交的危险字符，客户端提交方式包含GET、POST、COOKIE、User-Agent、Referer、Accept-Language等，其中危险字符如下：

[1] |
[2] &
[3] ;
[4] $
[5] %
[6] @
[7] ’
[8] ″
[9] <>
[10] ()
[11] +
[12] CR
[13] LF
[14] ,
[15] .
[16] script
[17] document
[18] eval

开发语言的建议:

[1]严格控制输入：
Asp:
request
Php:
$_GET、$_POST、$_COOKIE、$_SERVER
Jsp:
request.getParameter、request.getCookies

Asp.net:
Request.QueryString、Form、Cookies、SeverVaiables
客户端提交的变量一般从以上函数获得，严格限制提交的数据长度、类型、字符集。

[2]严格控制输出：
HtmlEncode：对一段指定的字符串应用HTML编码。
UrlEncode：对一段指定的字符串URL编码。
XmlEncode：将在XML中使用的输入字符串编码。
XmlAttributeEncode：将在XML属性中使用的输入字符串编码
escape：函数可对字符串进行编码
decodeURIComponent：返回统一资源标识符的一个已编码组件的非编码形式。
encodeURI：将文本字符串编码为一个有效的统一资源标识符 (URI)。

2.1.4.2.4 ． 允许TRACE方法

URL	http://172.16.80.11/
弱点	http://172.16.80.11/
等级	高危

2.1.4.2.4.1 ． 漏洞描述：

<bold>技术描述：</bold>

TRACE是一种HTTP方法，允许TRACE方法的web服务器存在跨站脚本漏洞。

实施攻击要素：
[1]需要目标web服务器允许TRACE参数；
[2]需要一个用来插入XST代码的地方；
[3]目标站点存在跨域漏洞。

2.1.4.2.4.2 ． 修复和改进建议：

<bold>一般性的建议：</bold>

[1]禁用TRACE方法，IIS可使用URLScan禁用，而Apache则可使用mod_rewrite模块禁用。

3 ． 参考标准

3.1 . 漏洞危害分级标准

目前定义有五类危害等级，危害等级定义依据为：

3.1.1 . 紧急

可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。

3.1.2 . 高危

被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成极大便利的漏洞。

3.1.3 . 中危

利用难度极高，或满足严格条件才能实现攻击的漏洞。或漏洞本身无法被直接攻击，但能为进一步攻击起较大帮助作用的漏洞。

3.1.4 . 低危

无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。

3.1.5 . 信息

本身对网站安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击，如社工等。

4 . 附录1：关于安恒信息

公司简介：
杭州安恒信息技术有限公司(DBAPPSecurity)，简称“安恒信息”，是业界领先的应用安全及数据库安全整体解决方案提供商，专注于应用安全前沿趋势的研究和分析，核心团队拥有多年应用安全和数据库安全的深厚技术背景以

及最佳安全攻防实践经验，以全球领先具有完全自主知识产权的专利技术，致力于为客户提供应用安全、数据库安全、网站安全监测、安全管理平台等整体解决方案。
“安恒信息“公司总部位于杭州高新区，在北京、上海、广州、深圳、成都、重庆、西安、济南、南京、美国硅谷等地都设有分支机构、遍布全国的代理商体系以及销售与服务网络能够为用户提供精准、专业的服务。公司成立以来安恒人始终以建立民族自主品牌为己任，秉承“精品创新，恒久品质”的理念，力争打造中国信息安全产业应用安全与数据库安全第一品牌。
多年来，“安恒信息”以其精湛的技术，专业的服务得到了广大客户的青睐，同时赢得了高度的商业信誉。其客户遍布全国，涉及金融、运营商、政府、公安、电力能源、教育、医疗、税务/工商、社保、等保评估/安全服务机构、电子商务企业等众多行业。
“安恒信息“目前拥有明鉴、明御两大系列自主研发产品，是应用安全、数据库审计、网站安全监测等领域的市场绝对领导者。其中明鉴?系列应用扫描器被公安部三所测评中心等国内权威等级保护测评机构广泛使用。
未来，“安恒信息“将继续秉承诚信和创新精神，继续致力于提供具有国际竞争力的自主创新产品和服务，全面保障客户应用与数据库的安全，为打造世界顶级的产品而不懈努力。 作为2008北京奥组委安全产品和服务提供商，“安恒信息”被奥组委授予“奥运信息安全保障杰出贡献奖”。
在2009年建国60周年全国网站安全大检查中，公安部和工信部安全中心均选用安恒信息明鉴应用弱点扫描作为安全检查工具并发挥了重大作用。
2010年，“安恒信息”作为上海世博会安全产品和服务的提供商，为上海世博会信息安全保驾护航。
2010年，“安恒信息”作为广州亚运会安全产品和服务的提供商，为广州亚运会信息安全保驾护航。
2011年，“安恒信息”作为深圳大运会安全产品和服务的提供商，为深圳大运会信息安全保驾护航。
全球领先的专利技术
安恒目前拥有国际领先的完全自主知识产权的信息安全领域专利技术：
国际专利：
WEB应用安全深度扫描（专利号：US60/835471）
WEB和数据库入侵异常检测（专利号：US60/835472）

国内专利：
SQL注入WEB攻击的实时入侵检测系统（专利号：ZL200810002168.0）
一种丢包环境下提升TDS协议解析正确率的方法（专利号：ZL200910101388.3
一种在大数据量存储中快速检索的方法(201110116710.7)
数据库内核对象入侵检测方法及系统（201110401023.X）
一种交互式半自动化安全事故追溯方法与系统（201210013693.9）
一种通过提取SQL模板对海量SQL压缩存储的方法（201210011602.8）
一种应用层透明代理技术的通信实现方法（201210012058.9）
一种在应用安全系统中进行精确风险检测的方法与系统（201210011117.0）

公司历程
2013年04月 安恒信息荣获2012年度浙江最佳创新软件企业。
2013年03月 安恒信息荣获网络与信息安全技术支持合作工作2012年先进单位

。
2013年02月 安恒信息应邀参加RSA Conference 2013(美国)大会。
2013年01月 安恒信息与人人网联合主办2012（首届）互联网安全高峰论坛。
2012年11月 浙江省卫生信息中心与安恒信息签署《网络安全合作协议》。
2012年11月 安恒信息总裁范渊当选杭州市知识分子联谊会副会长。
2012年11月 安恒信息安全研究院协助腾讯发现及修复安全漏洞。
2012年11月 安恒信息助力杭州高新技术创新公共服务平台，杭州公共服务平台软件安全测试功能正式上线。
2012年08月 明御数据库审计与风险控制系统--医疗防统方专版发布上市。
2012年07月 安恒信息数据库审计与风险控制系统产业化项目荣获国家信息安全专项资金。
2012年05月 安恒信息与国内权威信息安全杂志《中国信息安全》共同在杭州举办2012（首届）中国WEB应用防护与数据安全高峰论坛。
2012年04月 杭州市政协十届一次会议举行全体会议，经过无记名投票，会议选举产生政协第十届杭州市委员会主席、副主席、秘书长和常务委员。总裁范渊当选为十届市政协常务委员。
2012年03月 杭州安恒信息技术有限公司总裁范渊先生入选中组部国家“千人计划”。
2012年03月 中国移动网页漏洞综合扫描系统集中采购结果已经公布，安恒信息明鉴WEB应用弱点扫描系统成功入选，覆盖了3个典型配置，成为了覆盖全部典型配置的唯一厂商，并且其中2个典型配置独家中标，是入围产品款型最多的厂商，充分体现了安恒信息在WEB应用安全领域的领航地位。
2012年02月 安恒信息发明专利 《一种丢包环境下提升TDS协议解析正确率的方法》 、《SQL注入WEB攻击的实时入侵检测系统》已相继获得了国家专利。

2011年11月 安恒信息建立博士后工作站，加大研发及科技创新能力。
2011年10月 安恒信息通过信息安全服务资质证书认证。
2011年10月安恒信息荣获“2011年中国医药卫生信息技术金鼎奖”和“2011年中国医药卫生信息化首选品牌”。
2011年07月 安恒51websec正式发布，为网络安全界引爆一颗重磅炸弹。
2011年06月 安恒信息当选“中国电子商会物联网技术产品应用专业委员会”会员单位。
2011年04月 安恒信息在第十二届信息安全大会上荣获“2011年度中国信息安全最具影响力企业奖”和“2011年度中国信息安全最佳应用安全解决方案”。
2010年10月 安恒信息荣获“浙江省最具投资价值中小企业”称号。
2010年09月 安恒信息协办第25次全国计算机安全学术交流会。
2010年07月 安恒信息CEO范渊被授予浙江省特聘专家称号。
2010年06月 安恒信息网站应用安全项目获得2010年度国家火炬计划立项。
2010年06月 安恒信息承担国家电子信息产业发展基金项目。
2010年05月 安恒信息成功入围中央政府采购协议供货商。
2010年05月 安恒信息荣获杭州市创新科技“十佳科技型初创企业”称号。
2010年04月 安恒信息在“通信网络与信息安全高层论坛”上获得2010“通信安全卫士奖”。
2010年02月 安恒信息的《通信行业应用与数据库安全解决方案》获得2009年中国通信市场优秀解决方案。

2009年12月 安恒信息通过信息安全应急处理服务二级资质认证。
2009年11月 安恒信息成为上海世博会安全产品和服务提供商。
2009年10月 安恒信息成为国家计算机网络应急技术处理协调中心支撑单位。

2009年09月 安恒信息的明鉴应用弱点扫描器在公安部和工信部60周年网站安全大检查中发挥了重大作用。
2009年09月 安恒信息承担国家发改委信息安全专项产业化项目。
2009年07月 安恒信息成功引进风险投资资金。
2009年02月 安恒信息发布国内首款全透明直连部署、全面支持https和WEB加速的WEB应用防火墙。
2008年12月 安恒信息同时被认定为浙江省高新技术企业及软件企业。
2008年09月 安恒信息荣获2008北京奥运会/残奥会信息网络安全保障杰出贡献奖。
2008年07月 安恒信息推出国内首个基于SAAS模式的 WEB应用安全服务平台。
2008年05月 安恒信息安全研究团队在应急响应中首次发现并处理了全球性的网站群注风暴攻击，并且在国内首家发布了红色预警。
2007年12月 安恒信息发布全球首款既有深度网站风险扫描能力，又具备全面网页木马检测与溯源功能的Web风险深度扫描系统2.0——MatriXay WebScan 2.0版本。
2007年11月 安恒信息的《运营商数据库防御与审计解决方案》获得2007年通信行业网络信息安全优秀解决方案奖。
2007年11月 安恒信息发布国内领先的数据库弱点扫描器、数据库审计与风险控制系统。
2007年10月 安恒信息发布国内首款WEB应用深度防御系统----WEB应用深度防御审计系统。
2006年 安恒信息(DBAPPSecurity)创始人范渊(Frank)在美国黑帽子大会发布全球首款具有网站深度风险扫描和审计渗透能力的Web应用风险扫描器。
2005年 安恒信息(DBAPPSecurity)创始人范渊(Frank)在美国拉斯维加斯世界黑客大会(Blackhat)上发表WEB安全异常入侵检测演讲，成为第一个登上黑帽子大会的中国人。