MatriXay Web应用安全评估报告

应用安全和数据库安全的领航者

[WebScan Version: V6.0.1.7, Engine Version: V6.1.76, Policy Version: V6.1.75]

1 . 综述

本报告共检查了1个网站， 共访问了798个URL，完成了377325次测试。
本次扫描,以下站点因无法访问没有进行测试:fipa.gov.cn:80。

1.1 . 测试策略集

制定系统默认策略

1.2 . 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。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	备注
fipa.gov.cn	Server:null System:null Tech:null	-	-	-	无法访问

注：网络因素问题，可能会影响被扫描网站扫描结果的准确性;

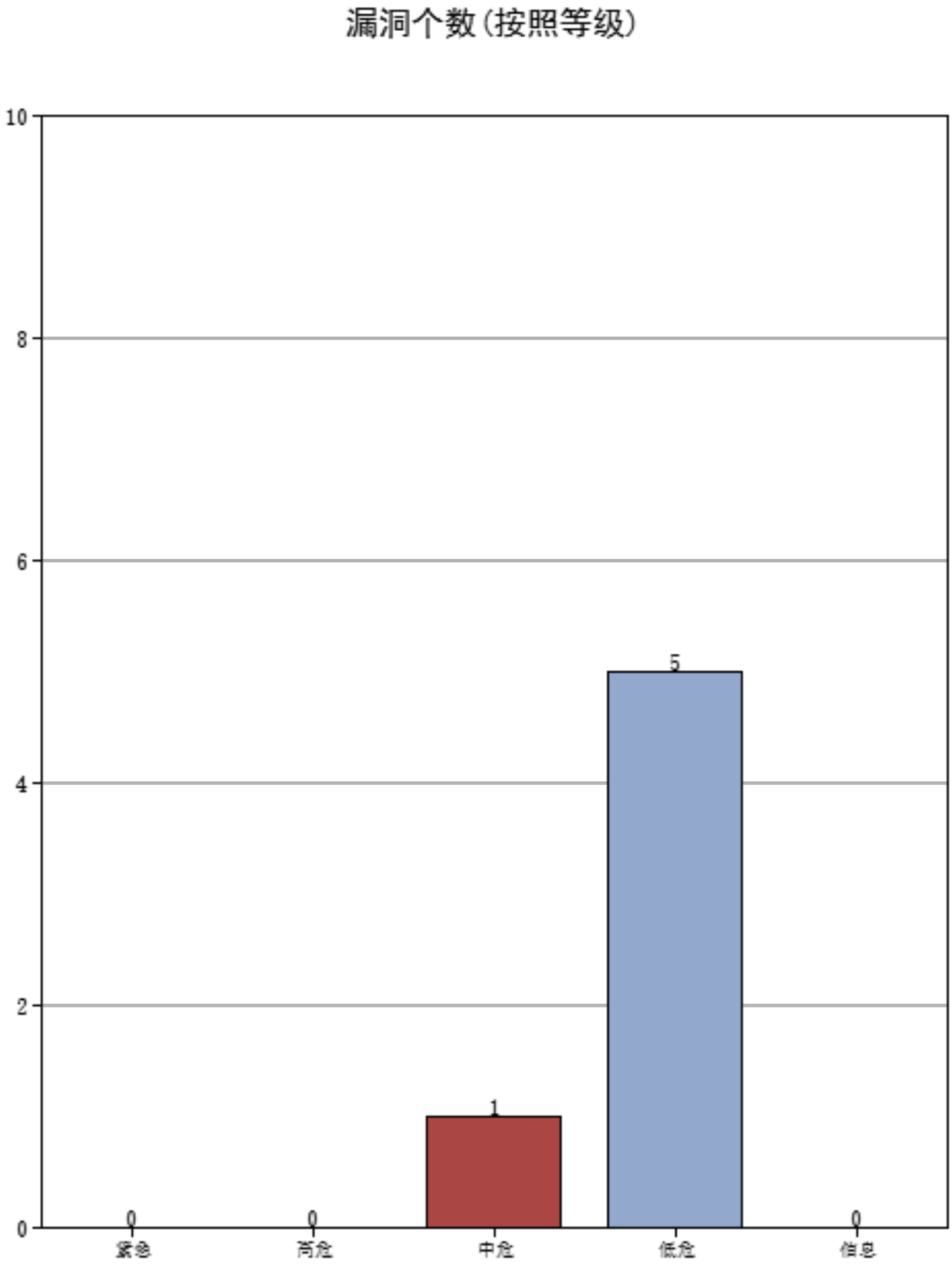
2 . 网站漏洞详细报告

2.1 . fipa.gov.cn:80详细报告

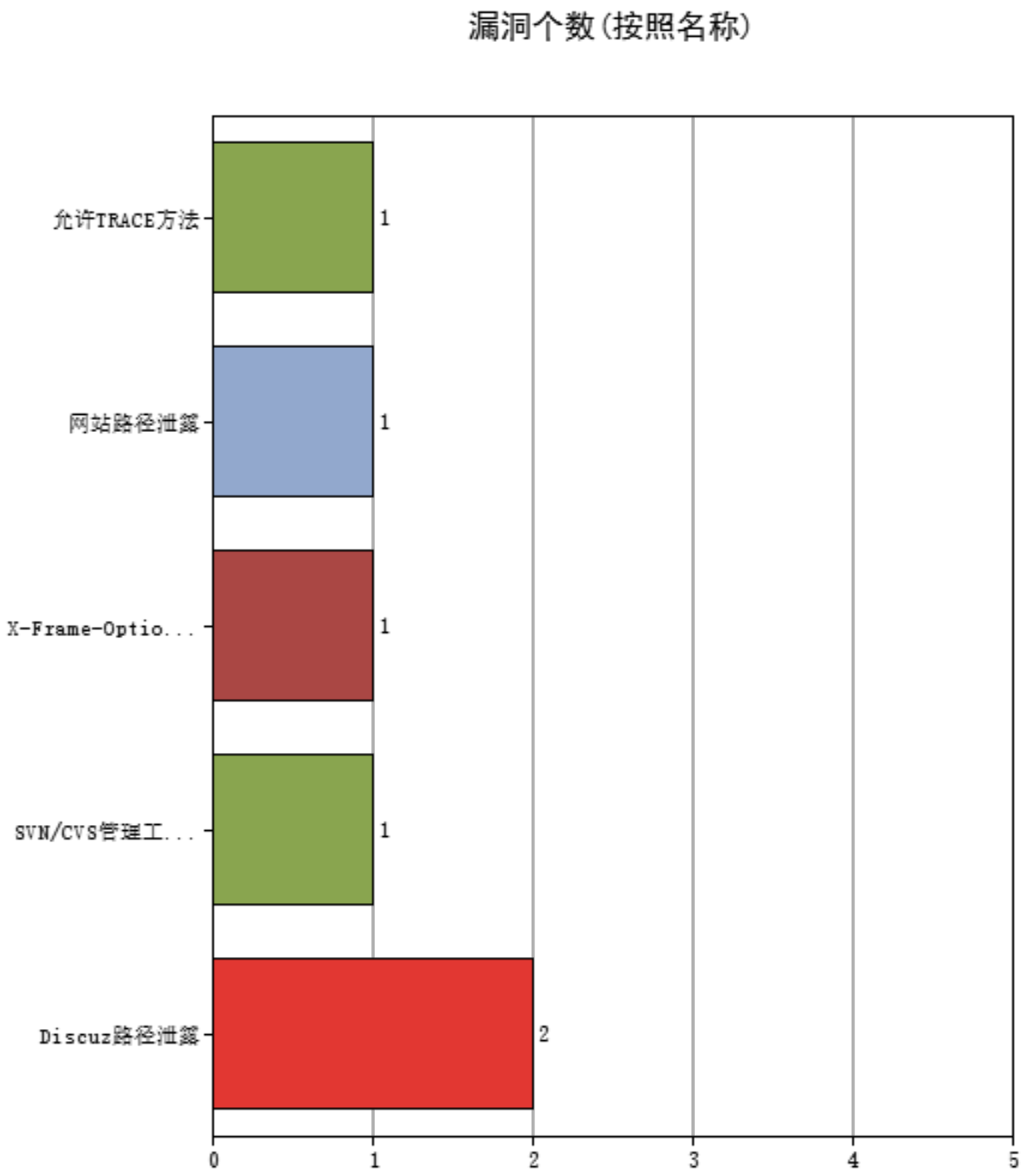
2.1.1 . 扫描信息列表

名称	内容
项目名称	scan_project_30(1)
扫描对象	fipa.gov.cn
主机端口	80
开始时间	2017-03-16 23:14:00
结束时间	2017-03-16 23:56:01
扫描用时(时:分:秒)	0:42:01
服务器信息	Server:nullSystem:nullTech:null
服务器时间	2017-03-17 11:48:30
协　　议	http
域　　名	fipa.gov.cn
已访问URL	798
URL总数	798
网站安全值	91
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
1
网站路径泄露
1
X-Frame-Optio...
1
SVN/CVS管理工...
1
Discuz路径泄露
2
0
1
2
3
4
5

2.1.4 . 漏洞详细信息列表

2.1.4.1 . 中危漏洞

2.1.4.1.1 . 允许TRACE方法

URL	http://fipa.gov.cn/
弱点	http://fipa.gov.cn/
等级	中危

2.1.4.2 . 低危漏洞

2.1.4.2.1 . Discuz路径泄露

URL	http://fipa.gov.cn/wp-json/
弱点	D:\xampp\htdocs\wp-includes\class-wp-tax-query.php
等级	低危

URL	http://fipa.gov.cn/wp-json/
弱点	D:\xampp\htdocs\wp-includes\category-template.php
等级	低危

2.1.4.2.2 . SVN/CVS管理工具文件信息泄露

URL	http://fipa.gov.cn/national-environmental-services-indutrial-cluster-region-in-south-china/np_application/portal/
弱点	http://fipa.gov.cn/national-environmental-services-indutrial-cluster-region-in-south-china/np_application/portal/CVS/Repository
等级	低危

2.1.4.2.3 . 网站路径泄露

URL	http://fipa.gov.cn/wp-content/plugins/revslider/rs-plugin/css/captions.php?rev=4.3.6&ver=4.4.2
弱点	D:\xampp\htdocs\wp-includes\theme.php
等级	低危

2.1.4.2.4 . X-Frame-Options Header未配置

URL	http://fipa.gov.cn/
弱点	http://fipa.gov.cn/
等级	低危

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。