ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1107—2013

信息安全技术
web 应用安全扫描产品安全技术要求

Information security technology—
Security technical requirements for web application security scanning products

2013-10-15 发布　　2013-10-15 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、杭州安恒信息技术有限公司、中联绿盟信息技术(北京)有限公司、北京国舜科技有限公司、上海天泰网络技术有限公司。

本标准主要起草人：俞优、张艳、沈亮、顾健、陆臻、杨元原、李毅、范渊、邹春明、张笑笑、顾建新、宋好好、孙小平、李晨、姜强、程胜年。

信息安全技术
web应用安全扫描产品安全技术要求

1 范围

本标准规定了web应用安全扫描产品的安全功能要求、性能要求、自身安全功能要求、安全保证要求及等级划分要求。

本标准适用于web应用安全扫描产品的设计、开发及检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 18336.3—2008和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

web应用安全扫描产品 web application security scanning product

一种扫描发现web系统应用层安全漏洞的产品，能够依据策略对web应用系统进行URL发现并扫描，对发现的安全漏洞提出相应的改进意见。

3.2

web应用 web application

由动态脚本、编译过的代码等组合而成的应用，通常架设在web服务器上，用户在web浏览器上发送请求，这些请求使用HTTP协议，经过网络和web应用交互，由web应用和后台的数据库及其他动态内容通信。

3.3

URL发现 URL detection

通过访问一个URL，发现通过该URL能够链接到的其他URL的过程，能够发现的URL包括在网页中出现的完整的URL、通过各种计算得出的URL、各种跳转的URL等。

3.4

web服务 web service

一个基于WSDL文件的应用程序，向外界提供一个能够通过web进行调用的API。WSDL是一个基于XML的语言，用于描述web service及其函数、参数和返回值。