ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37931—2019

信息安全技术　Web 应用安全检测系统安全技术要求和测试评价方法

Information security technology—Security technology requirements and testing and evaluation approaches for Web application security detection system

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第三研究所(公安部计算机信息系统安全产品质量监督检验中心)、国家信息技术安全研究中心、杭州安恒信息技术股份有限公司、网神信息技术(北京)股份有限公司、北京神州绿盟科技有限公司、上海天泰网络技术有限公司、北京天融信网络安全技术有限公司、浙江省电子信息产品检验所、上海嘉韦思信息技术有限公司、国家电网公司。

本标准主要起草人:俞优、贾徽徽、杨元原、陆臻、邹春明、顾健、万仁忠、李冰、方进社、纪崇廉、李蒙、刘楠、张君、沈亮、范渊、吴云坤、叶晓虎、程胜年、雷晓锋、孙小平、王志佳、金海俊、王伟、向智、赵建飞、邓琦、曲晓东、唐迪、孟亚豪、马海燕、杨灼其、蔡立军、李静、舒首衡、吴舜、刘永清、连纪文。

信息安全技术　Web应用安全检测系统安全技术要求和测试评价方法

1　范围

本标准规定了Web应用安全检测系统的安全技术要求、测评方法及等级划分。

本标准适用于Web应用安全检测系统的设计、开发与测评。

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/T 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.3—2015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应用安全检测系统　Web application security detection system

对Web应用的安全性进行检测的产品，能够依据策略对Web应用进行URL发现，并对Web应用漏洞进行检测。

3.2

URL发现　URL discovery

从一个URL开始，发现通过该URL能够链接到的其他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。

3.3

变形检测　deformation detection

一种通过编码、请求包变化等方法，实现绕过防护过滤的检测机制。

4　缩略语

下列缩略语适用于本文件。

CSRF：跨站请求伪造(Cross Site Request Forgery)

HTTP：超文本传输协议(HyperText Transfer Protocol)

HTTPS：安全套接字层的超文本传输协议(HyperText Transfer Protocol over Secure Socket Layer)

LDAP：轻量目录访问协议(Lightweight Directory Access Protocol)

OWASP：开放式网页应用程序安全项目(Open Web Application Security Project)