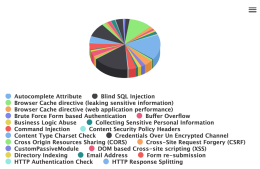
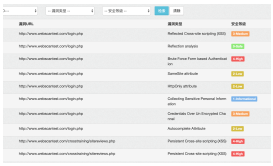


HTML报告

分享方便

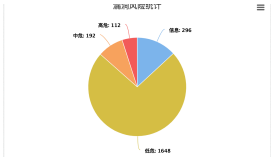
验证快捷



漏洞分级分类

归类清晰

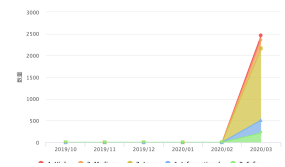
中英文描述



统一管理界面

多引擎统一管理界面

扫描任务自动执行



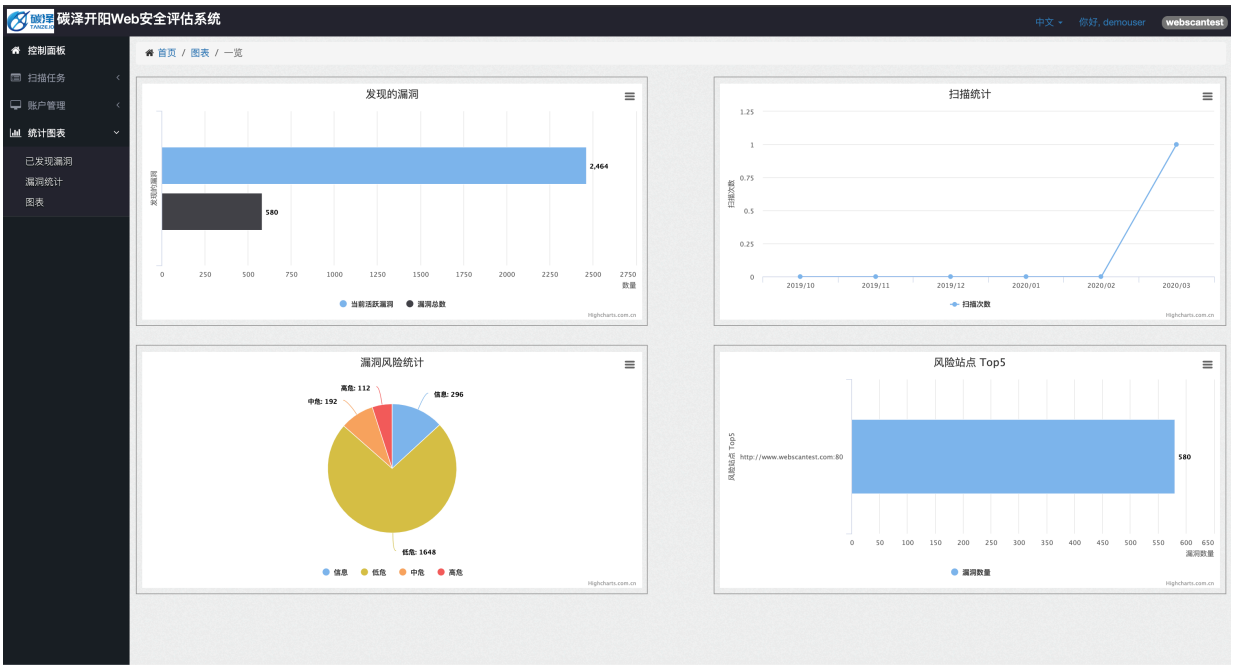
扫描结果比对

多次扫描任务结果比对

漏洞扫描任务统一呈现

碳泽应用安全评估系统

随着近几年互联网业务的极大发展，大量的Web应用和App加入到企业的网络中，从而面临更多的来自互联网的黑客攻击尝试和Web渗透。近几年，比较著名的数据泄露事件，例如某电商网站用户信息泄露及部分金融行业站点的用户信息泄露事件，主要都是由于Web安全漏洞导致的问题，应用安全也一直是SDLC建设的重点。



随着信息安全防御手段的发展，安全行业内面临两个很大的挑战，一个是越来越多的黑客针对Web站点进行攻击，试图获取用户数据，且攻击手段多样化；第二个是客户的站点为了能够更好的支持业务活动，加入了越来越多的互动内容和最新的开发技术，带来了更多的安全隐患。

当系统环境变的越来越复杂时，只有完美的动态应用安全评估系统（DAST）能带来最大的收益，包括为安全运维人员节省时间，为管理层提功决策辅助，避免任何人为带来的疏忽，满足合规需求等等。

DAST工具需要应付各种新技术，并提供二次开发的灵活性。

- 等保2.0
- OWASP
- PCI
- SOX
- GDPR

技术特点

应用安全漏洞扫描属于动态扫描系统，每个应用都有自己的特点和漏洞类别，评估系统在扫描性能和覆盖率上必须具有较好的平衡。

领先的漏洞扫描引擎

碳泽应用安全评估系统内置全球领先的Web扫描引擎，居于Gartner领先地位，不限制测试的URL数量。

多用户多引擎Web管理页面

整个系统支持多用户权限设定，支持多个分布式引擎统一管理，B-S管理架构。

全面的扫描策略覆盖

扫描引擎覆盖全面，涵盖等保、PCI、OWASP、SOX等多种合规需求。

应用登录支持多样化

支持表单登录、Cookie登录、脚本登录、验证码登录、NTML登录、手工输入等多种应用登录方式。

计划扫描任务及多任务

碳泽应用安全评估系统支持定制扫描计划，特定时间开启扫描，同时支持多任务设定，单引擎排队扫描或者多引擎并发扫描。

详细的漏洞修补建议

为每一个检测到的漏洞提供详细的漏洞扫描信息及修补建议，管理员能够快速定位漏洞原因和详情。

漏洞信息的手工验证

提供HTML漏洞报告，客户可以通过验证插件自己复现漏洞存在与否，验证漏洞修补结果。

LDAP认证整合、开放API、中英文报告

支持LDAP认证整合，支持中英文漏洞描述及报告，全开放API接口。

基于扫描站点

- 结果呈现和比对
- 扫描策略保存和复用

上海碳泽信息科技有限公司是位于上海的技术创新型企业，在深圳、上海、北京、杭州、香港具有分支机构；上海碳泽在漏洞扫描、自动化渗透测试、安全自动化响应等多个领域具有长期技术积累。

- 销售联系邮箱：sales@tanze.io
- 电话：400-1788-258