360政企安全

渗透测试服务使用指南

目 录

1. 背景

当前，以 5G、AI、大数据、物联网、云计算等为代表的新一代信息技术，深刻的改变着社会经济的交往形式、生产方式、运营模式。“加快数字化发展，建设数字中国”，被列入国家十四五规划纲要。随之而来的是多样化的网络攻击事件：APT 组织窃取国家机密；黑产组织盗取企业数据、对企业植入勒索病毒等。

互联网上 Web 网站数量巨多、规模庞大，给用户带来便利的同时又极易受到安全威胁。一旦网站被黑客入侵，就可能带来经济损失。近几年国内外发生的很多安全事件，例如：eBay 遭黑客入侵大量用户数据泄露，12306 网站用户数据泄露，信息安全提出极大的挑战。同时真的 Web 应用的攻击逐渐呈现低成本、可复制的特点，使得黑客针对 Web 应用及其服务器的攻击越来越频繁。

Web 应用是当今各大企业单位重要的对外展现形式，Web 安全是网络安全的重中之重，国家在《网络安全法》发布后，各关键行业对于网络安全的感知能力、预警能力、安全防护能力和应急响应能力都有待加强。面对日趋复杂、严峻的网络安全态势，从国务院到国家相关部委在网络和信息安全方面均开展了密集部署，在各大领域发展建设规划中也均提到 Web 应用系统安全防护工作要求。

Web 应用安全测试服务使用多种测试工具，按照标准测试流程，参考成熟的安全规范，在有限的时间内最大限度的发现 Web 应用中存在的安全问题，及时通知开发人员进行修复，保障网站程序和数据的安全。

2. 服务综述

三六零政企安全渗透测试服务是模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵。目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。通过渗透测试提升企业安全，进一步增强企业安全防护体系。

2.1. 服务对象

三六零政企安全渗透测试服务的服务对象，以及被服务对象的收益，如下表所示：

服务对象	服务对象收益
所有企业/团体	全面发现潜在风险：系统漏洞、业务漏洞、数据库漏洞、中间件漏洞、防护漏洞等

2.2. 服务原则

三六零政企安全在提供渗透测试服务过程中，将遵循下列原则:

- 保密性原则

服务过程中，获知的所有信息均属秘密信息，不泄露给第三方单位或个人；不利用获取到的信息，进行任何侵害客户的行为；提交的服务报告，不扩散给未经授权的第三方单位或个人。

- 标准性原则

三六零政企安全的渗透测试服务，将在国家法律、法规允许的范围内进行，特别是遵照并履行《全国人大常委会关于维护互联网安全的决定》中的相关规定。

- 规范性原则

三六零政企安全的渗透测试服务，按照三六零政企安全的安全服务工作规范、三六零政企安全相关服务实施规范严格落实。实施由专业的安全服务人员依照规范的操作流程进行，并提供完整的服务报告。

3. 服务信息

3.1. 服务方式

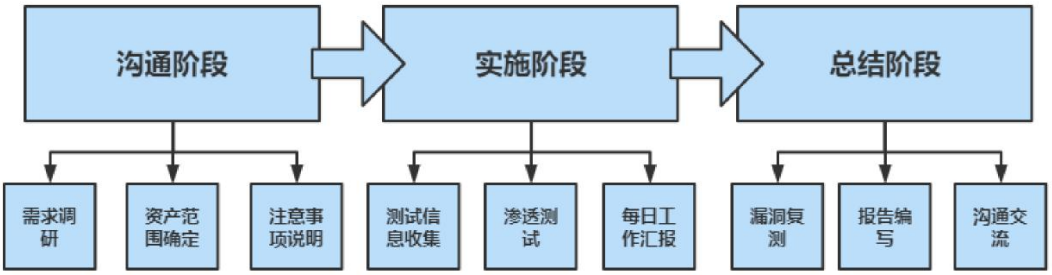
三六零政企安全渗透测试服务的服务方式为：

服务方式	服务描述	服务特点
远程渗透	通过互联网接入进行	无需提供场地
现场渗透	通过客户网络接入	便于流量审核、沟通交流
远程&现场渗透	互联网直接接入，内网通过客户网络接入	互联网测试便捷，内网便于流量审核、沟通交流

3.2. 服务资源

人力	漏洞	工具
中级工程师	三六零漏洞库	QUAKE 空间测绘
		资产梳理
		漏洞探测
		其他工具

3.3. 服务流程



沟通阶段，主要任务有：需求调研、资产范围确定、注意事项说明等。需求调研阶段，明确客户需要的渗透测试类别(WEB 应用渗透、API 渗透)；资产范围确定，明确客户待渗透资产域名/IP 等信息；注意事项说明，包含渗透时间(如：限

定时间段、安全设备加白)、渗透方式(如：限定不能使用大型扫描器)、渗透过程(如：爆破、上传 WebShell 报备)等。

实施阶段，主要任务有：渗透测试(应用渗透、中间件渗透、API 渗透等)；每日工作汇报(工作简述报告、渗透测试报告、漏洞复测报告)等。

总结阶段，主要任务有：漏洞复测及修复指导(复测漏洞、在客户需要时，提供修复指导)；整体报告产出(整体工作说明、整体渗透成果、整体复测记录)；沟通交流(渗透方式沟通交流、安全防护沟通交流)等。

3.4. 服务内容

3.4.1. WEB 应用渗透

<table>
<tr><th rowspan="2">服务人员</th><th rowspan="2">服务标准</th><th colspan="5">服务内容</th></tr>
<tr><th>第 1 天</th><th>第 2 天</th><th>第 3 天</th><th>第 4 天</th><th>第 5 天</th></tr>
<tr><td rowspan="3">中级工程师</td><td rowspan="3">二级域名-1 个</td><td>需求确认</td><td rowspan="3">渗透测试</td><td rowspan="3">渗透测试</td><td rowspan="3">渗透测试</td><td>漏洞复测</td></tr>
<tr><td>环境协调</td><td>报告编写</td></tr>
<tr><td>资产收集</td><td>沟通交流</td></tr>
</table>

一个二级域名，需中级工程师 1 名，为期 5 天。

需求确认，实施服务人员，基于获取的项目信息，与客户侧项目对接人，进行需求确认。确认内容包含：

1) 渗透测试范围

2) 渗透测试注意事项

3) 渗透测试交付时间节点

资产收集，基于客户提供的资产信息进行资产梳理。梳理内容包含：

1) 子域名

2) 中间件类型、版本

3) 开发语言

4) CMS 类别

环境协调，基于客户现场环境，协调如下内容：

1) 测试环境地址

2）测试环境账号

渗透测试，根据资产收集结果，进行渗透测试，测试的内容包含：

漏洞类型	威胁级别	具体漏洞
认证和授权类	高危	任意文件下载
		越权访问
		弱口令
		账户管理不规范
		文件上传
	中危	用户名可枚举
		暴力攻击
		会话标识未更新
		未授权访问
		脆弱的 SSL 加密算法
		会话令牌不应写入 URL
		密码明文传输
		验证码漏洞
	低危	脆弱的加密方式
		会话重放攻击
命令执行类	高危	Struts2 远程命令执行
		JBOSS 远程命令执行
		HTTP.sys 远程命令执行
		文件包含
		tnftp ftp 客户端命令执行
		HP Data Protector 命令执行
		GNU Bash 命令执行
		Elasticsearch 命令执行
		各类反序列化
		命令执行
逻辑攻击类	高危	支付绕过

		密码找回
		任意密码登陆
		绕过统一认证平台
	中危	并发漏洞
	低危	慢速 HTTP 攻击
		短信攻击
		邮件攻击
		批量注册
注入类攻击	高危	SQL 注入
		XML 注入
		XPATH 注入
		命令注入
		服务器模板注入（SSTI）
	中危	CRLF 注入
		XFF 注入
		链接或框架注入
		JSON 劫持注入
客户端攻击类	高危	XSS
	中危	CSRF
服务端攻击类	高危	WebServer Expect 头 XSS
		应用服务未授权访问
	中危	数据明文传输
		拒绝服务
	低危	使用低版本应用服务
信息泄漏类	高危	git 泄漏
		svn 泄漏
	中危	web 服务器控制台泄漏
		Phpinfo()信息泄漏
		目录遍历

		IIS 短文件名泄漏
		HTML 注释敏感信息泄露
		安装或示例页面未删除
		Cookie 信息泄漏
	低危	Cookie 缺少安全属性
		敏感信息泄漏
		异常信息泄漏
		内网 IP 地址泄漏
MS 系列漏洞	高危	所有 MS 系列
其他	高危	PHP multipart/form-data 远程 DOS 漏洞
		ASP.NET Padding Oracle 攻击
		SSRF
		Web 服务器解析漏洞
		Unicode 编码转换漏洞
		SMB 会话可获取远程共享列表
		Oracle Database Server 'TNS Listener'远程数据投毒
		Openssl 心脏滴血漏洞
		Linux Glibc GHOST 幽灵
		ssh 用户名暴力枚举
	中危	跨域访问
		URL 重定向
		DNS 域传送漏洞
		Web 服务器多余端口开放
		HTTP Host 头攻击
		Thc ssl dos 攻击
		jQuery 导致的 XSS
		TLS1/SSLv3 重协商漏洞

		spf 邮件伪造
		点击劫持

每日工作汇报，约定时间内，向客户侧对接人汇报每日工作情况。包含：

1）当日工作简报

2）渗透测试报告

3）复测报告

整体交付，在项目结束时，提供项目整体报告。包含：

1）整体资产收集量

2）整体渗透测试成果

3）整体漏洞复测结果

4）整改建议

3.4.2. API 渗透

服务人员	服务标准	服务内容			
		第 1 天	第 2 天	第 3 天	第 4 天
中级工程师	API-1 组（10 个）	需求确认	渗透测试	渗透测试	漏洞复测
					报告编写
		资产搜集			沟通交流

一组 API，需中级服务人员 1 名，工作周期 4 天。

需求确认，实施服务人员，基于获取的项目信息，与客户侧项目对接人，进行需求确认。确认内容包含：

1）API 信息

2）渗透测试注意事项

3）渗透测试交付时间节点

渗透测试，主要测试类型有：

漏洞类型	威胁级别	具体漏洞
认证和授权类	高危	OAuth 绕过
		失效的对象授权、控制访问

		失效的用户身份认证
		Token 不校验
		Token 可爆破
		未授权访问
	中危	用户名可枚举
		水平越权
命令执行类	高危	反序列化
		命令执行
逻辑攻击类	高危	接口调用可遍历
		接口参数可篡改
	中危	批量注册
注入类攻击	高危	SQL 注入
		XML 注入
		XPATH 注入
		命令注入
	中危	CRLF 注入
		XFF 注入
		JSON 劫持注入
信息泄漏类	高危	测试接口泄漏
		测试文档泄漏
	中危	web 服务器控制台泄漏
		目录遍历
	低危	Cookie 缺少安全属性
		敏感信息泄漏
		异常信息泄漏
		内网 IP 地址泄漏
其他	高危	SSRF
		Web 服务器解析漏洞
		Unicode 编码转换漏洞

	中危	跨域访问
		URL 重定向
		HTTP Host 头攻击

整体交付，在项目结束时，提供项目整体报告。包含：

1）整体渗透测试成果

2）整体漏洞复测结果

3）具体漏洞描述

4）整改建议

3.5. 服务交付

三六零政企安全渗透测试服务各阶段服务交付物清单如下：

服务项目	交付物
沟通阶段	项目沟通记录
	渗透测试范围确认单
	渗透测试注意事项确认单
攻击阶段	渗透测试报告
	渗透痕迹记录表
	漏洞复测报告
	每日工作简述报告
总结阶段	整体工作报告
	渗透痕迹清理确认单
	沟通交流记录

4. 服务优势

360 公司是中国最大的互联网和移动安全产品及服务提供商。公司创立于 2005 年，是互联网免费安全的首倡者，先后推出 360 安全卫士、360 手机卫士、360 安全浏览器等国民级安全产品，PC 安全产品月活用户 5 亿以上，移动安全产品月活超过 4.6 亿。同时，360 为上百万家国家机关和企事业单位提供包括安全评估、安

全运维、安全培训等全方位安全服务。

习总书记多次听取 360 公司汇报，对 360 公司维护国家网络安全工作高度评价，对上报的永恒之蓝勒索病毒反思报告等做出重要批示。

优势：

- 累计申请专利 11833 项，互联网安全公司排名第一
- 网络安全专利超过 5100 项，在国内处于绝对领先地位
- 政企用户 300 万
- 汇聚东半球最大的“白帽子军团”，拥有顶级安全人才 3800 余人
- ……