附件六：网站安全检测项标准

测试项目	测试内容	描述
代码漏洞	SQL 注入漏洞(id)	对网站各功能参数进行注入测试，查看是否存在 sql 注入漏洞
	XSS 跨站漏洞(id)	对核心业务 http 请求中的各参数进行 xss 测试
	OS 命令注入	检查网站是否存在命令注入漏洞
	XXE 注入漏洞	检查网站是否存在 xml 外部实体注入漏洞
	任意文件读取漏洞	检查网站资源调用模块是否存在文件非法读取漏洞、文件包含漏洞
	任意文件上传漏洞	检查网站文件上传写入模块是否允许向服务器写入 Webshell 文件
	任意文件修改删除漏洞	检查文件编辑模块是否存在删除、修改任意文件的问题
	URL 跳转漏洞	检查网站是否存在 URL 跳转漏洞
	CSRF 跨站请求伪造漏洞	检查网站重要表单是否使用图形验证码、短信验证等随机验证方式来避免 CSRF 攻击
	访问控制漏洞	检查网站各个模块用户权限控制问题，是否存在模块越权访问、访问控制缺失等问题
	身份认证漏洞	检查用户认证方式是否安全，登陆口令是否可被爆破
	会话管理漏洞	检查网站会话管理方式是否安全，是否存在固定

		会话、sessionid 泄露、登陆超时、cookie 错误使用等问题
	敏感注释信息或代码泄露	检查页面注释中是否包含敏感信息或测试代码
	第三方组件漏洞	检查网站是否使用了不安全的第三方组件
防护策略	http 请求签名绕过	检查移动端是否对请求进行防篡改签名，签名是否可被绕过
	应用防火墙规则绕过	检查防火墙防护能力，安全策略是否生效，策略是否可以绕过
	应用防火墙防护绕过	检查是否可通过直接访问网站 ip 等方式绕过安全防护
中间件配置	错误页面自定义	检查网站是否自定义错误页面
	控制台弱口令或漏洞	检查中间件控制台是否弱口令或存在漏洞
	列目录及其他错误配置	检查中间件配置是否合规
	危险的 http 方法	检查中间件是否开启危险的 http 方法
数据库安全	数据库允许远程链接	检查数据库端口是否对外开放，是否允许远程连接
	数据库补丁更新不及时	检查数据库是否存在已知漏洞

通信安全	http 明文传输	检查是否使用 https 加密传输
	https 证书未校验漏洞	检查 https 证书是否校验
	Get 方式传输关键参数	检查网站关键参数是否使用安全的 post 方式传输
	中间人劫持漏洞	检查网站数据传输是否存在中间人劫持风险
信息泄露	敏感文件泄露	检查网站目录中是否存在网站备份文件、说明文件、缓存文件、测试文件等，导致网站源码、配置信息泄露
	后台地址泄露	检查网站后台路径是否进行隐藏
	Google Hacking	检查搜索引擎、网盘、社区等是否收录网站重要的敏感数据，如用户 session、网站日志、其他敏感数据
	Git、svn、cvs 安全	检查代码管理方式是否存在信息泄露等安全隐患，是否在互联网上泄露源码信息
服务器安全	非业务端口开发	检查接口是否开放危险的非业务端口开放
	服务器补丁检查	检查服务器是否及时更新补丁，是否存在可利用高危漏洞
	远程管理口令安全	检查远程管理软件口令策略是否安全，是否存在弱口令、口令爆破等问题