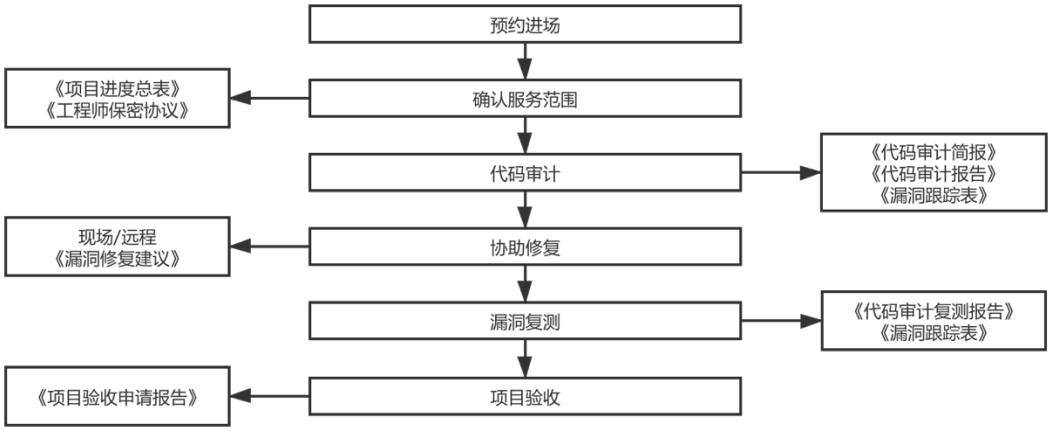
沃顿在线代码审计服务

使用指南

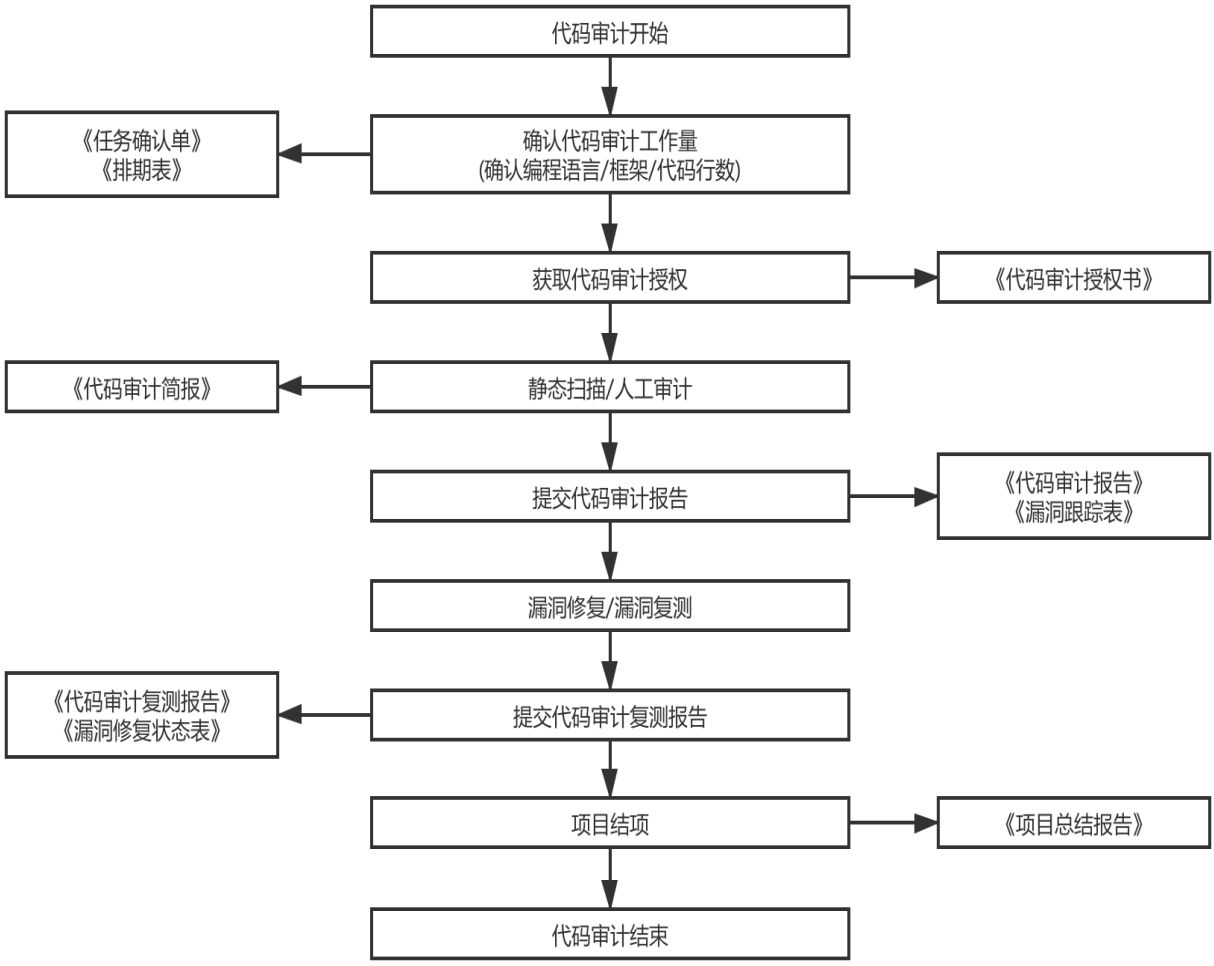
北京沃顿在线信息技术有限公司
Beijing Whartonlive Information Technology Co., Ltd

1. 代码审计流程

代码审计交付流程：



代码审计流程图：



2. 工具介绍

代码审计辅助工具介绍：

IDE	静态分析工具	环境部署	数据库
IDEA	CheckMarxCxSuite	Weblogic	Oracle
Pycharm	FindSecurityBugs	Tomcat	MySQL
PHPstorm	RIPS	Apache	SQLserver

工具介绍

审计工具：IDEA

工具名称	IDEA
工具用途	IDEA 是 Jetbrains 公认最好的 java 集成开发环境，由 jetbrains 公司开发。IDEA 的代码自动补全、重构、J2EE 支持、git/svn 等版本控制支持、代码分析等功能都远超其他 IDE。

审计工具：Escplice

工具名称	Pycharm
工具用途	Pycharm 是一个 Python IDE，由 jetbrains 公司开发。Pycharm 具备完善的项目管理、代码提示、单元测试、版本控制、第三方库安装等功能，同时支持使用 Django 框架进行 Python web 开发。

审计工具：PHPstorm

工具名称	PHPstorm
工具用途	PHPstorm 是一个 PHP IDE，由 jetbrains 公司开发。PHPstorm 支持 macOS、Linux、Windows 三大操作系统，支持自动生成 PHPdoc，非常适合大型项目开发。

审计工具：CheckMarxCuSuite

工具名称	CheckMarxCxsuite

工具用途	CheckMarxCxSuite 是以色列 CheckMarx 公司开发的一款商业源代码静态审计工具，是世界上最著名的源代码安全扫描软件之一。支持 Java、c、c++、c#、Python、js、PHP、asp 等多种开发语言。

测试工具：FindSecurityBugs

工具名称	FindSecurityBugs
工具用途	FindSecurityBugs 是 FindBugs 分析工具的一款插件，通过规则对代码进行静态分析以发现其中的安全漏洞，FindBugs 支持集成到 IDEA 之中。

测试工具：RIPS

工具名称	RIPS
工具用途	RIPS 是一款使用分析 PHP 项目的代码审计工具，能够检测 SQL 注入、XSS、文件泄露、文件包含、命令执行等常规 web 漏洞。

3. 漏洞测试清单

Penetration Testing List 19-1			
功能模块	**序列号**	**测试漏洞**	**是否安全**
注册	1	验证码重复利用	√
	2	验证码绕过	√
	3	验证码爆破	√
	4	恶意用户批量注册	√
	5	反射型 XSS	√
	6	存储型 XSS	√
	7	post 注入	√
	8	短信轰炸	√
	9	遍历用户名	√
登录	10	爆破用户登录密码	√
	11	遍历用户名	√
	12	反射型 XSS	√
	13	验证码重复利用	√
	14	验证码绕过	√
	15	验证码爆破	√
	16	平行越权（账户权限绕过）	√
	17	cookie 欺骗	√
	18	恶意锁定用户账户	√
	19	万能密码登陆	√
	20	垂直越权	√
	21	post 注入	√
	22	手机号撞库	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
密码找回	23	重置任意用户登录密码	√
	24	post 注入	√
	25	绕过重置密码验证	√
	26	验证码绕过	√
	27	验证码爆破	√
	28	批量重置用户登录密码	√
	29	短信验证码劫持	√
	30	用户邮箱劫持篡改	√
订单	31	订单遍历	√
	32	订单信息泄露	√
	33	用户信息泄露	√
抽奖/活动	34	刷取活动奖品	√
	35	盗刷积分	√
	36	修改抽奖结果	√
	37	修改抽奖次数	√
抢购活动	38	低价抢购	√
	39	抢购作弊	√
	40	刷单	√
第三方商家	41	盗号	√
	42	商家账户遍历	√
	43	越权访问其他商家用户	√
购买支付	44	商品金额篡改	√
	45	商品数量篡改	√
	46	交易信息泄露	√
代金券/优惠卷	47	批量刷取代金券/优惠卷	√
	48	修改代金券金额	√
	49	修改代金券数量	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
	50	爆破兑换码	√
运费	51	运费绕过	√
充值	52	修改充值金额	√
	53	修改购买数量	√
后台	54	后台路径泄露	√
	55	post 注入	√
	56	数据库备份 getwebshell	√
	57	配置文件写入木马	√
	58	任意文件上传漏洞	√
	59	万能密码登陆	√
	60	开源编辑器、插件漏洞	√
	61	后台越权访问	√
	62	暴力破解管理员账号	√
	63	CSRF	√
	64	存储型 XSS	√
	65	目录遍历	√
会员系统	66	用户越权访问	√
	67	个人资料信息泄露	√
	68	登陆验证绕过	√
	69	重置任意账户密码	√
	70	开源编辑框、插件漏洞	√
	71	GET 注入	√
	72	登录框 POST 注入	√
	73	CSRF	√
	74	用户组水平越权	√
	75	任意文件上传	√
	76	反射型 XSS	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
	77	存储型 XSS	√
	78	个人资料遍历	√
传输过程	79	COOKIE 注入	√
	80	COOKIE 跨站	√
	81	COOKIE 劫持	√
	82	用户凭证铭文传输	√
评论	83	中间人攻击	√
	84	流量劫持	√
	85	用户凭证明文传输	√
	86	恶意批量评论	√
	87	数据库插入木马	√
	88	任意文件上传	√
	89	CSRF	√
	90	反射型 XSS	√
	91	存储型 XSS	√
SQL 注入	92	注入点敏感文件读取	√
	93	注入点写入木马	√
	94	注入点拖库	√
	95	伪静态注入	√
	96	LDAP 注入	√
	97	搜索型 sql 注入	√
	98	POST 注入	√
	99	GET 注入	√
	100	宽字节注入	√
	101	HTML 代码注入	√
	102	XML 外部实体攻击（XXE）	√
	103	iframe 代码注入	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
安全配置错误	104	DOS/DDOS	√
	105	FTP/SSH/3389 弱口令	√
	106	使用存在漏洞的中间件	√
	107	高权限账号弱口令	√
	108	高危端口	√
	109	防火墙可被溢出、绕过	√
	110	不安全的 HTTP 方法	√
	111	文件夹访问/执行权限配置不正确	√
	112	本地文件包含 (SQLiteManager)	√
	113	远程文件包含	√
	114	登陆本地验证	√
	115	文件上传本地验证	√
	116	会话不过期	√
	117	跨域加载漏洞	√
	118	用户凭证明文传输	√
敏感信息泄露	119	敏感文件下载(数据库备份、网站备份)	√
	120	敏感信息泄露	√
	121	后台路径、数据库地址泄露	√
	122	用户身份标识泄露	√
	123	心脏滴血漏洞	√
	124	组件版本信息泄露	√
	125	报错页面信息泄露(中间件版本、网站路径)	√
	126	关键数据 web 存储	√
	127	前端代码注释中存在敏感信息	√
	128	Github 敏感信息泄露	√
	129	SVN 源代码泄露	√
	130	Resin 任意文件读取	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
	131	phpinfo 信息泄露	√
	132	Apache server-info 信息泄露	√
	133	日志文件泄露	√
	134	Apache server-status 信息泄露	√
	135	明文传输	√
	136	开启 HTTP OPTIONS 方法	√
	137	文本文件（账号）	√
权限控制不严格	138	垂直越权	√
	139	水平越权	√
	140	越权访问	√
	141	文件夹访问/执行权限配置不正确	√
	142	限制访问终端设备	√
	143	限制文件夹访问	√
	144	Server Side Request Forgery (SSRF)	√
存在漏洞的组件	145	缓冲区溢出（本地）	√
	146	缓冲区溢出（远程）	√
	147	Drupal SQL 注入 (Drupageddon)	√
	148	使用已爆出漏洞的低版本 cms	√
	149	心脏滴血漏洞	√
	150	PHP CGI 远程代码执行	√
	151	phpMyAdmin BBCode 标签 XSS	√
	152	IIS 短文件名遍历	√
	153	开源系统公开漏洞	√
	154	Apache Struts2 远程代码执行漏洞（S2-019）	√
	155	Apache Struts2 远程代码执行漏洞（S2-033）	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
	156	Apache Struts2 远程代码执行漏洞（S2-037）	√
	157	Apache Struts2 远程代码执行漏洞（S2-045）	√
	158	Apache Struts2 远程代码执行漏洞（S2-052）	√
	159	stust2 远程代码执行漏洞	√
	160	破壳漏洞 (CGI)	√
	161	Struts2 框架远程代码执行	√
	162	低版本 Mysql 密码碰撞	√
	163	Nginx 解析漏洞	√
	164	Apache 解析漏洞	√
	165	IIS 解析漏洞	√
	166	WordPress CSRF	√
	167	IIS 短文件名漏洞	√
	168	低版本 Apache cookie 泄露	√
	169	HTTPS 服务器未验证	√
失效的访问控制	170	跨站请求伪造(CSRF)	√
	171	水平越权	√
	172	垂直越权	√
	173	服务端请求伪造(SSRF)	√
	174	任意文件操作	√
	175	未授权访问	√
	176	管理后台任意访问	√
源代码安全	177	源代码反编译	√
	178	源代码泄露	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
客户端安全	179	键盘劫持	√
	180	服务端与客户端交互漏洞	√
	181	API 接口漏洞	√
远程代码执行	182	Struts 2 远程代码执行	√
	183	Tomcat 远程代码执行	√
	184	GoAhead 远程代码执行	√
	185	CredSSP 远程代码执行	√
	186	NodeJS 远程代码执行	√
	187	J2EE 远程代码执行	√
	188	swagger 远程代码执行	√
	189	IIS HTTP.SYS 远程代码执行	√
	190	Discuz! X 远程代码执行	√
	191	PHP 反序列化远程代码执行	√
	192	java 反序列化远程代码执行	√
	193	CouchDB 远程代码执行漏洞	√
	194	Apache ActiveMQ Fileserver 远程代码执行漏洞	√
	195	Android WebView 远程代码执行	√
	196	Spring-Boot 远程命令执行	√
	197	Jackson 框架任意代码执行	√
	198	IIS 6.0 WebDAV 远程代码执行漏洞	√
	199	Fastjson 远程代码执行漏洞	√
	200	Joomla 1.5 - 3.4 版本远程命令执行漏洞	√
	201	weblogic 反序列化远程代码执行	√
移动端/客户端	202	服务端与客户端交互漏洞	√
	203	API 接口漏洞	√
	204	XSS - 存储型	√

Penetration Testing List 19-1			
功能模块	序列号	测试漏洞	是否安全
	205	代码执行	√
	206	内存溢出	√
	207	DLL 劫持	√
	208	不安全的加密算法	√
	209	源代码泄露	√
	210	键盘劫持	√
	211	XSS - 反射型	√
	212	任意备份	√
	213	二次编译	√
	214	拒绝服务	√
	215	XSS - DOM 型	√
	216	内核提权	√
	217	弱证书校验	√
	218	第三方 SDK 漏洞	√

4. 安全等级评定

安全等级	资源内容描述
严重	严重的漏洞是指，发生在核心系统业务系统（核心控制系统、域控、业务分发系统、堡垒机等可管理大量系统的管控系统），可造成大面积影响的，获取大量（依据实际情况酌情限定）业务系统控制权限，获取核心系统管理人员权限并且可控制核心系统。 包括但不限于： 内网多台机器控制 核心后台超级管理员权限获取且造成大范围企业核心数据泄露，可造成巨大影响。
高危	系统的权限获得（getshell、命令执行等）。 系统的 SQL 注入（后台漏洞降级，打包提交酌情提升）。 敏感信息越权访问。包括但不仅限于绕过认证直接访问管理后台进行敏感操作、重要后台弱密码、获取大量内网敏感信息的 SSRF 等）。 任意文件读取。 涉及金钱的越权操作、支付逻辑绕过（需最终利用成功，优惠券相关问题除外）。 严重的逻辑设计缺陷和流程缺陷。包括但不仅限于任意用户登录漏洞、批量修改任意账号密码漏洞、涉及企业核心业务的逻辑漏洞等，验证码爆破除外 。 大范围影响用户的其他漏洞。包括但不仅限于重要页面可自动传播的存储型 XSS、可获取管理员认证信息且成功利用的存储型 XSS 等。

	大量源代码泄露。
中危	需交互方可影响用户的漏洞。包括但不仅限于存储型 XSS，涉及核心业务的 CSRF 等。 越权操作。包括但不仅限于包括但不限于绕过限制修改用户资料、执行用户操作等。 由验证码逻辑导致任意账户登陆、任意密码找回等系统敏感操作可被爆破成功造成的漏洞。 本地保存的敏感认证密钥信息泄露，需能做出有效利用。 四位验证码爆破重置密码或者登陆账号。 心脏滴血漏洞。 xml 注入。 普通的后台或者边缘系统的后台。 任意文件上传（例如上传 html 导致存储 XSS，其他情况除外）。
低危	本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由 Android 组件权限暴露、普通应用权限引起的问题等。 普通信息泄露。包括但不限于 web 路径遍历、系统路径遍历、目录浏览等。 反射型 XSS（包括 DOM XSS / Flash XSS）。 普通 CSRF。 URL 跳转漏洞。 一些影响有限的越权（不涉及敏感信息，修改个人描述等）。 短信炸弹。 其他危害较低、不能证明危害的漏洞。（如无法获取到敏感信息的 CORS 漏洞）。 无回显的且没有深入利用成功的 SSRF。 无法利用的 GITHUB 信息泄露。