WEB 渗透常见

1.信息泄露

特殊页面

404、403、500 等异常页面是否显示版本信息

HTTP **返回头**

返回头中是否显示服务器版本等信息

CMS **信息**

对使用的 cms 系统版本信息是否明确显示，是否特征信息、页面未做自定义处理

敏感文件

在根目录下留存有开发、测试、运维人员的数据文件，并可浏览下载（wwwscan、御剑）

后台管理页面

对于隐藏后台页面，若被猜解出来（wwwscan、御剑）

用户信息

在用户交互系统中,对用户的关键信息进行显示返回的,包括:手机、邮箱、银行卡号、密码（登录查看，包括页面未显示数据）

2.认证会话漏洞

登录认证

自动 登录页面缺乏抗自动化机制，

用户 登录过程可对用户进行暴力破解（burp）

令牌登录机制可绕过，通过对某一请求直接获取令牌（burp）

会话令牌 对于会话令牌是否设置了 http-only 和 session 属性

3.弱口令漏洞

远程桌面 RDP 远程 RDP 服务弱口令检查（hydra）

远程登录 SSH 远程登录 SSH 服务弱口令检查（hydra）

应用后台管理页面弱口令 后台管理页面弱口令检查（hydra）

其他组件、后台弱口令 Tomcat、weblogic、openfire 等管理弱口令(hydra）

4.信息未加密漏洞

应用数据传输 对于高安全级别应用，是否采用 https 加密传输其关键应用数据，尤其涉及到支付、密码传输等过程（观察）

页面显示 对于高安全要求级别数据，如手机、邮箱、银行卡等是否对外隐藏或模糊显示

5.SQL 注入漏洞

SQL 注入

sqlmap 多种情况下的 SQL 注入测试 ,包括查询、插入、修改、删除(SQLMAP、自动化扫描工具）

6.XSS 漏洞

反射 XSS

在 url 中未对参数进行过滤，直接将用户输入的返回。

在业务系统中对包含交互参数并返回原文的请求进行测试 ,是否存在反射型 XSS（手动测试、自动化工具）

存储 XSS

页面脚本植入

在业务系统中对所包含提交数据的业务进行测试，包括注册、留言版、地址信息等，探测当数据提交后再次显示后是否能触发 xss（手动测试）

7.CSRF 漏洞

在业务系统中对所包含跨站点请求伪造

8.文件包含漏洞

本地文件包含

对页面中内容由参数控制，且其中参数属于服务器文件的情况下，对其参数进行篡改成特性文件路径，探测其是否有本地文件包含漏洞（手动测试，自动化扫描）

远程文件包含

对页面中内容由参数控制，且其中参数属于服务器文件的情况下，对其参数进行篡改网络链接，探测其是否有远程包含漏洞（手动测试，自动化扫描）

9.目录遍历浏览漏洞

目录浏览

直接访问特定目录，探测是否开启目录浏览问题（手动测试，自动化扫描）

目录遍历

通过../或其他特殊字符访问到其他目录下的其他文件（手动测试，自动化扫描）

10.文件上传漏洞

上传校验

寻找业务交互过程中的所有上传点，通过对上传功能的全面手动测试，包括利用各类上传绕过手法测试

11.未授权访问漏洞

Web 敏感页面未授权访问

应用非授权访问

12.服务组件漏洞

web **服务器**

检测前段 web 服务器是否存在漏洞，如 IIS6.0 的解析漏洞，NGX 的解析漏洞，iis 的 put 方法开启问题，tomcat 样例漏洞等等

中间件、基础组件

检测中间件应用服务器漏洞 如 weblogic、Jboss 中的各类命令行执行漏洞、tomcat 中的管理界面弱口令漏洞、weblogic 等服务的管理弱口令问题；检测平台中使用的基础组件安全问题，如 Struts2、imagemigic、java、php 安全问题

CMS、**三方模块**

对应用中的使用的 cms、第三方组件进行检测发现，并确定其是否含有漏洞，三方模块包括编辑器如 fck 等、在线客服、

13.业务逻辑漏洞

平行权限查询

1. 在登录业务系统的情况下，对其中查询用户自身信息请求，分析其参数，若参数中出现指代自身的参数名，如 uid，username 等，通过把对应参数值修改为其他注册用户对应的参数值进行测试，若能够返回修改后用户的正确信息，可判定为平行越权查询漏洞

2. 在登录业务系统情况下，针对访问用户资源类请求（如银行卡，收获地址），若参数中出现可预料的资源指代参数，如递增的 id 号等，通过把其中资源 id 修改为其他用户对应的资源 id，若能正确请求到对应资源数据，可判定为越权查询漏洞

平行权限修改

1. 在登录业务系统的情况下，对其中操作修改用户自身信息类请求，分析其参数，若参数中出现指代自身的参数名，如 uid，username 等，通过把对应参数值修改为其他注册用户对应的参数值进行测试，若能够修改其他注册用户信息，可判定为平行越权修改漏洞

2. 在登录业务系统情况下，针对其用户资源变更的请求（如银行卡、收获地址），分析其种参数，若其资源参数值为可预测的规律值（如递增 id 号），把对应资源 id 修改成其他用户对应资源资源 id，若能成狗修改其他用户对应资源数据，可判定为越权修改漏洞

垂直权限操作

对于所有业务操作，包括但不限于增删改查，若对应请求资源中包含或隐含了权限级别参数，通过篡改其权限参数，实现越权操作到高级别账户权限，可判定为垂直权限操作

批量注册

所有注册入口是否有图形验证码或其他反自动化机制，在高安全级别系统中应要求提供有效手机号码进行短信验证码校验

用户密码修改

1. 在修改用户密码流程中未验证用户当前密码，或当前密码验证过程和修改密码过程分别判定导致当前密码验证流程被绕过

2. 在密码修改页面未提供反自动化机制或未限制尝试次数

密码暴力破解

1.登录功能密码破解，若无反自动化机制和次数限制，可判定为存在暴力破解；

2.业务系统中若存在探测当前是否正确的请求，若没有频率限制或反自动化机制，判定为暴力破解漏洞

密码找回功能

1.密码找回流程中最后一步变更密码，可以在不经过前面步骤的校验直接发起变更密码请求，导致重置任意用户密码；

2.在找回密码过程中，在通过手机或邮箱验证后，系统向用户分发重置密码 token，但若 token 未与相应用户绑定，可引发对任意用户密码重置

3.在变更密码的最后过程中，若参数中存在指代用户的参数，通过修改其中用户 id 实现对任意用户密码进行篡改

4.在找回密码过程中，向手机或邮箱发送验证码，若手机或邮箱地址不是从后台获取发送，而是发送到前台后再发送到后台，攻击者可以通过修改其手机、邮箱实现对指定手机或邮箱发送验证码，进而实现对任意用户密码重置。

验证码发送

业务系统中所有对手机或邮箱发送验证码功能 ,若不存在反自动化机制或次数限制，都可引发验证码炸弹攻击

图形验证码绕过

1.图形验证码是否完成随机

2.验证码在和业务结合的过程中是否，再次携带验证码参数到后台校验

3.验证码在完成对一次相应业务的反自动化检查后，是否强制无效掉使用过的验证码

验证码破解

1.邮箱、手机验证码是否随机

2.邮箱、手机验证码是否可能被暴力破解，即对验证码失败尝试次数是否有限制，并是否设置有效时间

商品价格

在商城类系统中，在购买商品到生成订单的过程中，分析其中参数，探测其中表示价格参数，若在订单的过程中有其他属性能够影响订单总价，同样在参数中进行修改（如优惠价格、折扣率、邮费等），通过前台修改其中价格数若能导致生产订单金额数异常，即变相的修改了对应商品价格

支付价格

1.在商城类系统中，当用户完成订单生成进而进入支付环节的过程中，分析其中参数，修改其中支付金额数据，并尝试让支付网关接收此支付信息

2.在支付过程中 ,若在支付请求数据中包含 HMAC 数据 ,即签名验证类数据，尝试能否破解，若采用简单算法进而破解此签名可判定存在漏洞

支付逻辑

1.在生成订单的过程中，商品件数是否支持负数数据

2.在订单生产过程中，所有影响订单总额的数据是否从后台获取

3.在支付订单的过程中，特别设计到第三方支付平台支付的过程中，是否采用了签名机制，防止攻击者修改支付数据