# 课后题解

1、【多选】以下属于CTF比赛题型的是?

[X] A.MISC杂项

[X] B.Crypto密码学

[X] C.Web渗透

[X] D.PWN二进制

1、【单选】下列哪个不属于CTF的比赛模式?

[ ] A.沙盒模式

[ ] B.AWD模式

[ ] C.漏洞挖掘模式

[X] D.白盒模式

1、【多选】CTF比赛中WEB类题目涉及到的漏洞有哪些?

[ A] A.文件下载

[ B] B.命令执行

[ ] C.栈溢出

[ D] D.反序列化

1、【多选】CTF中隐写用到的技术包括?

[X] A.图片中利用最低有效位隐藏信息。

[X] B.图片中利用DCT于隐写信息。

[X] C.把信息隐藏到音频或者视频文件中。

[X] D.利用行间距隐藏信息。

1、【多选】以下文件头中错误的是?

[X] A.PNG文件头：80594E47

[ ] B.GIF图片：GIF87a

[X] C.ZIP文件：52 61 72 21 1A 07 00

[ ] D.7zip：37 7A BC AF

1、【多选】文本隐写中常用的技术包括?

[X] A.利用行间距隐藏信息

[X] B.利用字间距

[X] C.利用字体颜色

[X] D.利用背景颜色

1、【多选】word类隐写题目的常见类型有?

[X] A.利用行间距隐藏信息

[X] B.word文件加密

[X] C.把信息隐藏到XML文件中

[X] D.改变字体及背景颜色

1、【多选】CTF隐写中以两张图片为解题线索的题目，常见类型有?

[ A] A.在图层中隐写信息。

[ B] B.图片中隐写了另外一张图片。

[ C] C.通过两张图片对比可以得到隐藏的信息。

[ D] D.盲水印攻击。

1、【多选】CTF隐写类题目中，和音频及视频文件相关的题目类型有?

[ A] A.把摩斯电码隐藏到一首歌中。

[ B] B.在视频的某一帧中隐藏信息

[ C] C.利用音频文件的波形隐藏信息。

[ D] D.DTMF音频隐写

1、【多选】压缩包类杂项题目的出题方式有?

[ A] A.在图片中隐写一个压缩包文件

[B ] B.在pcap数据包中，某次传输了一个zip文件。

[ C] C.破解压缩包的加密密码

[D ]D D.综合考察压缩包破解的各种技术。

1、【单选】以下描述中是伪加密的是?

[ ] A.50 4B 03 04 14 00 00 00 08 00 50 4B 01 02 14 00 00 00 08 00

[B ] B.50 4B 03 04 14 00 **09** 00 08 00 50 4B 01 02 14 00 00 00 08 00

[ ] C.50 4B 03 04 14 00 01 00 08 00 50 4B 01 02 14 00 01 00 08 00

[ ] D.50 4B 03 04 14 00 02 00 08 00 50 4B 01 02 14 00 02 00 08 00

1、【单选】Ajax调用的URL包含汉字，IE使用哪种URL编码

[ ] A.utf-8

[ ] B.%+16进制

[C ] C.操作系统指定

[ ] D.utf-16

**正确**解析：暂无

2、【多选】下面编码中那几个类似

[A ] A.base编码

[ ] B.u'r'l编码

[C ] C.Xxencode

[D ] D.Uuencode

**正确**解析：暂无

3、【单选】上一问中的编码，基于什么运算进行编码

[A ] A.二进制

[ ] B.十进制

[ ] C.ASCII码

[ ] D.暂无

**正确**解析：暂无

1、【多选】栅栏密码分为哪几种

[X] A.直线型

[X] B.WWW型

[ ] C.V型

[ ] D.Z型

1、【单选】普莱菲儿密码去除了哪个字母?

[ ] A. b

[ ] B.w

[ ] C. v

[ D] D. z

**错误**正确答案： D

解析：暂无

2、【判断】凯撒密码属于多表替换密码

[ ] A.正确

[ B] B.错误

**正确**解析：暂无

1、【单选】仿射密码和希尔密码都涉及了那种数学计算方式?

[ A] A.模运算

[ ] B.线性代数

[ ] C.矩阵

[ ] D.替换表

1、【判断】yafu和factordb可以分解所有大整数N

[ ] A.正确

[ B] B.错误

1、【单选】欧几里得算法又称为_____，常用来_____

[A] A.辗转相除、计算最大公约数

[ ] B.辗转相除、计算最小公倍数

[ ] C.转辗相除、计算最大公约数

[ ] D.转辗相除、计算最小公倍数

1、【单选】RSA的低加密广播攻击利用了

[ ] A.欧几里得算法

[B] B.中国剩余定理

[ ] C.扩展欧几里得算法

[ ] D.费马小定理

1、【单选】padding oracle attack主要针对

[A] A.对称加密的CBC模式

[ ] B.对称加密的ECB模式

[ ] C.非对称加密的CBC模式

[ ] D.非对称加密的ECB模式

1、【多选】序列密码分为哪两种?

[A] A.同步序列密码

[ ] B.同级序列密码

[C] C.异步序列密码

[ ] D.差级序列密码

**正确**解析：暂无

1、【单选】DES与AES的差别是什么?

[ ] A.IV

[ ] B.轮函数结构

[ ] C.ECB、CBC等加密模式

[ ] D.暂无

1、【单选】DES与AES的差别是什么?

[ ] A.IV

[B] B.轮函数结构

[ ] C.ECB、CBC等加密模式

[ ] D.暂无

1、【多选】逆向工程使用的工具有哪些?

[ ] A.vscode

[B] B.ollydbg

[C] C.jeb

[D] D.ida

**正确**解析：暂无

1、【多选】逆向题的解题一般步骤需要做什么?

[ ] A.直接放弃

[B] B.运行 观察程序特征

[C] C.使用IDA或者反编译工具查看

[D] D.使用OD动态调试

**正确**解析：暂无

1、【多选】观察完程序特征后动态调试的工具有哪些?

[A] A.OD

[B] B.x32dbg

[C] C.x64dbg

[ ] D.IDA

**正确**解析：暂无

1、【多选】根据用户名获取flag这类题目的解题方式正确的有?

[A] A.逆向算法 写还原代码

[B] B.写注册机

[ ] C.多次测试

[ ] D.直接运行

**正确**解析：暂无

1、【单选】对于加密算法描述正确的是?

[ ] A.MD5算法可以求逆

[B] B.MD5算法不可以求逆

[ ] C.Tea加密算法在题目中不常见

[ ] D.Base64加密算法在题目中不常见

**正确**解析：暂无

1、【多选】可以查看一个题目中使用了哪些算法的工具有?

[A] A.PEID工具

[B] B.Die

[C] C.exeinfo

[ ] D.jeb

**正确**解析：暂无

1、【多选】对于迷宫题目最好的办法是?

[A] A.使用IDA进行静态分析

[B] B.逆向分析关键代码

[C] C.理清出题人意图 走出迷宫

[ ] D.暴力测试

**正确**解析：暂无

1、【单选】pwn是什么?

[ ] A.漏洞测试

[B] B.软件漏洞挖掘

[ ] C.溢出

[ ] D.渗透测试

**正确**解析：暂无

1、【单选】pwn的解题步骤第一步是什么?

[ ] A.研究程序的保护方法

[B] B.运行程序观察程序特征

[ ] C.使用IDA进行静态分析

[ ] D.反汇编目标软件

1、【单选】与栈溢出对应的保护机制是什么?

[A] A.cannary

[ ] B.ESP

[ ] C.No-eXecute

[ ] D.shellcode

1、【单选】ret2text是什么?

[A] A.执行程序已有的代码

[ ] B.执行程序所需要的依赖

[ ] C.程序生成的代码

[ ] D.执行程序

提交答案

1、【单选】ret2syscalll是什么?

[ ] A.执行程序已有的代码

[ ] B.控制程序生成新程序

[C] C.控制程序执行系统调用来获取shell

[ ] D.执行程序调用系统

1、【单选】什么是动态链接?

[ ] A.运行后加载和链接程序所依赖的共享库的技术

[B] B.一直持续加载和链接程序所依赖的共享库的技术

1、【单选】ret2libc是什么?

[ ] A.控制程序执行的函数

[ ] B.执行程序函数的源代码

[ ] C.控制函数文件

[D] D.控制函数的执行libc中的函数

提交答案

1、【多选】移动逆向题目一般考察参赛选手的技能点有哪些?

[A] A.信息搜集能力

[B] B.Java层代码分析能力

[C] C.算法还原能力

[D] D.应用脱壳，加固分析能力

解析：暂无

# 就业育人项目-能力提升实践课（渗透测试工程师入门）

**OWASP Top 10 (2017)**

- A1 注入漏洞
- A2 失效的身份认证
- A3 敏感数据泄露
- A4 XML 外部实体漏洞
- A5 无效的访问控制
- A6 安全配置错误

- A7 跨站脚本攻击
- A8 不安全的反序列化漏洞

1、【单选】2017年版本OWASP top 10的排位第三位的漏洞是?

[ ] A.注入

[ ] B.失效的身份认证

[C] C.敏感信息泄露

[ ] D.跨站脚本

1、【多选】SQL注入产生的原因包括?

[A] A.不当的类型处理

[B] B.不安全的数据库配置

[C] C.不合理的处理结果查询

[D] D.不当的错误处理

1、【单选】sqlmap是可以getshell

[A] A.正确

[ ] B.错误

[ ] C.无

[ ] D.无

1、【单选】下面哪个语句可以看到数据库的信息?

[ ] A.order by

[ ] B.union select

[C] C.database()

[ ] D.version()

1、【多选】数据库注入绕过方式包括哪些?

[A] A.大小写

[B] B.编码

[C] C.注释符

[D] D.迭代

1、【单选】php://input的利用条件包括?

[ ] A.allow_url_fopen为on

[B] B.allow_url_include为on

[ ] C.php5.5

[ ] D.gpc为on

1、【多选】黑名单校验文件上传时包含哪些点?

[A] A.后缀

[B] B.Content-Type

[C] C.文件头

[ ] D.文件名称

1、【判断】反射型XSS可以盗取管理员的cookie

[ ] A.正确

[B] B.错误

1、【多选】密码常见组合包括?

[A] A.数字或字母

[B] B.生日+姓名

[C] C.短语密码

[D] D.常见管理口令

1、【多选】代码执行函数包括哪些?

[A] A.eval

[B] B.assert

[C] C.preg_replace

[D] D.call_user_func

1、【多选】信息泄露会泄露哪些信息?

[A] A.口令

[B] B.密钥

[C] C.证书

[D] D.会话标识