2021年兰州市职业院校技能大赛中职组

“网络空间安全”赛项规程

一、赛项名称

网络空间安全

二、竞赛目的

通过竞赛，检验参赛选手对网络、服务器系统等网络空间中各个信息系统的安全防护能力，以及分析、处理现场问题的能力。通过本赛项的训练和比赛，培养更多学生掌握网络安全知识与技能，发展成为国家信息安全领域的技术技能人才。引导中等职业学校关注网络安全技术发展趋势和产业应用方向，促进网络信息安全专业建设与教学改革。赛项紧密结合新一代信息产业发展对网络安全应用型人才的需求，促进产教互动、校企融合，增强中职学校学生的新技术学习能力和就业竞争力，助力新一代信息技术产业快速发展。

三、竞赛内容

重点考核参赛选手网络系统安全策略部署、信息保护、网络安全运维管理的综合实践能力，具体包括：

1.参赛选手能够在赛项提供的服务器上配置各种协议和服务，实现网络系统的运行，并根据网络业务需求配置各种安全策略，以满足应用需求。

2.参赛选手能够根据大赛提供的赛项要求，实施网络空间安全防护操作。

3.参赛选手能够根据网络实际运行中面临的安全威胁，确定安全策略并部署实施，防范并制止网络恶意入侵和攻击行为。

4. 参赛选手通过分组混合对抗的形式，能够实时防护自己服务

器，抵御外界的攻击，同时能够对目标进行渗透和攻击。

5.竞赛总时长为 3 个小时，各竞赛阶段安排如下：

序号	内容模块	具体内容	说明
第一阶段	单兵模式系统渗透测试	密码学和 VPN	密码学、IPSec VPN、IKE：PreShared Key（预共享密钥认证）、IKE：PKI（公钥架构认证）、SSL VPN 等。
		操作系统渗透测试及加固	Windows 操作系统渗透测试及加固、Linux 操作系统渗透测试及加固等。
		Web 应用渗透测试及加固	SQL Injection（SQL 注入）漏洞渗透测试及加固、Command Injection（命令注入）漏洞渗透测试及加固、File Upload（文件上传）漏洞渗透测试及加固、Directory Traversing（目录穿越）漏洞渗透测试及加固、XSS（Cross Site Script）漏洞渗透测试及加固、CSRF（Cross Site Request Forgeries）漏洞渗透测试及加固、Session Hijacking（会话劫持）漏洞渗透测试及加固
		网络安全数据分析	能够利用日志收集和分析工具对网络流量收集监控，维护网络安全。
		常用渗透扫描工具使用与脚本语言应用	能够利用如 Nmap、Nessus、metasploit 等常用渗透扫描工具进行信息收集及系统渗透；熟悉 shell，Python 等脚本语言的应用。
第二阶段	攻防对抗	参赛队之间进行对抗演练	Windows/Linux 操作系统安全攻防、Web 应用/数据库安全攻防等。

7.竞赛分值权重和时间安排

序号	内容模块	分值权重	阶段时间
第一阶段	单兵模式系统渗透测试	70%	100 分钟
备战阶段	攻防对抗准备工作	0%	20 分钟
第二阶段	攻防对抗	30%	60 分钟

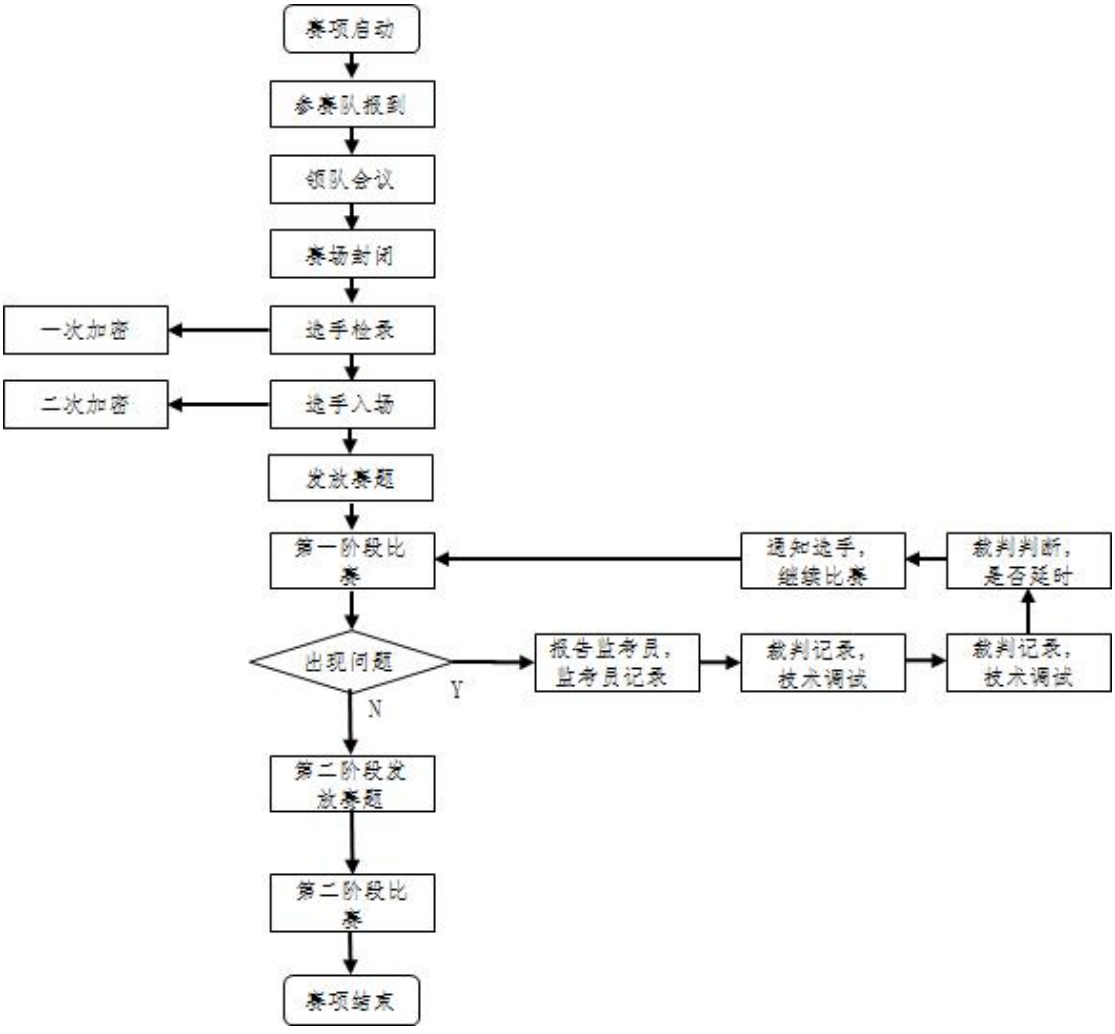
四、竞赛方式

1.本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。

2.每个参赛队由 2 名选手组成，每个参赛队限报 1 名指导教师。

五、竞赛流程

（一）竞赛流程图



（二）竞赛时间表

比赛限定在1天内进行，比赛场次为1场，赛项竞赛时间为3小时，具体日程安排以赛项说明会以赛项指南为准。

六、竞赛试题

（一）赛项执委会专家组下设的命题组负责本赛项命题工作。

（二）样题见附件。

七、竞赛规则

（一）报名资格

参赛选手必须是兰州市县区属公办、民办中等职业学校（含技工学校）具有正式学籍的在校生，年龄不超过21周岁，获得过省赛一、二、三等奖的选手不得参加本次市级大赛。如发现参赛选手资格不符，大赛组委会将取消其参赛资格，通报批评并严肃追责。

（二）竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

（三）竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前10分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

（六）竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损

坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非参赛选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（七）竞赛结束（或提前完成）后，参赛选手要确认已成功提交所有竞赛文档，裁判员与参赛选手一起签字确认，参赛选手在确认后不得再进行任何操作。

八、竞赛环境

1.竞赛场地。竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和通风；提供稳定的水、电和供电应急设备。同时提供所有指导教师休息室 1 间。

2.竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备比赛所需的软硬件平台，为参赛队提供标准竞赛设备。

3.竞赛工位。竞赛现场各个工作区配备单相 220V/3A 以上交流电源。每个比赛工位上标明编号。每个比赛间配有工作台，用于摆放计算机和其它调试设备工具等。配备 2 把工作椅（凳）。

4.技术支持区为参赛选手比赛提供网络环境部署和网络安全防范。

5.服务区提供医疗等服务保障。

6.竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线，每个相邻竞赛赛位隔离线之间间隔不低于 1.5 米。

九、技术规范

该赛项涉及的信息网络安全工程在设计、组建过程中，主要有以下 7 项国家标准，参赛选手在实施竞赛项目中要求遵循如下规范：

序号	标准号	中文标准名称
1	GB 17859-1999	《计算机信息系统安全保护等级划分准则》

2	GB/T 20271-2006	《信息安全技术信息系统通用安全技术要求》
3	GB/T 20270-2006	《信息安全技术网络基础安全技术要求》
4	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
5	GB/T 20273-2006	《信息安全技术数据库管理系统安全技术要求》
6	GA/T 671-2006	《信息安全技术终端计算机系统安全等级技术要求》
7	GB/T 20269-2006	《信息安全技术信息系统安全管理要求》

十、技术平台

（一）比赛器材

序号	设备名称	数量	设备型号
1	网络空间安全技能评测平台	1	中科软磐云 PY-B7 磐云 PY-B7 为 1U 设备，2 个千兆以太口，Intel 至强处理器,16G 内存,120G SSD +1T SATA 硬盘。支持多用户并发在线比赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板功能,为学员提供单兵闯关、分组混战和夺旗竞速等实际对战模式，能够提供 29 种不同级别的攻防场景。
2	PC 机	2	CPU 主频>=3.5GHZ,>=四核心 八线程；内存>=8G；硬盘>=1T；支持硬件虚拟化；具有串口或者提供 USB 转串口配置线缆

（二）软件技术平台：

比赛的应用系统环境主要以 Windows 和 Linux 系统为主，涉及如下版本：

1）物理机安装操作系统：Windows 7。

2）虚拟机安装操作系统：

✓ Windows 系统：Windows XP、Windows 7、Windows2003 Server、

Windows2008 Server（根据命题确定）。

- ✓ Linux 系统：Ubuntu、Debian、CentOS、Kali（根据命题确定）。

3）比赛提供 Putty 作为终端。

十一、成绩评定

（一）裁判工作原则

赛前建立健全裁判组。裁判组为裁判长负责制，并设有专职督导人员 1-2 名，负责比赛过程全程监督，防止营私舞弊。

本赛项全部分数由计算机自动评分，因此只需进行两次加密，加密后参赛选手中途不得擅自离开赛场。分别由 2 组加密裁判组织实施加密工作，管理加密结果。监督员全程监督加密过程。

第一组加密裁判,组织参赛选手进行第一次抽签,产生参赛编号,替换选手参赛证等个人身份信息,填写一次加密记录表连同选手参赛证等个人身份信息证件，装入一次加密结果密封袋中单独保管。

第二组加密裁判，组织参赛选手进行第二次抽签，确定赛位号，替换选手参赛编号，填写二次加密记录表连同选手参赛编号，装入二次加密结果密封袋中单独保管。

所有加密结果密封袋的封条均需相应加密裁判和监督人员签字。密封袋在监督人员监督下由加密裁判放置于保密室的保险柜中保存。

（二）成绩产生办法

计算机自动评分，由裁判长负责将竞赛两个阶段的分数汇总，产生每赛位号的对应成绩。

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平：

竞赛阶段	阶段名称	任务阶	竞赛任务	分值	评分方式

		段			
第一阶段 权重 70%	单兵模式系统渗透测试	任务 1	根据赛题确定内容	20	机考评分
		任务 2	根据赛题确定内容	20	机考评分
		任务 3	根据赛题确定内容	30	机考评分
第二阶段 权重 30%	分组对抗	系统攻防		30	机考评分

参赛选手应体现团队风貌、团队协作与沟通、组织与管理能力和工作计划能力等，并注意相关文档的准确性与规范性。

竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判组按照规定扣减相应分数，情节严重的取消竞赛资格。

十二、奖项设定

本赛项为团体赛，依照实际参赛队数量确定奖项：一等奖占参赛队总数的 15%，二等奖占参赛队总数的 25%，三等奖占参赛队总数的 35%。

十三、竞赛须知

（一）参赛选手须知

1. 各参赛选手要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2. 参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

3. 参赛选手应按照规定时间抵达赛场，凭统一印制的参赛证、有效身份证件检录，按要求入场，不得迟到早退。请勿携带任何电子

设备及其他资料、用品进入赛场。

4．参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

5．参赛选手应增强角色意识，科学合理做好时间分配。

6. 参赛选手应按有关要求在指定位置就坐。

7.参赛选手须在确认竞赛内容和现场设备等无误后开始竞赛。在竞赛过程中，确因计算机软件或硬件故障，致使操作无法继续的，经项目裁判长确认，予以启用备用计算机。

8. 各参赛选手必须按规范要求操作竞赛设备。一旦出现较严重的安全事故，经总裁判长批准后将立即取消其参赛资格。

9.参赛选手需详细阅读赛题中竞赛文档命名的要求，不得在提交的竞赛文档中标识出任何关于参赛选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

10. 竞赛时间终了，选手应全体起立，结束操作，将资料和工具整齐摆放在操作平台上，经工作人员清点后可离开赛场。离开赛场时不得带走任何资料。

11.在竞赛期间，未经执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

12.参赛选手若对竞赛过程有异议，在规定的时间内经由领队向赛项仲裁工作组提出书面报告。

（二）指导教师须知

1.各参赛代表队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2.各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3.竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4.参赛代表队若对竞赛过程有异议，在规定的时间内由领队向赛项仲裁工作组提出书面报告。

5.对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服而停止竞赛，否则以弃权处理。

6.指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

7. 参赛选手领队应对本队参赛选手和指导教师的参赛期间安全负责，参赛学校须为参赛选手和指导教师购买意外保险。

8. 领队和指导教师应在赛后做好赛事总结和工作总结。

（三）工作人员须知

1. 树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项执委会的领导下，按照各自职责分工和要求认真做好岗位工作。

2. 所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3. 注意文明礼貌，保持良好形象，熟悉赛项指南。

4. 自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5. 提前30分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

6. 熟悉竞赛规程，严格按照工作程序和有关规定办事，遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

7. 工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8. 保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。

附件：样题

“网络空间安全”项目竞赛任务书（样题）

一、赛项时间

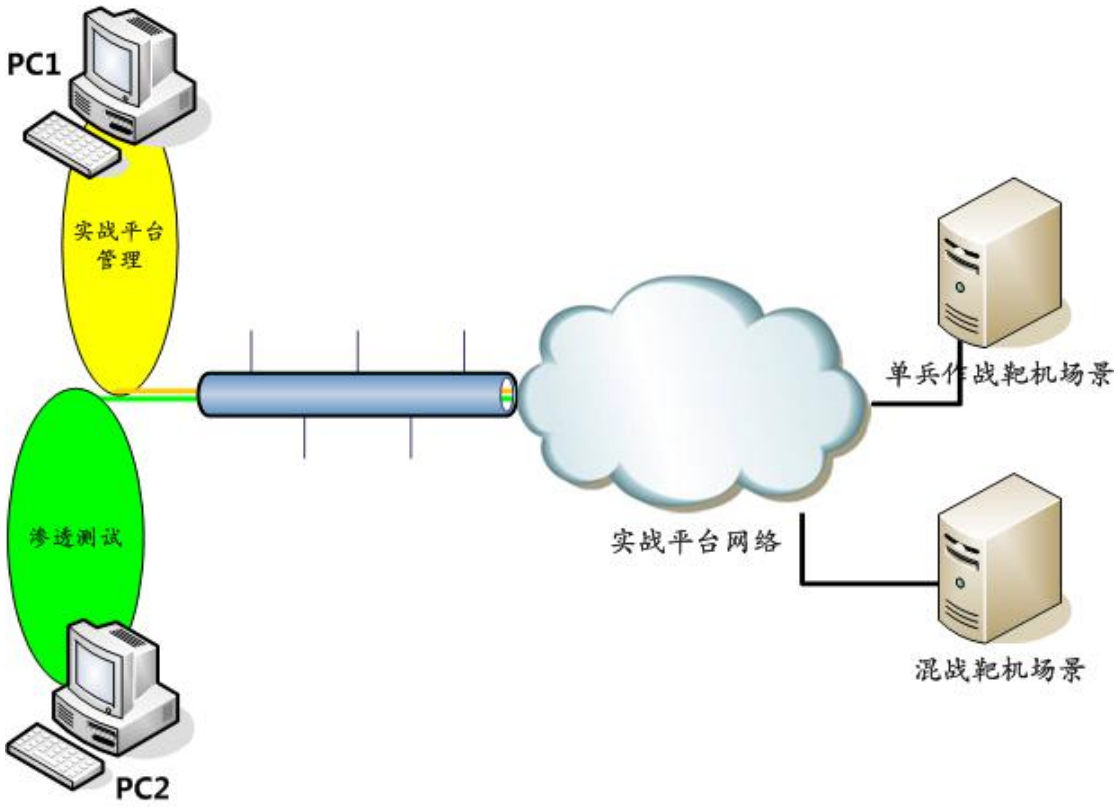
9:00-12:00，共计 3 小时。

二、赛项信息

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段 单兵模式系统渗透测试	任务 1	SQL 注入攻防	09:00-11:00	25
	任务 2	XSS 和 CSRF 攻防		25
	任务 3	命令注入与文件包含攻防		20
第二阶段 分组对抗	系统攻防		11:00-12:00	30

（一）赛项环境设置

1. 网络拓扑图



2. IP 地址规划表

设备名称	接口	IP 地址	互联	可用 IP 数量
PC-1：实战平台管理机	EthX	x.x.x.x/x	与实战平台管理网络相连	见赛场 IP 参数表
PC-2：渗透测试机	EthY	x.x.x.x/x	与渗透测试网络相连	见赛场 IP 参数表
服务器场景	无	详见赛题部分		见赛场 IP 参数表
备注	1.赛题可用 IP 地址范围见《赛场 IP 参数表》; 2.具体网络连接接口见《赛场 IP 参数表》-“赛场互联接口参数表”; 3.设备互联网段内可用地址数量见《赛场 IP 参数表》; 4.IP 地址分配要求，最节省 IP 地址，子网有效地址规划遵循 2n-2 的原则; 5.参赛选手按照《赛场 IP 参数表》要求，自行分配 IP 地址段、设备互联接口; 6.将分配的 IP 地址段和接口填入《赛场 IP 参数表》中（《赛场 IP 参数表》电子文件存于 U 盘“第一阶段”文件夹中，请填写完整后提交。）			

（二）第一阶段任务书（70 分）

任务 1：SQL 注入攻防

任务环境说明:

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2;

服务器场景安装服务/工具 2：Php6;

服务器场景安装服务/工具 3：Microsoft SqlServer2000;

服务器场景安装服务/工具 4：EditPlus;

1. 访问 WebServ2003 服务器场景,进入 login.php 页面,分析该页面源程序,找到提交的变量名，并将该变量名作为 Flag 提交;

2. 对该任务题目 1 页面注入点进行 SQL 注入渗透测试,使该 Web 站点可通过任意用户名登录，并将登录密码作为 Flag 提交;

3. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 loginAuth.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御

SQL 注入，并将修改后的 PHP 源程序中的 Flag 提交；

4. 再次对该任务题目 1 页面注入点进行渗透测试,验证此次利用该注入点对 WebServ2003 服务器场景进行 SQL 注入渗透测试无效，并将 Web 页面回显内容作为 Flag 提交；

5. 访问 WebServ2003 服务器场景，"/"->"Employee Information Query"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

6. 对该任务题目 5 页面注入点进行渗透测试，根据输入“%”以及“_”的返回结果确定是注入点，Web 页面回显作为 Flag 提交；

7. 通过对该任务题目 5 页面注入点进行 SQL 注入渗透测试，删除 WebServ2003 服务器场景的 C:\目录下的 1.txt 文档,并将注入代码作为 Flag 提交；

8. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 QueryCtrl.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 SQL 注入渗透测试，并将修改后的 PHP 源程序中的 Flag 提交；

9. 再次对该任务题目 5 页面注入点进行渗透测试,验证此次利用注入点对该 WebServ2003 服务器场景进行 SQL 注入渗透测试无效，并将 Web 页面回显内容作为 Flag 提交。

任务 2：XSS 和 CSRF 攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2；

服务器场景安装服务/工具 2：Php6；

服务器场景安装服务/工具 3：Microsoft SqlServer2000；

服务器场景安装服务/工具 4：EditPlus；

1. 访问 WebServ2003 服务器场景，"/"->" Employee Message Board"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

2. 对该任务题目 1 页面注入点进行 XSS 渗透测试，并进入"/"->" Employee Message Board"->"Display Message"页面，根据该页面的显示，确定是注入点，并将 Web 页面回显内容作为 Flag 提交；

3. 对该任务题目 1 页面注入点进行渗透测试，使"/"->" Employee Message

Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序：http://hacker.org/TrojanHorse.exe，并将注入代码内容作为 Flag 提交；

4. 通过 IIS 搭建网站（http://hacker.org/），并通过 PC2 生成木马程序 TrojanHorse.exe，将该程序复制到网站（http://hacker.org/）的 WWW 根目录下，并将该网站标题作为 Flag 提交；

5. 当"/"->" Employee Message Board"->"Display Message"页面的访问者执行网站（http://hacker.org/）中的木马程序 TrojanHorse.exe 以后，访问者主机需要被 PC-3 远程控制，打开访问者主机的 CMD.exe 命令行窗口，并将该操作结果回显作为 Flag 提交；

6. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 insert.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 XSS 渗透测试，并将修改后的 PHP 源程序中的 Flag 提交；

7. 再次对该任务题目 1 页面注入点进行渗透测试,验证此次利用该注入点对 WebServ2003 服务器场景进行 XSS 渗透测试无效，并将 Web 页面回显作为 Flag 提交；

8. 访问 WebServ2003 服务器场景，"/"->" Shopping Hall"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

9. 对该任务题目 1 页面注入点进行渗透测试，使"/"->" Employee Message Board"->"Display Message"页面的访问者向页面 ShoppingProcess.php 提交参数 goods=cpu&quantity=999999，查看"/"->"PurchasedGoods.php 页面，并将注入代码作为 Flag 提交；

10. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 DisplayMessage.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御 CSRF 渗透测试，并将修改后的源程序中的 Flag 提交；

11. 再次对该任务题目 1 页面注入点进行渗透测试,验证此次利用该注入点对 WebServ2003 服务器场景进行 CSRF 渗透测试无效,并将 Web 页面回显内容作为 Flag 提交；

任务 3：命令注入与文件包含攻防

任务环境说明：

服务器场景：WebServ2003

服务器场景操作系统：Microsoft Windows2003 Server

服务器场景安装服务/工具 1：Apache2.2；

服务器场景安装服务/工具 2：Php6；

服务器场景安装服务/工具 3：Microsoft SqlServer2000；

服务器场景安装服务/工具 4：EditPlus；

1. Web 访问 WebServ2003 服务器场景，"/"->" Display Directory"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

2. 对该任务题目 1 页面注入点进行渗透测试，使页面 DisplayDirectoryCtrl.php 回显 C:\Windows 目录内容的同时，对 WebServ2003 服务器场景添加账号“Hacker”，将该账号加入管理员组，并将注入代码作为 Flag 提交；

3. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 DisplayDirectoryCtrl.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御命令注入渗透测试，并将修改后的源程序中的 Flag 提交；

4. 再次对该任务题目 1 页面注入点进行渗透测试，验证此次利用注入点对 WebServ2003 服务器场景进行命令注入渗透测试无效，并将 Web 页面回显作为 Flag 提交；

5. Web 访问 WebServ2003 服务器场景，"/"->" Display Uploaded's File Content"，分析该页面源程序，找到提交的变量名，并将该变量名作为 Flag 提交；

6. 对该任务题目 5 页面注入点进行渗透测试，使页面 DisplayFileCtrl.php 回显 WebServ2003 服务器场景访问日志文件：AppServ/Apache2.2/logs/access.log 的内容，并将注入代码作为 Flag 提交；

7. 进入 WebServ2003 服务器场景的 C:\AppServ\www 目录，找到 DisplayFileCtrl.php 程序，使用 EditPlus 工具分析并修改 PHP 源程序，使之可以抵御文件包含渗透测试，并将修改后的源程序中的 Flag 提交；

8. 再次对该任务题目 5 页面注入点进行渗透测试，验证此次利用注入点对 WebServ2003 服务器场景进行文件包含渗透测试无效，并将 Web 页面回显作为 Flag 提交。

（三）第二阶段任务书：分组对抗（30 分）

假定各位选手是某公司的系统管理员，负责服务器（受保护服务器 IP、管理员账号见现场发放的参数表）的维护，该服务器可能存在着各种问题和漏洞（见漏洞列表）。你需要尽快对服务器进行加固，十五分钟之后将会有很多黑客对这台服务器进行攻击。

提示 1：该题不需要保存文档；

提示 2：服务器中的漏洞可能是常规漏洞也可能是系统漏洞；

提示 3：加固常规漏洞；

提示 4：对其它参赛队系统进行渗透测试，取得 FLAG 值并提交到裁判服务器。

十五分钟之后，各位选手将真正进入分组对抗环节。

注意事项：

注意 1：任何时候不能关闭 80 端口，否则将判令停止比赛，该阶段分数为 0 分；

注意 2：不能对裁判服务器进行攻击，否则将判令停止比赛，该阶段分数为 0 分。

注意 3：在加固阶段（前十五分钟，具体听现场裁判指令）不得对任何服务器进行攻击，否则将判令攻击者停止比赛，该阶段分数为 0 分。

注意 4：FLAG 值为每台受保护服务器的唯一性标识，每台受保护服务器仅有一个。

在这个环节里，各位选手需要继续保护你的服务器免受各类黑客的攻击，你可以继续加固你的服务器，你也可以选择攻击其他组的保护服务器（其他服务器网段见现场发放的参数表）。

漏洞列表：

1. 靶机上的网站可能存在命令注入的漏洞，要求选手找到命令注入的相关漏洞，利用此漏洞获取一定权限。

2. 靶机上的网站可能存在文件上传漏洞，要求选手找到文件上传的相关漏洞，利用此漏洞获取一定权限

3. 靶机上的网站可能存在文件包含漏洞，要求选手找到文件包含的相关漏洞，与别的漏洞相结合获取一定权限并进行提权

4. 操作系统提供的服务可能存在远程代码执行的漏洞，要求用户找到远程代码执行的服务，并利用此漏洞获取系统权限。

5. 操作系统提供的服务可能包含了缓冲区溢出漏洞,要求用户找到缓冲区溢出漏洞的服务，并利用此漏洞获取系统权限。

6. 操作系统中可能存在系统后门，选手可以找到后门，并利用预留的后门直接获取到系统权限。

选手通过以上的所有漏洞点，最后得到其他选手靶机的最高权限，并获取到其他选手靶机上的FLAG值进行提交。

样题完