第十一届全国大学生信息安全竞赛创新实践能力赛
决赛阶段应用场景开发需求

本次创新实践能力赛决赛阶段的应用场景开发需求分为二进制网络服务、Web应用服务两类场景，赛队需要根据场景开发的功能特性需求，选择其中的一个场景，开发出符合所要求功能特性的安全应用，并预设创新性的网络安全挑战（挑战其他赛队的网络安全实践能力），构建出在决赛阶段赛时环节中使用的靶标环境。

一、二进制网络服务PWN场景（消息队列实现RPC服务）

1. 基于消息队列实现RPC服务，例如启动后台程序完成耗时长的功能等，将Web、App的后端任务执行部分分离，将服务器压力分散，类似的有`rabbitmq`等。
2. 实现能通过Checker程序检查的服务程序（比赛时二进制程序提供给参赛队），确保基本功能完整（服务程序python实现示例`service_example.py`）；
3. 必须包含预设的安全漏洞（创新性安全挑战即为对预设安全漏洞的某种检测和利用技巧），不限制漏洞类型；
4. 采用C/C++语言实现，提供源码和编译环境，编译运行在x64或ARM或MIPS架构上；
5. 服务端口统一为`1337`，请不要使用其他端口。

附件：Checker程序（包含服务程序Python示例），出题格式要求模板
附件下载地址：链接：https://share.weiyun.com/5aQdmE0 密码：2mj8kj

二、Web应用服务场景（电子商城限时抢购活动）

1. 实现电子商场Web应用，其中必须包含有限时抢购活动，比赛时Web访问URL提供给参赛队。
2. 所实现的基本功能要求包括：用户注册、用户登录、找回密码/修改密码；推荐其他用户注册并获得积分奖励；电子商场显示若干商品，用户可选购商品进入购物车，使用积分结账购物；每小时限时抢购秒杀活动
3. 用户注册、登录和找回密码功能需要实现人机识别验证码的特性，其中人机识别验证码必须采用附件中的验证码数据集；

4. 采用PHP/Python/Java等语言实现，提供源码和部署环境，运行在Apache或Nginx或Weblogic等Web服务器；后段必须有数据库，如mysql、sqlite、mongodb等。
5. 必须包含预设的Web应用安全漏洞（创新性安全挑战即为对预设安全漏洞的某种检测和利用技巧），不限制Web应用安全漏洞类型；
6. 业务逻辑上设计防止“薅羊毛”的特性，植入创新性网络安全挑战，比如必须要进行某些绕过防止“薅羊毛”特性的攻击操作后，才能到达漏洞利用条件（如某些高等级用户才具备的功能特性，其中才包含网络安全挑战预设安全漏洞）
7. 服务端口统一为’80’，请不要使用其他端口。
附件：验证码数据集，Checker程序，出题格式要求模板等
验证码测试数据集下载地址：链接：https://share.weiyun.com/5QlpOIi 密码：h6uvtf
WEB要求模板+Checker程序：链接：https://share.weiyun.com/5h1VH5C 密码：uct9dn

提交靶标环境要求

1. 赛题环境提供Dockerfile + docker-compose容器环境，平台方使用`docker-compose up -d`启动选手提供的环境

（docker环境内初始对于二进制网络服务**只包含源码，不要预编译二进制**，编译命令和运行命令写入Dockerfile，由Docker自动编译和运行）；
2. Flag可即时更新，不接受固定flag的赛题。请在文档内提供更新flag的命令，例如`echo xxx > /home/ctf/flag`等；
3. 在Flag位置使用初始Flag为`CISCN{this_is_a_sample_flag}`；
4. 提交靶标环境格式请参照`challenge_template`文件夹下的出题格式要求。
5. 提交3个Hint并标注次序，此3个Hint会在BreakIt环节中按照1/4时间如无队伍解出放第一个Hint，1/2时间如无队伍解出放第二个Hint，3/4时间如无队伍解出放第三个Hint，如有队伍解出不再放后续Hint的约定放出
6. 提交EXP脚本的源代码行数小于300行（采用标准的编码规范，不特意进行代码混淆变形缩略行等操作），其中不包含和靶标环境预先共享的key、弱口令列表等信息。

7. 提交Writeup请详细描述创新性网络安全挑战的解题步骤、设计思路、创新性以及考察的技能、技巧和思维点。

提交截止时间：

2018年5月24日23:59分

提交途径：

发送邮件和附件至：ciscn2018@126.com，请在邮件标题中标明赛区、战队和场景类型（Pwn、Web）

第十一届全国大学生信息安全竞赛

创新实践能力赛技术委员会

2018年5月12日