

2020 年第二届“网鼎杯”网络安全大赛

官方资格赛参赛指引

一、大赛背景

第二届“网鼎杯”网络安全大赛（以下简称“第二届‘网鼎杯’大赛”）是由国家网络与信息安全信息通报中心、深圳市人民政府、广东省公安厅联合支持，深信服科技股份有限公司、北京永信至诚科技股份有限公司联合主办，阿里巴巴（中国）网络技术有限公司、百度在线网络技术（北京）有限公司、奇安信科技集团股份有限公司、清华大学网络科学与网络空间研究院、深圳市腾讯计算机系统有限公司、中国科学院信息工程研究所联合协办的国家顶级网络安全赛事。

“网鼎杯”网络安全大赛 2018 年在北京举办了第一届，共吸引了全国 7000 支队伍、2.25 万人参赛，是我国迄今为止规模最大、覆盖面最广的一次高水平网络安全大赛，这对于进一步磨砺网络安全攻防能力，发现网络安全专门人才，提升全社会网络安全意识具有重要意义。

按照“网鼎杯”大赛两年一届的举办原则，第二届“网鼎杯”大赛线下半决赛、总决赛和颁奖典礼定于 2020 年 6 月 19 日至 21 日在广东省深圳市举办。

二、比赛时间

1. 官方资格赛（青龙组）：5 月 10 日 09:00 - 17:00 参赛行业：高

等院校、职业院校、社会参赛队伍

2. 官方资格赛（白虎组）：5月14日 09:00 - 17:00 参赛行业：通信、交通、国防、政务部门等单位
3. 官方资格赛（朱雀组）：5月17日 09:00 - 17:00 参赛行业：能源、金融、政法、其他行业单位
4. 官方资格赛（玄武组）：5月21日 09:00 - 17:00 参赛行业：科研机构、科技企业、互联网公司、网安企业等单位

三、比赛地址

比赛登录地址：www.wangdingcup.com

四、比赛方式

各参赛队员登录第二届“网鼎杯”大赛官网，进入到赛题界面，以团队为单位进行答题，每道赛题均内置1个flag，可以多次提交答案，直到提交了正确答案或比赛结束或被禁赛。每道题目有不同的网络或应用场景，参赛者需要采用在线操作或离线分析的方式，获取到埋藏在题目中的特殊字符串（俗称“flag”），通过在平台提交正确的flag获取得分。未提交或提交错误不得分。比赛结束后8小时内，每组前240名参赛队需提交每道赛题详细的解题报告（WriteUp），经组委会审核后，确定各参赛队最终得分和排名。

五、积分规则（动态积分）

每一道题的初始分数相同，随着其被解答出来的队伍数增加，其分数减少，所有解出此题的队伍所持有的分数都会动态减少。如下图

所示，如果没有队伍解出来，该题的初始分为 500，



如果陆续有队伍解出题目，题目的分数就会减少（如下图），所有解出该题的队伍的分数也会随之减少。



六、考核范围

赛题类型主要包括：逆向、漏洞挖掘与利用、Web 渗透、密码、隐写、安全编程等类别，考察参赛者不同维度的网络安全理论、技术水平。

	主要考察范围
Web 安全	涉及 SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、文件上传、文件包含、框架安全、PHP 常见漏洞、代码审计等

逆向分析与移动安全	涉及 Windows、Linux、Android 平台的多种编程技术，要求利用常用工具对源代码及二进制文件进行逆向分析，掌握 Android 移动应用 APK 文件的逆向分析，掌握加解密、内核编程、算法、反调试和代码混淆技术等
二进制漏洞挖掘利用	涉及 Linux 平台应用二进制漏洞挖掘与利用等
密码学	涉及古典密码学、现代密码学、国密算法等，包括单表替换加密、多表替换加密、对称加密、非对称加密、哈希函数、数字签名等
杂项	涉及信息搜集、编码分析、取证分析、隐写分析等

七、晋级规则

1. 比赛共分三轮，分别是官方线上资格赛、线下半决赛、总决赛。其中，官方线上资格赛和线下半决赛为晋级赛。

2. 参加官方线上资格赛的参赛队伍，按照行业属性分成四组，分别是青龙组（高等院校、职业院校、社会参赛队伍）、白虎组（通信、交通、国防、政务部门等单位）、朱雀组（能源、金融、政法、其他行业单位）、玄武组（科研机构、科技企业、互联网企业、网安企业等单位）。通过官方线上资格赛晋级线下半决赛。晋级参赛队伍名额分别为：青龙组 130 支，白虎组 130 支，朱雀组 140 支，玄武组 100 支。

3. 同一单位（跨区域集团公司按集团算做一个单位）晋级线下半

决赛的队伍总数不超过 5 支。

(具体信息详见官网《2020 年第二届“网鼎杯”网络安全大赛规则(发布稿)》)

八、平台界面说明

1. 平台登录

第二届“网鼎杯”大赛工作组将会在官方资格赛开赛前给参加本场比赛的战队队长发送一条赛前通知短信，请各战队队长注意查收。如未接收到相关短信，请联系第二届“网鼎杯”大赛工作人员，联系方式详见底部。



竞赛登陆界面

“用户名”处输入：您在报名表中填写的参赛选手手机号；

“密码”处输入：该手机号对应官网账号密码；

“验证码”处输入：右侧图案中数字及字母（不区分大小写）；

点击“登录”，即可。如果遇到问题，您可以联系第二届“网鼎杯”大赛工作人员，联系方式详见底部。

2. 比赛公告

该比赛公告内容较多，右侧有滚动条，请仔细阅读。



3. 比赛题目

点击题目图标进入题目

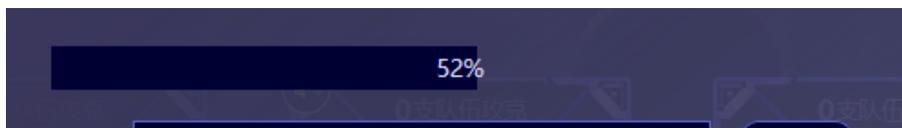


4. Docker 容器下发

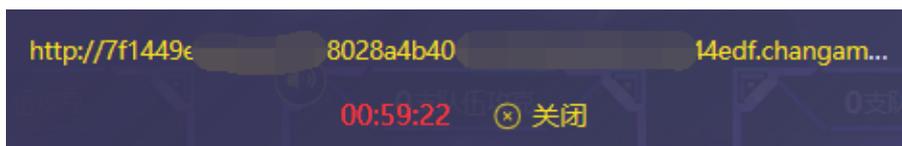
Docker 是一个开源的应用容器引擎，我们的部分赛题部署在使用 Docker 技术的容器当中，当您打开一道 Docker 容器下发的题目：



点击“下发题目”，将有进度条加载



加载后，将呈现一个链接



点击链接访问，即可开始做答。

如果您打开页面，显示如下：



这可能是由于容器开启需要一定时间，可稍候尝试刷新页面，若依旧无法打开，可返回平台点击“重新下发”。



本次比赛规定：每个队伍同时只能下发一个容器。请由成功申请下发容器的队员，用自己的账号提交 flag。

5. 提交 flag

当您打开一个题目，如下图：

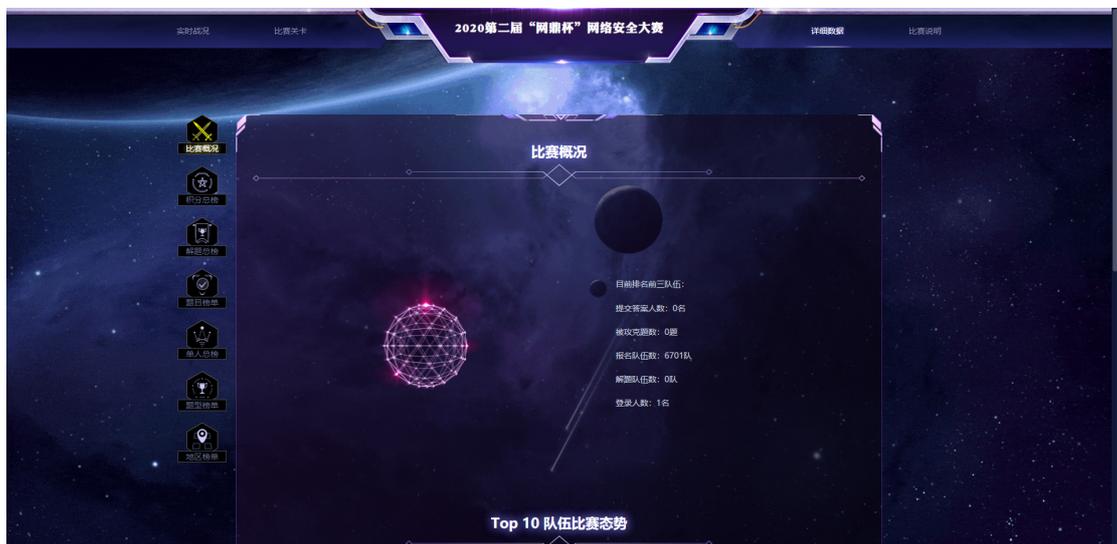


参赛团队通过漏洞挖掘与利用、代码分析等方式，从题目环境中得到一串具有一定格式的字符串或其他内容，并将其在平台上提交，从而夺得分数。

而这个一定格式的字符串，我们称之为 flag，例如图示中 Flag 框中的 `flag{ChunQiuGame}`，常见的 flag 格式是由 `flag{}` 给框住，提交的时候一般需要包含 `flag{}` 的整体内容，如果 flag 有其他的特殊格式要求，一般在题目的描述里会提及到。



实时战况界面



详细数据界面——比赛概况



详细数据界面——积分总榜

实时战况 比赛关卡 **2020第二届“网鼎杯”网络安全大赛** 详细数据 比赛说明

解题总榜

输入队伍名称查询

排名	队伍名	总分	Crypto		Web	
			1	2	3	3
1	T305158	417	✓			
2	T305163	417	✓			
3	T305175	417	✓			
4	T305181	417	✓			
5	T305222	417	✓			

共 1 页

详细数据界面——解题总榜

实时战况 比赛关卡 **2020第二届“网鼎杯”网络安全大赛** 详细数据 比赛说明

题目榜单

输入题目名称查询

全部 Misc Crypto PWN Reverse Web

序号	题目名称	题目类型	攻克队伍数	题目分值
1	赛b题目 (普通题目)	Crypto	5	417
2	赛c题目 (docker题目)	Web	0	500
3	赛d题目 (docker 动态答案)	Web	0	500

共 1 页

详细数据界面——题目榜单

实时战况 比赛关卡 **2020第二届“网鼎杯”网络安全大赛** 详细数据 比赛说明

单人总榜

所属行业: 全部 高等院校 职业院校 社会参赛队伍

输入队伍名称查询

排名	姓名	队伍名	总分	个人强项	解题数量	一击数量
1	U5057810	T305158	417	Crypto	1	1
2	U5690493	T305163	417	Crypto	1	0
3	U6193081	T305175	417	Crypto	1	0
4	U5544446	T305181	417	Crypto	1	0
5	U4891552	T305222	417	Crypto	1	0

共 1 页

详细数据界面——单人总榜



详细数据界面——题型榜单



详细数据界面——地区榜单

九、比赛说明

1. 网鼎杯是国家级网络安全大赛。为确保大赛公平、公正、公开举办，公安机关将依法查处和打击对比赛平台进行恶意攻击的人员、组织。

2. 关于 Docker 容器下发：每个队伍同时只能下发一个容器。请由成功申请下发容器的队员，用自己的账号提交 flag。容器下发后，

如访问不到地址请稍候重试刷新，如果提示错误可稍后再重新申请下发。

3. 选手在解题过程中，如遇到需要输入 token 的题目，请使用本队伍的唯一 token（在平台左上角处），该 token 为队伍的唯一标识，随便乱输视该 payload 为无效。请各参赛者妥善保护好本队伍 token 信息，输入其他队伍的 token，两队同时将被视为作弊处理。

4. 比赛排名：按分数高低进行实时排名，分数相同情况下以成功提交正确 flag 的时间先后排序。

5. WriteUp 提交时间：比赛结束后，请积分榜前 240 名的队伍于比赛结束后 8 小时内提交完整的解题思路（Writeup），逾期提交或不提交视为放弃本次比赛排名。

6. 友情提醒：本次比赛进行严格的作弊审查制度，所有破坏比赛公平性的行为一经发现确认，将取消比赛成绩。

7. 关于比赛收费：第二届“网鼎杯”大赛不会以任何名义向参赛选手收取任何费用，如有任何人以第二届“网鼎杯”大赛组委会、工作组名义向您收取费用，请立即联系工作人员。

十、联系我们

如您在使用过程中有任何问题，可通过以下方式与我们沟通

电 话：010-50866160（工作时间 工作日 9:00-18:00）

邮 箱：wdc@wangdingcup.com（工作时间 工作日 9:00-18:00）

Q Q：3624154301（工作时间 工作日 9:00-18:00）