

CTF竞赛介绍及刷题网址更新---2020.08

原创

RiskAI 于 2020-08-15 14:57:26 发布 7402 收藏 165

文章标签: [CTF 夺旗赛](#) [网络安全竞赛](#) [DEFCON](#) [CTF刷题](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/jhsword/article/details/108021024>

版权



[黑客技术&网络安全 专栏收录该内容](#)

3 篇文章 1 订阅

订阅专栏

CTF (Capture The Flag) 中文一般译作夺旗赛, 在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会, 以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今, 已经成为全球范围网络安全圈流行的竞赛形式, 2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地, **DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛, 类似于CTF赛场中的“世界杯”。**

对于 CTF 更详细的介绍参见: [百度百科](#)

以下介绍几个常用的 CTF 刷题网址 (截至 **2020.08.15** 可正常访问的网站)。

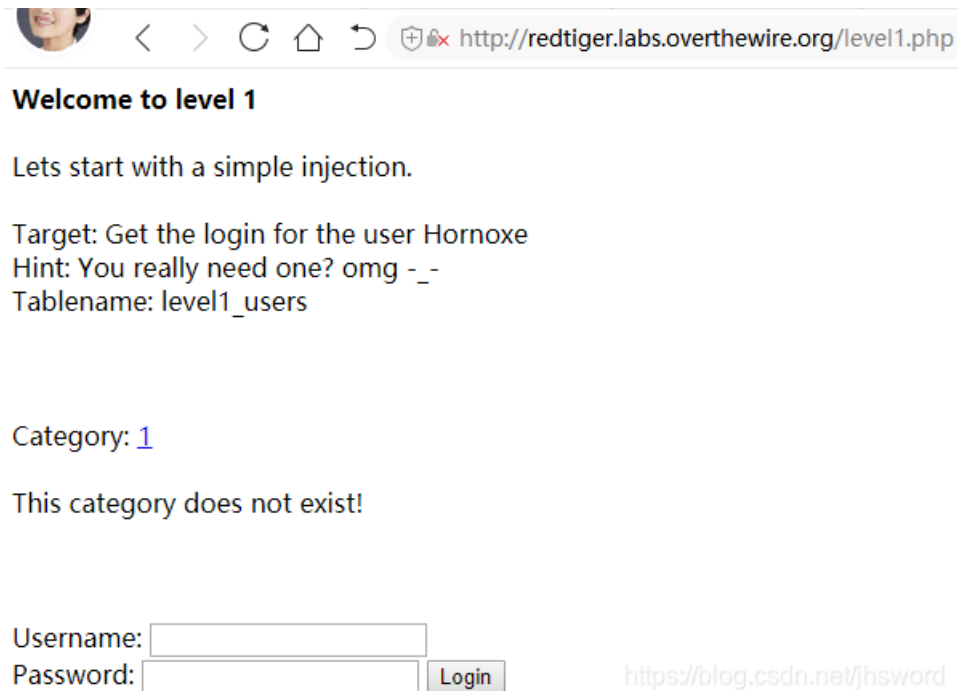
文章目录

1. [RedTigers-Hackit](#)
 2. [XCTF\(攻防世界\)竞赛平台](#)
 3. [网络信息安全攻防学习平台](#)
 4. [OWASP 中国](#)
 5. [实验吧CTF训练营](#)
 6. [全国大学生信息安全竞赛官方网站](#)
 7. [MS09067WEB靶场](#)
 8. [合天网安实验室](#)
 9. [封神台](#)
 10. [SQL Fiddle在线练习](#)
 11. [BUUCTF](#)
 12. [CTFHUB](#)
- [已停止访问\(以前著名\)CTF网站](#)
- [参考](#)

1. RedTigers-Hackit

官网: <http://redtiger.labs.overthewire.org/>

RedTigers-Hackit是一个训练SQLi（SQL注入漏洞）和PHP方面的网站。



The screenshot shows a web browser window with the URL <http://redtiger.labs.overthewire.org/level1.php>. The page content includes:

- Welcome to level 1**
- Lets start with a simple injection.
- Target: Get the login for the user Hornoxe
- Hint: You really need one? omg -_-
- Tablename: level1_users
- Category: [1](#)
- This category does not exist!
- Username:
- Password:

A watermark <https://blog.csdn.net/jhsword> is visible in the bottom right corner of the screenshot.

2.XCTF(攻防世界)竞赛平台

官网: <https://adworld.xctf.org.cn/>



The screenshot shows the homepage of the XCTF competition platform. The main banner features the text "WMCTF 国际赛 48小时" (WMCTF International Competition 48 Hours) with the event dates "2020.8.1 9:00 - 8.3 9:00" and the competition URL <https://wmctf2020.xctf.org.cn/>. The banner also includes contact information: "联系方式: Telegram: <https://t.me/WMCTF> QQ群: 282546".

The website features a navigation menu with categories like "答题", "竞赛", "排行榜", "队伍", and "商城". The footer includes logos of various sponsors and partners, such as HUAWEI, 360企业安全, 字节跳动, 天融信, OPPO安全应急响应中心, 京东安全, 滴滴出行安全应急响应中心, and 奇安信. A watermark <https://blog.csdn.net/jhsword> is present in the bottom right corner.

3.网络信息安全攻防学习平台

官网: <http://hackinglab.cn/>

网络信息安全攻防学习平台

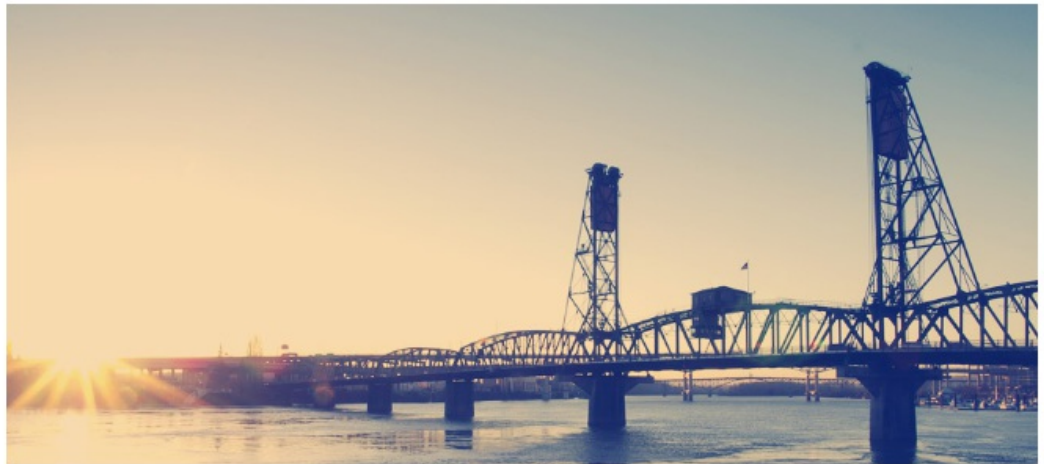
题目区

- 选择题
- 基础关
- 脚本关
- 注入关
- 上传关
- 解密关
- 综合关
- 创新关

子系统

功能区

推荐区



平台公告

HawkEye鹰眼系统上线,在您登陆系统后,可通过点击左边[子系统]-[HawkEye]进入HawkEye!

HawkEye支持在线充值开通啦!点击下面的[在线充值]即可进入HawkEye并使用支付宝自助充值开通!

在线充值: [点击进行在线充值](#)

HawkEye功能介绍: [点击查看功能介绍](#)

HawkEye使用手册: [点击查看使用手册](#)

<https://blog.csdn.net/jhsword>

4.OWASP 中国

官网: <http://www.owasp.org.cn/>



网站搜索
 仅在本栏目

首页	OWASP项目	OWASP培训	OWASP峰会	OWASP活动	OWASP会员	OWASP分会	OWASP中国手册
----	---------	---------	---------	---------	---------	---------	-----------

- OWASP项目
- OWASP培训
- OWASP峰会
- OWASP活动
- OWASP会员
- OWASP分会
- OWASP中国手册

您位于: 首页

Welcome to OWASP CHINA

专注十年, OWASP中国再谱新篇

OWASP是一个开源的、非盈利的全球性安全组织,致力于应用软件的安全研究。我们的使命是使应用软件更加安全,使企业和组织能够对应用安全风险做出更清晰的决策。全球拥有250个分部近7万名会员,共同推动了安全标准、安全测试工具、安全指导手册等应用安全技术的发展。

近几年,OWASP峰会以及各国OWASP年会均取得了巨大的成功,推动了数以百万的IT从业人员对应用安全的关注以及理解,并为各类企业的应用安全提供了明确的指引。

OWASP在业界影响力:

- OWASP被视为web应用安全领域的权威参考。2009年下列发布的美国国家和国际立法、标准、准则、委员会和行业实务守则参考引用了OWASP。美国联邦贸易委员会所有企业需遵循OWASP十大WEB弱点防护守则
- 国际信用卡数据安全技术PCI标准更将其列为必要组件
- 为美国国防信息系统局(DISA)应用安全和开发清单参考
- 为欧洲网络与信息安全局(ENISA),云计算风险评估参考
- 为美国联邦首席信息官(CIO)理事会,联邦部门和机构使用社会媒体的安全指南
- 为美国国家安全局/中央安全局,可管理的网络计划提供参考
- 为英国GovCERTUK提供SQL注入参考

<https://blog.csdn.net/jhsword>

5.实验吧CTF训练营

官网: <http://www.shiyanbar.com/>

在 2020.08.15 访问时处于维护期。

<https://www.shiyanbar.com/upgrade.html>

尊敬的用户, 您好

为了给您提供更优质的在线云服务, 实验吧对平台进行维护。维护期间对您的使用带来的不便, 我们深表歉意。

- 1、在此期间, 实验吧CTF训练营将无法正常使用。
- 2、购买人邮出版社与U-SaaS合作教材的用户将不受影响。
- 3、用户注册及密码找回

注册用户: <http://passport.shiyanbar.com/register>

密码找回: <http://passport.shiyanbar.com/find-password>

购买人民邮电出版社与平台合作教材用户

登陆地址: <http://rymooc.shiyanbar.com/>

绑定信息: 刮开所购丛书的激活码进行绑定。

学习课程: 进入“学生中心--我的课程”进行学习。

4、服务支持

联系电话: 010-82327658转8018 或 18610530606 (工作日9: 30-18: 30)

服务邮箱: service@shiyanbar.com 或 2953194086@qq.com

6.全国大学生信息安全竞赛官方网站

官网: <http://www.ciscn.cn/>

全国大学生信息安全竞赛
NATIONAL COLLEGE STUDENT INFORMATION SECURITY CONTEST

大学生信息安全题库 会员数: 50694 注册 登录

首页 | 竞赛章程 | 竞赛目录 | 访谈集萃 | 参赛高校 | 支持单位 | 发展论坛 | 专家库

为云
未来 值得信赖
息安全竞赛独家云服务提供商

国卫信安
网络空间安全
人才服务网
教育部高等学校信息安全专业教学指导委员会
全国大学生信息安全竞赛技术支撑单位

1 人才服务 2 测评认证 3 竞赛实训 4

精彩回顾 更多

最新公告 更多

[创新赛通知] 关于“第十三届全国大学生信息安全竞赛-...”

[创新赛通知] 关于举办“第十三届全国大学生信息安全竞赛...”

[通知] “强网杯”全国网络安全挑战赛的通告

[创新赛通知] 关于“第十三届全国大学生信息安全竞赛-...”

2020年第十三届全国大学生信息安全...
为积极响应国家网络空间安全人才需求, 加快攻防兼备创新人才培养步伐, 推动网络空间安全人才培养和产学研用的生态体系。由教育部高等学校网络空间安全专业教学指导委员会主办、华中科技大学承办的第十三届全国大学生信息安全竞赛---创新实践能力赛(以下简称“大赛”), 大赛将于2020年7月至2020年9月举行。面向全国高校在校学生开放。

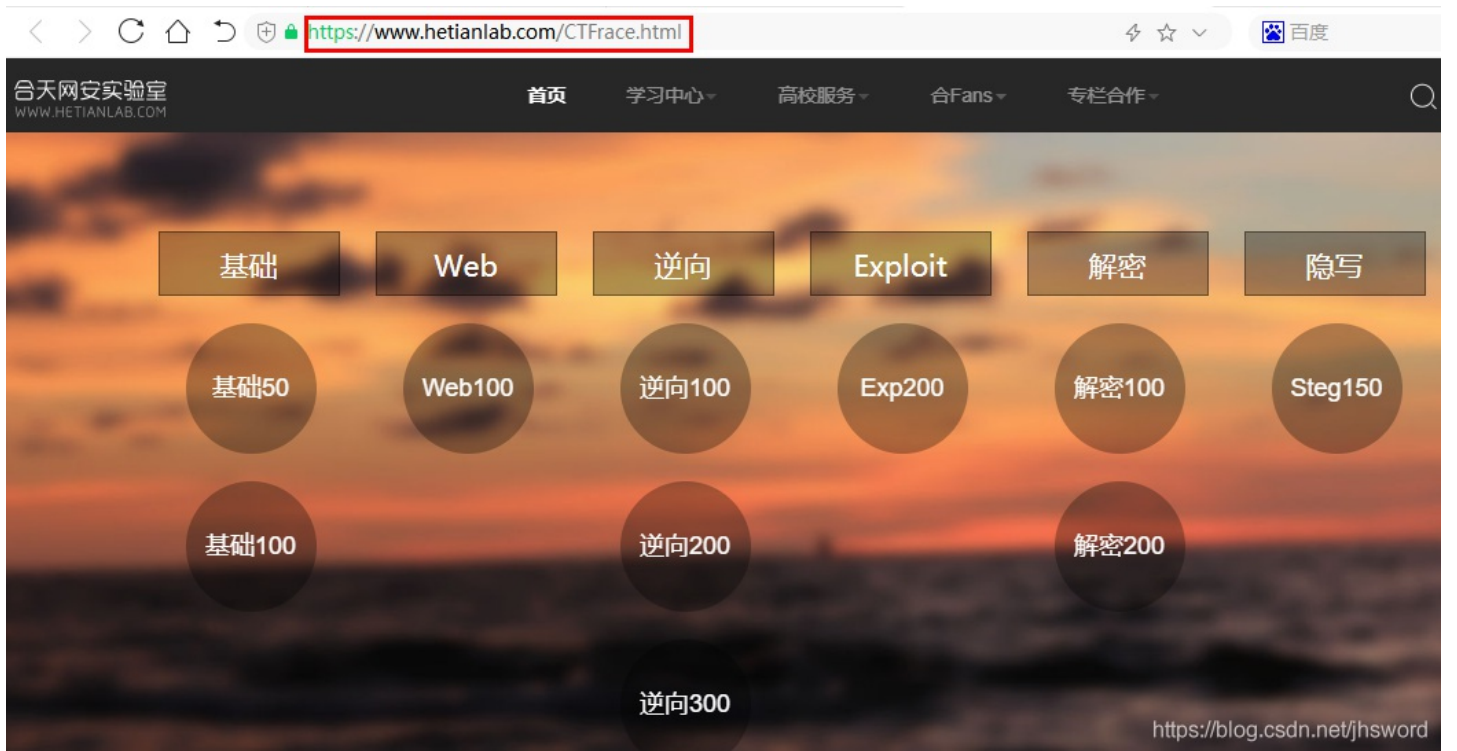
7.MS09067WEB靶场

官网: <https://www.ms08067.com/about/bachang.html>



8. 合天网安实验室

官网: <https://www.hetianlab.com/CTFace.html>



9. 封神台

官网: <https://hack.zkaq.org/?a=battle>

公开课基础演练靶场 >	比赛名称	分数	状态	突破	查看详情
正式课 - 从入门到进阶 >	第一章: 为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】	5	正常进行	6939次	查看
工具篇 - 从Kali入门学安全	第二章: 遇到困难! 绕过WAF过滤! 【配套课时: SQL注入攻击原理 实战演练】	10	正常进行	3338次	查看
训练营 - 0基础学渗透测试	第三章: 爆破管理员账户登录后台 【配套课时: burp到支付和爆破 实战演练】	10	正常进行	195次	查看
Kali训练营 - 玩转工具 >	第四章: 为了更多的权限! 留言板! 【配套课时: cookie伪造目标权限 实战演练】	10	正常进行	2019次	查看
AWD提升靶场 >	第五章: 进击! 拿到Web最高权限! 【配套课时: 绕过防护上传木马 实战演练】	15	正常进行	1247次	查看
技能实战篇演练靶场	第六章: SYSTEM! POWER! 【配套课时: webshell控制目标 实战演练】	15	正常进行	881次	查看
2019网络空间竞赛	第七章: GET THE PASS! 【技能点: 进程中抓下管理员明文密码】	20	正常进行	356次	查看
基础练习场	萌新也能找CMS漏洞	1	正常进行	0次	查看
	绕过防护getshell	5	未开始	0次	查看

欢迎关注掌控安全官方公众号: 掌控安全EDU

<https://blog.csdn.net/jhsword>

10. SQL Fiddle在线练习

官网: <http://www.sqlfiddle.com/>

SQL Fiddle MySQL 5.6 View Sample Fiddle Clear Text to DDL

Schema Panel
 Use this panel to setup your database problem (CREATE TABLE, INSERT, and whatever other statements you need to prepare a representative sample of your real database). Use "Text to DDL" to quickly

[Build Schema](#) [Edit Fullscreen](#) [Browser](#) [\[:\]](#)

[Run SQL](#) [Edit Fullscreen](#) [\[:\]](#)

Please build schema.

Improve Entity Framework Performance

[Bulk Insert](#)
[Bulk Delete](#)

[Bulk Update](#)
[Bulk Merge](#)
LEARN MORE

<https://blog.csdn.net/jhsword>

11. BUUCTF

官网: <https://buuoj.cn/faq>

Q: 请问可以提供一下 PWN 题的 libc 吗?

Q: Libc.so for PWN challenges?

A: 请在 <https://buuoj.cn/resources> 下载。

A: Download at <https://buuoj.cn/resources>.

Q: 我在做 PWN 题时遇到了 "timeout: the monitored command dumped core" 的提示, 请问我该怎么办?

Q: I got a message said 'timeout: the monitored command dumped core' when I PWN, how I can do?

A: 请参考 <http://blog.eonev.cn/archives/958>。

A: Please check it(Chinese version): <http://blog.eonev.cn/archives/958> .

Q: 我在做 Real 类题时找不到 flag, 我该怎么办?

Q: I can't find flag of Real challenge, how can I do?

A: Real 类题目仅供复现漏洞, flag 不是最终目的, 虽然大部分 flag 都在环境变量里能找到, 但本站不保证该类题一定能找到 flag。

A: Real challenge only for study, since You may get the flag at the environmental variable, sometimes You can't get the flag, never mind about that.

12.CTFHUB

官网: <https://www.ctfhub.com/#/skilltree>

CTFHub
开箱即用的CTF学习解决方案

登录 注册账户

历年真题

热门搜索: mheap, MissingLib, SSRFlow, 随便挂, 德夫的工作日, CNJ PC, 文件管理, PiuPuPu, HackNote

https://blog.csdn.net/jhsword

已停止访问(以前著名)CTF网站

1. 白帽学院 <http://www.baimaoxueyuan.com/>
2. IDF实验室 <http://www.idf.cn/> , <http://ctf.idf.cn/>
3. CTFwiki <https://ctf-wiki.bearychat.com/>

参考

1. <https://blog.csdn.net/xiaoqi199915/article/details/106489743>
2. 攻防世界XCTF黑客笔记刷题记录
3. CTF学习路线指南(附刷题练习网址)

(本文完)