



华中科技大学-网络空间安全学院 丁鹏宇 2024.05.25

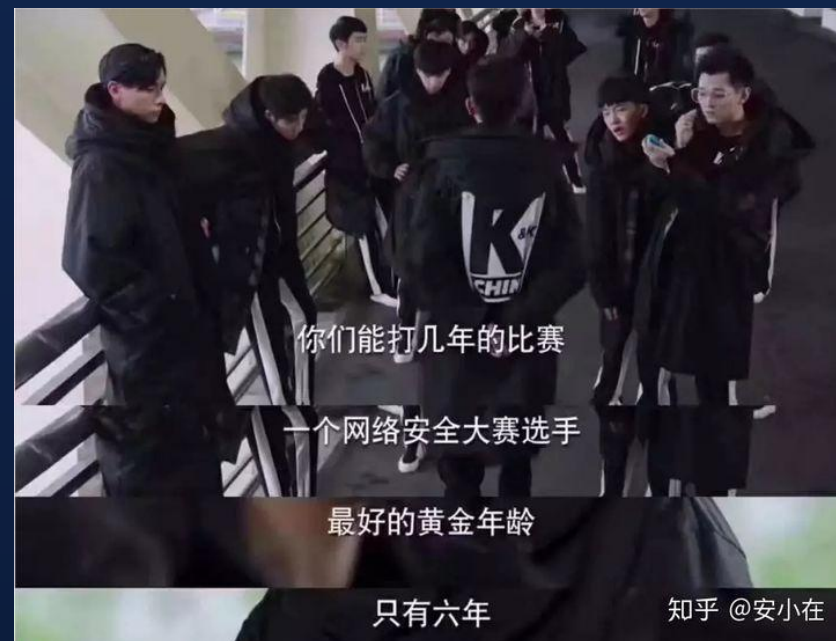
开源安全实践与教育平台



- 前情提要
- Dojo 的前世今生
- Dojo 功能介绍
- Q & A

前情提要

●什么是CTF?



前情提要



● 什么是CTF?

- CTF（夺旗赛）是一种特殊的信息安全竞赛。有三种常见的CTF类型：解题式、攻防式和混合式。
- 解题式CTF分布在不同的类别中。比赛时间结束后，积分总和最高的队伍即为CTF的获胜者。
- 攻防式CTF是另一种有趣的竞赛形式。你需要保护自己的服务以获得防守积分，并攻击对手以获得攻击积分。

前情提要



● 什么是PWN?

- PWN是CTF竞赛中的一个重要类别，通常涉及对二进制程序的分析 and 利用
- PWN挑战考验参赛者的逆向工程、漏洞分析和利用开发能力。
- PWN这个词源于黑客文化中的一个拼写错误。在黑客圈子里，"own" 被用来表示成功地攻破系统或服务器，并获得对其的控制权。由于拼写错误，"own"变成了"pwn"，并逐渐被黑客社区广泛接受和使用。

前情提要



- 什么是Dojo?

- DOJO (道馆) 是一个最先进的开源实践网络安全教育平台，旨在降低学生和教师的使用门槛。
- 平台借鉴了CTF（夺旗赛）社区的经验，通过实践挑战，教学网络安全。

Dojo的前前前世



- ASU（亚利桑那州立大学）的杰出黑客团队维护，并开源在 <https://github.com/pwncollege/dojo>
- 支撑亚利桑那州立大学的网络安全课程，并向全球有兴趣的人免费开放。
- 被誉为国外排名第一教学平台。

Dojo的前前前世



./ [pwn.college](#) [Dojos](#) [Workspace](#) [Desktop](#) [? Help](#) [Chat](#)

[Register](#) [Login](#)

pwn.college

Learn to hack!

Welcome to pwn.college!

pwn.college is an education platform for students (and other interested parties) to learn about, and practice, core cybersecurity concepts in a hands-on fashion. In martial arts terms, it is designed to take a “white belt” in cybersecurity to becoming a “blue belt”, able to approach (simple) cybersecurity competitions (CTFs) and wargames. Our philosophy is “practice makes perfect”.

The platform is maintained by an [awesome team](#) of hackers at Arizona State University. It powers much of ASU's cybersecurity curriculum, and is open, for free, to participation for interested people around the world!

If you have comments, suggestions, and feedback, please email us at pwn@pwn.college!

Great! How do I jump in?

pwn.college is organized into a series of dojos, each of which covers a high-level topic area. Please start your journey with the [Getting Started](#) dojo:

Getting
Started



[Click here to get started!](#)















Dojo的前世

- pwn.hust.college
- <https://pwn.cse.hust.edu.cn>
- 在慕冬亮副教授的大力支持下，将 Dojo 引入了课堂，并让同学们进行实践操作，题目均为自主出题，更符合中国 pwner 宝宝体质。
- 在 2016 学年软件安全理论课程教学投入使用。
- 在 2017 学年软件安全实验课程教学投入使用。
- 受到学生的广泛好评。

Dojo的前世



排名	黑客	徽章	分数
#1	 U202115951		63
#2	 U202112052		63
#3	 U202110940		63
#4	 U202112141		63
#5	 U202112131		63
#6	 U202112041		63
#7	 U202112143		63
#8	 U202112111		63
#9	 U202111995		63
#10	 U202111238		63
#11	 U202112167		63
#12	 U202112196		63
#13	 U202112076		62
#14	 U202110722		62
#15	 U202117242		62
#16	 U202112068		62
#17	 U202117266		62
#18	 U202112723		62
#19	 U202112145		62
#20	 U202112046		62

Dojo的前世



我对于这门课还是非常满意的，尤其是 `pwn.hust.college` 网站，成功地实现了课堂理论与实践相结合，在学习完理论知识之后如果不进行实践训练的话，知识的遗忘速度是非常快的，并且通过自己手动操作，也能对于学科知识有更深一步的理解。

本次课程使用 `pwn.hust.college` 平台授课，体验非常好，建议所有此类安全实验都可以用这种平台进行（我们的 PE32 恶意代码的实验体验就非常差，和漏洞利用实验形成鲜明对比），这种获取 `flag` 的常规 `ctf` 形式也能提高学生对于网络安全、软件安全、信息安全等知识的学习兴趣。

我认为这个课程给我的感受还是很好的，主要原因之一就是教学和实践相结合，不像以前的一些课程，我就不点名了，明明是要多实践多写代码的内容，却全是理论教学，做的都是些理论题，这样就算理论基础学的还行，一到实战就傻眼了。关于 `pwncollege` 这个平台也很棒，主要是每次获得 `flag` 的时候让我很有成就感，也会大大激励我的兴趣和信心。

在本次实验中，我感受到 `pwn.college` 平台确实非常的方便高效，让软件安全的漏洞不止于纸上谈兵，能让同学们切身实践地感受在程序运行时漏洞的产生和利用，希望以后的软件安全实验能提供更多样化的 `pwn` 实验和更明晰的漏洞展现，让学生体会到软件安全的魅力。

另一方面，鉴于慕老师对于开源平台的热心投入，以后的软安实验可以进一步提高同学的参与感，可以让我们利用课上学到的漏洞自己设计出复杂的漏洞程序供大家学习参考，更丰富了我们的解题思路，也让我们更深入地理解漏洞原理。

希望软件安全实验课程和开源社区越来越好。

1. 感觉这两个题很棒，尤其是第二个实验的实验指南写的非常详细，虽然感觉提示的很多，但是对于初学者来说还是很有必要的。希望能继续把这两个题留给学弟学妹。
2. `pwn.hust.college` 平台也很好，留给下一届。

总的来说，软件安全这门课确实能学到不少东西，算是开启一个新的天地，`pwncollege` 上面的题目也基本做完了，收获还是挺大的，是我这学期最惊喜的一门课程，要说唯一的不足应该就是要是能早一点开这门课就好了。

Dojo的今生

- 大版本更新，就是你了，宝可梦！做题===闯关。
- 接入华中科技大学 one_pass 统一认证。
- 无缝接入kook，提供课程学习和沟通平台。
- 支持 X86 和 国产 ARM 双架构。





?????
我是誰

新トモスタ
POCKET MONSTERS



Dojo 功能介绍

- Vscode + Desktop + SSH 多端做题，共享数据。
- 所有题目所需环境，无需配置一键使用。
- 后端 docker 轻量级启动。
- 防止学生 cheat，实例隔离，使用动态 Flag。
- 题目与平台架构分离，保护平台安全。
- 题目难度可视化，星级越高，难度越难。
- 综合类题目结合之前的关卡知识点。

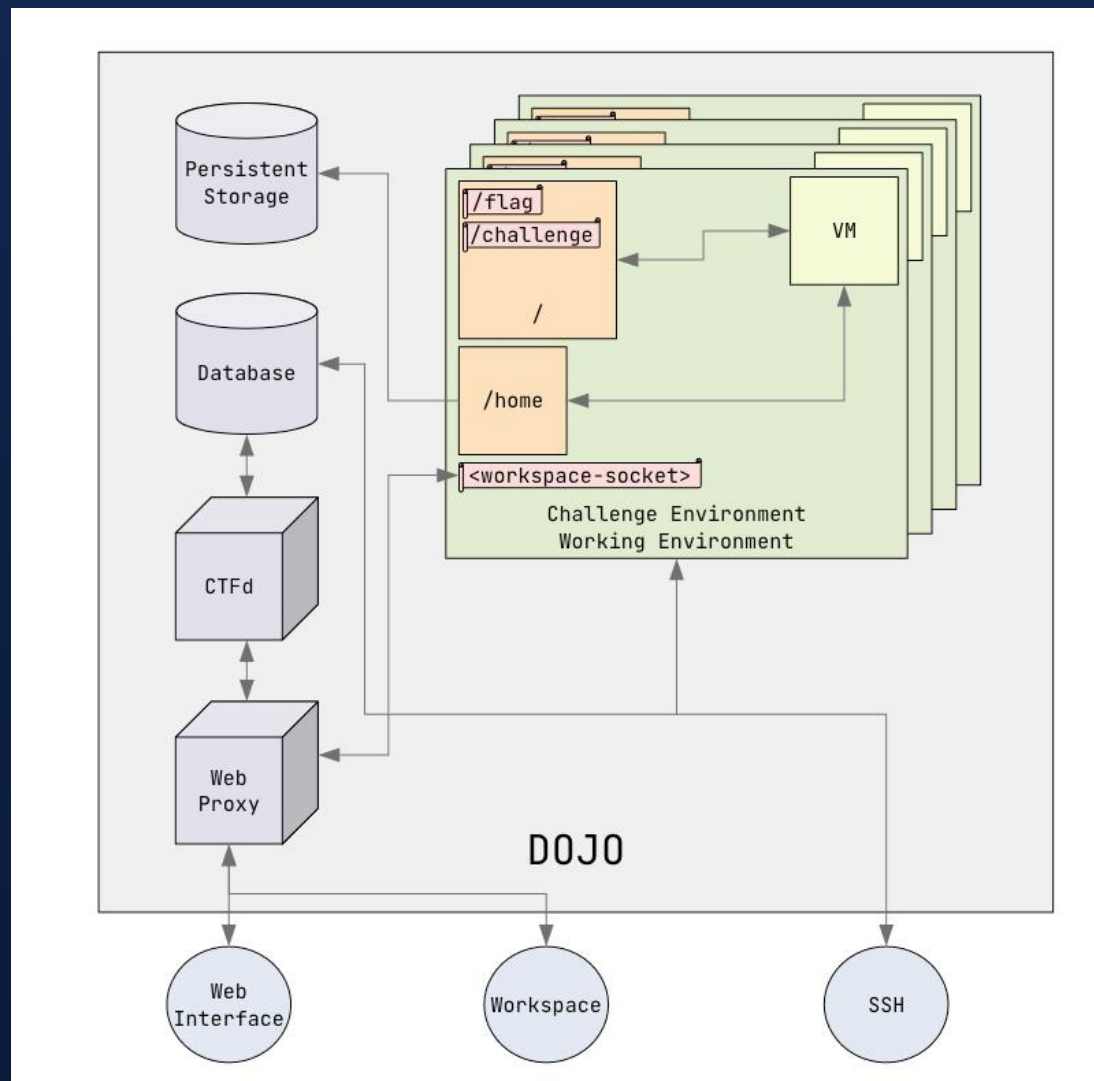


Dojo 技术实现

- CTFd 基础后端 + dojo 插件优化。
- docker 嵌套虚拟化，一站式解决所有环境。
- 持久化增量平台数据，保证更新速度，保证数据不丢失。
- nginx-proxy自动化配置反代。



Dojo 技术实现



Dojo实机演示



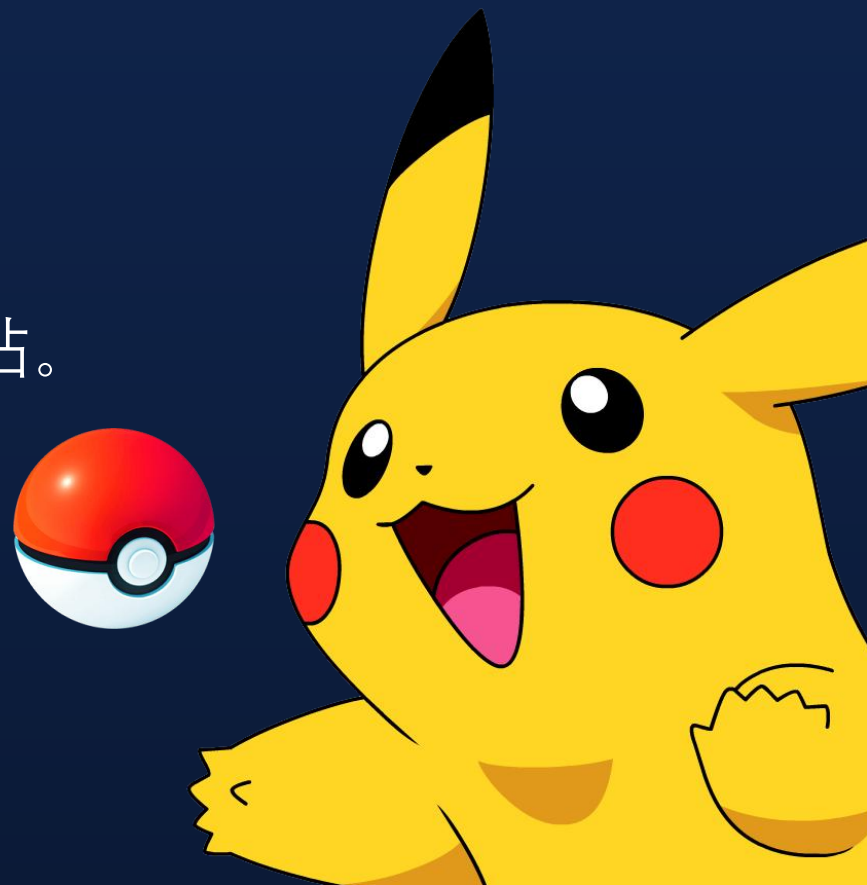
- <https://pwn.cse.hust.edu.cn>
- <https://www.kookapp.cn/app/invite/soUkFL>



Dojo 未来展望

● Dojo To do

- 班级/课程自动算分，避免繁杂的统计成绩。
- 校内上线ARM专版，从零开始学习ARM pwn。
- pwn.hust.college 上线公网，做到国内一流教育网站。
- 取之开源，回馈开源。



Dojo 未来展望



hust-open-atom-club / dojo Public

Notifications Fork 21 Star 7

Code Issues 8 Pull requests 1 Discussions Actions Projects Wiki

hustsec_dev Go to file **Code**

This branch is **835 commits ahead of**, **620 commits behind** `pwncollege/dojo:master`.

wumingzhilian Fix user_network networ... a5d5040 · 7 hours ago 1,641 Commits

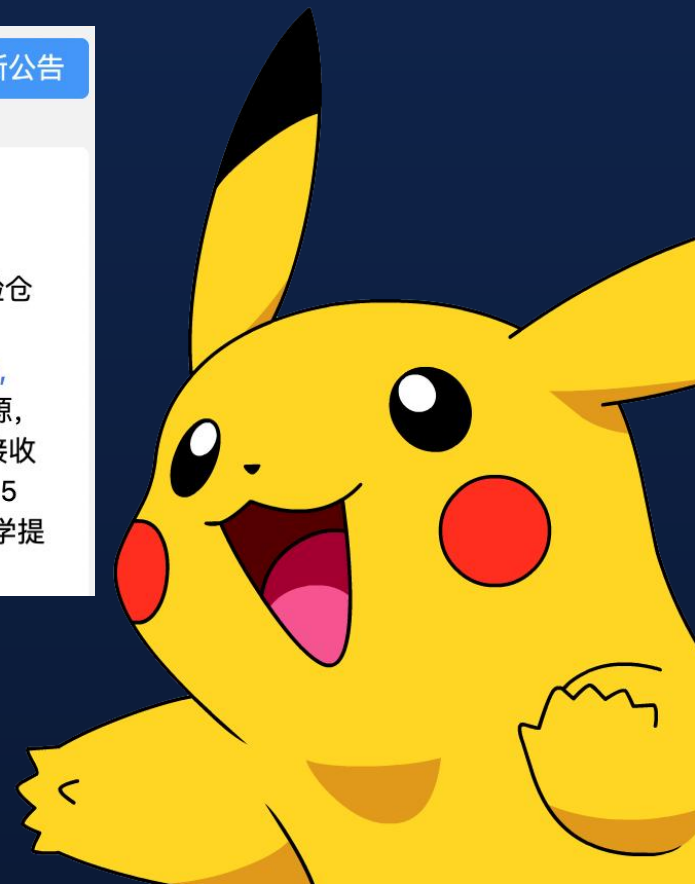
.devcontainer	Add "course" page (pwncolle...)	9 months ago
.github/workflows	update test CI port from 808...	last month
challenge	change https to http in dock...	last week

23年秋网安与本硕博软件安全课程群

[发布新公告](#)

慕冬亮 2024/01/16 18:04 [置顶](#)

各位同学，我们 `pwn.hust.college` 平台的基础架构仓库（<https://github.com/HUSTSeclab/dojo>）和理论课实验课实验仓库（<https://github.com/HUSTSeclab/software-security-dojo>，<https://github.com/HUSTSeclab/software-security-lab-dojo>，<https://github.com/HUSTSeclab/welcome-dojo>）已经完全开源，欢迎大家进行开源贡献！课程结业的时候，我们会根据大家被接收的开源贡献酌情加分（满分3分，单个PR如果修改代码，每个0.5分；若修改文档，每个0.25分，PR可累加）。请注意：各位同学提交PR时可以修改题目源代码，但请不要重新编译二进制文件！





Q & A

- <https://github.com/hust-open-atom-club>
- <https://github.com/hust-open-atom-club/S2VulnHub>
- <https://github.com/hust-open-atom-club/dojo>



