MoeCTF2025 Web方向入门指北

撰写：fifker

一、什么是Web方向?

Web 技术支撑着日常网站和 APP 的运行——你浏览的页面、点击的按钮，都由它实现。
Web 安全方向的核心，就是寻找这些应用中的漏洞，像侦探一样破解系统！

核心目标：通过前端（用户界面）或后端（服务器/数据库）的漏洞（如代码错误、配置缺陷），找到隐藏的 flag（竞赛通关密钥）。

给新手的破局关键：拆解网站！
别急着找漏洞！先看懂网站的“身体结构”：
1.前端 = “脸面”（用户看到的界面）
→ 技术：HTML/CSS/JavaScript（布局/样式/交互）
2.后端 = “大脑”（处理逻辑+存储数据）
→ 技术：Python/PHP/Java + MySQL等数据库
3.协作方式 = “神经传导”（浏览器⇄服务器通过HTTP请求传递数据）

当你了解了一个网站的构造后，就相当于拥有了 X 光透视眼：
一眼看穿网站“骨架”如何拼接；
精准定位漏洞“关节”薄弱点；
从根源理解漏洞为何产生！

二、如何高效学习 Web 安全?

漏洞挖掘本质是**精准提问+高效验证**的能力，这三件武器助你快速升级：

1、最重要也是最主要的，就是善用搜索引擎。
现在互联网如此发达，小到软件怎么使用，大到某一个庞大的知识点，都可以通过搜索引擎轻而易举的查到，关键问题只是你怎么才能更好地使用它。
tips：**不要**再用360浏览器啦！！！建议使用Chrome、Firefox、Edge等浏览器。

2、利用好AI工具。
当前AI技术非常的发达，很多问题都可以通过AI工具来解决。在搜索引擎里的数据太过于眼花缭乱的时候，问问AI是一个不错的选择。但是要注意，AI不会直接帮你做题，它只能给你一个思路和大概知识点范围。
tips：推荐打开**深度思考**和**联网搜索**！

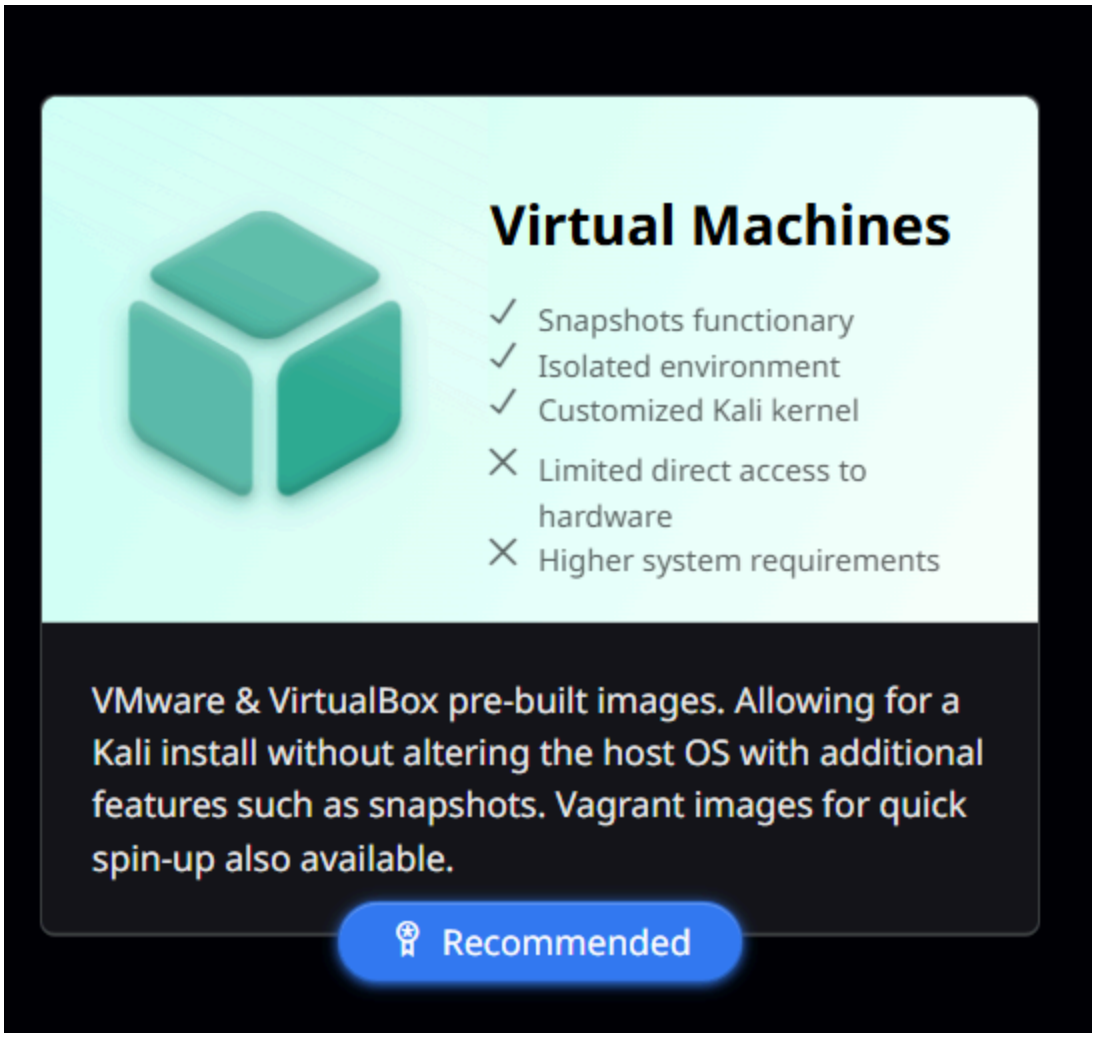
3、学会如何提问。
当搜索引擎+AI都没办法解决你的问题的时候，可以考虑去询问他人。
但是请注意，每个人都有自己要做的事情，**回答你的问题并不是他们的义务**。所以提问的时候最重要的一点就是要信息详细，说清楚你的思路、你已经做过的尝试、你卡在哪一个点或者对于AI给出的回答有什么疑问，而不是让回答者去猜测，白白浪费时间。
tips：可以去看一看群文件中《提问的艺术》。

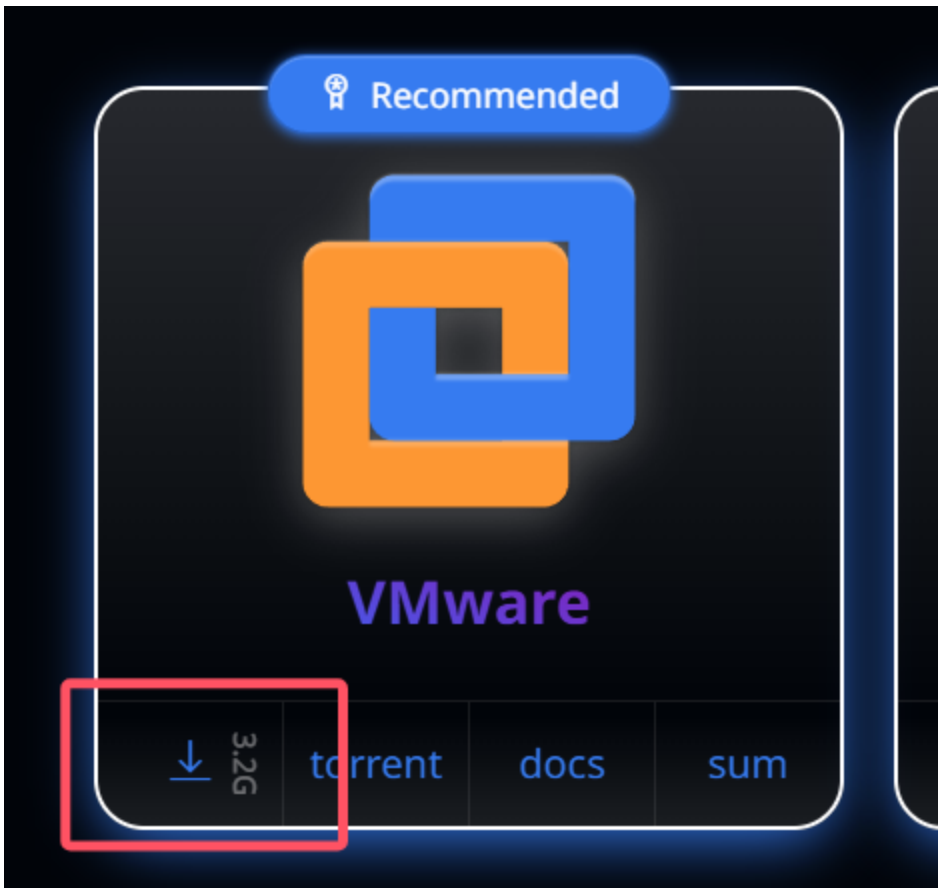
三、要学习些什么知识?

首先最最最最最最麻烦的，就是下载软件配置环境：

这会是一个漫长繁琐的过程，这是必经之路，但是完成这个就相当于成功了一半！

1.Linux入门：
安装 VMware + Kali Linux（实战渗透系统）
掌握基础 Shell 命令：cd/ls/cat/sudo
方案1（推荐）：安装 VMware Workstation + Kali Linux 镜像


Virtual Machines
Snapshots functionary
Isolated environment
Customized Kali kernel
Limited direct access to hardware
Higher system requirements
VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.
Recommended


Recommended
VMware
3.2G
torrent
docs
sum

方案2（简化版）：使用在线靶场立即练习 → PortSwigger Web Security Academy
可供参考的资料：

- Linux命令学习

2.浏览器武装之必装插件：
HackBar（漏洞调试）｜Wappalyzer（技术识别）｜ProxySwitchyOmega（代理切换）
tips：进入插件商店可能需要科学上网

3.核心工具集：
BurpSuite（抓包攻击）｜PHPStudy（一键PHP环境）
SQLMap（自动化SQL注入）｜Dirsearch（网页目录扫描）
BurpSuite注意事项：

- 首次使用需配置代理：浏览器设置 → 127.0.0.1:8080
- HTTPS抓包需安装证书

PHPStudy启动流程：

- 安装后点击「启动」按钮
- 网站文件放在安装目录的 `WWW` 文件夹
- 浏览器访问 `http://localhost/你的文件名.php`
- 实验结束后务必关闭PHPStudy，防止长期开启产生安全风险！

4.效率工具：
Everything（文件秒搜）｜Clash（科学上网）按需安装

基础知识：

1.网络协议根基：
重点掌握 HTTP协议（请求头/响应头、GET/POST方法、状态码）
可供参考的资料：

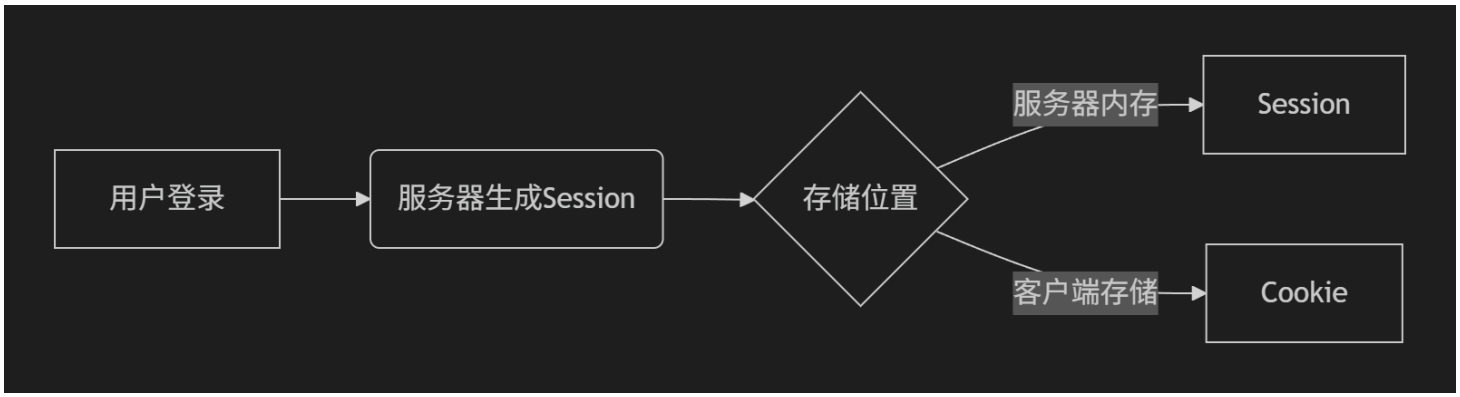
- HTTP学习

2.编码与加解密：
Base64｜URL编码｜MD5/SHA1哈希（使用 CyberChef 练习）
可供参考的资料：

- CTF编码

3.认证机制：

Cookie｜Session｜JWT 的作用与差异



4.前端三件套：

HTML（结构）｜ JavaScript（核心交互）｜ CSS（了解即可）

可供参考的资料：

- HTML学习
- JavaScript学习

5.后端初探：

PHP 基础语法 + MySQL 增删改查（用 PHPStudy 快速搭建）

可供参考的资料：

- PHP学习

6.脚本语言：

Python 优先：能写简单爬虫（Requests库）和自动化脚本

可供参考的资料：

- Python官方手册
- Python学习

7.新手阶段聚焦工具：

- BurpSuite 抓包改包
- SQLMap 基础使用（自动化注入）
- 浏览器开发者工具（F12调试）

学习漏洞路线

web漏洞多到数不清，一个一个列出来并不现实。先从最基本常见的漏洞学起吧！

第一阶段：必须掌握的四大核心漏洞

漏洞类型	本质危害	学习重点	靶场推荐
SQL注入	窃取/篡改数据库	手工注入流程、Union查询、报错注入	在线靶场
文件上传	获取服务器控制权	绕过前端校验、MIME类型欺骗、路径穿越	Upload-Labs（全关卡）
PHP安全	代码执行漏洞	弱类型比较（==）、文件包含（`include`）、危险函数（`eval`）	PHP类型把戏测试
XSS攻击	劫持用户会话	反射型/DOM型XSS、Cookie窃取	XSS挑战

第二阶段：进阶漏洞

漏洞	核心原理	实践技巧
CSRF	伪造已认证用户请求	构造恶意转账链接实验
SSRF	利用服务器访问内网	file://协议读取/etc/passwd
XXE	滥用XML解析器	外部实体注入读取系统文件
SSTI	模板引擎代码执行	{{7*7}}检测漏洞
反序列化	篡改数据触发恶意代码	重点研究PHP魔术方法

具体信息

CSRF：

核心：伪造已认证用户的请求（利用浏览器自动携带Cookie的特性）

关键：构造恶意链接/表单 → 诱骗用户点击 → 以用户身份执行操作（如改密码）

SSRF：

核心：操纵服务器发起任意HTTP请求（攻击内网服务）

关键：file://协议、127.0.0.1探测

SSTI：

核心：控制模板引擎执行代码（通过注入模板语法）

关键：检测 `{{7*7}}` → 若返回 `49` 则存在漏洞

XXE：

核心：利用XML解析器读取文件/触发SSRF

关键：

```
<!-- 基础Payload -->
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<foo>&xxe;</foo>
```

反序列化：
核心：篡改序列化数据触发恶意代码执行
关键 **（以PHP为例）** ：
魔术方法：__wakeup()、__destruct()在反序列化时自动调用
工具：phpggc（生成Payload）
tips:反序列化需结合语言特性深入，无需着急学习。

四、要如何练习?

法律红线警示

> **授权测试原则**：
>
> 1. 仅攻击自己控制的虚拟机/容器
> 2. 禁止扫描 `.gov.cn` / `.edu.cn` 等敏感域名
> 3. 公共靶场需确认允许渗透测试（如HackTheBox规则）

靶场推荐

靶场名称	特点	入门建议
攻防世界	自带新手村（基础关卡分层清晰）	从难度1开始建立信心
CTFHub	漏洞专题训练（如SQL注入专项）	学完一个漏洞立即实战
BugKu	题目趣味性强	优先做“Web安全”分类
BUUCTF	题目全面（含历年赛题）	配合WriteUp对比思路
NSSCTF	活跃度高/新题多	参与“每周练习”赛

不会可以查看WriteUp（题解），一定要搞清楚原理而不要一知半解的，**千万不要看完WriteUp直接复制payload**，可以学完一个漏洞就找相同类型的靶场打一打。

看完这些，是不是想要上手大干一场呢？看一看附件的题目吧！希望这是你获得的第一个flag！

五、MoeCTF2025 Web方向

为了增加本次Web方向的趣味性和代入感，也为了降低难度，我特意设计了一个符合CTF背景和修仙世界的设定，由此为基础写了一系列的小说作为题目描述（**感谢另一位出题人HDdss客串小说主角，感谢其他出题人客串小说其他角色**）。

题目描述部分的小说对引入题目有一定作用（对于不想看的师傅也会有一个省流版本，剧情不影响做题）。

而当你历经艰险解出题目（这不比翻几页就可以看到主角突破有代入感多了），就可以看到剩下一部分的小说剧情。

tips：小说剧情中，前期每一个知识点的基础题目会讲解当前考点的一些基本知识，可以提前学习后对照小说剧情进行复习，说不定做题更加简单自如！

当比赛结束，回顾小说剧情的时候，你会发现主角一路修炼变强的荣耀，不也属于你吗？

星辰大海就在眼前，当你解出第一个flag时——整个世界都会为你亮起「Access Granted」的绿灯！