MoeCTF2021—Web入门指北

本文作者水平有限，内容大家仅作学习Web方向参考就好。

Web方向概述

- Web方向是传统的线上CTF比赛中一块重要的组成部分，Web方向初期的学习相比于Pwn和Re不需要太强的系统底层知识，相比于Crypto不需要深厚的数学功底与编程能力，所以算是CTF中入门门槛较低的一个方向。
- Web方向的特点是知识点琐碎，题目种类很多，出题方向经常是紧跟时下的热点漏洞，做题过程多为与服务器进行不断的交互，具有很强的实战性。

Web方向需要具备的基础

Web虽说入门门槛相对较低，但是知识体系还是挺大的，所以需要的基础知识也挺多的。

首先我们应该了解Web应用的发展历程，最开始的web1.0，网站都是静态页面的，也就是用户向服务器请求什么，服务器就返回给用户什么，展现给用户的东西都是被事先编辑好的，用户与web应用之间缺少交互，可以说这时候的web应用和用户之间是单向的，即网站到用户。web2.0变得更注重与用户之间的交互，这时用户可以在浏览网站的时候参与到网站的建设中，比如用户可以在网站上通过评论，留言分享自己的想法等等。

其次至少应该理解当我们在谷歌浏览器上搜索一个关键字后，浏览器发生了什么?

这里简单来说，实际就是

- 浏览器解析拼接上我们所搜索内容的url
- 与服务器进行建立连接
- 服务器收到请求，处理请求，返回相应
- 浏览器接收响应，处理响应将其展示给用户
- 关闭连接

基于上述过程我们又需要了解什么是url，什么是服务器，服务器做了什么，服务器与客户端是通过什么建立连接的，我们所看到的页面本质是什么样的，TCP/IP协议族（HTTP协议，TCP协议……）等等

泛泛地了解了上述概念我们才能真正理解Web入门题目—GET，POST,COOKIE。

当然想要继续深入学习Web方向仅仅泛泛了解是远远不够的，关于如何深入学习web方向在下面就写啦!

Web方向学习历程

- 最开始作为萌新入门，大多数人都是通过PHP的一系列问题来入门的。
- 刚开始遇到的题目都是给予一些Weber应该具有的基础能力的，比如，如何get，post，如何上传cookie。浏览器的F12中都能为我们提供什么信息。再比如对于burpsuite的基本使用。还有

最最最最最重要的基本能力是我们应该学会如何利用谷歌，百度等搜索引擎去获得我们想要得到的信息，知识等。

- 具备了作为一个Weber的基本能力后，就要面对一些常见的漏洞，像是SQL 注入、SSTI模板注入、文件上传、文件包含、PHP反序列化、XSS 跨站脚本攻击、CSRF 跨站请求伪造、SSRF服务器端请求伪造等。我们不仅需要理解它们的基本原理，还要能够在题目环境中完成对它们的一些利用，这就又引出了针对各种常见的过滤我们如何bypass的问题。

- 当我们了解上述全部内容后，恭喜自己，Web方向终于入门了。在这个时候可能Weber都会遇到一个问题，即我了解了php这些常见的漏洞，但是我在比赛题目中完全不知道怎么去利用，甚至题目所考察的漏洞放在面前依然无法通过所学的知识去解决它。别灰心别放弃大多数人学习Web方向愉快地入门以后都会遇到类似的问题。这时候积累广阔的知识面就显得格外重要了，通过复现比赛的题目、多看师傅们的博客中发的文章，我们可以学到一些各种各样地利用漏洞的方式，bypass的手法，在这篇入门指北中我就不详细讲述了。

- PHP的相关内容我们学习并在一定程度掌握后，我们可以去了解node.js的原型链污染及它所带来的相关问题，再深入我们可以去学习Javaweb安全。

学习平台

- MoeCTF 2021
- Bugku CTF
- https://adworld.xctf.org.cn/

最初的学习方式：可以通过搜索题目writeup的方式来了解基础知识与拓宽知识面

！！！Web方向学习过程中遇到无法解决的困难私戳moectf比赛群内管理员：宣传委员（qq：872269819）

flag：moectf{Web_1s_interesting!}