# 混战攻略

### 0x01-何为AWD

**Attack With Defence**，简而言之就是你既是一个**hacker**，又是一个**manager**。

**比赛形式**：一般就是一个ssh对应一个web服务，然后flag五分钟一轮，各队一般都有自己的初始分数，flag被拿会被拿走flag的队伍均分，主办方会对每个队伍的服务进行check，check不过就扣分，扣除的分值由服务check正常的队伍均分。

### 0x02-AWD题目类型

**01)题目类型**

1、出题人自己写的cms，附加了一些常见web漏洞。

2、常见或者不常见的cms

3、一些框架漏洞，比如thinkphp这种

**02)web程序代码类型**

目前来说，国内比赛依旧是php居多，当然也会有一些别的，比如py，lua这种。

**03)漏洞类型**

1、sql注入居多

2、文件包含

3、各种rce

4、文件上传

**04)出题人思路**

一般来说比较多见的是某些cms漏洞，为了减少现场挖洞的难道，一般出题人会放置一些很明显的漏洞代码，获取一些常用的web工具（漏洞工具），等等，再放几个比较简单的洞，直接在index.php或者web根目录下放个一句话木马?

### 0x03如何攻击

AWD模式的比赛跟日常的渗透测试有共同之处。

**1)如何拿flag**

一般来说就是以下两种模式：

1. 是向内网一台机器发送http请求，返回请求中包含flag。

② 是例如系统根目录下放置flag文件。

**2)一个黑客需要具备的一些东西，大致有以下几点:**

1. 快速的漏洞反应能力。因为有的时候，一些比赛放的漏洞都是网上能查到的，所以这个时候需要一个好的搜索技巧。或者是一些rec显而易见的那种。
2. 快速编写脚本的能力。因为大家的服务都是一样的，而你如果能通过比如注入的方式拿到flag，如果用hackbar一个个去弄，显然不够优雅，而且有时候特别会容易遗漏，那么这个时候写个小python脚本无疑是极好的。

**3)一个好的心态**

毕竟跟你同场竞技的都是各位大佬，所以当你发现自己被打的时候，心态不要崩，一旦崩了就基本宣布失败了。

①当我们处于优势地位时

除非处于那种绝对优势的时候，我们可以什么都不在乎。当我们处于一个微弱优势时，这个时候我们需要一个比较腹黑的思想，比如说，A队与B队只差了可能几百的分数，而A队这个时候有B队的webshell，那么如何把B队拖下水，相信大家都懂。

②当我们处于劣势地位时

首先还是那句话，心态不要崩。其次因为web比较容易抓取流量，所以即使我们被打，我们也可以及时通过分析流量去查看别的队伍的payload，从而进行反打。

如果自己的服务器上被种了shell，删除是肯定的，但是要这样想，如果给你种了shell，那么这种一般是自动化脚本打的，就意味着别的队伍也可能被种，路径密码什么的都一样。

### 0x04如何防守

其实防守更多看的是谁比较细心。适合运维人员。

**01)比赛开始的加固阶段**

比赛开始时，当我们连上ssh的时候，我们首先应该做的是修改一下服务器密码，然后把源码down下来，及时做好备份。以方便进行代码审计。然后在尽量不违反主办方赛事的原则下挂上自己的waf，以及删除一些敏感性的文件或者数据等。在比赛开放攻击的时候需要我们自己去抓流量。监控网站日志等信息，以做好应急响应。

修改常见的一些弱口令密码，像网站后台密码等，如果能有权限都系统、web容器、数据库配置做一些更改的话，进行相应的加固操作（都在相应的ppt中，大家可以自行去看看我给的加固ppt）。数据库密码一般在网站的配置文件中可以看到，对数据做了密码用户更改等操作也需要修改配置文件，以保证网站能正常运行。

**2)然后的工作**

当然是审计，审计，再审计。挖掘漏洞。

**3)当发现被攻击时**

当发现自己被打时，首先尝试还原以前的备份(记得备份当前)，如果依然被打，这个时候应该跟队友分好工，查看抓取的流量以及查看服务器上是不是存在shell。

### 0x05一些建议

**1)如果自己拿到了flag**

当自己拿到了flag。淡定一点，整理出漏洞思路，然后与队友交流，写出批量脚本，所以。

**2)特别熟悉的cms**

比如看到wordpress，那么第一个反应肯定是上wpscan。着常见的漏洞扫描工具进行漏洞。

**3)拿到了shell怎么办**

通过漏洞的利用拿到shell，需要做的是进行权限维持，比如种植web木马，每当flag刷新时进行提交

### 0x06最后要说的一些话

比赛还是需要有会代码的需要提高自己的代码审计能力以及自动化脚本的编写能力，才能去挖出漏洞，写出批量处理脚本，走向赛场巅峰。