CTF AWD

Attack With Defense

主要内容

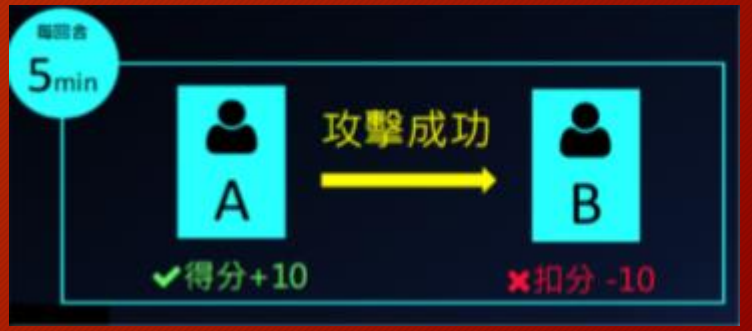
- 常见套路
  - 攻击
  - 防守
  - 下套
- AWD 现场友谊赛
  - 没啥奖品，送个巧克力?
- Writeup
  - 咳咳

什么是AWD

- 攻击与防守：Attack With Defense
- 每个队伍都有一台服务器，且每个队伍的初始环境相同
- 采用回合制，每个回合 flag 值不同

怎么得分，怎么被扣分

- 每个比赛主办方不同，赛制亦不同
- 每回合内，攻击对手的服务器
- 获取到对手服务器上的 flag 则自己得分、对手扣分
- 如果自己服务器上的服务不可用，被监控机制发现则会扣分



攻击/防御

- 以渗透为主
- 以 PHP 和 Python 为主
- 以 Linux 为主
- 以 get Shell 为主
- SQL 注入
- 文件包含
- 文件上传
- 实在不想多说..你们都懂，不懂的去刷 GOCTF 吧

SQL注入

- 漏洞原因：参数可控，SQL语句被修改
- 是门大学问，建议了解注入基础知识之后，多看大神经验分享
- Sqlmap 是个好工具，希望大家都有 (说明文档)

- 防御方法：SQL预处理，特殊符号转义

命令注入

- 漏洞原因：运行 cmd/shell 命令的函数或运行语言代码的函数例如（PHP：eval、assert，Python：eval、Java：反序列化）参数可控
- 防御方法：根据实际情况确定，一般可试试过滤一下特殊字符，甚至给Java打个补丁

```
<?php
eval($_GET[‘cmd’]);
```

文件上传

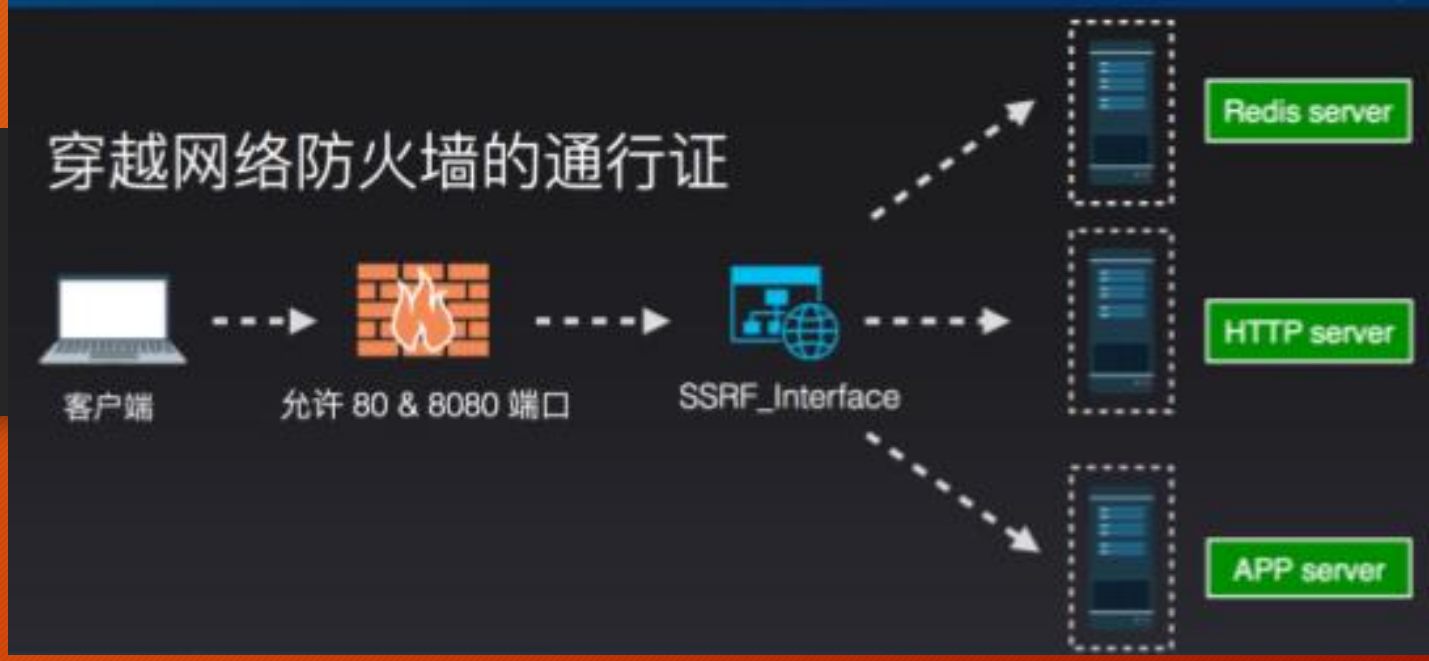
- 漏洞原因：仅仅在前端/浏览器做上传的校验
- BurpSuit 修改 HTTP 请求通常可以绕过

- 防御方法：后端白名单

文件包含/文件读取/文件下载

- 还是因为程序猿太菜，导致参数可控
- 做多几次过滤即可

SSRF



- 服务器端跨站
- 用来攻击内网
- 一台服务器对另一台服务器传过来的东西太过于信任

- 防御方式：对传过来的目标地址或协议进行限制
- http://www.zzfly.net/xnuca-18-writeup/

弱口令、弱密码

- 别说，在大比赛还真的有
- 这个……主要靠运气叭

防守

- 改密码
- 备份网站目录
- 备份数据库
- 上监控（PHP WAF）
- 代码审计（seay 源码审计系统）

- 是什么操作系统
- 有啥特性？安装了什么软件？怎么安装软件？
- IP 地址

PHP 代码怎么安装

- 复制粘贴，修改数据库配置，运行
- Composer 依赖管理
  - composer update

AWD 友谊赛

- 咳咳，欢迎参加第一届(可能没有下一届)的CTF分享会·线下赛

- 比赛类型：AWD
- 比赛时间：一个小时（如果没人AK，则延长半个小时）
- 比赛奖项：得分最高的队伍 -> 小零食
- 比赛环境运行于 DigitalOcean 公有云，请勿对非比赛 ip 以及端口进行非法操作

注意事项

- 10分钟为一个回合
- 存活检测
- 一题签到题目，一题多个 flag，一题动态 flag
- 请根据 GOCTF 上关于“AWD友谊赛”的提示完成比赛

- GOCTF: ctf.scau.edu.cn/goctf | 172.26.14.35:10020/goctf
- 比赛靶机： do.x64.men + 队伍端口

友谊赛 Writeup

- 进攻部分
  - WebSocket 窃听
  - 文件上传校验

- 防守部分
  - Alpine Linux
  - PHP + SQLite 环境
  - Laravel 框架业务部分源码审计