



AWD (Attack With Defence)

模式比赛技巧

第6课 AWD常见套路题

内置的 webshell

代码审计工具

字符串搜索



代码审计工具



字符串搜索

```
find.-name "*.php" |xargs grep-in 'eval( '
```



常见套路--公布的 RCE漏洞

已知 CMS或者框架漏洞

google/ baidu已有漏洞

验证找到的 POC



判断是否为已知CMS或者框架

Joomla

Wordpress

ThinkPHP

带有特征的cms



常用插件

Wappalyzer

Shodan



收集一些具有特征的专属cms的扫描器

是什么类型的CMS

CMS的version是多少

是否有插件漏洞可以选择

最安全的版本号是多少



收集更多信息

透过现象看本质

换汤不换药

报错, robots.txt, 路径探测工具



验证找到的POC能不能一次成功?

如果不能, 在本地复现源码环境调试

判断是不是漏洞被修补了

还是exp中细节有问题(tp5.1.11中和tp5.0.x)



Discuz!查看网站底部的信息版本号

x3.4!目前最完善，但是也要关注随时发的一些1day,后台getshell也要收集

一些利用步骤复杂的漏洞也要关注，可能作为联合考点来进行考察



从验证代码到python Exp

Reissue Request Scripter (Burp plugin)

<https://github.com/h3xstream/http-script-generator>



断网 = gg??

不存在的



乌云镜像站

Seebug (<https://paper.seebug.org/>)

<http://0day5.com/>

先知社区

安全客

vulhub (<https://github.com/vulhub/vulhub>)



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered across the scene, suggesting themes of cybersecurity, data protection, or digital privacy. The overall aesthetic is futuristic and high-tech.

谢谢观赏