

The background features a dark blue color scheme with a glowing network of white and light blue lines connecting various nodes. Two stylized globes are positioned on the left and right sides. Several padlock icons are scattered throughout the background, some appearing to be part of the network structure.

AWD (Attack With Defence)

模式比赛技巧

The background features a dark blue color scheme with a glowing hexagonal grid pattern. Several padlock icons are scattered across the grid, some appearing to be open and some closed. In the bottom-left corner, there is a stylized globe composed of a network of white dots and lines, representing a global network or data flow.

# 第5课 AWD中WEB向常见的题目类型- sql\_server

思路就是确保上传的文件不会被服务器解析成可执行的脚本



标识函数

require()

require\_once()

include()

include\_once()



## 利用方式

PHP 伪协议

包含上传文件

包含日志

session文件包含

远程文件包含(allow\_url\_fopen On

allow\_url\_include On)



文件包含漏洞

PHP 伪协议

php://filter/read=convert.base64-  
encode/resource=

Phar://

phar://1.zip/shell.txt

— 文件包含漏洞

包含上传文件

上传一个 TXT 文档

文档内容为 webshell

包含该文件



赛博梦工厂

Cyber Works

包含 session

前提

session文件路径已知

内容可控

保存路径: 通过phpinfo页面获得

session文件名: sess\_[phpsessid]



赛博梦工厂

Cyber Works

防御方式

搜索标识函数所在位置

尽量避免使用动态包含

使用白名单验证

进行访问路径限制



直接拿 flag  
flag值就在数据库  
flag 为本地文件  
用户权限足够高  
secure\_file\_priv不为NULL  
select load\_file('filename')



数据库存在漏洞写入webshell  
写文件

```
Select ... into outfile '/path/to/save';
```

```
Select ... into dumpfile '/path/to/save'
```



换个思路，别人丢分你就加分，删库跑路



防御：  
代码层面时间成本太大  
建议从waf层面入手



PHP序列化函数  
Serialize()  
Unserialize()



Magic function

构造函数 `_construct()`

当对象创建(new)时会自动调用, 但在 `unserialize()`时不会自动调用。

析构函数 `_destruct()`

当对象被销毁时会自动调用 `_wakeup()`



利用方式

全局搜索 unserialize() 函数看输入是否可控

查找带有 magic 函数的 class

构造调用的 rop 链



防御方式  
分析该函数是否有用  
是否只是为了出题



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 concern. 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 throughout, symbolizing security and technology. A horizontal semi-transparent blue bar runs across the middle of the image, containing the text.

谢谢观赏