[00:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=0s" \t "https://www.youtube.com/) - Introduction 介绍

[01:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=60s" \t "https://www.youtube.com/) - Start of nmap 工具开始于nmap

[02:50](https://www.youtube.com/watch?v=C78yku9WC0o&t=170s" \t "https://www.youtube.com/) - Discovering a likely LFI in product.php but cannot use filters, likely because there is a file\_exists() check 发现了一个类似于LFI本地文件包含的漏洞但是不能利用，似乎是因为file\_exists()函数检查。

[05:30](https://www.youtube.com/watch?v=C78yku9WC0o&t=330s" \t "https://www.youtube.com/) - Playing with the File Upload functionality 使用文件上传功能

[08:40](https://www.youtube.com/watch?v=C78yku9WC0o&t=520s" \t "https://www.youtube.com/) - Talking about the PHAR wrapper in PHP, showing it will bypass the file\_exist and we can go into the ZIP to bypass the .pdf check 谈论PHP中的phar包含，绕过file\_exist()，我们可以使用zip绕过PDF检查

[10:55](https://www.youtube.com/watch?v=C78yku9WC0o&t=655s" \t "https://www.youtube.com/) - Uploading the phar archive, and getting RCE through the LFI and PHAR wrapper 上传phar压缩包，然后获取一个RCE，通过本地文件包含和Phar包含。

[16:40](https://www.youtube.com/watch?v=C78yku9WC0o&t=1000s" \t "https://www.youtube.com/) - Showing the intended File Disclosure vulnerability, by uploading a zip with a symlink 查看意图中的文件泄露漏洞，通过symlink上传zip压缩包。

[18:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=1080s" \t "https://www.youtube.com/) - Creating a python script to automate the file disclosure vulnerability, making it easier for us to download files 创建一个python脚本自动化文件泄露漏洞，使得对我们来说更容易下载文件。

[28:30](https://www.youtube.com/watch?v=C78yku9WC0o&t=1710s" \t "https://www.youtube.com/) - Script completed, looking at the PHP Code, then showing another unintended solution with a zip file and null byte 脚本完成，查看php代码，发现了另一个意料之外的解决方案，使用zip压缩包空字节。

[37:30](https://www.youtube.com/watch?v=C78yku9WC0o&t=2250s" \t "https://www.youtube.com/) - Explaining what happened with the null byte 解释空字节发生了什么？

[40:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=2400s" \t "https://www.youtube.com/) - Showing the intended solution with the null byte, talking about how we can bypass this regex with CRLF Injection due to lack of multi-line 展示了意料之中的解决方案：使用空字节，谈论我们可以使用CRLF注入绕过正则表达式，由于缺乏多线。

[48:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=2880s" \t "https://www.youtube.com/) - Dumping the SQL Database with a union injection 使用union注入下载Mysql数据库

[51:15](https://www.youtube.com/watch?v=C78yku9WC0o&t=3075s" \t "https://www.youtube.com/) - Dropping a file from MySQL and then including it with the LFI to get a shell 从Mysql数据库中下载文件，然后使用本地文件包含获取shell。

[58:00](https://www.youtube.com/watch?v=C78yku9WC0o&t=3480s" \t "https://www.youtube.com/) - As Rektsu we can execute a binary with sudo, running strings discovers a hard coded password. Strace reveals it loads a library that doesn't exist, so we can use MSFVenom to create a malicious library我们可以执行一个二进制，并且是sudo权限，查看字符串发现了一个硬编码。Strace发现了一个不存在的库，所以我们可以使用MSF创建一个恶意程序库。