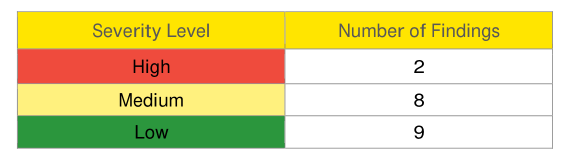
# 总结的问题



# 高级问题

## Stored Cross Site Scripting

### 端口

443

### 影响的资源

#### UAT环境

https://uat.aia.com.cn/mypage/listProductInfo

#### 本地环境

http://localhost:8080/mypage-cn/listProductInfo

这个接口在ProductMgrCtrl.java类中的queryProductInfo这个方法。

### 发现的问题

据观察，Web应用程序容易受到存储跨站点脚本（XSS）攻击。存储的XSS攻击允许攻击者将任意脚本注入Web应用程序数据库，随后在每次加载页面时加载这些脚本。

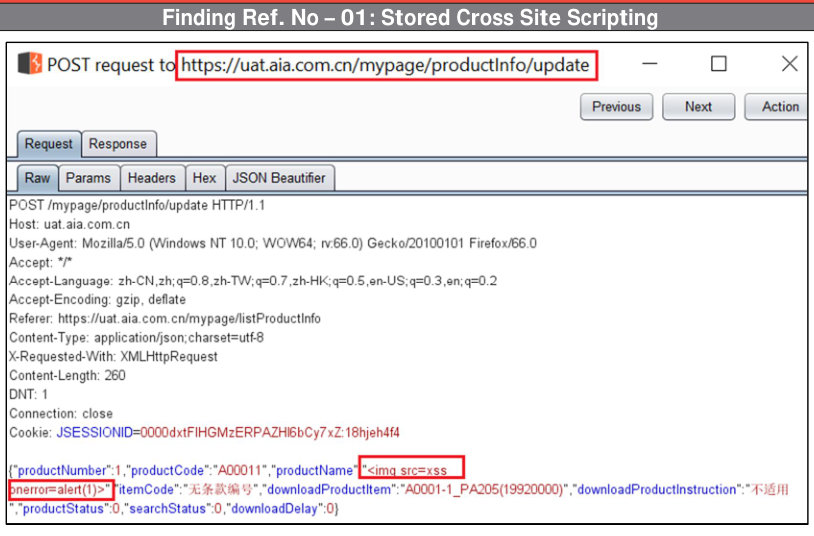
### 风险

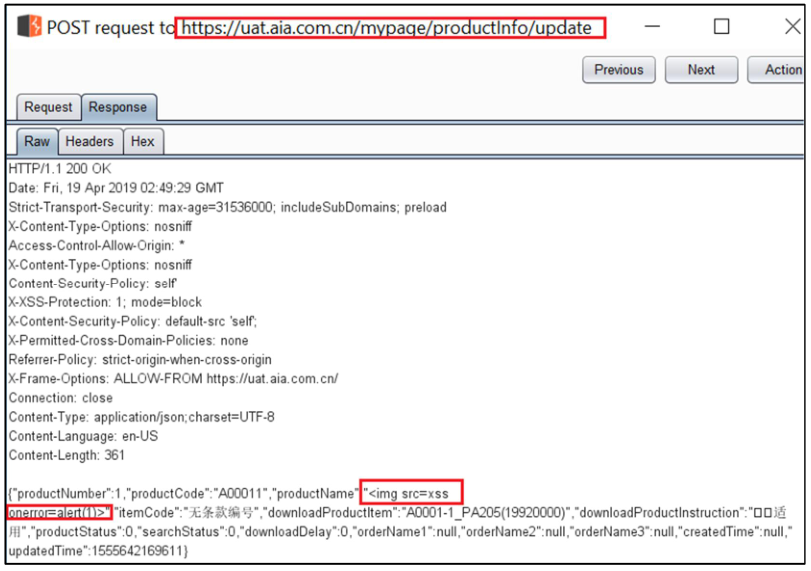
攻击者可利用XSS攻击窃取其他用户的会话ID，代表他们执行操作或执行网络钓鱼攻击。存储的XSS比反映的XSS具有更高的风险，因为注入的脚本存储在服务器的数据库中，并且随后在其他用户浏览社区论坛或主页时加载和执行。

### 结果

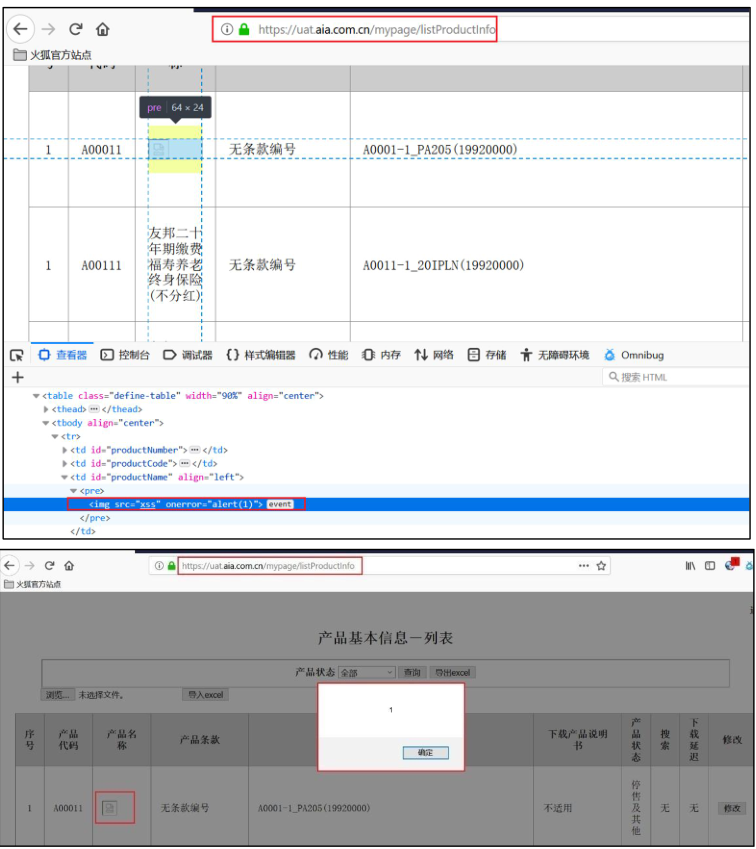
下面的屏幕截图说明了参数” Product Name” 是易受存储的XSS攻击，有效载荷<img src=xss onerror=alert(1)>是提交的，如下图：





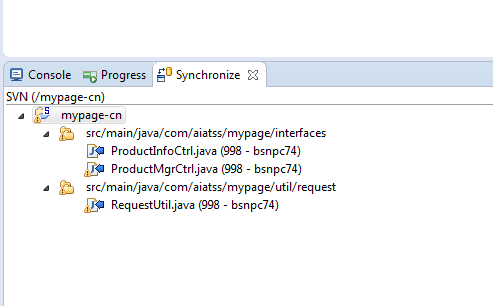


以下屏幕截图说明注入的脚本存储在应用程序中，并在触发易受攻击页面上受影响的参数时，有效负载由客户的浏览器执行：



### 风险缓解

我们建议在客户端和服务器端对用户输入进行适当的清理和过滤。 诸如<>'“％;）（＆+等危险字符应该在屏幕上显示之前不允许或HTML编码。此外，我们建议使用框架级修复程序来覆盖整个应用程序，以防止在Web应用程序中发生重复的XSS攻击。



## Authentication Bypass via Forceful Browsing

### 端口

443

### 影响的资源

#### UAT环境

https://uat.aia.com.cn/mypage/upload

https://uat.aia.com.cn/mypage/listProductInfo

https://uat.aia.com.cn/mypage/email/initService

https://uat.aia.com.cn/mypage/email/inialPurchase

#### 本地环境

http://localhost:8080/mypage-cn/upload

这个接口在ProductMgrCtrl.java这个类中的upload方法

### 发现的问题

任何用户（包括未通过该应用程序进行身份验证的用户）都可以使用直接URL访问经过身份验证的页面，强制访问包含敏感信息的某些页面，例如有关AIA Insurance的产品详细信息。

### 风险

未受身份验证检查保护的文件，页面或功能可能导致未经授权的用户或攻击者执行任务或访问他们无权访问的信息。 这可能包括访问特权功能或敏感信息。

### 结果

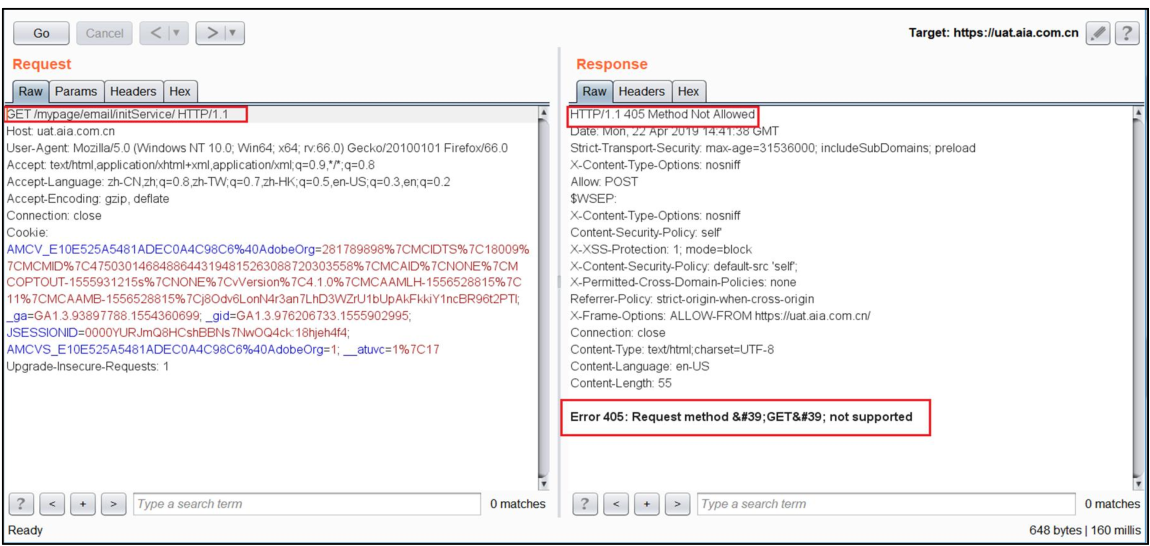
以下屏幕截图显示，无需登录应用程序即可直接访问某些敏感页面：

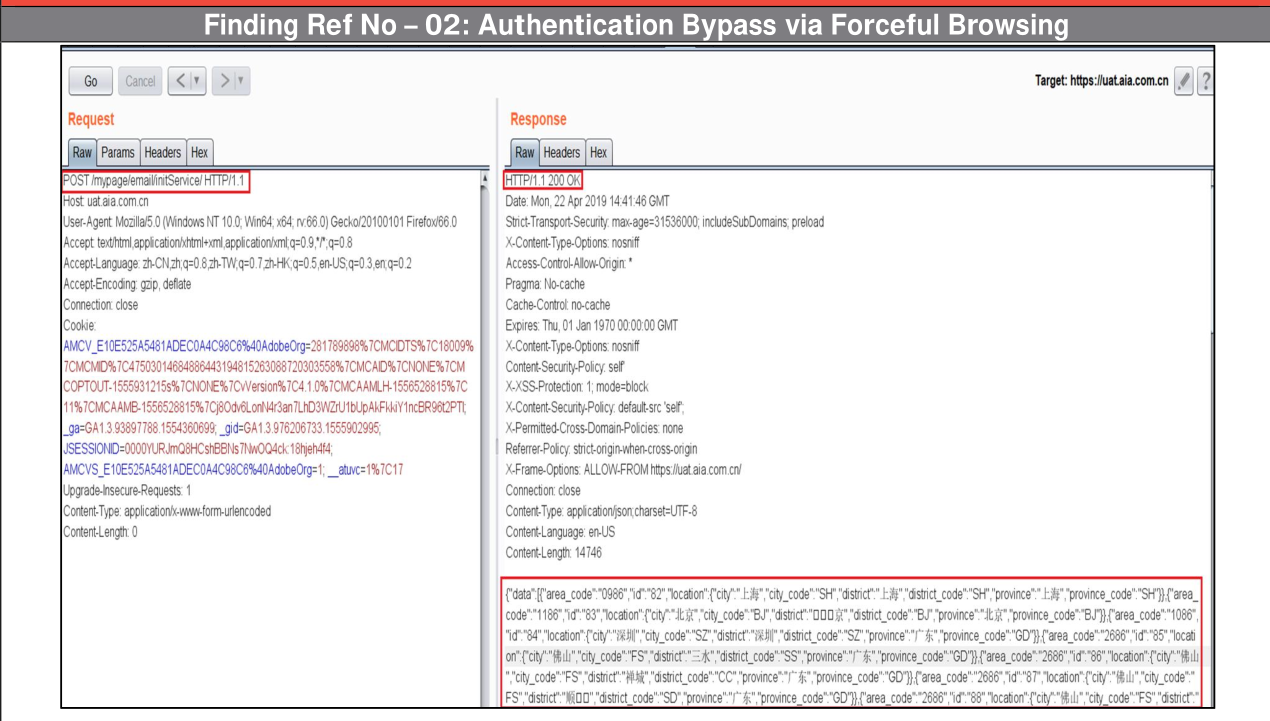




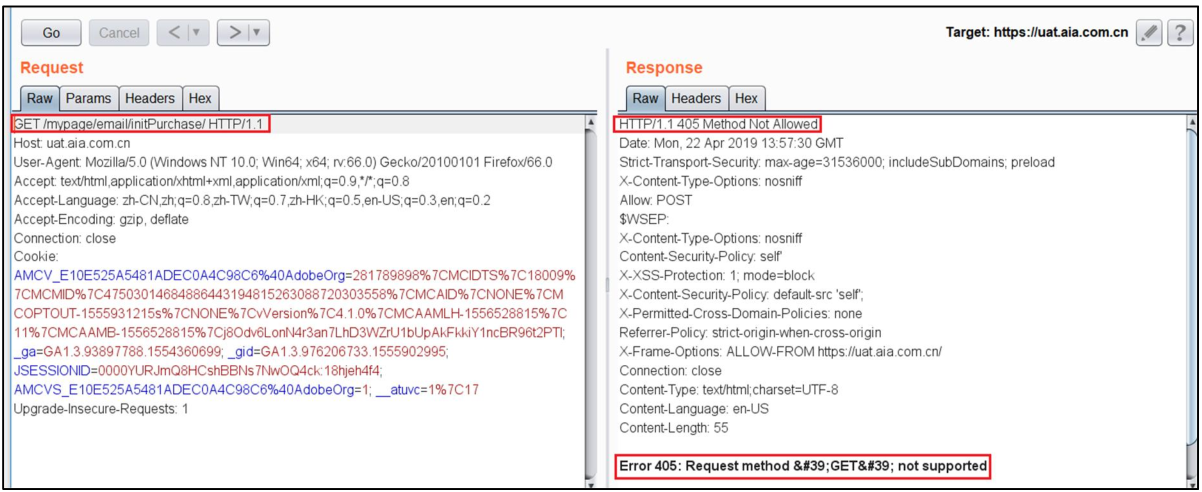
以下屏幕截图说明攻击者可以通过将HTTP方法从GET更改为POST来获取对敏感信息的访问权限

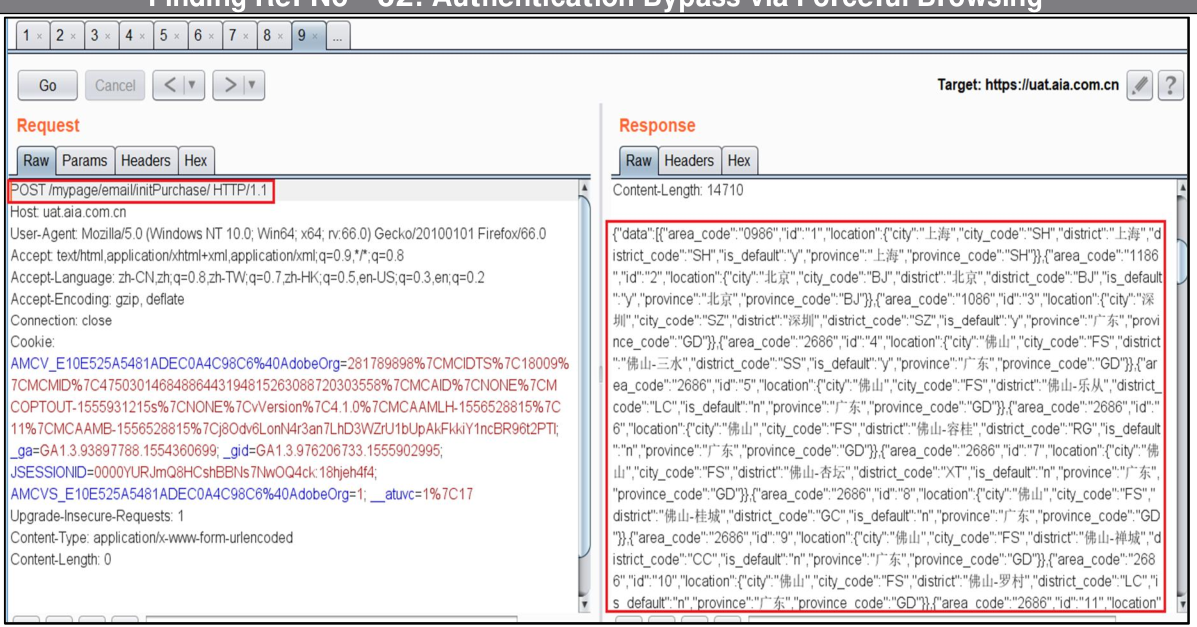
#### 场景一：





#### 场景二：





### 风险缓解

我们建议实施适当的访问控制（身份验证和授权），以便仅管理和限制对授权用户的所有受限制的URL，脚本或文件的访问，不存在包含非加密凭据的此类文件。这些控制应该在服务器端实现。

# 中级问题

## OTP Implementation Flaw

### 端口

443

### 影响的资源

https://uat.aia.com.cn/mypage/sendSms

### 发现的结果

我们注意到发送到手机号码的OTP也在HTTP响应中返回。我们还可以注意到，OTP验证仅在客户端实现，并且未执行服务器端验证。

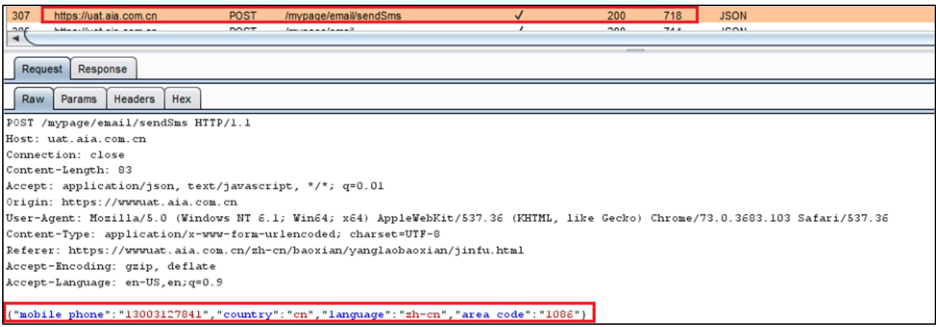
### 风险

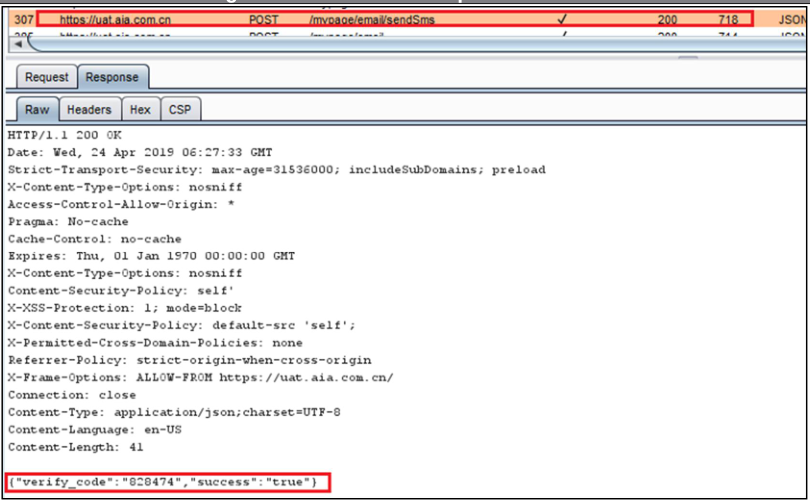
恶意用户可以通过冒充其他用户发送多个投诉/查询表格，因为该应用程序验证了HTTP响应中提供的OTP。这可能导致为AIA团队处理的查询/投诉表格泛滥，他们不会 能够区分真实和虚假的请求。 这可能会导致他们对数量被滥用并对AIA造成声誉损害的人进行不必要的呼叫。 如果潜在客户需要及时回答，它还可能导致他们对真实请求做出反应，从而导致业务损失。

此外，攻击者可能会利用自动脚本重复填充表单并将表单提交给具有大量无意义数据的后端系统。 这可能会导致拒绝服务（DoS）方案，耗尽处理表单提交所需的资源，并阻止系统处理合法请求。

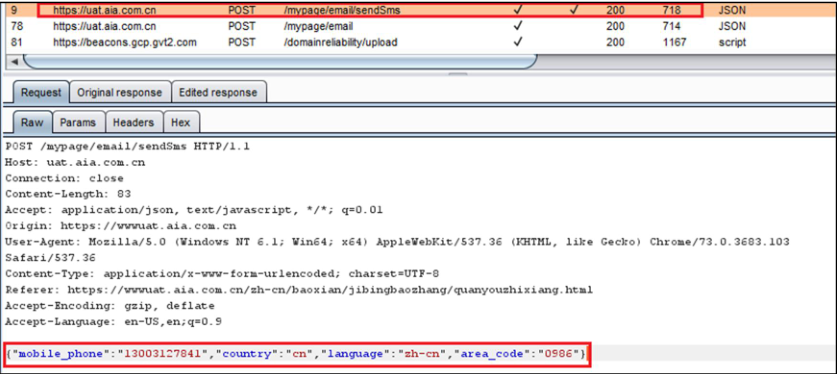
### 结果

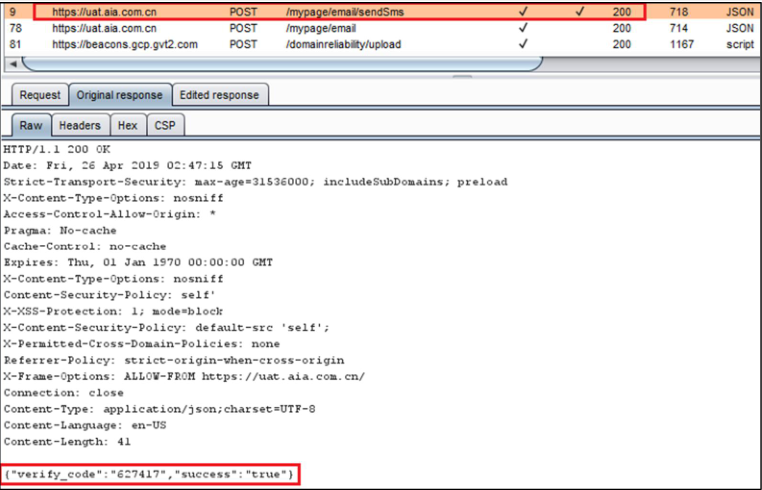
以下屏幕截图说明了响应中返回的验证码。

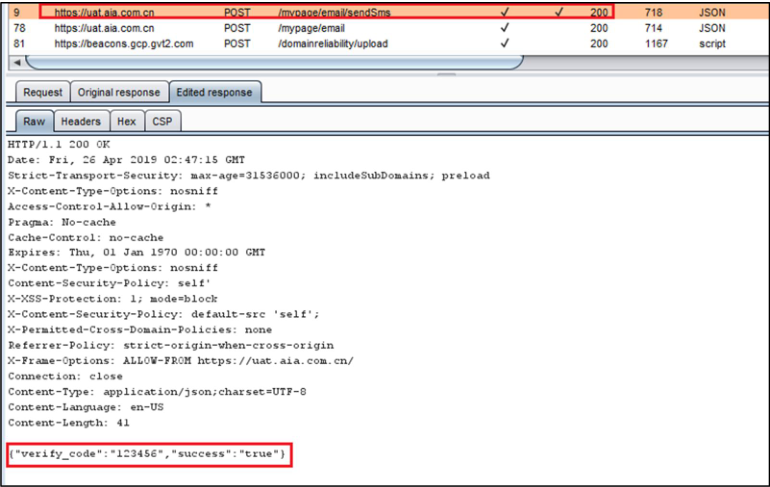




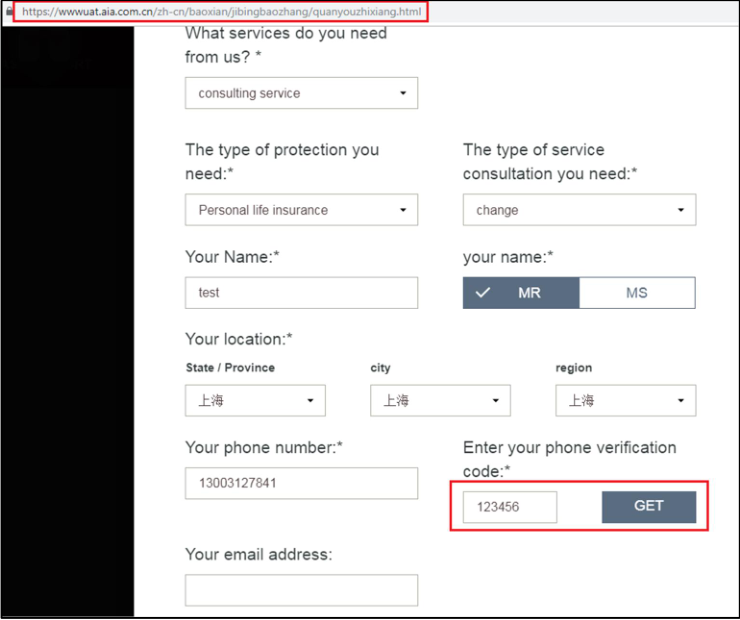
此外，我们注意到验证码的验证仅在客户端实施。 我们能够更改HTTP响应中的验证码，并使用修改后的验证码提交表格，如下图所示。

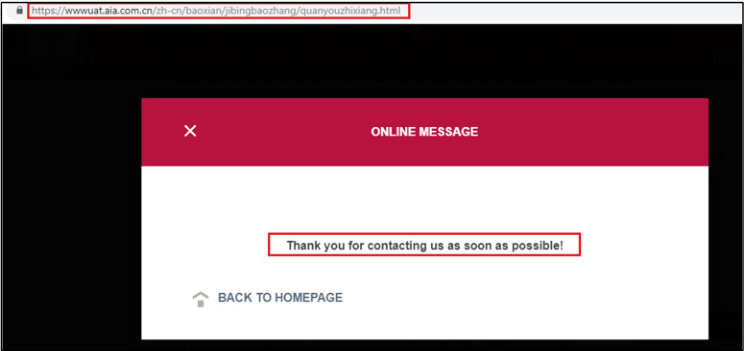






以下屏幕截图说明请求已使用修改后的验证码成功发送。





### 风险缓解

我们建议从HTTP响应中删除OTP以防止模拟或自动表单提交攻击。 此外，应在服务器端执行OTP验证。

## Internet Accessible Administrative Interface

### 端口

443

### 影响的资源

https://uat.aia.com.cn/ind-cal/blue

### 发现的结果

据观察，Web应用程序的管理控制台暴露于Internet，并且尚未启用控制来限制对管理控制台的访问。

### 风险

攻击者可能会执行凭据枚举攻击（例如强力攻击和字典攻击），并可能在发现有效凭据时冒充用户。

获得对管理界面的访问权限的攻击者可以完全控制应用程序，更改应用程序配置设置，在站点页面中嵌入恶意代码以感染最终用户或破坏系统。

### 结果

以下屏幕截图说明了可从互联网访问的后台管理系统：



### 风险缓解

建议限制从外部网络访问管理控制台，并确保适当的访问控制限制。

## Reflected Cross Site Scripting

### 端口

443

### 影响的资源

https://wwwuat.aia.com.cn/zh-cn/fuwu/lipeigongshi2.html

### 发现的问题

据观察，发现Web应用程序易受反映的跨站点脚本（XSS）的影响。

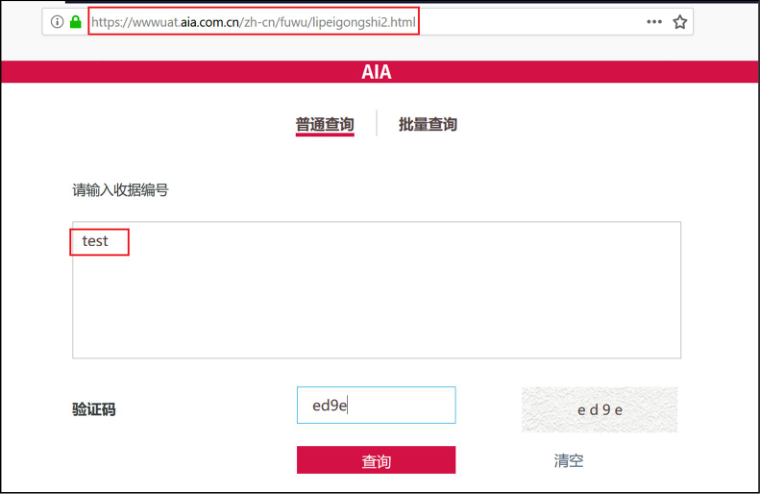
通过引导经过身份验证的用户通过社交工程/鱼叉式网络钓鱼通过预先设定的易受攻击的应用程序页面链接访问应用程序，可以在应用程序用户的浏览器上执行恶意代码，从而使发送给他们的输入能够在他们的浏览器中执行。

### 风险

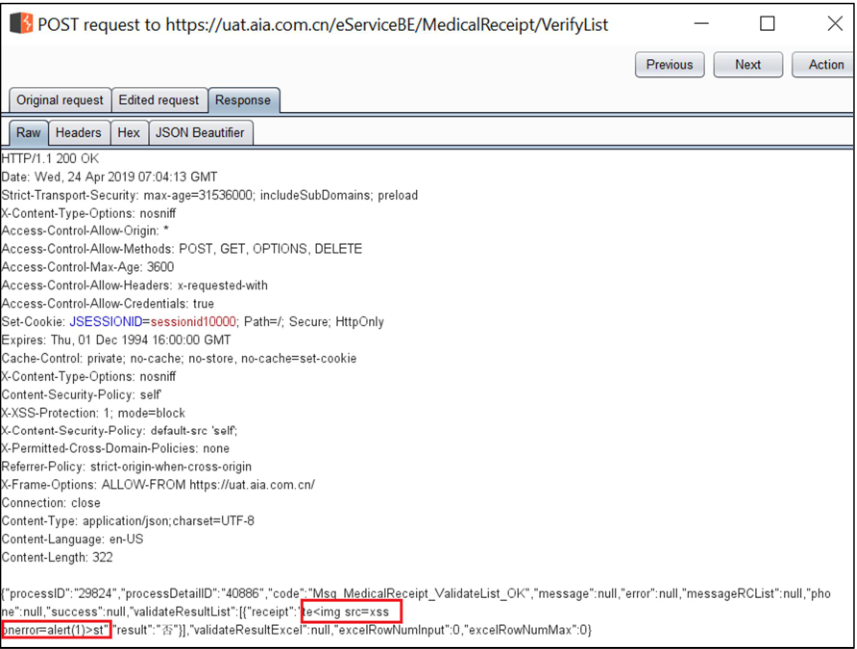
XSS攻击允许攻击者将任意脚本注入到随后显示给其他用户的网页中。攻击者可以利用XSS攻击来窃取用户的会话ID，代表他们执行操作或执行网络钓鱼攻击。

### 结果

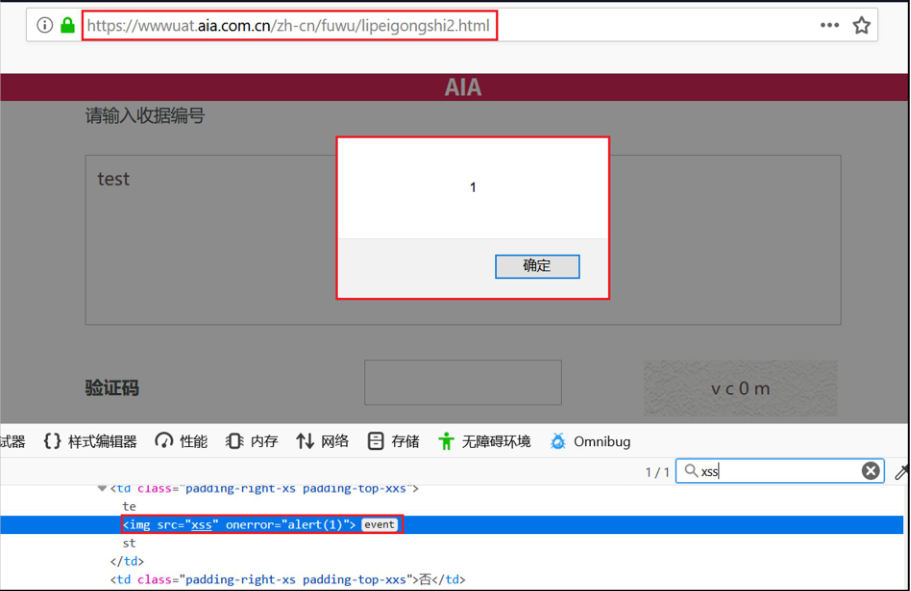
以下屏幕截图显示参数“Receipt Number”易受XSS攻击和有效载荷<img src=xss onerror=alert(1)>被提交，如下图：







有效载荷成功执行，如下图：



### 风险缓解

用户输入应该在客户端和服务器端进行适当的清理和过滤。危险的特殊字符集，例如<>'“％;）（＆+应该被禁止或HTML编码，然后才能在屏幕上显示它们。

## Malicious File Upload

## Outdated and Vulnerable Version of Software in Use

## Host Header Injection

## Business Logic Bypass

## Sensitive Information Passed over GET Request