MOPCMS\_V1.0\_UTF8 XSS 跨站脚本 　漏洞评分工作表

1. **漏洞基本属性**

漏洞名称（参考附件一：CNNVD命名规范）：　MOPCMS\_V1.0\_UTF8 XSS 跨站脚本漏洞

漏洞类型（参考附件二：CNNVD分类规范）：　　XSS 跨站脚本漏洞

漏洞评分（参考附件二：CNNVD分级规范）：　　　　　7.3

漏洞危害等级（参考附件二：CNNVD分级规范）：　　　　高危

1. **漏洞评估属性**

**１、影响范围**

【判定结果】：

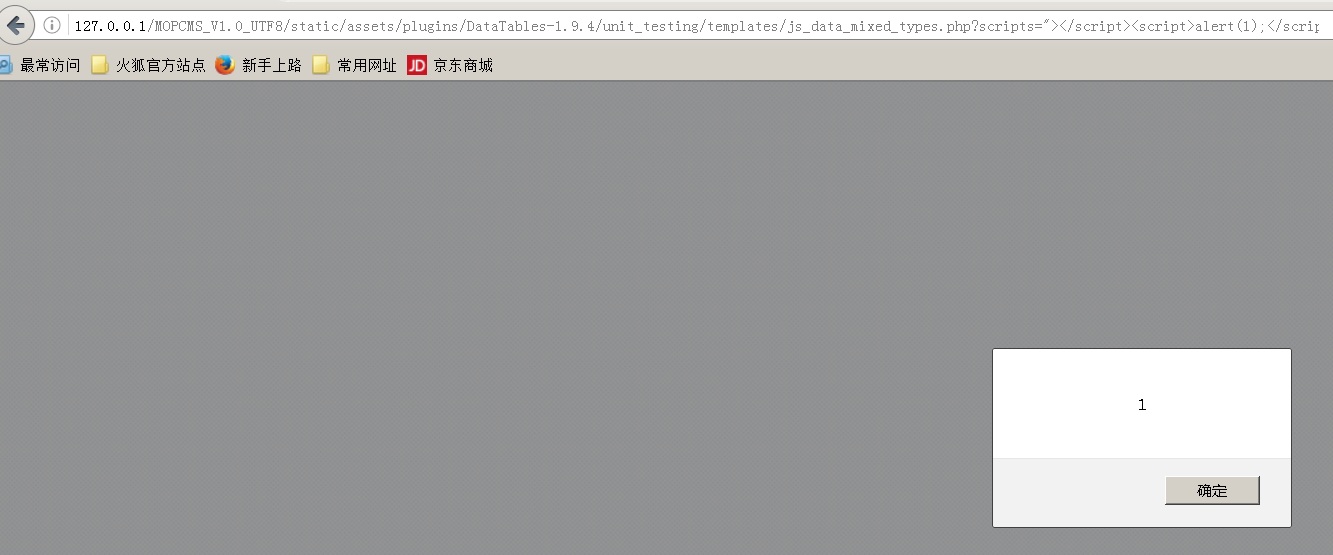
MOPCMS\_V1.0\_UTF8 2019-03-25及之前版本中MOPCMS\_V1.0\_UTF8/static/assets/plugins/DataTables-1.9.4/unit\_testing/templates/js\_data\_mixed\_types.php

【判定说明】

MOPCMS\_V1.0\_UTF8/static/assets/plugins/DataTables-1.9.4/unit\_testing/templates/js\_data\_mixed\_types.php存在XSS跨站脚本漏洞，攻击者通过构造scripts参数可以执行任意的web 脚本或者html 文件。

【证明截图】

注入脚本，反弹对话框。



**2、攻击途径**

【判定结果】：

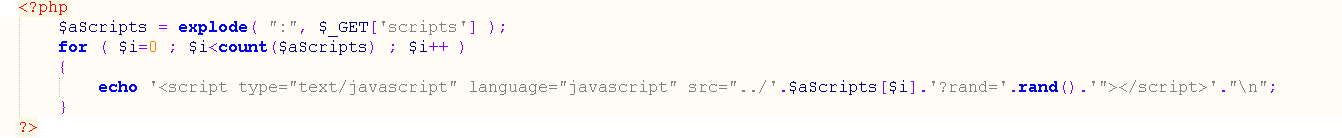
网络

【判定说明】

可以从互联网发起攻击

【证明截图】

攻击者通过$\_GET方法获得scripts参数，因此是可以从互联网发起攻击的



**3、攻击复杂度**

【判定结果】：

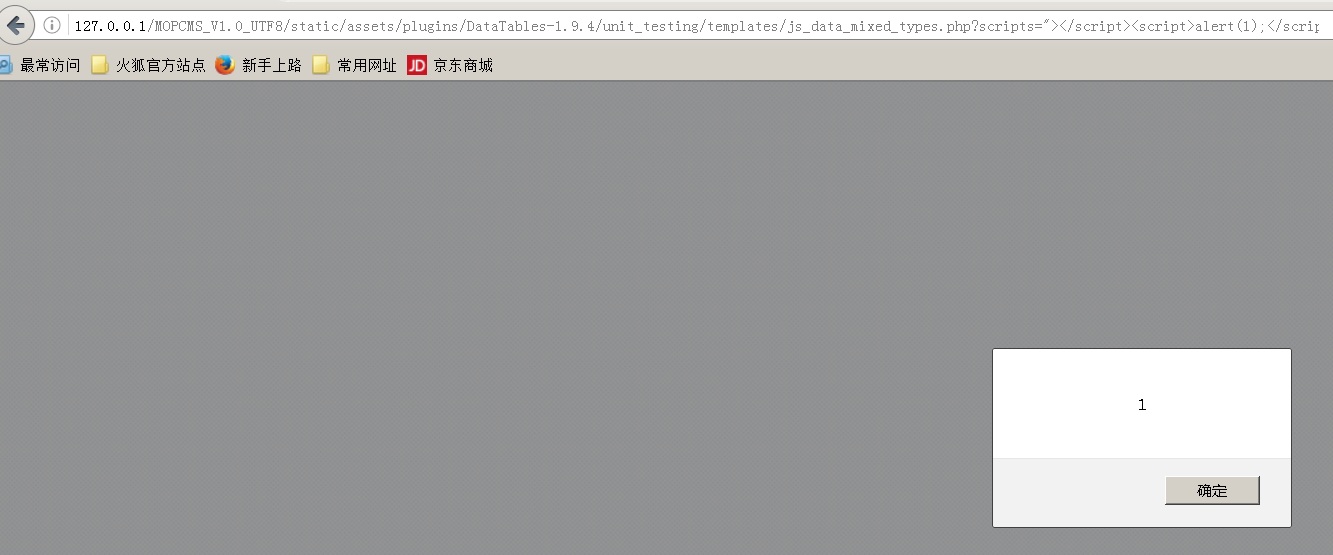
低

【判定说明】

攻击者只需要在URL中通过scripts参数注入脚本，不需要做任何其他事情。

【证明截图】

只需要执行脚本就攻击成功



**4、权限要求**

【判定结果】：

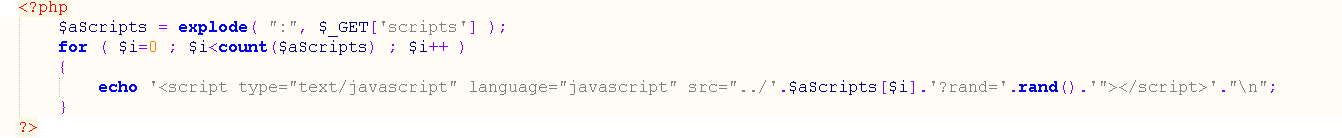
无

【判定说明】

攻击者不需要任何权限，直接构造含有攻击代码的URL即可攻击成功。

【证明截图】

漏洞代码中只是通过$\_GET方法获得scripts的参数，随即将其输出，并没有做任何的权限判定。



**5、用户交互**

【判定结果】：

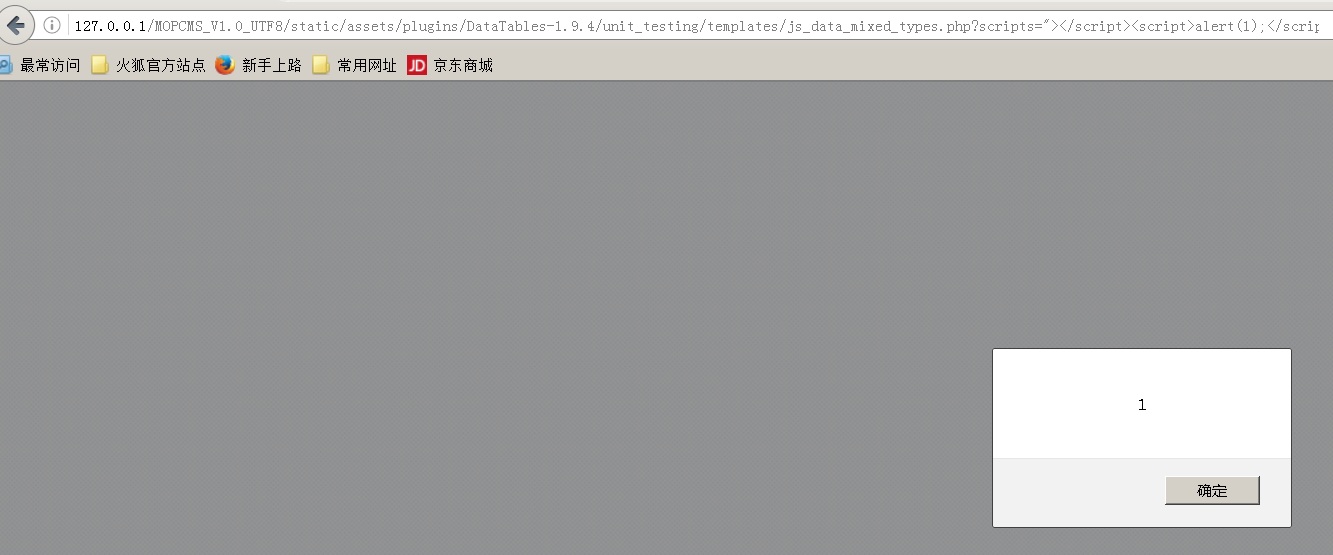
不需要

【判定说明】

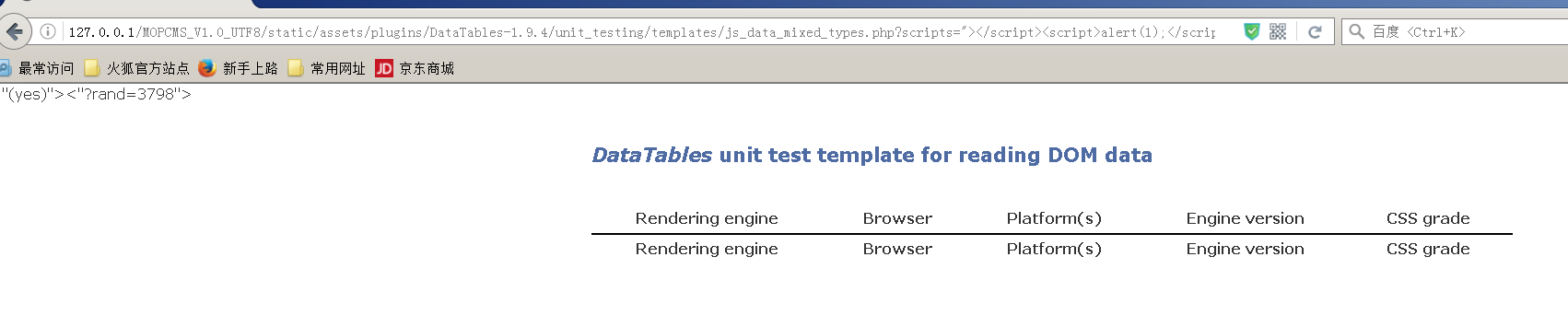
攻击者不需要任何其他用户操作，直接可执行注入的脚本。

【证明截图】

只需要攻击者通过scripts参数构造恶意的URL，注入的脚本就会成功执行。



点击确定：



**6、机密性影响**

【判定结果】：

低

【判定说明】

通过scripts参数向目标URL注入恶意脚本，即可执行恶意代码。

【证明截图】

**7、完整性影响**

【判定结果】：

低

【判定说明】

通过scripts参数向目标URL注入恶意脚本，即可执行恶意代码

【证明截图】

**8、可用性影响**

【判定结果】：

低

【判定说明】

通过scripts参数向目标URL注入恶意脚本，即可执行恶意代码

【证明截图】