XSS\_DOM

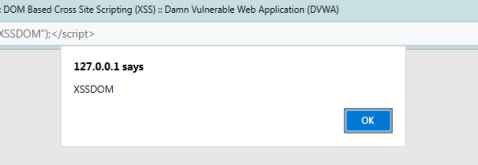
Low:



可以看出该表单通过GET方式获得了default参数

尝试直接在English后加入脚本 <script>alert(“XSSDOM”)</script>

成功！

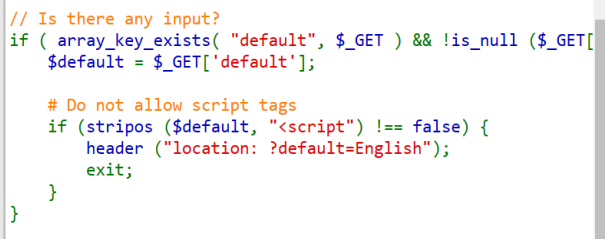


Medium：

插入任何script脚本后只显示default = English

大小写和双写尝试失败

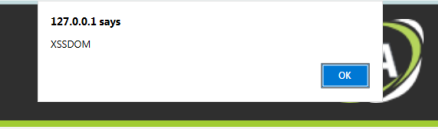
考虑是js脚本被替换掉了



尝试使用html标签

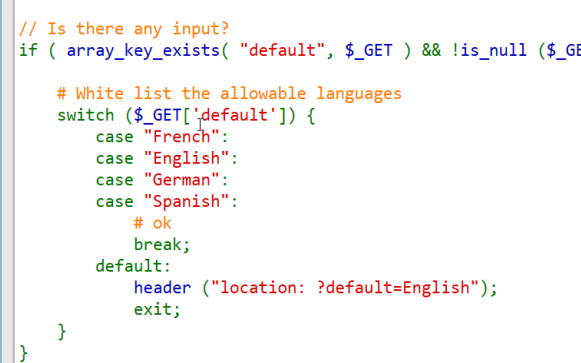
First step 闭合之前的标签 </option> </select>

Then 插入一张不存在的图片 <img src = “x” onerroe = ‘alert(“XSSDOM”)’> </img>



High:

防御原理：



服务器端只识别固定的四个选项

尝试方法 绕过服务端

# 位置标识符 后面的内容会被看做一个位置

不会随src发送到服务器端

#<script>alert(“XSSDOM”);</script>

