XSS Filter Evasion Cheat Sheet (XSS BYPASS备忘录)

legend / 2017-11-28 14:26:00 / 浏览数 3345 安全技术 资源分享 顶(0) 踩(0)

应冰总要求发这里啦!

Xss Bypass备忘录

技术要发展,免不了风波. 也许这些攻攻防防会更好的促进技术的发展也说不定 就让这一次次的爆破换来将来更精练的技术的无比的宁静吧 我们静观其变吧!

缅怀当初那份最纯真Hacker精神!!

2017.深圳 By:Legend

译文源起

翻译本文最初源自国内在对2014年老道翻译的一个版本,发现此版本有些翻译个人认为不太满意,在加上2017年国庆长假漫漫,无人陪伴(主要还是约妹子没约出来!)。 BYPASS备忘录。文中所有代码参考OWASP官方复制,同时对于官方文档里面有些描述不太清楚地方译者通过自己对XSS理解加入一些自己见解,来帮助各位对XSS理解更_ 翻译官方修订的版本:10/2/2017

关于译者:ID太多自己都忘记叫那个比较合适,就叫笑摸二楼狗头吧!

译者说明

译者为legend,当然也有人叫我小黑.或者...名字这些都不重要.本文部分章节采用了, OWASP Cheat Sheet Series翻译项目, XSS过滤绕过备忘单[XSS过滤绕过备忘单-http://cheatsheets.hackdig.com/?4.htm

部分小段,大概位于"URL字符串绕过"章节特此说明.因为译者认为他们翻译比我更为通顺.其他部分皆为译者结合全文与相关资料而编写,鄙人不认为说比老道版本好多少或者差如果有兴趣一起交流技术也欢迎联系我.作为一位安全圈萌新,还需要各位大佬带带,最后感谢自己的团队还有各位老铁们支持,如果没有你们意见或许就没有这份文档出现.关于;因上努力,果上随缘

特此说明:备忘录中译者标注和添加解释部分均用插入脚注方式或者如(译者注:)颜色标明,望知晓.

目录

```
6
6
XSS
XSS
6
XSS
■■image■■■■Java Script■■
-----7
7
HTML
<IMG>
fromCharCoded 8
SRC SRC , SRC
■SRC■■■■■. 8
SRC 8
■■erro■■■■ 9
IMG onerror■Java script■■■■ 9
■■■html■■■■ 9
■■■■■■■■■■html■■■■ 9
html
■■TAB■■ 10
TABLE 10
INTERPORT STATE
THE SECUENCY
          10
Null■■■■javascript■■
Javascript 10
```

XSS Filter Evasion Cheat Sheet ■ Chinese ■ 1

```
XSS 11
11
■■</script>■■■ 11
Script
■■■■■■■■HTML/JavaScript ■■XSS
                                                          11
12
Javascript 12
■■</title>■■■XSS 12
<input>
BODY >
                                   13
■■<img>■■■Dynsrc■■■■XSS 13
■■<img>■■■Lowsrc■■■■XSS 13
<img>
WBscript
XSS 13
■■Livescript■■■■XSS(■■■■■Netscape) 13
SVG <object> XSS 13
■■ECMAScript 6■XSS 13
■■<BODY>■■ONLOAD■■■■XSS 14
14
BGSOUND >
■■& JavaScript includes■■■■XSS 20
Image: Image: All the control of the control o
EXECUTE XSS 20
XXXX part 3 21
■■■■■■■■■■■XSS part 4 21
<style>
XSS payload 21
Style>
Style
STYLE> ( Netscape) 21
■■<style>■■■background-image■■■■XSS 21
<style> background XSS 22
Style HTML XSS 22
HTCHHHXSS 22
US-ASCII■■ 22
■■< META >■■■XSS 22
META>
Content
META
22
META>
URL
XSS
<IFRAME>
XSS 23
STRAME
STRAME
23
■■<FRAME>■■XSS 23
TABLE> XSS
                                      23
■■<TD>■■■■XSS 23
■■<DIV>■■ 23
■DIV■■■background-image■■■■XSS 23
■■background-image■■■■unicoded■■■■XSS
DIVERSE 24
TIETT XSS 24
■■<BASE>■■■■XSS 24
■■<OBJECT>■■■■XSS 24
■■■■■■■XSS payload■SVG 25
■■ActionScript■■■■■XSS payload 25
XML CDATA XXS 25
XML embedded XML Javascript 26
■■XML■■■HTML+Time■■■■XSS 26
■■■■■■■■■■■■■".js"■■■ 26
SSI(■■■■■)■■XSS 26
■■PHP■■XSS 26
■■IMG■■■■■■■XSS 27
■■IMG■■■■■■■■XSS part II
Cookie■■ 27
■■UTF-7■■■■XSS 27
HTML
■■■■■■■XSS payload 28
URLEEEE 28
III III
■■URL■■ 28
28
```

29 ■■Google"■■■■" part 1 29 ■■Google"■■■■" part 2 30 ■■Google"■■■■" part 3 30 **TIME**cnames 30 30 ■■Javascript■■■ 30 ■■■■■■■payload 30 30 32 XSS■■■■ 32 ■■XSS bypass WAF■■■■ 33 34 ■■■ 35 35

XSS Filter Evasion Cheat Sheet_最终版.rar (0.109 MB) <u>下载附件</u> 点击收藏 | 0 关注 | 0

上一篇: leave_msg的wp 下一篇: 利用 LLMNR 名称解析缺陷劫持...

1. 54 条回复



only 2017-11-28 16:19:33

动动手指,沙发就是你的了!

0 回复Ta



trysma**** 2017-11-28 17:21:22

前端菜鸡前来膜拜



小马哥 2017-11-28 17:24:28

搬个小板凳

0 回复Ta



<u>王天</u> 2017-11-28 18:03:13

还要回复才能看得到啊,不知道是什么样的

0 回复Ta



黑风里 2017-11-28 18:26:40

前端菜鸡前来膜拜



xingxingye 2017-11-28 18:37:04

感觉很厉害的样子,要看看

0 回复Ta



godsec 2017-11-29 09:35:57

还要回复才能看得到啊,不知道是什么样的

0 回复Ta



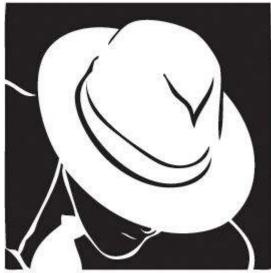
gdygz 2017-11-29 09:53:09

前端菜鸡前来膜拜



@gdygz @godsec @王天 已经更新了目录

0 回复Ta



anothery 2017-11-29 11:03:52

这样就可以拿到了 get123

0 回复Ta



evilox 2017-11-29 13:58:28

谢谢..这个牛逼了

0 回复Ta



north 2017-11-29 16:37:35



haha182 2017-11-30 08:48:47

谢谢分享

0 回复Ta



hackbar 2017-11-30 13:09:47

膜拜~





primzahl 2017-11-30 23:58:36

来学习了, 打卡

0 回复Ta



hyp3r 2017-12-02 13:28:54

学习



ambulong 2017-12-03 15:01:12



<u>梦</u> 2017-12-03 17:07:06

很高深的姿势啊

0 回复Ta



building 2017-12-04 10:12:20

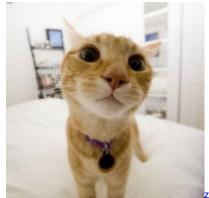
前端菜鸡前来膜拜口

0 回复Ta



anxlang 2017-12-04 10:41:32

主要是为了看附件



ze7o 2017-12-04 12:54:58

0 回复Ta



hope 2017-12-04 16:36:50

学习,感谢分享!

0 回复Ta



A0xpge 2017-12-05 13:56:05

杜绝伸手党,请回复后查看附件



<u>r00tuser</u> 2017-12-05 14:04:03

感谢~

0 回复Ta



toysweet 2017-12-06 14:35:49

杜绝伸手党,请回复后查看附件

0 回复Ta



fry**** 2017-12-07 11:28:57

看看学习一波技术



<u>1686091361468381</u> 2017-12-07 13:36:18

主要是为了附件才回复的

0 回复Ta



mayter1 2017-12-08 10:36:14

---来学习下----

0 回复Ta



torah 2017-12-11 11:25:40

刚好非常需要,可以根据这个文档结合以前的整理搞点事情。



<u>1310703988967481</u> 2017-12-13 11:26:26

刚好非常需要,可以根据这个文档结合以前的整理搞点事情。

0 回复Ta



fantasy70 2017-12-13 14:23:43

来学习下

0 回复Ta



<u>182****1615</u> 2017-12-14 20:21:46

学习一下



green 2017-12-16 17:15:01

学习一下

0 回复Ta



backlion 2017-12-18 21:43:36

最近在整理xss漏洞,参考下

0 回复Ta



nok1a 2017-12-18 23:05:48

大牛给力



noosec 2017-12-20 11:22:30

learn

0 回复Ta



test 2017-12-21 12:17:56

来学习一下

0 回复Ta



舞阻 2017-12-24 19:34:11

学习学习



<u>0x17</u> 2017-12-26 23:15:34

感谢分享过来学习~ ;)'{}'【】[]:"''

0 回复Ta



九尾妖狐 2017-12-28 19:39:10

学习学习"/><xss>



就是个id吧 2017-12-29 23:23:44



beianks 2018-01-08 15:22:10

学习学习 xss 很不错

0 回复Ta



旋风洗衣机 2018-01-15 16:16:48

膜拜大佬,学习学习



<u>187****9064</u> 2018-02-01 10:06:17

动动手指 沙发就是睡得



dar****@qq.com 2018-02-03 23:41:03

膜拜一波

0 回复Ta



finger 2018-06-18 09:11:48

测试 回复~~

0 回复Ta



am4zing 2018-07-21 22:32:56

前来学习



川川的zoey 2019-04-28 15:54:49

谢谢楼主~感恩

0 回复Ta



<u>肉haoyo</u> 2019-08-01 13:48:47

学习学习

0 回复Ta



mr_s1e**** 2019-08-08 15:38:35

膜拜大佬



windmill_kn**** 2019-08-12 00:02:35

学习学习

0 回复Ta



Apaperrrrr 2019-08-12 21:38:37

学习

0 回复Ta



又是一年落花shi 2019-08-28 14:08:38

学习

ᅏᆿ	一四十
⇔ऋ	

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板