xssfork-一款xss探测工具

b5mali4 / 2017-07-24 12:14:00 / 浏览数 3493 安全工具 工具 顶(0) 踩(0)

---

xssfork简介

xssfork作为sicklescan的一个功能模块，其开发主要目的是用于检测xss漏洞。
传统的xss探测工具，一般都是采用 payload in
response的方式，即在发送一次带有payload的http请求后，通过检测响应包中payload的完整性来判断，这种方式缺陷，很多。
第一：不能准确地检测dom类xss
第二：用类似于requests之类的库不能真正的模拟浏览器
第三：网页js无法交互
怎么解决？如果能够用浏览器代替这个模块，去自动hook是最好的。所幸，我了解到phantomjs，当然现在google浏览器也支持headless模式，类似的，你也可以采用go

原理

对于这类fuzz过程,基本都是预先准备好一些payload,然后加载执行。对于这类io型密集的扫描模型，后端使用多线程就比较适用，但是由于phantomjs你可以理解为一个无

编码脚本

由于基础的payload模块，我收集了71个。

基础pyaload会在现有的基础上，会添加上各种闭合的情况。

除了这些基础的payload,xssfork还提供了几个编码脚本，查看脚本，可以看help

现阶段提供了10进制，16进制，随机大小写，关键字叠加四个脚本。

10hex_encode

将html标签内部字符10进制化

```
<a href=javascript:alert(65534);>aaa</a>
```

其效果如下

16hex_encode

将html标签内部字符16进制化

uppercase

随机大小写
将

```
<script>alert(65534);</script>
```

转换成

```
<ScRIPt>alert(65534);</ScRIpT>
```

addkeywords

主要是应对过滤为replace('keywords','')的情况

```
<script>alert(65534);</script>
```

变成

```
<<script>script>alert(65534);</script>
```

当然默认开启的是轻量模式，即只返回一个payload，开启重量模式，可以生成更加丰富的pyaload，效果如下

```
<script>alert(65534);</script>
<script>alert(65534);</ScrIpt>
<ScrIpt>alert(65534);</sCrIpt>
<scRiPt>alert(65534);</script>
```

```
<ScrIpt>alert(65534);</script>
```

演示

post类型
python xssfork.py -u xx -d 'xx'
存储型
python xssfork.py -u xx -d 'xxx' -D '输出位置'
当然还可依携带cookie

说明

开源只为分享，请勿将本脚本做任何商业性质的集成。开发的时候，有可能很多情况没有考虑到，如果你有更好的建议或者发现bug，可以联系我邮箱,xssfork.codersec.net
root@codersec.net
开源地址 https://github.com/bsmali4/xssfork
记得不要吝啬你的star

上一篇：狗汪汪玩转嵌入式——I2C 协议分析 下一篇：代码审计之 Appcms SSRF...
1. 0 条回复
   - 动动手指，沙发就是你的了！