【low】Bee-box writeup---html injection-reflected（get）

原创

xiaomi_qwe 于 2017-03-22 15:52:00 发布 1131 收藏
分类专栏： web安全 文章标签： web漏洞测试平台

1 html injection-reflected(get)

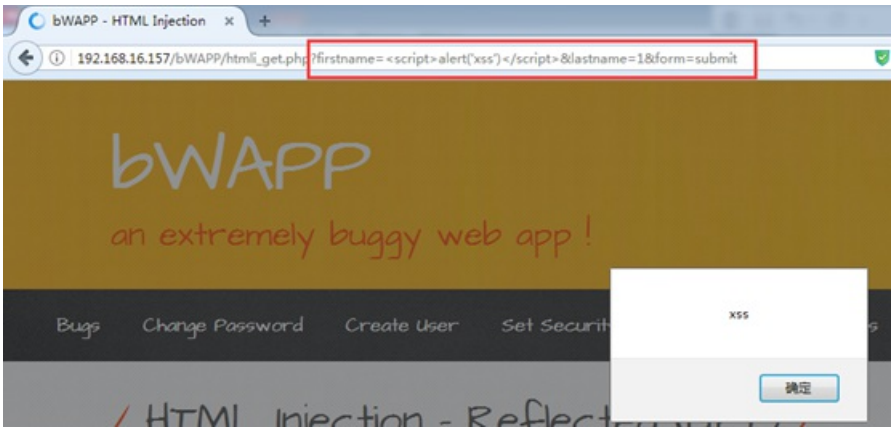
0x00：

因为题目是HTML注入，所以看到登录框不要以为是sql注入了，特意查看页面源代码，请求方式是get，处理页面是本页显示，所以根本没有数据库交互，源码其他的就是加载一些css样式和一些Google js的apl了。源码截图如下：

```
<div id="main">

    <h1>HTML Injection - Reflected (GET)</h1>

    <p>Enter your first and last name:</p>

    <form action="/bWAPP/htmli_get.php" method="GET">

        <p><label for="firstname">First name:</label><br />
        <input type="text" id="firstname" name="firstname"></p>

        <p><label for="lastname">Last name:</label><br />
        <input type="text" id="lastname" name="lastname"></p>

        <button type="submit" name="form" value="submit">Go</button>

    </form>

    <br />
    Welcome 1 1
```

0x01：

当然接下来就进入正题了，既然是HTML注入，那就在输入框中输入恶意的js代码看看效果；当然你可以输入：<script>alert('xss')</script>,输入后页面将会执行js代码执行弹窗；再查看源码，并没有对输入的恶意字符串进行过滤和编码；成功注入到HTML中：




```
68
69      <br />
70      Welcome <script>alert('xss')</script> 1
71  </div>
```

0x02：

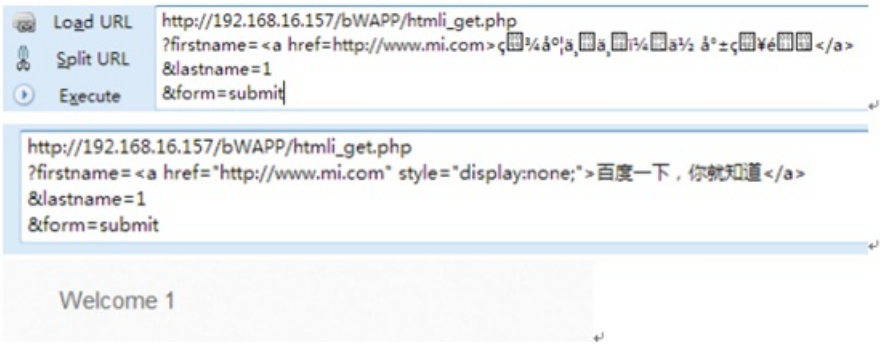
HTML注入的危害都有1：引起页面错乱，破坏结构；2：影响SEO，pr高的网址，如果链到你的网站，可以加大自己网站的权重，这也是为什么有人喜欢在高pr的网站灌水的原因了；

接下来开始灌水了：

<ahref=http://www.mi.com>百度一下，你就知道【会显示在前端】

<ahref="http://www.mi.com" style="display:none;">百度一下，你就知道【前端不显示】

如图所示：成功注入到HTML中，可以点击连接跳到别的网站：



查看源代码成功注入：

”

```
69      <br />
70      Welcome <a href="http://www.mi.com" style="display:none;">百度一下，你就知道</a> 1
71  </div>
```