

XSS 是什么？

作者：方应杭

链接：<https://zhuanlan.zhihu.com/p/22500730>

来源：知乎

著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

新人经常在不知不觉中写出一个 XSS 漏洞，甚至连老司机也偶有湿鞋。

请用自己的语言简述：

1. XSS 是什么（举例说明）
2. 如何防治 XSS

XSS 是什么？

是英文 Cross-Site Scripting 的缩写。



简单来说

1. 正常用户 A 提交正常内容，显示在另一个用户 B 的网页上，没有问题。
2. 恶意用户 H 提交恶意内容，显示在另一个用户 B 的网页上，对 B 的网页随意篡改。

造成 XSS 有几个要点：

1. 恶意用户可以提交内容

2. 提交的内容可以显示在另一个用户的页面上
3. 这些内容未经**过滤**，直接**运行**在另一个用户的页面上

举例说明

假设我们有一个评论系统。

用户 A 提交评论「小谷你好」到服务器，然后用户 B 来访问网站，看到了 A 的评论「小谷你好」，这里没有 XSS。

恶意用户 H 提交评论「<script>console.log(document.cookie)</script>」，然后用户 B 来访问网站，这段脚本在 B 的浏览器直接执行，恶意用户 H 的脚本就可以任意操作 B 的 cookie，而 B 对此毫无察觉。有了 cookie，恶意用户 H 就可以伪造 B 的登录信息，随意访问 B 的隐私了。而 B 始终被蒙在鼓里。

XSS 的成因以及如何避免

继续上面例子，之所以恶意脚本能直接执行，有两个可能

1. 后台模板问题

```
<p>
评论内容：<?php echo $content; ?>
</p>
```

\$content 的内容，没有经过任何过滤，原样输出。

要解决这个问题，只需要后台输出的时候，将可疑的符号 < 符号变成 < (HTML 实体) 就行。

2. 前端代码问题

```
$p.html(content)
```

或者

```
$p = $('<p>' + content + '</p>')
```

content 内容又被原样输出了。解决办法就是不要自己拼 HTML，尽量使用 text 方法。如果一定要使用 HTML，就把可疑符号变成 HTML 实体。

示例代码

以上，就是 XSS 的简单介绍。

更多前端知识，尽在前端交流 4 群：392054247

