Atitit 注入安全风险行为总结

目录

[1. 常见注入类型 1](#_Toc13400)

[1.1. Xssr注入问题 1](#_Toc27755)

[1.2. Sql注入问题 1](#_Toc27377)

[1.3. Xpath注入 1](#_Toc12114)

[1.4. Sehell注入非法行为 1](#_Toc17865)

[1.5. Nosql注入 1](#_Toc11590)

[2. TOP1-注入的防范与解决 1](#_Toc13588)

[2.1. TOP1-注入的防范 2](#_Toc26119)

[2.2. TOP1-使用ESAPI（https://github.com/ESAPI/esapi-java-legacy） 2](#_Toc12429)

# 常见注入类型

## Xssr注入问题

## Sql注入问题

## Xpath注入

## Sehell注入非法行为

[Web Shell 攻击](https://baike.baidu.com/item/webshell/966625?fr=aladdin" \t "https://www.infoq.cn/article/_blank)是一种隐蔽方法，用于获得对服务器的未经授权的远程访问。Web Shell 是利用 Web 服务器核心功能（为远程客户端提供服务）获得持久远程访问并通过与服务器 Shell 的接口获得对服务器的完全或有限控制的后门程序。根据 Verizon DBIR 由 Web Shell 后门造成的 Web 应用程序攻击破坏数量仅次于凭据被盗。

## Nosql注入

# TOP1-注入的防范与解决

## **TOP1-注入的防范**

如何防范：

1.使用安全的API，避免使用解释器

2.对输入的特殊的字符进行ESCAPE转义处理。例如：LIKE '%xxx%' ESCAPE ‘xxx’

使用ESCAPE关键字定义了转义字符“xxx”，告诉DBMS将搜索字符串“%xxx%”中的第二个百分符（%）作为实际值，而不是通配符

3.使用白名单来规范化的输入验证方法

## **TOP1-使用ESAPI（https://github.com/ESAPI/esapi-java-legacy）**