WEB安全防护

歌曲：林中鸟

输入检查

输出检查（可利用转义和编码）

Xss 攻击本质：一种“HTML注入”，用户的数据当成了html代码一部分被执行，从而混淆了原本的语义，产生新的语义

Xss防护基础：

输出页面用 htmlencode

Js 使用javascriptencode

Base 标签必须禁用

Flash：一定要设置参数allowscriptAccess 的参数和allownetwork的参数

Cookie劫持：针对需要保护的cookie要设置httponly 禁止js访问cookie

富文本禁止：iframe script base form 坚持提交的html 标签是否带有事件和标签属性 标签采用白名单的形式