

# Web安全从入门到放弃

CplusHua | 36W白帽大佬，青藤云安全分析师

# OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE) [NEW]

A5:2017-Broken Access Control [Merged]

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

A8:2017-Insecure Deserialization [NEW, Community]

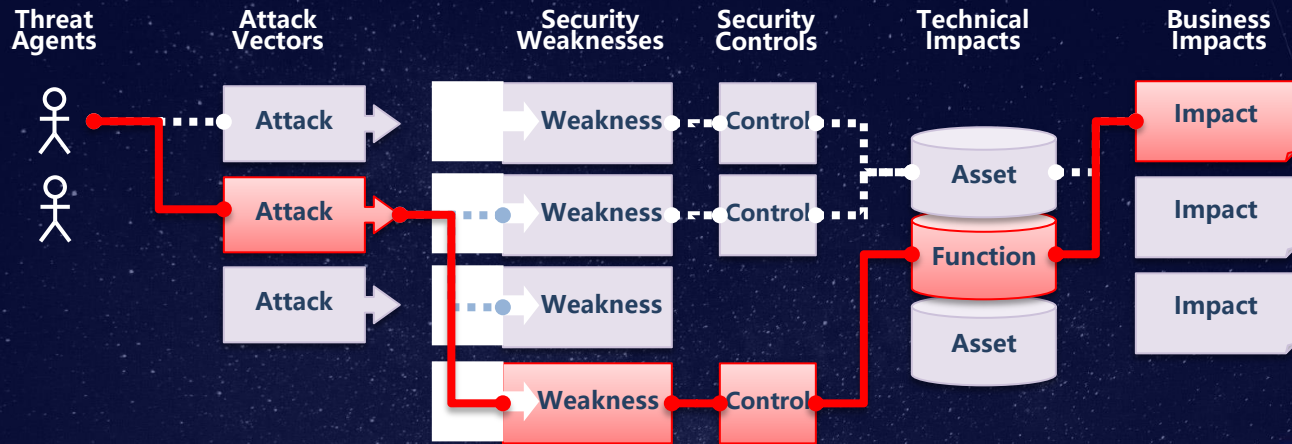
A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

20分钟，你买不了吃亏，买不了上当

20分钟，我们来聊一聊几个有意思的攻击思路

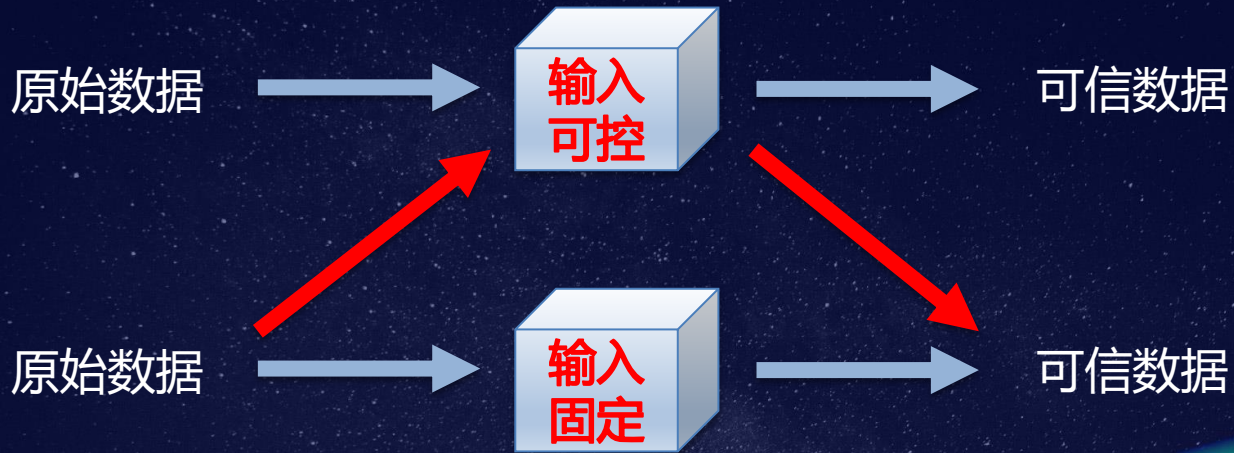
# Attacking Route



1. 看不到的攻击面
2. 无法避免的中低危漏洞
3. 意想不到的网络边界

目标被攻陷!

## 黑盒加密机



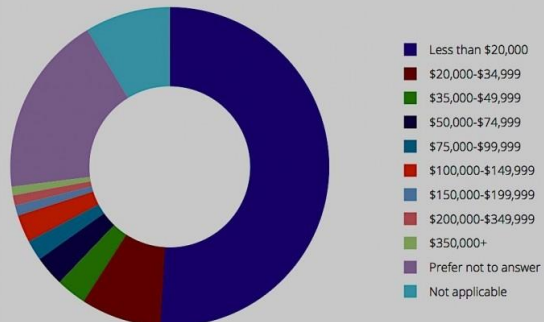
1. 生成支付签名
2. 会话信息伪造
3. 重置用户密码
4. ...





# 挖洞收入图 vs 比特币涨势图

We are frequently asked, can hackers live off bounties full-time? Seventeen percent said they rely solely on bug bounty programs for their income, whereas 26% of hackers reported that 76-100% of their annual income comes exclusively from bug bounty programs.



谢谢观赏!

CplusHua