cezurity

An Exceptionally Simple Practice of AppSec .NET

Mikhail Shcherbakov
Product Manager at Cezurity

cezurity

About me

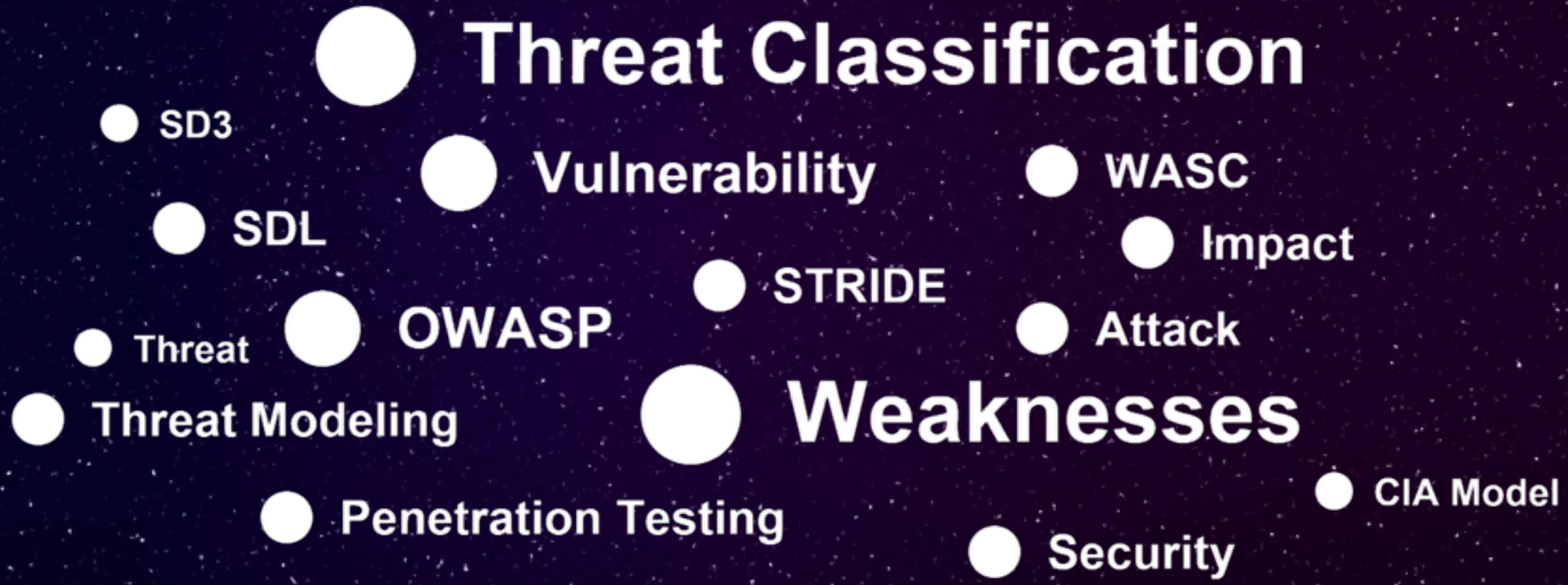
- Product Manager at Cezurity
- One of the core developers of the source code analyzer PT Application Inspector
- Former Team Lead at Acronis, Luxoft, Boeing

Who is it for?

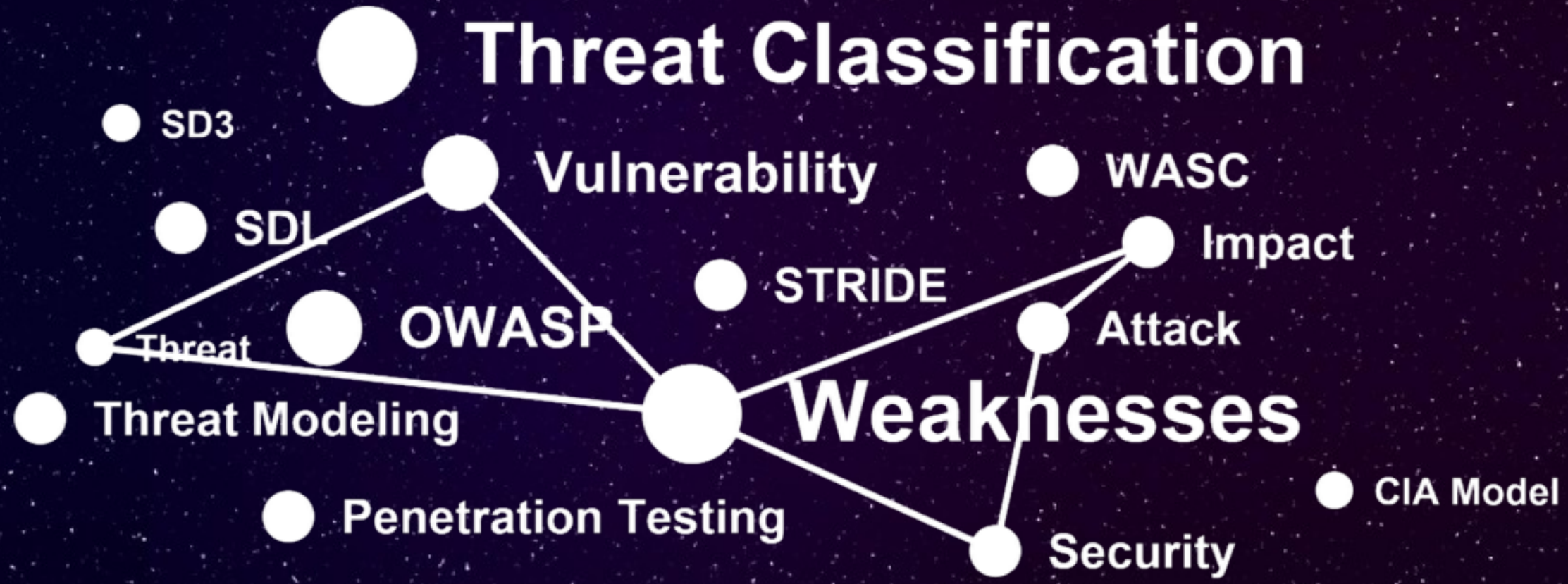
Security Development

Where to Begin?

Security Development



Glossary


Threat Classification
SD3
Vulnerability
WASC
SDL
Impact
STRIDE
OWASP
Attack
Threat
Threat Modeling
Weaknesses
CIA Model
Penetration Testing
Security

Glossary

Need to Deal with Weaknesses!

Security Development

Create a classification for developers!

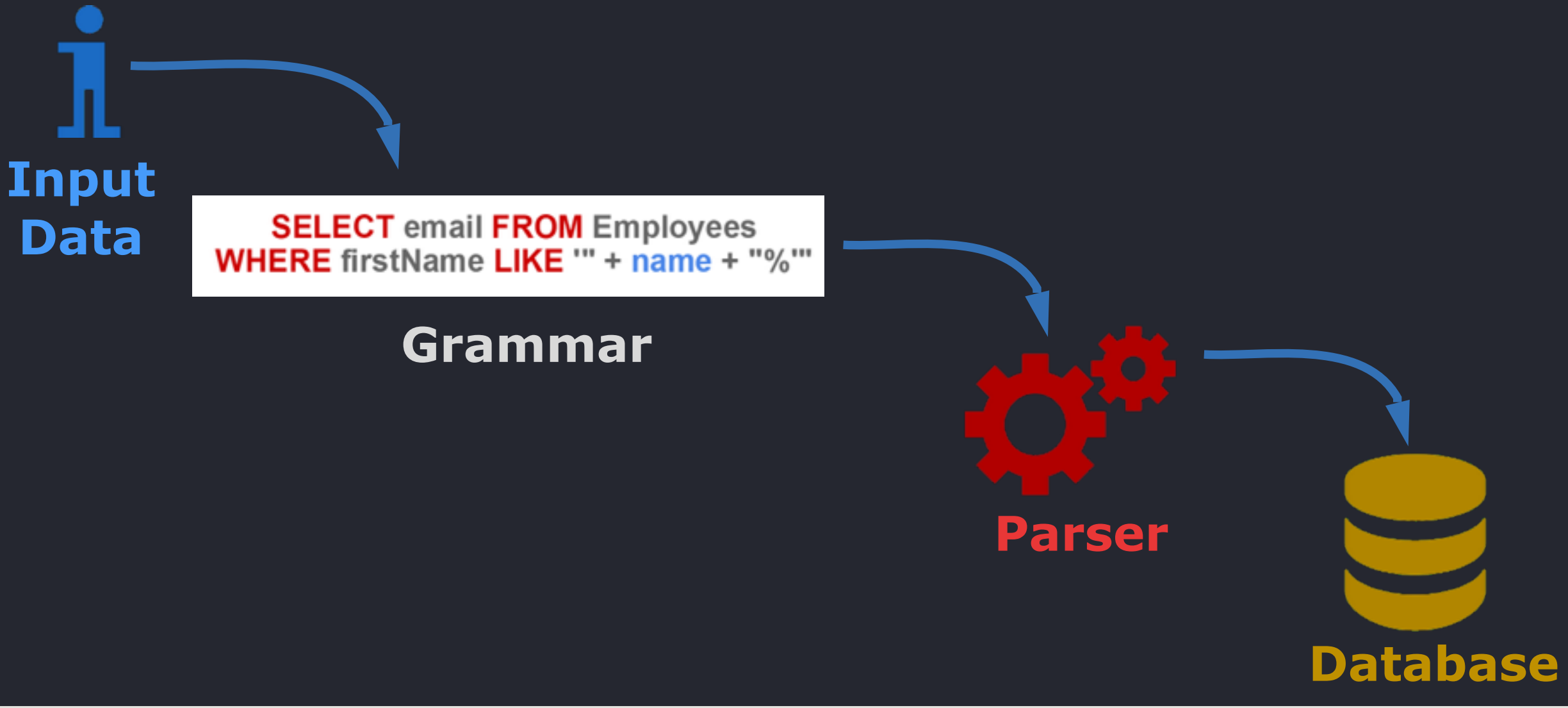
Improper Input / Output Handling

Implementation

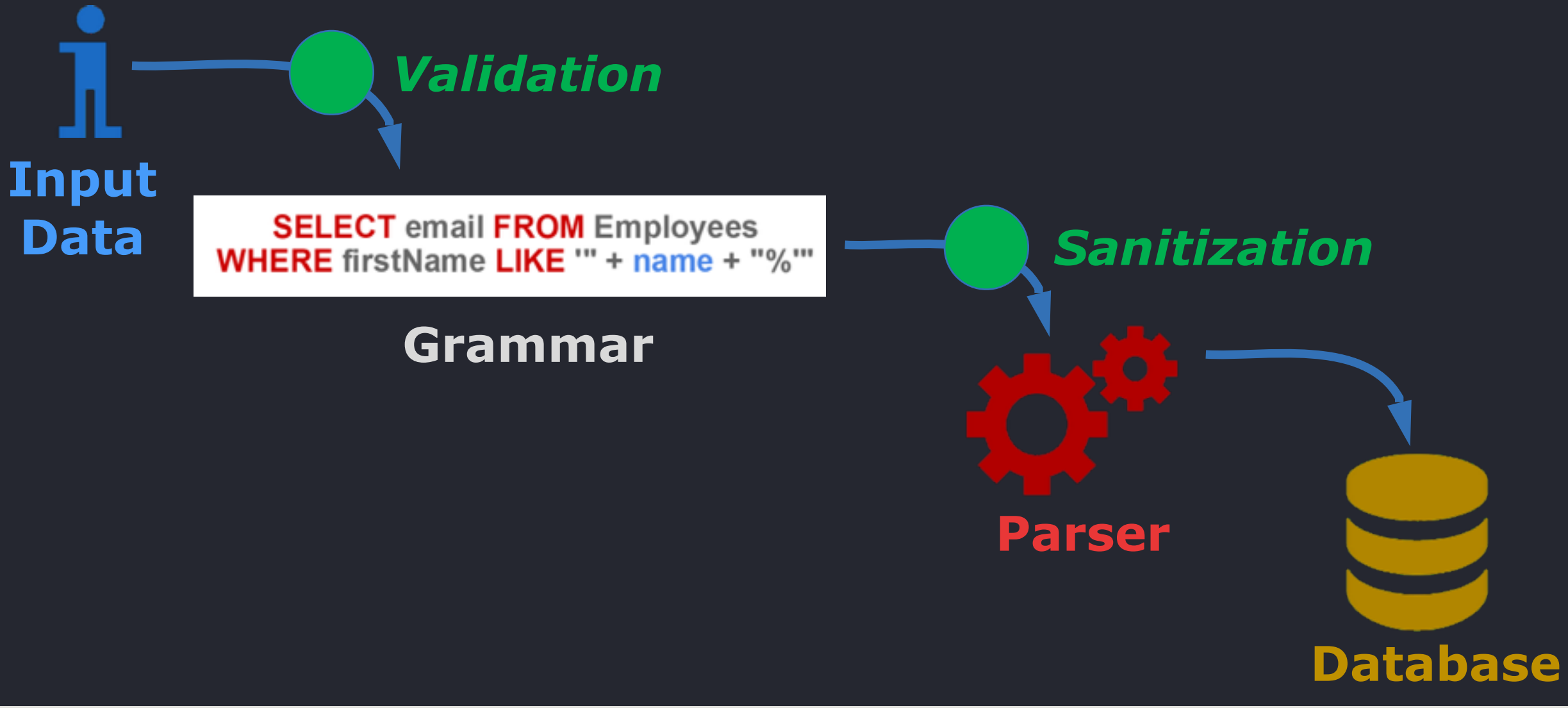
Improper Input / Output Handling

- SQL Injection
- OS Commanding
- Cross-Site Scripting (XSS)
- XML Injection
- XPath Injection
- XQuery Injection
- LDAP Injection
- Mail Command Injection
- Null Injection
- Unrestricted File Upload
- Path Traversal
- HTTP Response Splitting
- Content Spoofing
- Buffer Overflow

Injection Anatomy



Injection Anatomy



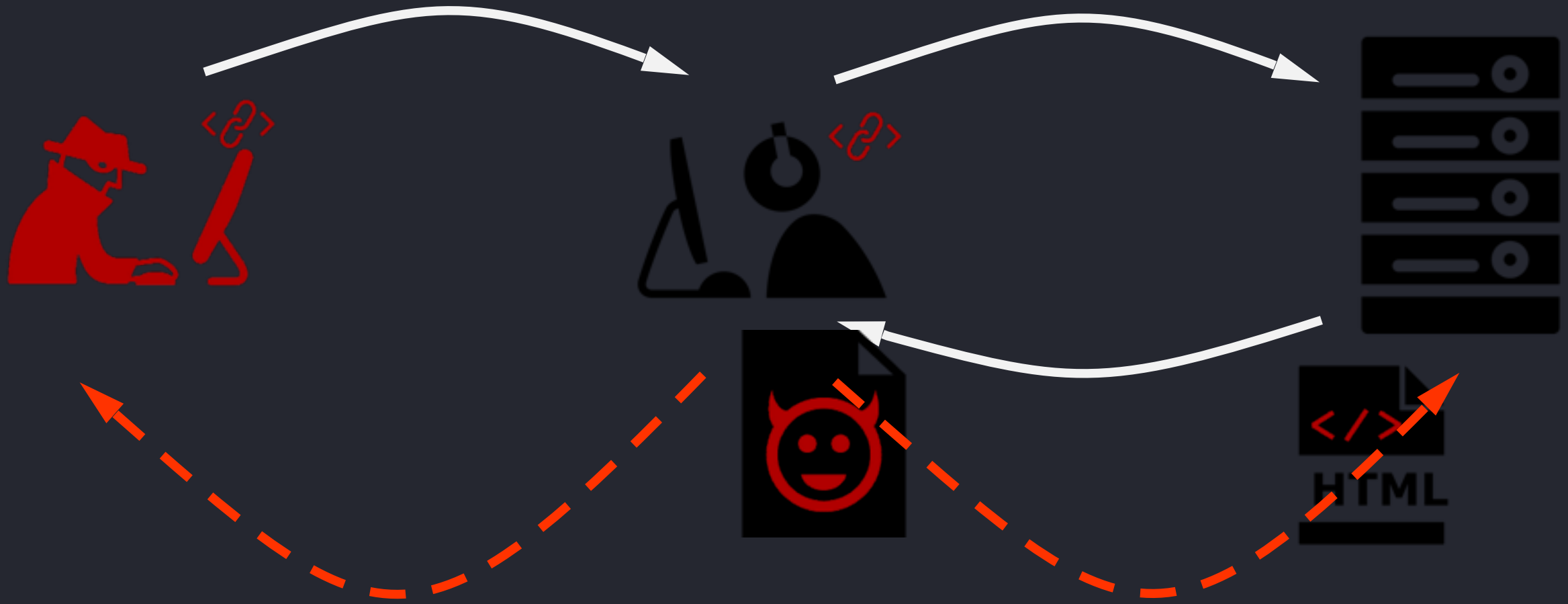
SQL Injection with Entity Framework

Show me the code!

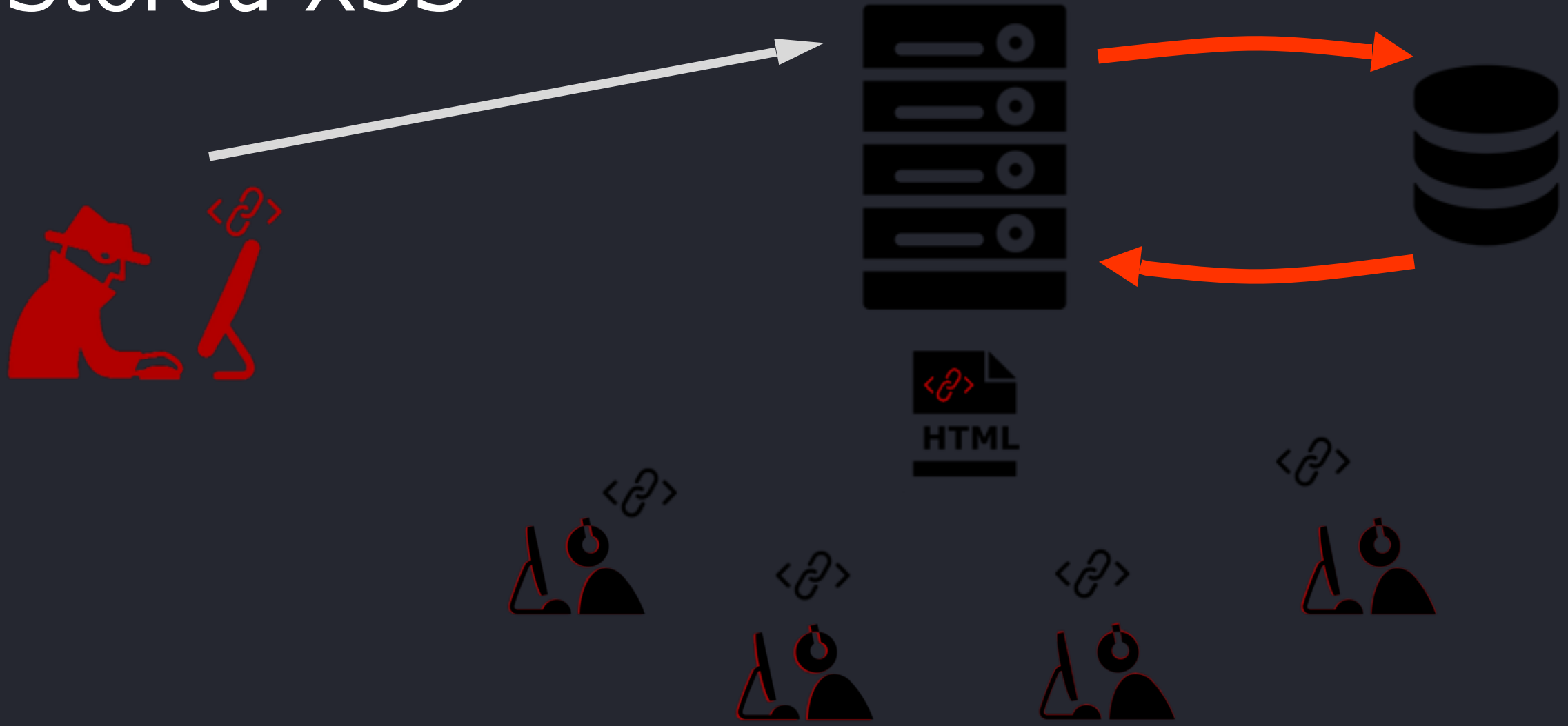
Cross-Site Scripting (XSS)

- Reflected
- Stored
- DOM-based

Reflected XSS



Stored XSS



Stored XSS

Show me the code!

DOM-based XSS

Show me the code!

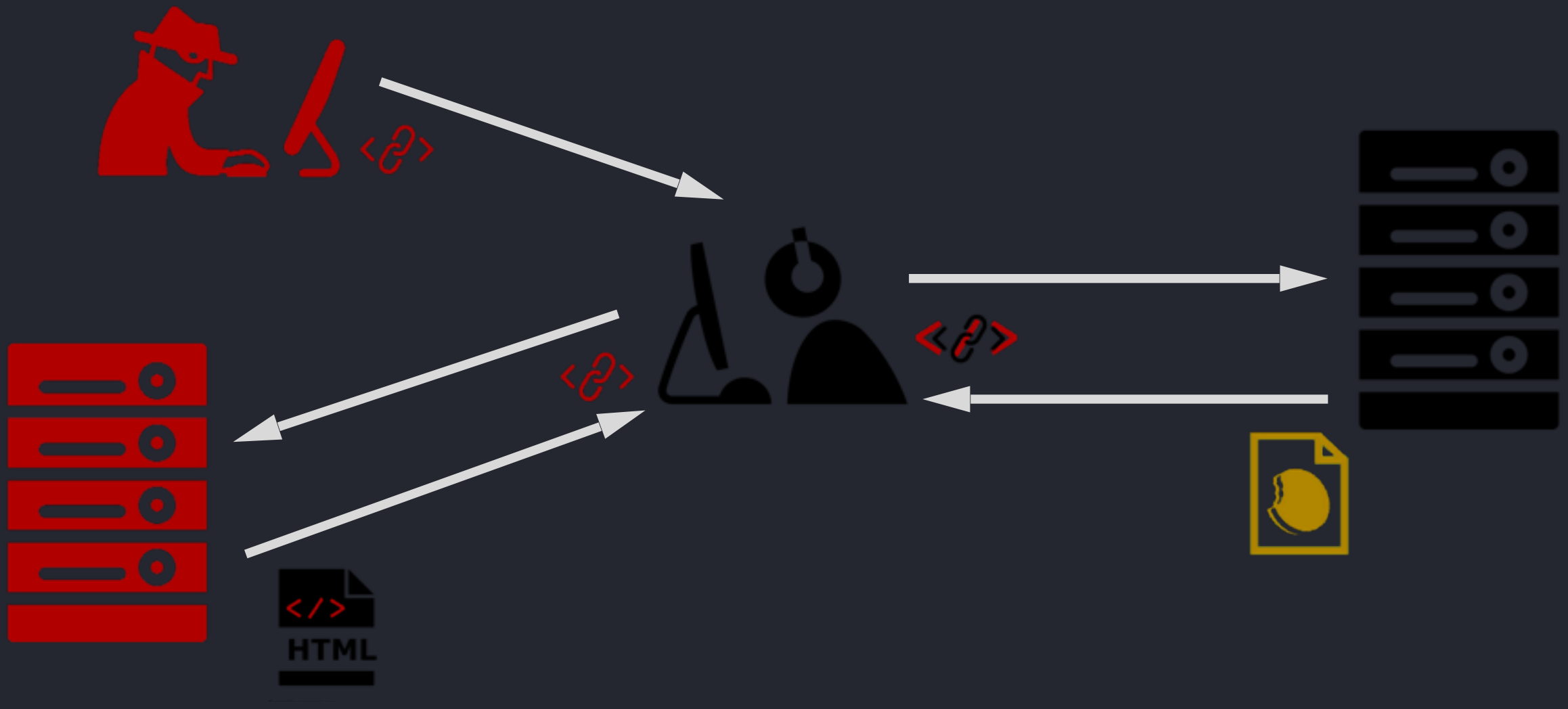
Insufficient Control Flow Management

Design / Implementation

Insufficient Control Flow Management

- Cross-Site Request Forgery (CSRF)
- Mass Assignment
- Business Logic Errors
- Abuse of Functionality

Cross-Site Request Forgery (CSRF)



CSRF

Show me the code!

CSRF

- ASP.NET MVC

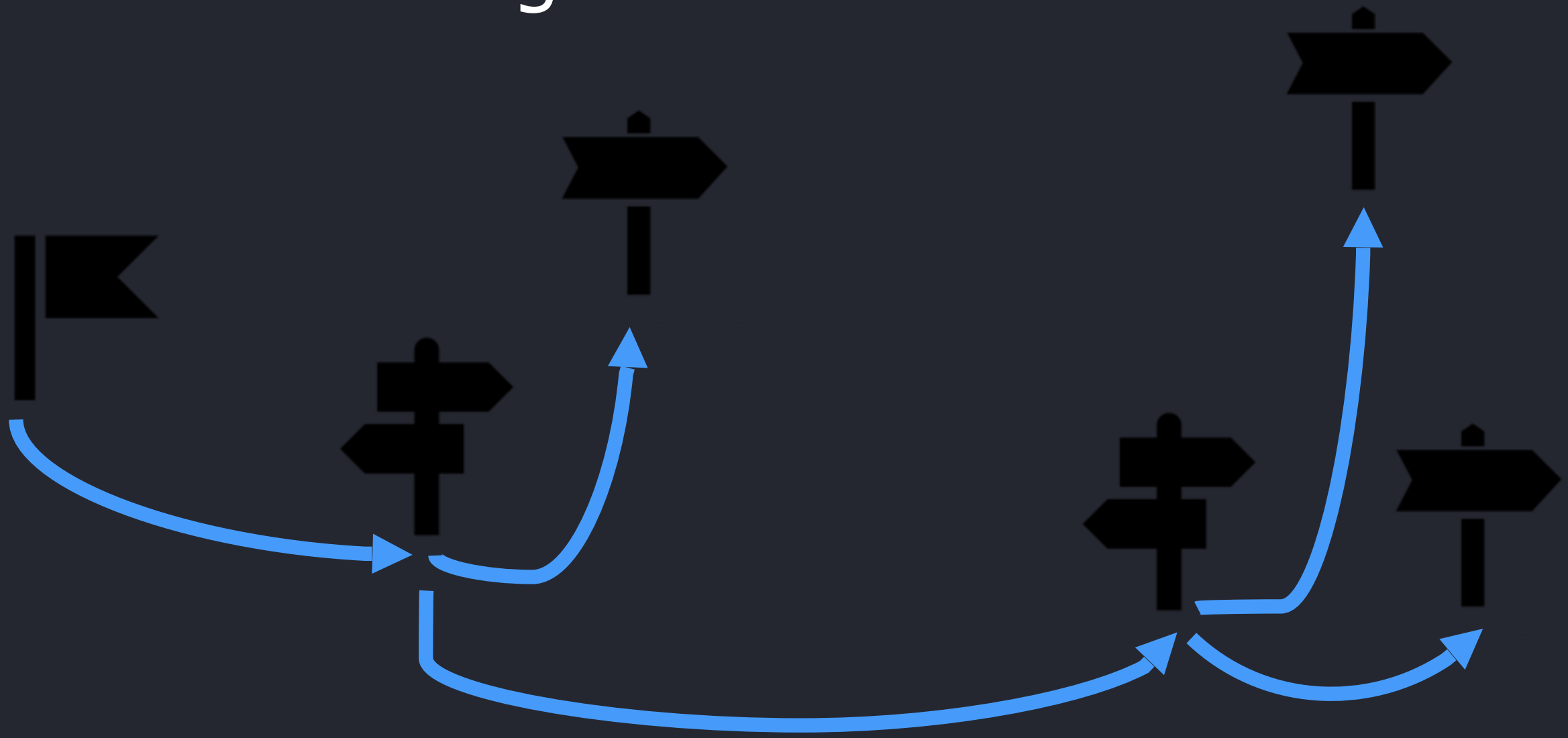
  <%= Html.AntiForgeryToken() %>

  <input name="__RequestVerificationToken" type="hidden“ …

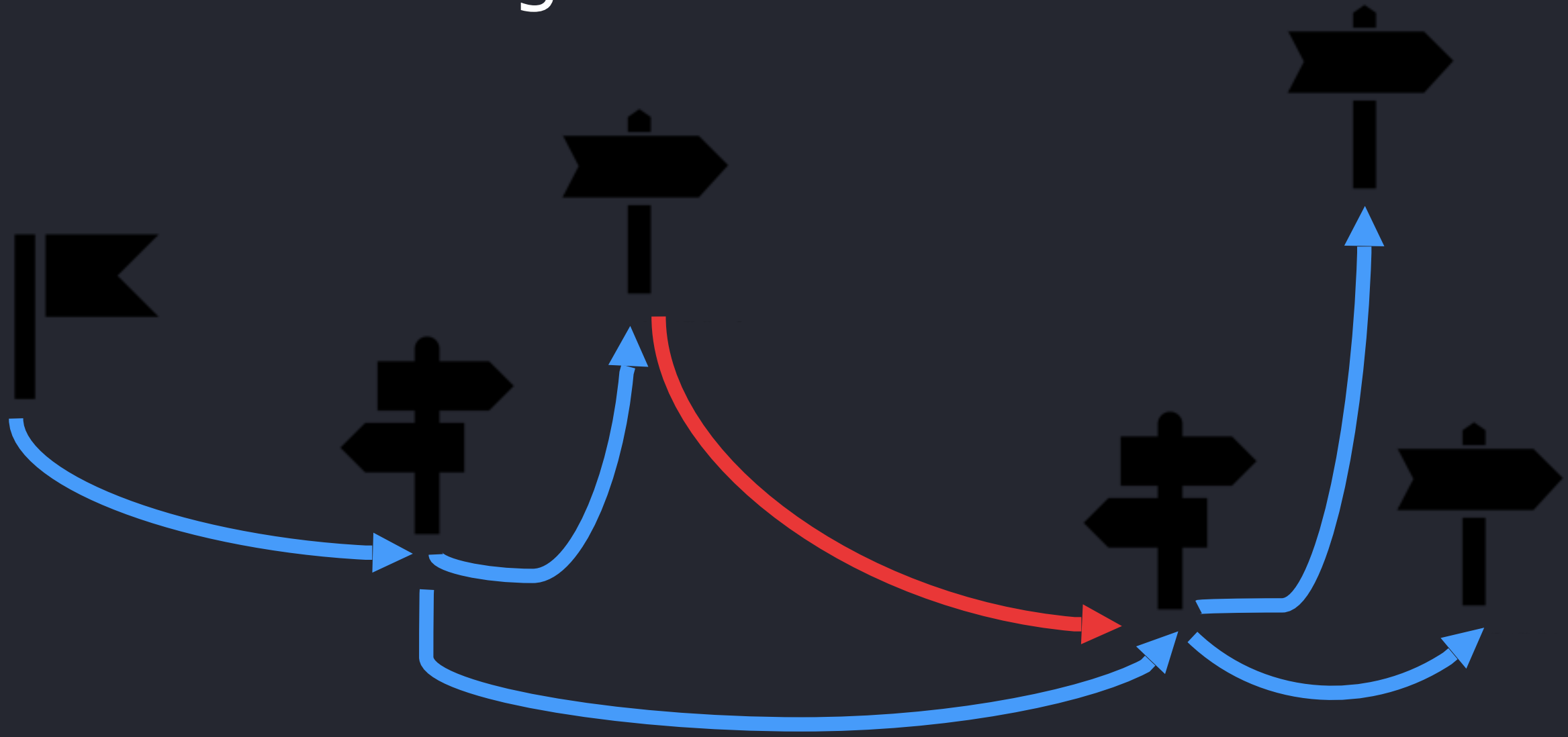
- ASP.NET Web Forms

  __VIEWSTATE, __EVENTVALIDATION

Business Logic Error



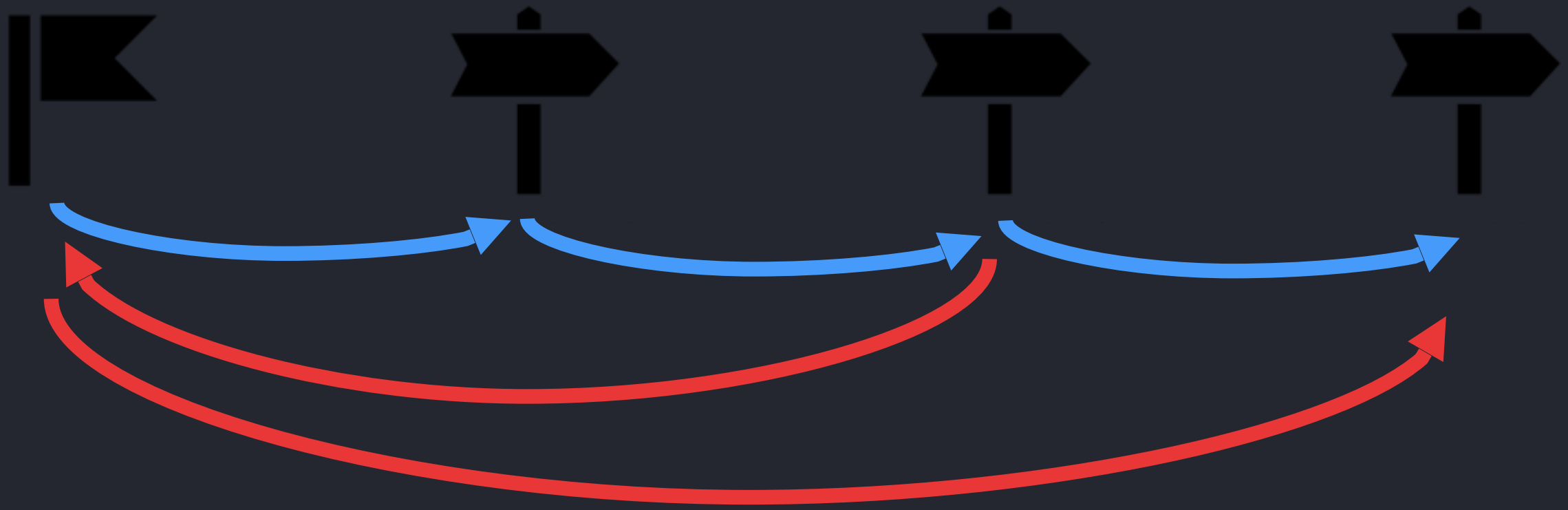
Business Logic Error



Business Logic Error

Show me the code!

Business Logic Error



Sensitive Data Exposure

Design / Implementation / Deployment

Sensitive Data Exposure

- Insufficient Transport Layer Protection
- Insecure Cryptographic Storage
- Insufficient Client-side Protection

Improper Access Control

Design / Implementation / Deployment

Improper Access Control

- Insufficient Authentication
- Insufficient Authorization
- Insufficient Password Recovery
- Insufficient Session Expiration
- Credential / Session Prediction
- Improper File System Permissions
- Insufficient Anti-Brute Force and Anti-automation

Session Fixation

Show me the code!

Security Misconfiguration

Implementation / Deployment

Security Misconfiguration

- Information Exposure Through an Error Message
- Information Leakage
- Directory Indexing
- Using Components with Known Vulnerabilities

Summary

- Improper Input / Output Handling
- Insufficient Control Flow Management
- Sensitive Data Exposure
- Improper Access Control
- Security Misconfiguration

Summary

- OWASP Top Ten Project (2010/2013) http://bit.ly/1OffewO
- Vladimir Kochetkov Blog and Workshop http://bit.ly/1DecXWI
- Troy Hunt Blog www.troyhunt.com
- OWASP Developer Guide http://bit.ly/1JcQLoh
- CWE/SANS Top 25 Most Dangerous Software Errors (2011) http://bit.ly/1bjDTOH
- OWASP Classification http://bit.ly/1GlKmGz http://bit.ly/1DE3852
- WASC Classification http://bit.ly/1d3EXYd

Thank you for your attention!

Mikhail Shcherbakov
Product Manager at Cezurity

ms@cezurity.com
linkedin.com/in/mikhailshcherbakov
github.com/yuske
@yu5k3

cezurity