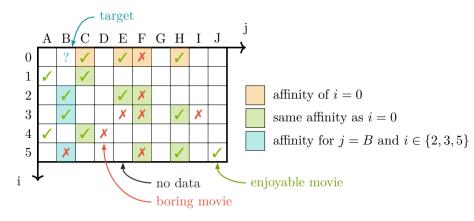
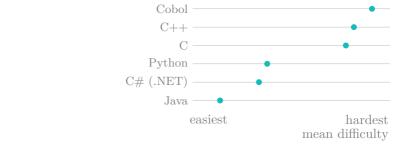
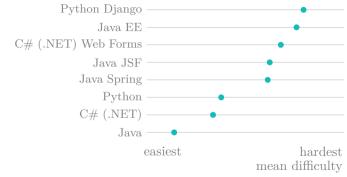


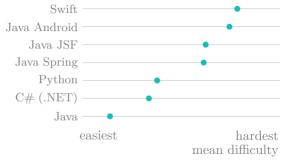
	•
Business logic flaws	•
Cross site request forgery (CSRF)	•
Denial of service (DoS)	•
Code tampering	•
Insecure authentication (M)	•
Extraneous functionality	•
Cross site scripting (XSS)	•
Reverse engineering	•
Unintended data leakage	•
Insufficient transport layer protection (M)	•
Broken cryptography (W)	•
Access control	•
Insecure data storage	•
Sensitive data storage	•
Insecure authentication (W)	•
Information exposure	•
	•
Misconfiguration	•
Insufficient logging	•
Mass assignment	•
Unvalidated redirects and forwards	•
Broken cryptography (M)	•
Insufficient transport layer protection (W)	•
Improper platform usage	•
Use of vulnerable components	•
Session management	•
	•
XML external entity (XXE)	
(easiest hardest
	mean difficulty

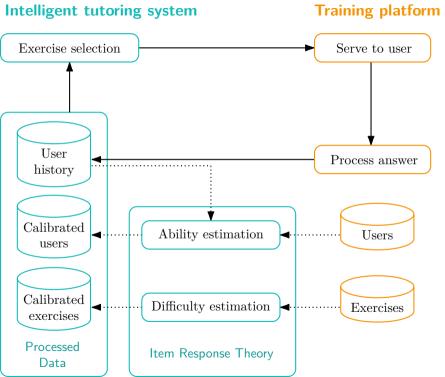


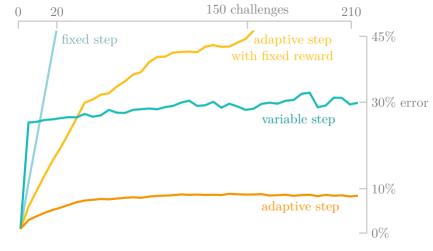
Cobol		
		•
C++		•
Python Django		
Swift		•
JavaScript React		•
_		•
JavaScript Angular.io		
		•
Java Android		•
Node.js Express		•
Kotlin		•
C# (.NET) Web Forms		•
C# (.NET) Core		•
		•
Java Spring		•
C# (.NET) MVC		•
C# (.NET) Web API		•
PLSQL		•
Ruby Rails		•
Docker		•
Python		•
Pseudocode		•
C# (.NET)		•
Scala Play		•
PHP Symfony		
Java EE API	-	
Java	•	
Terraform	•	
Java Spring API	•	
Python Flask		
	easiest	hardest
(casiesi	mean difficulty
		mean difficulty

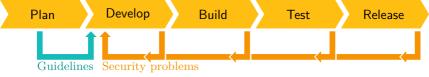


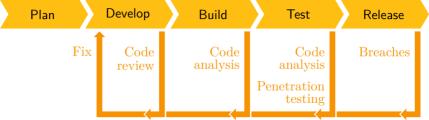




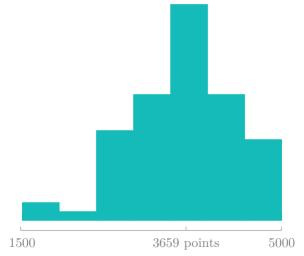


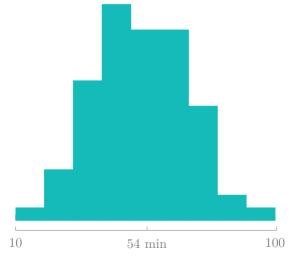




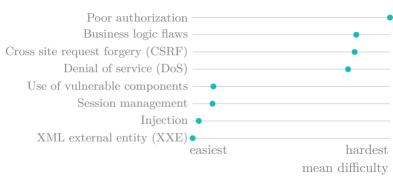


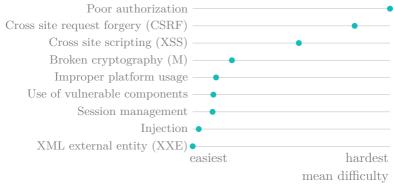






	mean removal time [s	s]
File size	38	3
File extension	35	ó
File path	32	2
Log forgery	30)
Information leakage)
Input validation (1)	27	7
Stacktrace printing	21	Ĺ
Input validation (2)		ó
XSS	7	
SQL	4	
overall mean)







OWASP Top 10 2017		OWASP Top 10 2021 Draft
Injection		Broken Access Control
Broken Authentication		Cryptographic Failures
Sensitive Data Exposure		Injection
XML External Entity (XXE)		Insecure Design
Broken Access Control)	Security Misconfiguration
Security Misconfiguration		Vulnerable and Outdated Components
Cross-Site Scripting (XSS)		Identification and Authentication Failures
Insecure Deserialization		Software and Data Integrity Failures
Using Components with Known Vulnerabilities		Security Logging and Monitoring Failures
Insufficient Logging and Monitoring		Server-Side Request Forgery (SSRF)