Развој безбедног софтвера

Сигурносно тестирање софтвера

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Шта је сигурносно тестирање софтвера?

Тестирање могућности система/софтвера да спречи неауторизовани приступ ресурсима и подацима

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Шта треба да буде тестирано?

Потребно је покрити шест основних сигурносних концепата:

Тајност (Confidentiality)

Интегритет (Integrity)

Аутентикацију (Authentication)

Ауторизацију (Authorization)

Доступност (Availability)

Непорецивост (Non-repudiation)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Пример – OSSTMM v3

Open Source Security Testing Methodology Manual

Information Assurance Objectives	Operation Controls
Confidentiality	Confidentiality Privacy Authentication Resilience
Integrity	Integrity Non-repudiation Subjugation
Availability	Continuity Indemnification Alarm

Одбрамбени процеси

Интерактивне контроле

ISSES

Co-funded by the Erasmus+ Programme of the European Union

OSSTMM v3 – интерактивне контроле

Ове контроле утичу директно на видљивост, приступ и поверење

Аутентикација – кредeнцијали
Idemnification – упозорење на правне последице непоштовања правила
Отпорност – способност да се задржи заштита вредности (asset) у случају грешке
Subjugation – обезбеђује интеракцију према правилима које дефинише власник вредности
Континуитет – способност задржавања интерактивности са вредностима у случају грешке

ISSES
Co-funded by the Erasmus+ Programme of the European Union

OSSTMM v3 – одбрамбени процеси

Ове контроле не утичу на интеракцију већ штите вредности када је претња присутна:

Непорицање – онемогућава порицање
Тајност – заштита доступности вредности само легитимним странама
Приватност – заштита начина на који је вредност доступна легитимним странама
Интегритет – контрола која омогућава да легитимне стране знају за промене вредности
Аларм – конрола која обавештава да се интеракција догодила или се догађа

ISSES
Co-funded by the Erasmus+ Programme of the European Union

OSSTMM v3 – ограничења

Дефинисано је пет ограничења

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

ISSES
Co-funded by the Erasmus+ Programme of the European Union

OSSTMM v3 – дефинисање сигурносног теста

1. Дефинисати шта се штити, то су вредности. Заштитни механизми су контроле које тестирамо да пронађемо ограничења
2. Идентификати начине интеракције са вредностима, тј. зону интеракције.
3. Дефинисати опсег тестирања (шта је ван зоне интеракције, шта је део инфраструктуре).
4. Дефинисати како опсег интерагује ка споља а како унутар себе. Ово су вектори.
5. Идентификовати потребну опрему за сваки тест. Дефинисано је пет начина интеракције: људска, физичка, бежична, телекомуникациона и преко рачунарске мреже. Сваки канал тестирати за сваки вектор.
6. Дефинисати врсту теста на основу тога што желимо да откријемо помоћу теста (шест уобичајених типова).
7. Уверити се да је сигурносни тест у складу са правилима ангажовања.

Резултат ће бити мерење површине напада која представља незаштићени део опсега за дефинисани вектор.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

OSSTMM v3 – опсег тестирања

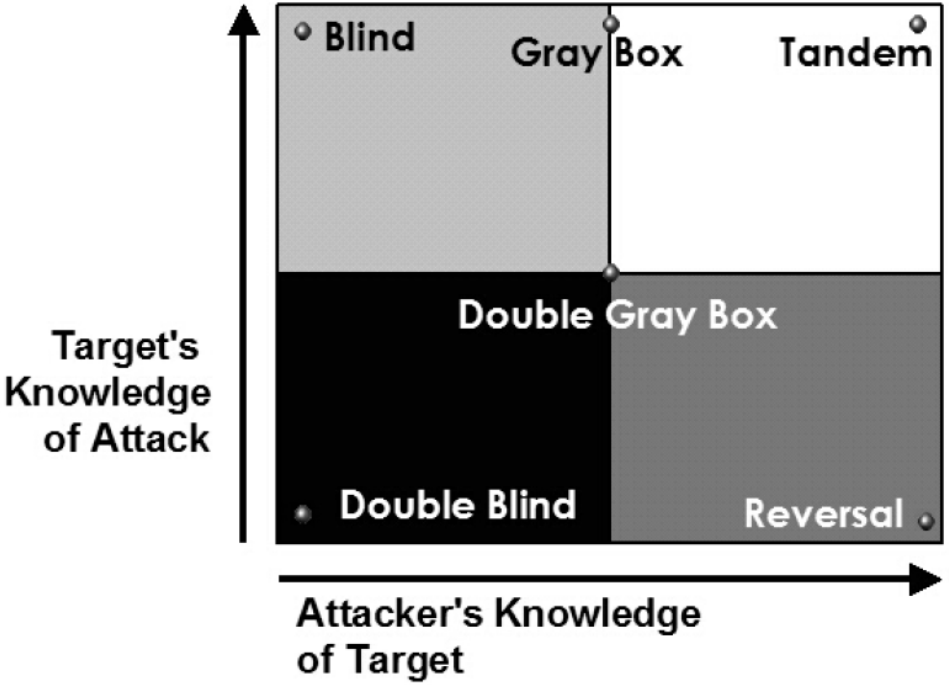
Class	Channel
Physical Security (PHYSSEC)	Human
	Physical
Spectrum Security (SPECSEC)	Wireless
Communications Security (COMSEC)	Telecommunications
	Data Networks

Опсег тестирања обухвата све интеракције са било којим вредностима.

Обухвата три класе са пет канала интеракције.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Врсте сигурносног тестирања – OSSTMM v3



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Врсте сигурносног тестирања (2)

Слепо тестирање
- Аналитичар нема предзнање о систему који тестира
- Мета је спремна за тестирање и зна унапред све детаље тестирања
- Користи се за проверу способности аналитичара
- Чест назив: етичко хаковање

Двоструко слепо тестирање
- Аналитичар нема предзнање о систему који тестира
- Мета није унапред упозната са тестирањем
- Користи се за проверу способности аналитичара, али и припремљености мете
- Чест назив: тестирање црне кутије или пенетрационо тестирање

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Врсте сигурносног тестирања (3)

Тестирање сиве кутије

- Аналитичар познаје канале напада и делимично одбране система
- Мета је спремна за тестирање и зна унапред све детаље тестирања
- Користи се за проверу ефикасности
- Чест назив: тестирање рањивости

Двоструко тестирање сиве кутије

- Аналитичар познаје канале напада и делимично одбране система
- Мета је обавештена о обиму и временским оквирима тестирања, али не и о каналима напада и векторима напада
- Користи се за проверу способности аналитичара и мете у променљивим околоностима
- Чест назив: тестирање беле кутије

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Врсте сигурносног тестирања (4)

Тандем

- Аналитичар познаје све детаље о могућим нападима
- Мета је спремна за тестирање и зна унапред све детаље тестирања
- Користи се за проверу заштитних механизама мете и темељности
- Чест назив: интерна ревизија

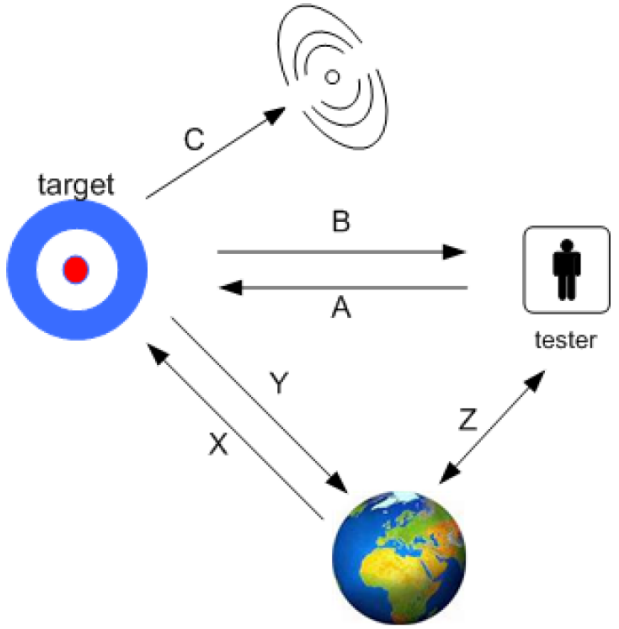
Реверзно тестирање

- Аналитичар познаје све детаље о могућим нападима
- Мета није унапред упозната са тестирањем
- Користи се за проверу спремности мете у непредвиђеним ситуацијама
- Чест назив: вежба црвеног тима

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Процес у четири тачке – 4PP

1. **Индукција** (Z) – препознавање принципијелних чињеница о мети
2. **Истрага** (C) – препознавање индикатора о слабостима мете
3. **Интеракција** (A/B) – стандардна и нестандардна интеракција са метом како би се изазвали одговори
4. **Интервенција** (X/Y/Z) – промена интеракције ресурса са метом или између различитих мета.



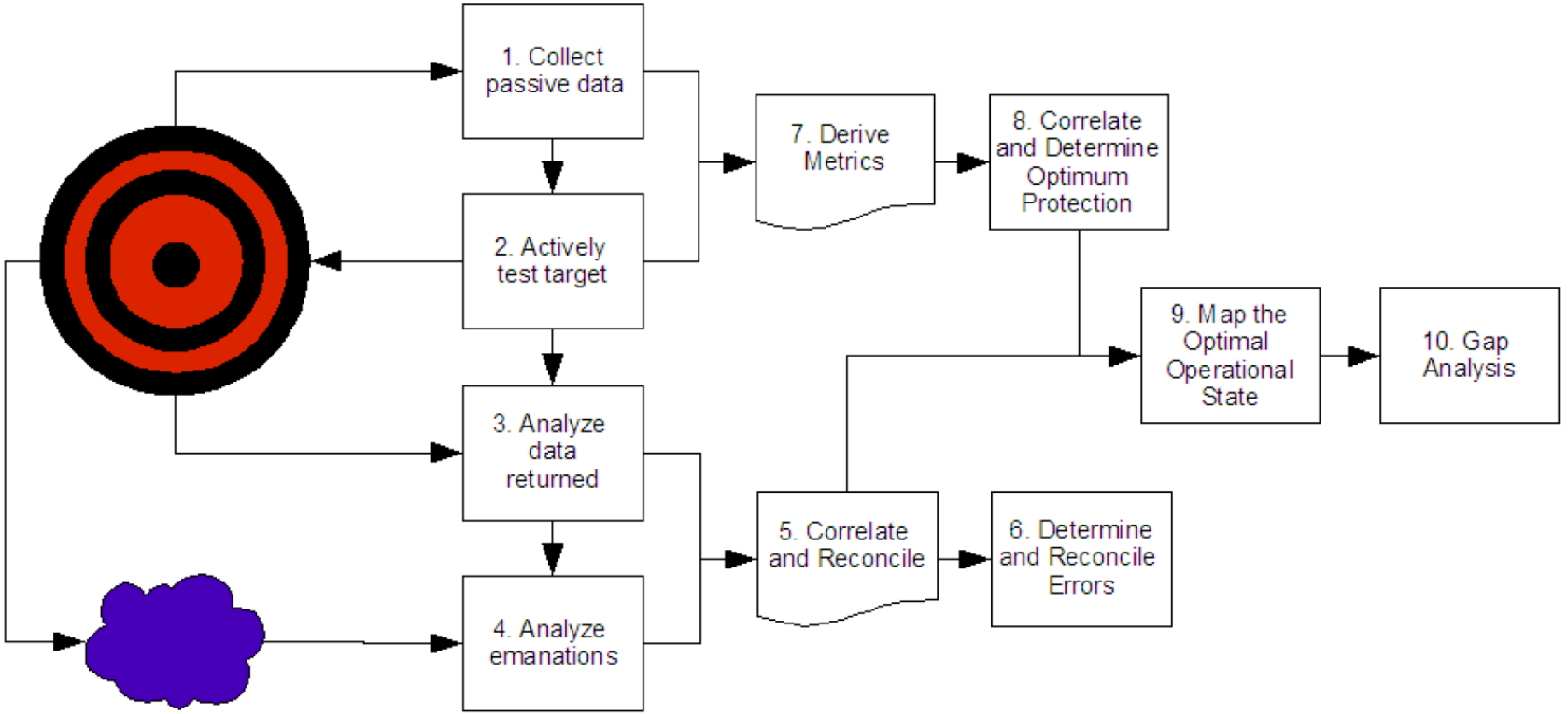
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Trifecta методологија

- Методологија која одговара на следећа три питања:
    1. Како тренутно операције раде?
    2. На који начин раде другачије него што руководство мисли да раде?
    3. Како треба да раде?

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Комбинација Trifecta и 4PP



STAR – Security Test Audit Report

- Извештај након тестирања који садржи следеће:
  - Датум и време тестирања
  - Трајање тестирања
  - Имена одговорних аналитичара
  - Тип теста
  - Опсег теста
  - Метод енумерације мете
  - Канал који је тестиран
  - Тест вектор
  - Метрику вектора напада
  - Који тестови су завршени, који нису завршени, који су делимично завршени
  - Проблеми у извођењу теста или валидности добијених резултата
  - Процеси који утичу на сигурносна ограничења
  - Било какве аномалије или непознати догађаји

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Осам фундаменталних сигурносних питања

1. Колико новца би требало потрошити на сигурност?
2. Шта би прво требали заштити?
3. Која заштитна решења су нам потребна и како их успоставити да би били максимално ефикасни?
4. Колико унапређења је добијено са конкретним решењем?
5. Како да периодично измеримо сигурносне напоре?
6. Како да знамо да ли смањујемо изложеност претњама?
7. Колико смо отпорни на нападе?
8. Да ли смо у сагласности са регулативама?

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Квантификација резултата тестирања

OPERATIONAL SECURITY VALUES	
Visibility	
Access	
Trust	

LIMITATIONS VALUES	
Vulnerability	
Weakness	
Concern	
Exposure	
Anomaly	

OpSec	
Limitations	

CONTROLS VALUES	
Authentication	
Indemnification	
Resilience	
Subjugation	
Continuity	
Non-Repudiation	
Confidentiality	
Privacy	
Integrity	
Alarm	

True Controls	
Security Δ	

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Квантификација – пример

- Визибилитет - број мета у тестираном опсегу. Нпр. уколико посматрамо запослене у компанији која запошљава 50 људи, али само 38 их је интерактивно кроз одабрани тест вектор и канал, визибилитет би био 38.
- Приступ – број приступа по месту интеракције по појединачном тесту. Нпр. уколико посматрамо физичку безбедност зграде која има двоје врата и 5 прозора приступ има вредност 7, али ако су сва врата и прозори запечаћени, онда би приступ био 0.
- Поверење – број поверења по месту интеракције по појединачном тесту. Нпр. уколико посматрамо физичку безбедност зграде која има двоје унутрашњих врата која раздвајају просторије онда је поверење 2, али уколико су врата запечаћена, онда је поверење 0.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Квантификација – операционе контроле

- Аутентикација - број инстанци да би се добио приступ. Нпр. ако нам треба и ИД картица и отисак палца то је 2, а ако је једно од ова два онда је 1.
- Idemnification – број упозорења. Нпр. улаз дозвољен само запосленима.
- Subjugation – сваки приступ или поверење које не дозвољава кориснику да одступи од дефинисаног протокола. Нпр. да би преузео документ радник мора да потпише реверс.
- Континуитет – избројати сваки приступ или поверење које ће радити чак и у случају грешке. Нпр. ако веб сервер престане да одговара на захтеве због превеликог оптерећења а редундантни сервер настави да пружа услугу без прекида, то се рачуна као континуитет.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Квантификација – операционе контроле (2)

- Отпорност – избројати сваки приступ или поверење који обрађује грешке на безбедан начин. Нпр. ако веб сервер који захтева логовање изгуби конекцију са базом, онда сви покушаји логовања треба да буду неуспешни да би се рачунало да постоји отпорност.
- Непорицање – Нпр. камера на улазу и биометријски скенер за отварање врата.
- Тајност – енкрипција
- Приватност – прикривање интеракције
- Интегритет – хеш фајла
- Аларм – избројати сваки приступ или поверење који остаје забележен у логу.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Квантификација – ограничења

- Рањивости – избројати свакуману због које неко може да добије недозвољен приступ, ускрати легитиман приступ или сакрије трагове или вредности у оквиру опсега. Нпр. нападач који заузме 100% процесорске снаге.
- Слабости – Избројати мане у интерактивним контролама. Нпр. логовање које дозвољава неограничен број покушаја.
- Забринутости - Избројати мане у одбрамбеним механизмима. Нпр. употреба самопотписаних сертификата за HTTPS.
- Изложености – неоправдане акције које омогућавају приступ вредностима. Нпр. прозор кроз који се виде вредности.
- Аномалије – неидентификовани или непознати елементи. Нпр. сигнал који се не може лоцирати и за који се не зна чему служи.

Квантификација резултата тестирања - вежба

- Поделити се у тимове
- За апликацију која се користи на вежбама квантификовати:
  - Аутентикацију
  - Отпорност
  - Рањивост
  - ...

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Како изводити сигурносно тестирање?

Треба изводити у свакој фази развоја софтвера (SDLC)

SDLC фазе	Безбедносне процедуре
Прикупљање захтева	Сигурносна анализа захтева и провера случајева злоупотребе.
Дизајн	Анализа безбедносних ризика. Развој плана тестирања укључујући безбедносна тестирања.
Развој и тестирање модула	Статичко и динамичко тестирање кода и тестирање беле кутије
Интеграционо тестирање	Тестирање црне кутије
Системско тестирање	Тестирање црне кутије и тестирање рањивости
Имплементација	Пенетрационо тестирање и тестирање рањивости
Одржавање	Анализа утицаја исправки кода

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Алати за сигурносно тестирање апликација

Категорије алата:

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Origin Analysis/Software Composition Analysis (SCA)
- Database Security Testing
- Interactive Application Security Testing (IAST) and Hybrid Tools
- Mobile Application Security Testing (MAST)
- Application Security Testing as a Service (ASTaaS)
- Correlation Tools
- Test-Coverage Analyzers
- Application Security Testing orchestration (ASTO)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Static Application Security Testing (SAST)

Тестирање по принципу беле кутије
Аналитичар познаје детаље система
Тестира се изворни програмски код да би се уочили сигурносни пропусти који могу довести до рањивости
Примери: SonarQube, Fortify, FindBugs, …
Постоје три врсте

Алати који раде са некомпајлираним кодом

Алати који раде са бинарним кодом

Хибридни

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Dynamic Application Security Testing (DAST)

Тестирање по принципу црне кутије
Аналитичар нема увид у детаље система
Тестира се апликација која је покренута
Користе се познати тест случајеви и прати се реакција апликације
Примери: Acunetix, Arachni, Burp Suite, …

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Origin Analysis/Software Composition Analysis (SCA)

Проверава се порекло свих компоненти које су коришћене у пројекту
Проналазе познате рањивости у често коришћеним заједничким компонентама (нарочито када је у питању отворени код)
Не детектују рањивости самостално произведених компоненти
Раде тако што пореде препознате модуле у коду са листом познатих рањивости
Већина алата користи NIST National Vulnerability Database Common Vulnerabilities and Exposures (CVEs) као извор рањивости
Примери: GitHub SCA, Nexus IQ, Veracode SCA, …

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Database Security Scanning

Иако базе података нису део апликације, веома често апликације се у значајној мери на њих ослањају

Ови алати проверавају познате слабости као што су неажурне верзије базе података, слабе лозинке, лоша конфигурација, итд.

Раде над статичким подацима

Примери: MSSQL DataMask, Scuba, Nmap, …

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Interactive Application Security Testing (IAST) and Hybrid Tools

Користе комбинацију статичке и динамичке анализе
Проверавају да ли су познате рањивости које пронађу у коду заиста могле бити искоришћене
Креирају сценарије напада користећи рекурзивно анализу резултата претходних покушаја
Примери: Checkmarx IAST, Veracode IAST, Acunetix IAST, …

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Mobile Application Security Testing (MAST)

Ови алати су мешавина статичких, динамичких и форензичких алата

Сличне функције као традиционални алати, али прилагођене окружењу мобилних уређаја

Воде рачуна о проблемима специфичним за мобилне уређаје

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Application Security Testing as a Service (ASTaaS)

Сигурносно тестирање софтвера као екстерна услуга
Значајнији развој са појавом рачунарства у облаку

ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

Correlation Tools

Алати који служе за обраду резултата свих претходно поменутих алата

Укрштањем резултата рада различитих алата могу се елиминисати неки потенцијални сценарији

Co-funded by the Erasmus+ Programme of the European Union

Test-Coverage Analyzers

Служе за мерење количине покривеног програмског кода који је анализиран
Користе се за квантификацију резултата тестирања
Могу се унапред задати прихватљиве вредности покривености
Могу детектовати делове кода до којих се никада неће доћи

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Application Security Testing Orchestration (ASTO)

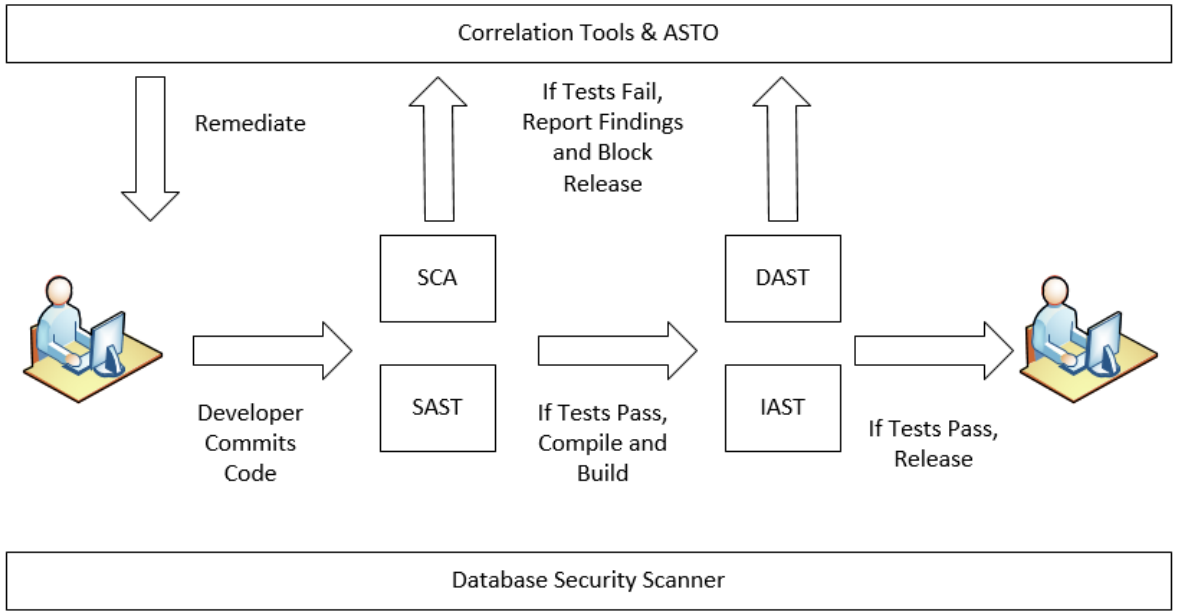
Методологија за интеграцију описаних алата у процес развоја софтвера (SDLC)

Постоје алати који су користили методологију и пре него што је званично именована

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Application Security Testing Tools Reference Model



ISSES
Co-funded by the Erasmus+ Programme of the European Union

ОБАВЕШТЕЊЕ ЗА СТУДЕНТЕ

- Настава на предмету Развој безбедног софтвера подразумева изучавање различитих механизама којима се нарушава информациона безбедност и врше напади на интернет апликације и софтверске системе.
- Примена ових механизама када се извршавају према системима физичких и правних лица која нису упозната и сагласна са активностима на провери рањивости и тестирању упада у њихове системе је кажњива према Кривичном законику Републике Србије (Чланови 298 до 304а).
- Студенти на предмету Развој безбедног софтвера могу ове методе за потребе изучавања да користе искључиво у оквиру затвореног лабораторијског окружења које је обезбеђено за наставу на предмету Развој безбедног софтвера.
- Студенти не могу да подразумевају да су на било који начин охрабрени од стране наставника или да им се препоручује да користе ове методе који се изучавају према другим апликацијама Електротехничког факултета или апликацијама било ког трећег правног или физичког лица.
- Свака евентуална активност коју би предузео неки студент коришћењем ових метода и механизама према апликацијама које нису у оквиру лабораторије на предмету искључива је одговорност студента.

ISSES
Co-funded by the Erasmus+ Programme of the European Union