Развој безбедног софтвера

Моделовање претњи

ISSES

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

Садржај

- Каналисање сигурносних напора
- Моделовање претњи
- Безбедоносна анализа система
- Анализа тока података
- Анализа претњи
- Анализа ризика

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

Каналисање сигурносних напора

- Развој софтверског производа X захтева Y ресурса (нпр. времена, новца)
- Заштита производа X захтева Z додатних ресурса:
  - Дизајнирање безбедности и увођење безбедносних контрола
  - Писање и рецензирање безбедног кода
  - Безбедносно тестирање
- Када се штитимо од шаљивих напада, Z може бити занемарљиво
- Када се штитимо од напада хакера, Z може бити веће од Y
- *Није сав софтвер заштићен на исти начин*

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

Каналисање сигурносних напора (2)

- Стопостотна сигурност није могућа, чак ни са неограниченим ресурсима
- Са ограниченим ресурсима важно је одредити колико сигурности је довољно
  - Шта представља систем, које функције нуди, које податке обрађује, ко интерагује са њим?
  - Ко би напао систем, шта нападач жели да постигне, на који начин ће нападач поступити?
  - Који је правац напада и како можемо ефикасно заштитити систем?
- Одговори на ова питања дефинишу разумну сигурност софтвера
- Да бисмо одговорили на ова питања треба да обавимо моделовање претњи

ISSES

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

Моделовање претњи

- Моделовање претњи је процес анализе модула (нпр. компоненте, апликације, читавог система) како би се установио тренутни и жељени статус по питању безбедности
- Даје одговоре на следећа питања:

1. Шта правимо? – који је опсег и циљ анализе
2. Шта може кренути наопако? – ко су нападачи, које су претње
3. Шта треба да предузмемо? – које су контрамере
4. Да ли смо обавили довољно добар посао? – ретроспектива

- Како би се исправно одговорило на ова питања мора се консултовати широк круг заинтересованих страна како би се утврдило да ли је исправно разумевање система постигнуто

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

Моделовање претњи (2)

- Моделовање претњи се може обавити на веома високом нивоу апстракције (нпр. истражити цео систем као јединствену целину), али и на ниском нивоу апстракције (истражити интеракцију између Java објеката), или негде између
- Уобичајен приступ је безбедоносна анализа система која:
  - Истражује архитектуру и дизајн система
  - Идентификује применљиве безбедносне пројектне узорке
  - Идентификује компоненте које захтевају додатну инвестицију у сигурност (нпр. у форми темељне сигурносне ревизије кода)

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

Безбедоносна анализа система

- Безбедоносна анализа система као улаз узима сигурносне захтеве на високом нивоу апстракције и архитектуру и дизајн система (нпр. Дијаграми тока података, дијаграми инсталације) и као резултат дефинише претње које нису отклоњене као и предложене мере отклањања
- Уобичајена структура безбедоносне анализе система подразумева:

1. Декомпоновање модула коришћењем анализе тока података
2. Анализу претњи, укључујући откривање напада и планирање избегавања напада
3. Анализу ризика, која укључује приоритирање идентификованих инвестиција везаних за безбедност

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

Анализа тока података – декомпоновање модула

- Циљ овог корака је да се разуме анализирани модул, укључујући било које осетљиве ресурсе, интерни ток података и интерфејсе ка екстерним ентитетима

Улази

1. Захтеви модула, са фокусом на сигурносним захтевима
2. Описи дизајна (нпр. Случајеви коришћења, дијаграми тока података, модели инсталације)

Излази

1. (Делимична) листа објеката
2. Улазна тачка модула (могући правац напада)
3. Дијаграми тока података (DFD)
4. (Делимична) листа екстерних зависности и претпоставки о ширем окружењу модула

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

Анализа тока података – листа објеката

- Нешто што нападач жели да оштети и нешто што организација жели да заштити (нпр. како би испунила регулаторну обавезу)
    - Сет пословних података (нпр. PII, кредитне картице)
    - Сет техничких података (нпр. лог фајлови, сесијски колачићи)
    - Делови система (нпр. компоненте, функције, сервиси)
- Листа свих објеката, посебно у раној фази, може бити тешка и временски захтевна
- Објекти помажу у смишљању мапирања тока података
- Објекти помажу анализу ризика

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

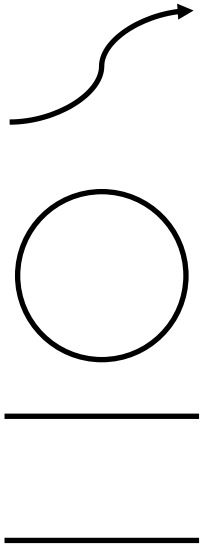
Анализа тока података – улазне тачке

- Улазна тачка представља интерфејс модула ка екстерним ентитетима
- Потпуни скуп улазних тачки модула представља његов правац напада, где мора постојати граница поверења између модула и свих екстерних ентитета
- Примери улазних тачки система:
  - Јавно доступни API (нпр. REST, WebSocket, SOAP)
  - Кориснички интерфејси (нпр. интернет сајт, десктоп апликација)
  - Фајлови које модул користи али којима управља екстерни ентитет (нпр. администратор система)
  - Други модули (нпр. интерни или екстерни сервиси, библиотеке или алати треће стране)

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

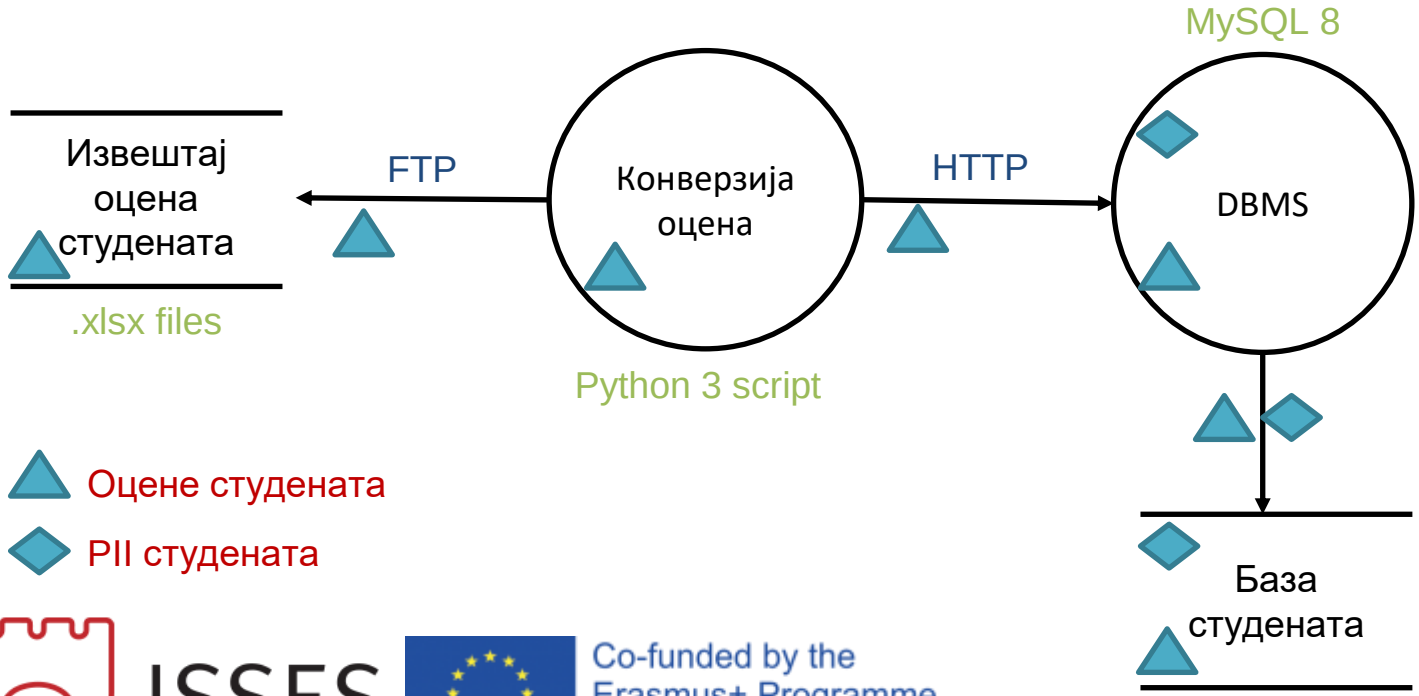
Анализа тока података DFD - елементи

- Дијаграми тока података илуструју:
  - Где подаци улазе, напуштају и пролазе унутар модула (нпр. HTTP, FTP, трансфер бинарних података)
  - Где и на који начин се подаци обрађују (нпр. компоненте модула, апликације, функције)
  - Где се подаци складиште (нпр. фајл, база података, меморија)



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

Анализа тока података DFD - пример

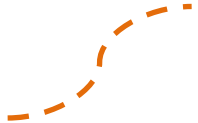


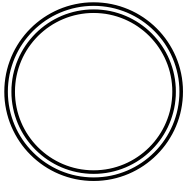
ISSES

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

Анализа тока података DFD – елементи (2)

- Дијаграми тока података такође илуструју:
  - Екстерне ентитете са којима модул интерагује (нпр. екстерне сервисе, кориснике)
  - Које границе поверења дијаграми тока прелазе (нпр. мрежне зоне, физичке машине, апликације и оперативне системе)
  - Који комплексни процеси постоје у оквиру модула (декомпонују се на посебном DFD)

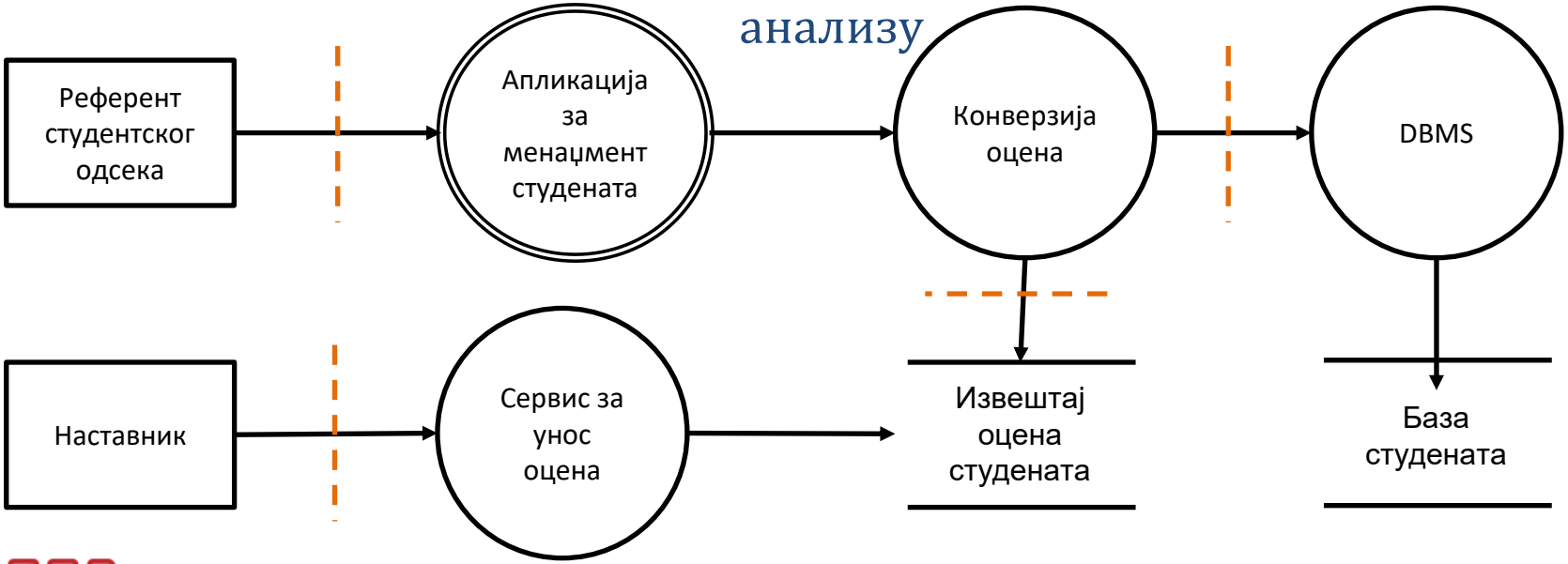




ISSES
Co-funded by the Erasmus+ Programme of the European Union

Анализа тока података DFD – пример (2)

Сортирајте границе поверења према приоритету за безбедоносну анализу



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

Анализа тока података DFD - добре праксе

- Пре анализе претњи потребно је пажљиво проучити елементе дијаграма тока података, јер недостајући елементи на дијаграму могу довести до пропуштене претње
- Почети од контекстног дијаграма који представља посматрани модул као јединствени комплексни процес и дефинисати екстерне ентитете са којима интерагује
- Произвести дијаграм првог нивоа декомпоновањем комплексног процеса
- Ако се дијаграм првог нивоа састоји од комплексних процеса, произвести дијаграм другог нивоа за сваки такав процес
- Дијаграми трећег нивоа су ретки и често представљају знак сувише детаљне анализе

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

Цртање DFD - вежба

- Поделити се у тимове
- Одабрати систем или подсистем (нпр. банка, библиотека, продавница, фабрика, школа)
- Дискутовати пословни процес
- Нацртати дијаграм првог нивоа и бар два дијаграма другог нивоа
- Укључити све елементе

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

Анализа тока података – екстерне зависности и претпоставке

- Листа екстерних зависности садржи софтверске и хардверске компоненте (нпр. OS, апликације, библиотеке, алате) које користи неки модул, а које могу бити мапиране на елементе дијаграма тока података
- Претпоставке о окружењу модула помажу да се смањи оптерећење приликом безбедоносне анализе ограничавањем опсега анализе (нпр. физичка и мрежна безбедност је одговорност клијента)

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

Анализа претњи

- Циљ овог корака је да се идентификују претње по модул који се анализира, како се оне могу остварити кроз нападе и како напади могу бити спречени

Улази

1. Дијаграми тока података са назначеним правцима напада
2. Листа објеката са припадајућим сигурносним захтевима
3. Екстерне зависности и претпоставке

Излази

1. Листа претњи
2. Скуп напада којима се реализује свака претња
3. Постојеће контрамере за избегавање идентификованих напада
4. Предложене мере за избегавање могућих напада

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

Анализа претњи - идентификација

- Идентификовање претњи може се постићи на различите начине:
  - Фокус на нападача (*Attacker-centric*) – претња је циљ нападача
  - Фокус на објекат (*Asset-centric*) – претња је губитак сигурносне особине објекта (нпр. CIA)
  - Фокус на софтвер (*Software-centric*) – претње су изведене на основу дизајна система
- Идентификација претњи са фокусом на софтвер је погодна за софтверске инжењере и често је потпомогнута класификацијом претњи уз помоћ одређене методологије, нпр. STRIDE

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

Анализа претњи - идентификација STRIDE

STRIDE је мнемоник који дефинише шест категорија претњи:

- Сакривање идентитета (*Spoofing of identity*) – нападач се лажно представља кориснику, сервису, фајлу, машини, итд. Ово је претња аутентикацији.
- Измена (*Tampering*) – нападач врши неауторизовану измену података, понашања система, итд. Ово је претња интегритету.
- Порицање (*Repudiation*) – нападач оспорава догађаје и акције или тврди да су се догодиле у време када нису. Ово је претња непорецивости.

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

Анализа претњи - идентификација STRIDE (2)

STRIDE је мнемоник који дефинише шест категорија претњи:

- Откривање информација (*Information disclosure*) – нападач спроводи науторизовани приступ подацима. Ово је претња тајности.
- Одбијање услуге (*Denial of service*) – нападач у потпуности или делимично онемогућава легитимне кориснике да приступе подацима, функцијама, сервисима, итд. Ово је претња доступности.
- Подизање привилегија (*Elevation of privilege*) – нападач добија веће привилегије у систему него што је то предвиђено. Ово је претња за ауторизацију.

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

Анализа претњи - STRIDE и DFD

- STRIDE-по-елементу је метод којим се примењује STRIDE методологија за откривање претњи на сваки елемент дијаграма тока података, без обзира на границе поверења
- За сваки елемент DFD претње се генеришу на основу табеле

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data flow		X		X	X	
Data store		X		X	X	
Process	X	X	X	X	X	X
External E.	X		X			

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

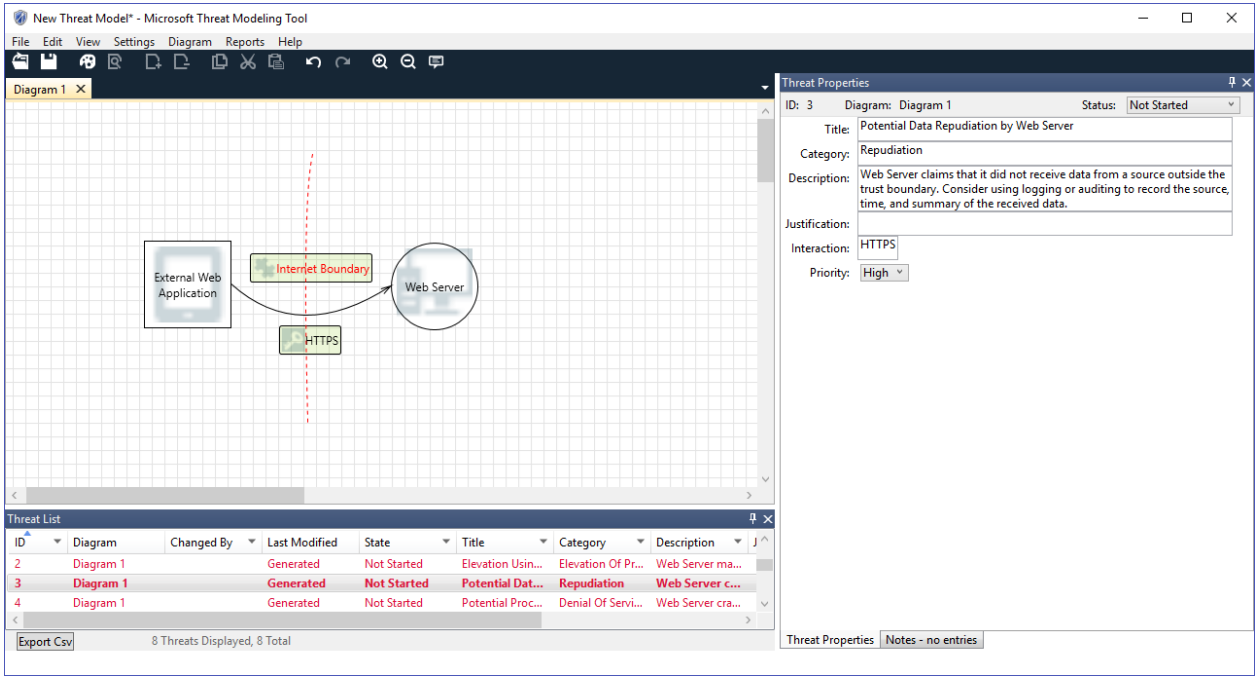
Анализа претњи - STRIDE и DFD (2)

	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data flow		X		X	X	
Data store		X		X	X	
Process	X	X	X	X	X	X
External E.	X		X			

- Слепо генерисање претњи за сваки елемент може да произведе велику листу претњи чак и за једноставне дијаграме
- STRIDE представља смернице, а не генератор претњи – треба се фокусирати на границе поверења, али држати се одбране у дубину

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

Анализа претњи – алати за моделовање претњи



Microsoft Threat Modeling Tool

ISSES

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

Анализа претњи – декомпоновање претњи

- Генеричке STRIDE претње су погодне за идентификацију недостајућих безбедносних пројектних узорака и добрих пракси за сигурносне контроле (нпр. ауторизација, логовање, HTTPS)
- Када су генеричке претње идентификоване, треба обавити декомпоновање претњи како би се идентификовале специфичне врсте напада које могу да остваре ове претње
- Напад може бити једноставна злоупотреба рањиве функције (нпр. контрола приступа је обезбеђена простим сакривањем дугмића на корисничком интерфејсу) или то може бити специјализовани напад који захтева знање из области информационе безбедности како би се идентификовао (нпр. XSS)
- Случајеви злоупотребе и стабла напада могу се користити како би се потпомогла декомпозиција претњи (нпр. корен стабла напада је идентификована претња)

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

Анализа претњи – декомпоновање претњи (2)

- Квалитет декомпоновања претњи зависи од стручности експерта који спроводи моделовање претњи
- Сваки идентификовани напад мора да буде процењен у односу на постојећи модул и све контрамере које спречавају напад треба да буду забележене, као и тачке где су контрамере недовољне
- Искусни стручњаци ће пронаћи и могућности за секундарне нападе који заобилазе успостављене контрамере
- Примарни циљ декомпоновања претњи је прављење листе могућих напада и препорука како да се избегну

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

Анализа претњи - вежба

- Поделити се у тимове
- Одабрати активност у DFD
- Идентификовати претње
- Декомпоновати једну претњу у неколико напада
- Одредити контрамере
- Покушајте да идентификујете један напад који избегава контрамере
- Пронађите додатне контрамере

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

Анализа претњи – добре праксе

- Избећи “експлозију” претњи груписањем претњи за сличне елементе дијаграма

  Сви HTTP-базирани токови података могу се посматрати као један или два елемента (нпр. интерни комуникациони токови и токови података преко интернета)

  SQL база података у једном делу модула вероватно треба да има исте сигурносне контроле као база података у другом делу модула

- Треба наћи начин да се ефикасно спроведе анализа претњи за сопствени контекст
- Истражити и бити у току са актуелним алатима и каталозима напада

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

Анализа ризика

Циљ овог корака је да се на ефикасан начин каналишу инвестиције везане за безбедност тако што ће се приоритизирати претње и напади који захтевају мере за избегавање

Улази

1. Листа претњи, неизбегнутих напада и предложених контрамера
2. Листа угрожених објеката са придруженим сигурносним захтевима

Излази

1. Сортирана листа ризика са стратегијом за баратање са сваким ризиком
2. Приоритизирана листа акција за избегавање и радних задатака везаних за безбедност

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

Анализа ризика – утицај, вероватноћа и ризик

Утицај
Утицај реализоване претње мери негативни ефекат искоришћене претње по систем (финансијски губитак уобичајено)

Вероватноћа
Утврђује се посматрањем рањивости система и проценом могућности нападача који би желели да остваре претњу

Ризик

Најједноставније ризик се израчунава множењем утицаја и вероватноће конкретне претње

Како није могуће бити стопостотно сигуран, анализа ризика је примарна смерница приликом улагања везаних за безбедност

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

Анализа ризика – процена вероватноће

- Вероватноћа да ће претња бити остварена се одређује посматрањем напада који нису спречени да се остваре, узимајући у обзир:
- Коју врсту приступа нападач треба да има да би започео напад (нпр. напад може започети анонимно преко интернета или напад може извести само администратор система)
- Која врста ресурса је нападачу потребна (у смислу времена и новца)
- Који ниво знања и стручности је потребан да би се започео напад (нпр. да ли је тривијални добро познати напад који не захтева никакво посебно знање или специјализовани напад који захтева познавање детаља мете)
- Вероватноћа претње се може израчунати као просечна вероватноћа свих напада који нису спречени

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

Анализа ризика – процена утицаја

Процена утицаја се одређује посматрањем угрожених ресурса и шта губитак одређене сигурносне особине значи за пословање

- Експлицитни сигурносни захтеви често дефинишу цену губитка одређене сигурносне особине (нпр. поверљивости PII)
- SLA-ови дефинишу која је цена губитка неке могућности
- Утицај губитка могућности или интегритета функционалности која је добијена на основу приче корисника (user story) може се извести из приоритета те корисникове приче

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

Анализа ризика

Уобичајени приступ је да се мапирају процењене вредности вероватноће и утицаја користећи једноставну скалу са свега неколико вредности

Када су одређени вероватноћа и утицај ризик се може израчунати на следећи начин:

		Likelihood		
		LOW	MEDIUM	HIGH
Impact	LOW	Low	Low	Medium
	MEDIUM	Low	Medium	High
	HIGH	Medium	High	High

Иако једноставна ова формула за процену ризика се користи у већини случајева, јер брзо производи резултате

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

Стратегије избегавања ризика

Сваки идентификовани ризик можемо адресирати на следећи начин:

- Смањивањем, може се променити дизајн модула, могу се додати нови радни задаци, могу се купити додатни алати, итд.
- Уклањањем, избацивањем модула који уводи ризик (нпр. уклонити застарели систем)
- Преносом (дељењем), ангажовањем треће стране да избегне претњу (нпр. Cloudflare за DDoS) или информисањем клијента да је његова обавеза да се позабави са претњом (нпр. контрола мрежне безбедности)
- Прихватањем, обично када би умањивање ризика коштало више него штета коју уноси у модул

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