

Студијски програм : Информационе технологије и системи			
Назив предмета: Безбедност апликација			
Наставник/наставници: Душан Стефановић			
Статус предмета: Обавезан			
Број ЕСПБ: 7			
Услов: Нема			
Циљ предмета Оспособити студента да препознаје различите врсте, карактеристике и начине напада на апликације као и да исте ефикасно детектује, онемогући и уклони из информационог система.			
Исход предмета Објасни улогу и важност примене сигурносних мера код апликација на web-у, дефинише различите врсте напада на информациони систем, препознаје и објасни различите начине угрожавања сигурности апликација, опише основне функције и карактеристике расположивих сигурносних решења, примени одговарајуће заштите и неутралише могуће нападе на сигурност апликације, наброји, објасни и примени начине заштите на Интернету, наброји, објасни и примени начине заштите код оперативних система и апликација, примени организационе, физичке и правне методе заштите информационог система.			
Садржај предмета <i>Теоријска настава</i> Појам сигурности, претње, напади, сигурност и методе заштите, Сигурносне архитектуре и модели, Основи криптографски појмови и њихова примена, Сигурносни протоколи, Системи за откривање и спречавање упада, Злонамерни програми, Електронско пословање и сигурност на Интернету, Сигурност база података, Сигурносни аспекти програмирања, Организационе, физичке и правне методе заштите, Планирање одржања континуитета посла и опоравак од злонамерних упада. Безбедносни стандарди. Алати за проверу рањивости web апликација. <i>Практична настава</i> Подешавање Kali Linux окружења за тестирање безбедности апликација на Интернету. Извиђање и профилисање сервера апликације. Недостаци провере идентитета и управљање сесијом. Детектовање и експлоатација недостатака заснованих на убацивању (Sql Injection). Проналажење преноса извршења скрипта кроз сајт (XSS). Употреба аутоматизованих скенера у web апликацијама. Упознавање са сигурносним стандардима и програмима сертификације, Упознавање са криптографским таблицама, Криптоанализа Vigenereове шифре, Криптоанализа RSA алгоритама, ElGamalов криптосистем, Diffie-Hellmanов протокол за размену кључева, RSA генератор псеудослучајних секвенци, BBS генератор.			
Литература 1. Gilberto Najera-Gutierrez, Juned Ahmed Ansari, <i>Kali Linux - Testiranje neprobojnosti veba</i> , Компјутер библиотека, 2018 2. Д.Плескоњић, Н.Мачек, Б.Ђорђевић, М.Царић, <i>Сигурност рачунарских система и мрежа</i> , Микро књига, 2007 3. Bryan Sullivan, Vincent Lui, <i>Web application security</i> , McGraw-Hill, 2012			
Број часова активне наставе: 75	Теоријска настава: 45	Број часова активне наставе: 30	
Методe извођења наставе Монолошко – дијалогска, интерактивна и показна уз коришћење савремених мултимедијалних средстава и презентација.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе	поена	Завршни испит	поена
активност у току предавања	5+5=10	писмени испит	30
практична настава	20	усмени испит	
колоквијум-и	10+15=25		
семинар-и	15		