KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo aplikacji

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	45	0
Ćwiczenia	Projekty/seminaria	
0	0	

Liczba punktów ECTS

5

Wykładowcy

Responsible for the course/lecturer:
dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl
tel: 61 665 3531
Wydział Informatyki i Telekomunikacji
adres: ul. Piotrowo 3, 60-965 Poznań

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl
tel: 61 665 3992
Wydział Informatyki i Telekomunikacji
adres: ul. Piotrowo 3, 60-965 Poznań

mgr inż. Łukasz Matuszczak
lukasz.matuszczak@put.poznan.pl
tel: 61 665 3993
Wydział Informatyki i Telekomunikacji
adres: ul. Piotrowo 3, 60-965 Poznań

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z programowania strukturalnego i obiektowego oraz podstawową wiedzę z zakresu projektowania baz danych. Powinien posiadać umiejętność rozwiązywania podstawowych problemów związanych z procesem projektowania systemów informatycznych oraz umiejętność pozyskiwania informacji ze wskazanych źródeł. Powinien również rozumieć konieczność poszerzania swoich kompetencji / mieć gotowość do podjęcia współpracy w ramach zespołu. Ponadto w zakresie kompetencji społecznych student musi prezentować takie

postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

-przekazanie studentom wiedzy dotyczącej projektowania bezpiecznych aplikacji internetowych na przykładzie systemów typy: CMS/CRM/e-commerce oraz bezpiecznych aplikacji mobilnych.

- rozwijanie u studentów umiejętności rozwiązywania problemów związanych z projektowaniem aplikacji internetowych oraz mobilnych z wykorzystywania rozwiązań typu open-source, frameworków i bibliotek wspomagających budowę tego typu rozwiązań

- kształtowanie u studentów umiejętności pracy zespołowej oraz samodzielności w rozwiązywaniu problemów.

Przedmiotowe efekty uczenia się

Wiedza

-ma uporządkowaną, podbudowaną teoretycznie wiedzę w zakresie bezpieczeństwa aplikacji internetowych oraz mobilnych,

-ma szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki i zna technologie wykorzystywanych przy budowie bezpiecznych systemów internetowych oraz mobilnych

-ma wiedzę o cyklu życia aplikacji internetowych oraz mobilnych oraz zagrożeniach na jakie narażone są tego typu aplikacje,

Umiejętności

-potrafi przy formułowaniu i rozwiązywaniu zadań inżynierskich integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) jak również wiedzę z obszaru działania aplikacji internetowych/mobilnych oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne,

-potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć techniki (metod, narzędzi, bibliotek, framework'ów, usług),

-potrafi wykorzystać do formułowania i rozwiązywania zadań inż. i prostych problemów badawczych, dotyczących specyfiki aplikacji internetowych/mobilnych, metody analityczne, symulacyjne oraz eksperymentalne (takie jak: oszacowanie liczby żądań do aplikacji, obciążenia serwera zapytaniami SQL), potrafi poprawnie zaprojektować i zaimplementować wydajne aplikacji,

-potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych, w tym ocenić podatność aplikacji na znane zagrożenia,

Kompetencje społeczne

-rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe, w szczególności technologie internetowe i mobilne

-rozumie potrzeby wykorzystywania najnowszych osiągnięć techniki oraz zna przykłady i rozumie przyczyny wadliwie działających aplikacji internetowych/mobilnych, które doprowadzić mogą do poważnych strat finansowych, wizerunkowych lub społecznych

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
-wykład - wiedza zdobyta na wykładach weryfikowana jest na egzaminie, formę pisemną. Próg zaliczenia egzaminu to 50%. Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta.

-laboratorium/projekt - na podstawie oceny bieżącego postępu realizacji zadań;

Treści programowe

Wykłady

Program wykładu obejmuje omówienie następujących zagadnień:

Z zakresu bezpieczeństwa aplikacji internetowych: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring

Z zakresu bezpieczeństwa aplikacji mobilnych: Improper Platform Usage, Insecure Data Storage, Insecure Communication, Insecure Authentication, Insufficient Cryptography, Insecure Authorization, Client Code Quality, Code Tampering, Reverse Engineering, Extraneous Functionality

Laboratoria/projekt

Zajęcia praktyczne realizowane są samodzielnie przez studentów. Zadania obejmują następujące zagadnienia: przegląd i analiza wybranych open-sourcowych aplikacji internetowych typu CMS/CRM/e-commerce oraz wybranej aplikacji mobilnej pod kątem podatności na znane zagrożenia.

Projekt i implementacja własnej bezpiecznej aplikacji internetowej oraz mobilnej. Opracowanie dokumentacji projektowej systemu zawierającą: wymagania funkcjonalne i pozafunkcjonalne aplikacji, diagramy UML, audyt bezpieczeństwa OWASP. Uwzględnienie w projekcie najnowszych technologii i trendów.

Metody dydaktyczne

Wykład: prezentacja multimedialna uzupełniona przykładami i dodatkowymi objaśnieniami na tablicy. Wykłady prowadzone są zgodnie z zasadami wykładu tradycyjnego, w uzasadnionych przypadkach w formie wykładu konwersacyjnego.

Laboratoria/projekt: prezentacja multimedialna, prezentacja ilustrowana przykładami.

Literatura

Podstawowa

1. *OWASP Top 10 Web Application Security Risks*, [https://owasp.org/www-project-top-ten/]

2. *OWASP Mobile Top 10*, [https://owasp.org/www-project-mobile-top-10/]

Uzupełniająca

1. *Web Application Security*, Andrew Hoffman, O'Reilly 2020

2. *Tworzenie bezpiecznych aplikacji internetowych*, Lis M., Helion 2014

3. Learning iOS Security, Allister Banks , Charles S. Edge, Packt 2015

4. Learning Pentesting for Android Devices, Aditya Gupta, Packt 2014

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	125	5,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	65	2,5

[1] niepotrzebne skreślić lub dopisać inne czynności