



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo aplikacji internetowych [S2Inf1-GiTI>BAIN]

Przedmiot

Kierunek studiów
Informatyka

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Gry i technologie internetowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
15

Laboratorium
15

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z programowania (m.in. aplikacji internetowych) 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 typu: CMS/CRM/e-commerce. - rozwijanie u studentów umiejętności rozwiązywania problemów związanych z projektowaniem i aplikacji internetowych z wykorzystywaniem narzędzi typu open-source, frameworków i bibliotek wspomagających budowę, testowanie i analizę tego typu aplikacji - 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,
- ma szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki i zna technologie wykorzystywanych przy budowie bezpiecznych systemów internetowych,
- ma wiedzę o cyklu życia aplikacji internetowych 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 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 inżynierskich i prostych problemów badawczych, dotyczących specyfiki aplikacji internetowych, metody analityczne, symulacyjne oraz eksperymentalne (takie jak: oszacowanie liczby żądań do aplikacji, obciążenia serwera zapytaniami SQL), potrafi poprawnie zaprojektować i zaimplementować wydajne i bezpieczne aplikacje,
- 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,
- rozumie potrzeby wykorzystywania najnowszych osiągnięć techniki oraz zna przykłady i rozumie przyczyny wadliwie działających aplikacji internetowych, 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 sprawdzianie, który ma formę pisemną. Próg zaliczenia sprawdzianu to 50%. Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta.
- laboratorium - na podstawie oceny bieżącego postępu realizacji zadań;

Treści programowe

Program modułu obejmuje wprowadzenie do bezpieczeństwa aplikacji internetowych ze szczególnym uwzględnieniem podatności z projektu OWASP Top 10.

Tematyka zajęć

Program wykładów 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.

Zajęcia laboratoryjne realizowane są samodzielnie przez studentów. Zadania obejmują następujące zagadnienia: przegląd i analiza wybranych open-source aplikacji internetowych typu CMS/CRM/e-commerce pod kątem podatności na znane zagrożenia. Projekt i implementacja własnej aplikacji oraz audyt jej bezpieczeństwa.

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: prezentacja multimedialna, prezentacja ilustrowana przykładami.

Literatura

Podstawowa:

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

Uzupełniająca:

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

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

3. Web Application Security. Exploitation and Countermeasures for Modern Web Applications, O'Reilly 2019

4. Secure Web Application Development, Baker M., Apress 2022

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwίων/egzaminu, wykonanie projektu)	20	0,50