KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo aplikacji internetowych [S1Cybez1>BAI]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

mgr inż. Norbert Langner
norbert.langner@put.poznan.pl

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 zakresie budowy systemów informatycznych, zasad działania systemów operacyjnych, sieci komputerowych, mechanizmów kryptograficznych 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 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,[K1_W05]
-ma szczegółową wiedzę związaną z wybranymi zagadnieniami z zakresu informatyki i zna technologie wykorzystywanych przy budowie bezpiecznych systemów internetowych, [K1_W10]
-ma wiedzę o cyklu życia aplikacji internetowych oraz zagrożeniach na jakie narażone są tego typu aplikacje, [K1_W09]
-ma zaawansowaną wiedzę w zakresie zasada tworzenia programów komputerowych, struktur języków programowania, ich poziomów oraz używanych algorytmów; ma zaawansowaną wiedzę z zakresu inżynierii oprogramowania; [K1_W06]

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, [K1_U01]
-potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć techniki (metod, narzędzi, bibliotek, framework'ów, usług),[K1_U08]
-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,[K1_U02]
- na podstawie dostępnej dokumentacji i specyfikacji oraz standardów potrafi zaprojektować i zaimplementować w językach wysokiego poziomu bezpieczną aplikację internetową lub mobilną [K1_U10]
-potrafi dokonać krytycznej analizy istniejących rozwiązań technicznych, w tym ocenić podatność aplikacji na znane zagrożenia, [K1_U09]

Kompetencje społeczne:
-Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują,[K1_K01]
-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, [K1_K02]
-ma świadomość znaczenia pracy własnej i konieczności przestrzegania zasad etyki zawodowej, jest gotowy do podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania, a także dbałości o dorobek i tradycje zawodu. [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
-wykład - wiedza zdobyta na wykładach weryfikowana jest na egzaminie, formę pisemną. Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta,
-laboratoria/projekt - na podstawie oceny bieżącego postępu realizacji zadań.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów

elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Program przedmiotu obejmuje zagadnienia związane z bezpieczeństwem aplikacji internetowych, w tym techniki ochrony przed atakami, takie jak injection, cross-site scripting (XSS), cross-site request forgery (CSRF), a także zabezpieczenia komunikacji (SSL/TLS). Przedstawiane są także zasady zarządzania tożsamościami i autoryzacją użytkowników oraz implementacja bezpiecznego przechowywania danych (np. haseł, tokenów). W ramach przedmiotu omawiane są również techniki ochrony aplikacji przed atakami DoS (Denial of Service) oraz monitorowanie i audyt bezpieczeństwa aplikacji.

Tematyka zajęć

Podczas wykładów omawiane są zagrożenia związane z bezpieczeństwem aplikacji internetowych, metody zabezpieczania aplikacji przed atakami oraz techniki zapewnienia poufności, integralności i dostępności danych. Przedstawiane są teoretyczne podstawy ataków na aplikacje internetowe, jak i środki obrony, w tym metody szyfrowania i uwierzytelniania użytkowników.
Zajęcia laboratoryjne realizowane są samodzielnie przez studentów. Zadania obejmują następujące zagadnienia: przegląd i analiza wybranych aplikacji internetowych (open-source) typu CMS/CRM/e-commerce lub własnych rozwiązań pod kątem podatności na znane zagrożenia.

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

Uzupełniająca:
Uzupełniająca
1. Web Application Security, Andrew Hoffman, O'Reilly 2020
2. Web Application Security. Exploitation and Countermeasures for Modern Web Applications, O'Reilly 2019

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	90	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	48	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	42	1,50