



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo usług sieciowych [S2Teleinf2-STRC>BUs]

Przedmiot

Kierunek studiów
Teleinformatyka

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Sieci teleinformatyczne i rozwiązania chmurowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
14

Laboratorium
24

Inne
14

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Piotr Zwierzykowski prof. PP
piotr.zwierzykowski@put.poznan.pl

mgr inż. Błażej Nowak
blazej.nowak@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawowa wiedza na temat sieci: Studenci powinni posiadać podstawową wiedzę na temat sieci komputerowych, w tym pojęć takich jak adresacja IP, routing, switching, protokoły sieciowe, firewalle i architektura sieci. Znajomość tworzenia aplikacji: Studenci powinni znać koncepcje i język(i) (np. Java, Python, C#, PHP, JavaScript) tworzenia aplikacji webowych. Dużą zaletą będzie znajomość choćby jednego frameworka związanego z tworzeniem aplikacji webowych. Studenci powinni być dobrze zaznajomieni z tworzeniem i używaniem relacyjnych baz danych. Wymagane jest też aby student znał podstawy protokołu http / https. Podstawy bezpieczeństwa: Studenci powinni posiadać podstawową wiedzę na temat ogólnych zasad i koncepcji bezpieczeństwa, w tym uwierzytelniania, szyfrowania, kontroli dostępu i typowych zagrożeń bezpieczeństwa.

Cel przedmiotu

Celem jest edukacja Studentów w zakresie podstawowych pojęć, zasad i najlepszych praktyk związanych z bezpieczeństwem usług sieciowych i bezpieczeństwem warstwy aplikacji. przedmiot ma na celu zwiększenie świadomości uczestników na temat potencjalnego ryzyka, zagrożeń i słabych punktów w tych obszarach oraz dostarczenie im wiedzy umożliwiającej podejmowanie świadomych decyzji dotyczących środków bezpieczeństwa. Dzięki zrozumieniu zagrożeń i słabych punktów wynikających z danych rozwiązań omawianych na tym przedmiocie, Studenci nauczą się skutecznych strategii ograniczania ryzyka i ochrony swoich sieci i aplikacji przed nieautoryzowanym dostępem, naruszeniami danych i innymi incydentami związanymi z bezpieczeństwem.

Przedmiotowe efekty uczenia się

Wiedza:

1. Szczegółowa wiedza o podstawowych procesach autoryzacji takich jak OAuth i BasicAuth
2. Wiedza o działaniu podstawowych algorytmach szyfrowania w warstwie aplikacji
3. Wiedza o zarządzaniu sesjami i przechowywaniu wrażliwych danych
4. Wiedza w zakresie zasady działania, skutkach i środkach zapobiegawczych podstawowych ataków warstwy aplikacji takich jak:
 - a. SQL injection
 - b. Cross site request forgery
 - c. Cross site scripting
 - d. Zatrucie DNS
 - e. WiFi SSID spoofing
 - f. Session hijacking
 - g. Brute force
5. Znajomość architektury standardowych aplikacji webowych
6. Znajomość podstawowych ataków, ich skutków i środków zapobiegawczych warstwy sieciowej i łącza danych takich jak:
 - a. Zatrucie ARP
 - b. WiFi SSID spoofing
 - c. IP spoofing
 - d. DDoS
 - e. ICMP flood
 - f. Zatrucie tabeli routingu
 - g. Ping death

Ma poszerzoną i pogłębioną wiedzę w zakresie [K2_W02] :

- nowoczesnych systemów transmisji i przetwarzania danych,
- urządzeń wchodzących w skład systemów teleinformatycznych.

Zna i rozumie algorytmy wykorzystywane w systemach teleinformatycznych z obszaru specjalizacji [K2_U05].

Ma pogłębioną wiedzę w zakresie przetwarzania i bezpieczeństwa informacji w systemach teleinformatycznych [K2_W08].

Umiejętności:

1. Umiejętność tworzenia prostych aplikacji webowych odpornych na podstawowe ataki
2. Umiejętność wykorzystania szyfrowania do zabezpieczania danych
3. Umiejętność projektowania sieci i wykorzystywania protokołów routingu przy jednoczesnym zabezpieczaniu się przed podstawowymi atakami
4. Umiejętność wykorzystywania podatności aplikacji na wybrane ataki

Potrafi opracować szczegółową dokumentację wyników realizacji eksperymentu, zadania projektowego lub badawczego; potrafi przygotować opracowanie zawierające omówienie tych wyników [K2_U03].

Potrafi wykorzystać poznane metody i modele matematyczne, w razie potrzeby odpowiednio je modyfikując, do realizacji projektów w obszarze teleinformatyki [K2_U06].

Potrafi zaproponować ulepszenia lub rozwiązania alternatywne dla istniejących rozwiązań projektowych i systemów teleinformatycznych [K2_U09]

Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć w zakresie technik, metod projektowania do projektowania i wytwarzania układów i systemów teleinformatycznych zawierających rozwiązania o charakterze innowacyjnym [K2_U10].

Kompetencje społeczne:

Studenci znają i rozumieją wagę i skutki luk bezpieczeństwa, rozumieją, że nowe ataki, wykorzystania podatności i obrona przed nimi to proces ciągły.

Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny odbieranych treści[K2_K01].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są podstawie kolokwium zaliczeniowego, składającego się z 5-10 zadań różnie punktowanych w zależności od stopnia ich trudności lub na podstawie opracowanego projektu przykładowej aplikacji lub sieci. Próg zaliczeniowy: 50+% punktów.

Wiedza nabyta w ramach wykładu jest weryfikowana przez kolokwium końcowe realizowane na ostatnim wykładzie. Każde z kolokwium składa się z 10-15 pytań (testowych i otwartych), różnie punktowanych. Próg zaliczeniowy: 50+% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania zostaną przesłane studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej lub platformy eKursy.

Treści programowe

Przedmiot obejmuje zagadnienia związane z zapewnieniem bezpieczeństwa usług sieciowych.

Bezpieczeństwo usług sieciowych przedstawione głównie w oparciu o bezpieczeństwo usług świadczonych w oparciu o platformę WWW.

Tematyka zajęć

Wykłady:

1. Wprowadzenie do bezpieczeństwa usług sieciowych.
2. Omówienie standardowych aplikacji webowych i najczęstszych podatności.
3. Omówienie podstawowych sposobów wykorzystania / zabezpieczania się przed najczęstszymi podatnościami i aplikacji webowych.
4. Omówienie sposobów i praktyk związanych z zarządzaniem sesją i przechowywaniem wrażliwych danych.
5. Omówienie podstawowych metod autoryzacji.
6. Omówienie podstawowych ataków, sposobów zabezpieczania się i wykorzystywania podatności w warstwie sieci i łącza danych.
7. Kolokwium zaliczeniowe.

Laboratoria:

1. Wprowadzenie do bezpieczeństwa usług sieciowych / zajęcia organizacyjne
2. Stworzenie przykładowej aplikacji webowej bez wykorzystania frameworka.
3. Stworzenie przykładowej aplikacji webowej z wykorzystaniem frameworka.
4. Zaprojektowanie i stworzenie baz danych związanych z napisanymi aplikacjami.
5. Zlokalizowanie podatności napisanych aplikacji.
6. Przeprowadzenie ataków, wykorzystujących zlokalizowane podatności, na własne aplikacje.
7. Modyfikacje napisanych aplikacji zabezpieczające przed równocześnie przeprowadzonymi atakami.
8. Zabezpieczanie i redundancja danych wrażliwych.
9. Wykorzystanie podstawowych algorytmów szyfrujących.
10. Stworzenie przykładowej aplikacji wykorzystującej jeden ze standardowych sposobów autoryzacji.
11. Przeprowadzenie ataku man in the middle z wykorzystaniem WiFi SSID spoofing.
12. Przeprowadzenie ataku ICMP flood na jedną ze swoich aplikacji/maszyn.
13. Przeprowadzenie ataku brute force na wybraną, własną sieć WiFi.
14. Kolokwium zaliczeniowe lub omówienie projektów.

Metody dydaktyczne

Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy oraz pokazami praktycznymi.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne wykonywane samodzielnie lub w grupach z wykorzystaniem komputera.

Literatura

Podstawowa:

Sekurak: Bezpieczeństwo aplikacji webowych, Sekurak, 2019, ISBN:10010302135.

A.Muller, M. Meucci: OWASP Testing Guide v4, OWASP, 2014.

W. Stallings: Network Security Essentials: Applications and Standards, Pearson, 2016.

Uzupełniająca:

C. Sanders: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, No Starch Press, 2011.

J. Wright, J. Cache: Hacking Exposed Wireless: Wireless Security Secrets & Solutions, McGraw Hill, 2015.

C. McNab: Network Security Assessment. Know Your Network, O'Reilly Media, 2016.

D. Stuttard, M. Pinto: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, Wiley, 2011.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	78	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	40	1,50