

KARTA KURSU

| | |
|-----------------|---|
| Nazwa | Bezpieczeństwo aplikacji internetowych 2 |
| Nazwa w j. ang. | Web Application Security 2 |

| | | |
|-----------------|---|--------------------------|
| Koordinator | Dr inż. Rafał Szklarczyk | Zespół dydaktyczny |
| Punktacja ECTS* | st. stacjonarne: 2 st. niestacjonarne: 2 | dr inż. Rafał Szklarczyk |

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z:

- zagrożeniami bezpieczeństwa aplikacji internetowych,
- popularnymi metodami ataków na aplikacje webowe,
- metodami do diagnostyki i zabezpieczania aplikacji

Kurs prowadzony jest w języku polskim.

Warunki wstępne

| | |
|--------------|---|
| Wiedza | Działanie i funkcjonowanie sieci z szczególnym naciskiem na protokół HTTP |
| Umiejętności | Programowanie w jednym z popularnych języków do tworzenia aplikacji webowych, np. PHP, Ruby, Python, Java, JavaScript, C# |
| Kursy | <u>Wymagane zaliczenie kursu:</u> <ul style="list-style-type: none"> • Aplikacje Internetowe (Web Applications) • Zaawansowane technologie webowe • Bezpieczeństwo Aplikacji Internetowych 1 |

Efekty uczenia się

| | Efekt uczenia się dla kursu | Odniesienie do efektów kierunkowych |
|--------------|---|-------------------------------------|
| Wiedza | Po zakończeniu kursu student: | |
| | W01: Zna podstawowe zagrożenia bezpieczeństwa aplikacji webowych (w tym OWASP TOP 10). | K_W03, K_W06, K_W07, |
| | W02: Wie jak zidentyfikować podatność na atak i zabezpieczyć system internetowy przed popularnymi atakami | K_W03, K_W06, K_W07 |
| Umiejętności | Po zakończeniu kursu student: | |
| | U01: Potrafi przeskanować i przetestować podatności w aplikacji (poszerzoe umiejętności) | K_U01, K_U05, K_U06 |
| | U02: Potrafi wdrożyć i skonfigurować mechanizmy zabezpieczania aplikacji webowych (poszerzone umiejętności) | K_U03, K_U06, K_U10 |

| Kompetencje społeczne | Efekt uczenia się dla kursu | | | | | | Odniesienie do efektów kierunkowych | |
|-----------------------|---|--|--|--|--|--|-------------------------------------|--|
| | Po zakończeniu kursu student: | | | | | | | |
| | K01: Potrafi zaprojektować i implementować podstawowe elementy bezpieczeństwa w systemach informatycznych | | | | | | K_K02, K_K04, K_K05 | |

Studia stacjonarne

| Organizacja | | | | | | | | | | | | |
|---------------|---------------|---------------------|--|---|--|----|--|---|--|---|--|---|
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | | |
| | | A | | K | | L | | S | | P | | Z |
| Liczba godzin | | | | | | 30 | | | | | | |

Studia niestacjonarne

| Forma zajęć | Organizacja | | | | | | | | | | | |
|---------------|---------------|---------------------|--|---|----|---|--|---|--|---|--|---|
| | Wykład (W) | Ćwiczenia w grupach | | | | | | | | | | |
| | | A | | K | | L | | S | | P | | Z |
| Liczba godzin | | | | | 20 | | | | | | | |

Opis metod prowadzenia zajęć

Kurs składa się z ćwiczeń prowadzonych w formie laboratoriów. W ramach zajęć laboratoryjnych zostaną studentowi przedstawiona podstawowa ogólna wiedza z zakresu bezpieczeństwa systemów komputerowych z uwagą skupioną na bezpieczeństwie aplikacji internetowych. Na laboratorium studenci będą wykonywać ćwiczenia polegające na: diagnostyce podatności na zagrożenia aplikacji internetowych (z wykorzystaniem narzędzi skanujących); przygotowaniu prostych aplikacji internetowych demonstrujących podatność na atak (np. SQLi) a następnie dokonaniu zabezpieczenia aplikacji przed danym atakiem, a także wykorzystaniem zasad secure coding; konfiguracji narzędzi umożliwiających demonstrację a następnie demonstracji technik uwierzytelnienia. W trakcie zajęć studenci będą wykorzystywać wiedzę z pierwszej części kursu przedmiotu (Bezpieczeństwo Aplikacji Internetowych 1) do identyfikacji zagrożeń, wykrycia luk bezpieczeństwa, wdrożenia mechanizmów obrony w oparciu o narzędzia open source dostępne na rynku oraz o opracowania własne.

Formy sprawdzania efektów uczenia się

| | E – learning | Gry dydaktyczne | Ćwiczenia w szkole | Zajęcia terenowe | Praca laboratoryjna | Projekt indywidualny | Projekt grupowy | Udział w dyskusji | Referat | Praca pisemna (esej) | Egzamin ustny | Egzamin pisemny | Zadania problemowe |
|-----|--------------|-----------------|--------------------|------------------|---------------------|----------------------|-----------------|-------------------|---------|----------------------|---------------|-----------------|--------------------|
| W01 | | | | | | | | X | | | | | |
| W02 | | | | | X | | | X | | | | | |
| U01 | | | | | X | | | X | | | | | X |
| U02 | | | | | X | | | X | | | | | X |
| K01 | | | | | X | | | X | | | | | X |

| | |
|----------------|--|
| Kryteria oceny | <p>Przygotowanie i przedstawienie projektu wdrożenia zabezpieczeń lub opisu wybranego zagadnienia bezpieczeństwa aplikacji internetowych, wykorzystującego wiedzę z laboratoriów w szerokim zakresie jest warunkiem niezbędnym zaliczenia przedmiotu.</p> <p>Osiągnięcie efektów kształcenia podanych powyżej uprawnia studentów do uzyskania oceny nie wyższej niż dostateczna. Ocenę dobrą lub bardzo dobrą może uzyskać student, który:</p> <ul style="list-style-type: none"> - umiejętności na ocenę 4 Potrafi poprawnie zidentyfikować oraz zabezpieczyć aplikację internetową oraz w jasny i zrozumiały sposób wyjaśnić metody ataku i obrony. - umiejętności na ocenę 5 Zna mechanizmy i narzędzia minimalizujące ryzyko wystąpienia podatności oraz potrafi je zademonstrować ich działanie + umiejętności na ocenę 4. |
|----------------|--|

| | |
|-------|--|
| Uwagi | |
|-------|--|

Treści merytoryczne (wykaz tematów)

| |
|---|
| <ol style="list-style-type: none"> 1. SQLi metody zabezpieczeń (walidacja wejścia, użycie sparametryzowanych zapytań, użycie ORM), 2. Secure Coding (implementacja przechowywania i weryfikacji haseł) 3. Metody uwierzytelnienia / kontroli dostępu (basic, session based, JWT, OAuth2) 4. mod_auth_basic 5. Praca z mechanizmami zabezpieczeń przeglądarki (Same-origin policy, Protokół CORS, Cross-document messaging) 6. Testowanie aplikacji internetowych, 7. SSL / TLS, CSR, CA, łańcuch certyfikatów x.509, komenda openssl |
|---|

Wykaz literatury podstawowej

| |
|--|
| <ol style="list-style-type: none"> 1. Bezpieczeństwo aplikacji internetowych dla programistów. Rzeczywiste zagrożenia, praktyczna ochrona, M. McDonald, Helion 2021. 2. Podręcznik pentestera. Bezpieczeństwo systemów informatycznych, P. Kim, Helion 2015. 3. Testowanie bezpieczeństwa aplikacji internetowych, P.Hope, Helion 2012. |
|--|

Wykaz literatury uzupełniającej

| |
|---|
| <ol style="list-style-type: none"> 1. Kali Linux i testy penetracyjne. Biblia, G. Khawaja, Helion 2022. 2. Dokumentacja OWASP; Dokumentacja Apache; Dokumentacja MDN Web Docs; Repozytorium dokumentów RFC. 3. Bezpieczeństwo aplikacji mobilnych, D.Chell, Helion 2018. |
|---|

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – studia stacjonarne

| | Wykład | |
|---|--|----|
| Liczba godzin w kontakcie z prowadzącymi | Konwersatorium (ćwiczenia, laboratorium itd.) | 30 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 5 |
| Liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 5 |
| | Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu | 5 |
| | Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie) | 5 |
| | Przygotowanie do egzaminu/zaliczenia | |
| Ogółem bilans czasu pracy | | 50 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 2 |

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) – **studia niestacjonarne**

| | | |
|---|--|----|
| Liczba godzin w kontakcie z prowadzącymi | Wykład | |
| | Konwersatorium (ćwiczenia, laboratorium itd.) | 20 |
| | Pozostałe godziny kontaktu studenta z prowadzącym | 2 |
| Liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 5 |
| | Realizacja zadań domowych (problemowych) po zapoznaniu się z niezbędną literaturą przedmiotu | 15 |
| | Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna lub w grupie) | 8 |
| | Przygotowanie do egzaminu/zaliczenia | |
| Ogółem bilans czasu pracy | | 50 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 2 |