Załącznik nr 1. Specyfikacja i harmonogram Szkolenia Santander | Cyberbezpieczeństwo dla każdego z Politechniką Poznańską 2024

Harmonogram konkursu	
do 6 maja 2024 r.	Wyślij aplikację na Santander Open Academy
do 7 maja 2024 r.	Wykonaj test umiejętności
14 maja 2024 r.	Ogłosimy wyniki rekrutacji do konkursu
od 14 do 20 maja 2024 r.	Pierwszy termin potwierdzenia udziału w kursie i rejestracja na stronie wskazanej w instrukcji, którą otrzymasz mailowo
od 21 maja do 27 maja 2024 r.	Drugi termin potwierdzenia udziału w kursie (dla listy rezerwowej) i rejestracja na stronie wskazanej w instrukcji, którą otrzymasz mailowo
od 28 maja 2024 r. w przypadku rezygnacji innego zwycięzcy	Dodatkowy termin potwierdzenia udziału w kursie w przypadku rezygnacji wcześniej wybranych uczestników i rejestracja na stronie wskazanej w instrukcji, którą otrzymasz mailowo

Terminy nauki własnej na platformie eNauka	
od 21 maja 2024 r. lub w terminie wskazanym w wiadomości mailowej	Nadamy Ci dostęp do platformy eNauka, jeżeli potwierdziłaś/potwierdziłeś udział w nim i zarejestrowałaś/zarejestrowałeś się na stronie wskazanej w instrukcji, którą otrzymałaś/otrzymałeś mailowo.
do 7 dni kalendarzowych od nadania dostępu do platformy eNauka	Rozpocznij naukę na platformie eNauka. Jeżeli tego nie zrobisz w tym terminie to możemy to potraktować jako rezygnację i Twoje miejsce przyznamy innej osobie z listy rezerwowej.
od nadania dostępu do platformy eNauka do 31 sierpnia 2024 r.	Możesz korzystać z platformy eNauka ze szkolenia z podstaw cyberbezpieczeństwa.
od nadania dostępu do platformy eNauka do 90 dni od rozpoczęcia warsztatów live, na które się zapiszesz	W przypadku gdy wybierzemy Cię do drugiego etapu, możesz korzystać z platformy eNauka ze szkolenia warsztaty live z podstaw testowania web aplikacji, szkolenie z podstaw cyberbezpieczeństwa nie będzie dostępne po 31 sierpnia 2024 r.

Lp.	Rodzaj szkolenia (forma)	Ilość modułów	Szacunkowy czas nauki	Wzmacniane kompetencje	Rodzaje ćwiczeń
1	Szkolenie z podstaw cyberbezpieczeństwa (live)	11	ok. 12h live'ów oraz nauka własna na platformie eNauka	Poznasz podstawowe narzędzia zapobiegające cyberatakom, zbudujesz swoją świadomość zagrożeń w świecie cyfrowym i dowiesz się jak nim zapobiegać	Słowniczek podstawowych pojęć, live z prowadzącymi, bezpieczne hasła, menedżer hasła, kopie zapasowe, szyfrowanie komputera, tworzenie zaszyfrowanych kontenerów i dysków zewnętrznych, szyfrowanie poczty elektronicznej, metody wymiany kluczy publicznych, filmy instruktażowe, prezentacja ataku na algorytm AES w trybie ECB
2	Warsztaty live z podstaw testowania web aplikacji (bezpośrednia interakcja z mikrofonem i kamerą uczestników)	8	ok. 10h warsztatów live'ów	Poznasz podstawy testowania aplikacji webowych	Konfiguracja oraz zapoznanie ze środowiskiem pracy, zarządzanie sesją użytkownika, XXS, SQL injection, XML, OWASP Top Ten.

Terminy realizacji live'ów		
	Szkolenie z podstaw cyberbezpieczeństwa	**Warsztaty live z podstaw testowania web aplikacji** (w przypadku zakwalifikowania się do drugiego etapu)
1.	23 maja 2024 r., czwartek, godz. 18:00 – 20:00 • **Dlaczego smartphone to szatan?** Prowadzący: Piotr Konieczny, niebezpiecznik.pl • **Spotkanie organizacyjne dotyczące szkolenia** Prowadzący: mgr inż. Piotr Kontowicz	Grupa I 7 czerwca 2024 r., piątek godz. 18:00 – 21:00 8 czerwca 2024 r., sobota godz. 10:00 – 15:00 9 czerwca 2024 r., niedziela godz. 10:00 – 15:00
2.	24 maja 2024 r., piątek, godz. 18:00 – 20:00 • **Dlaczego hasła są ważne i jak nimi zarządzać?** • **Przybliżenie urządzeń sieciowych.** Prowadzący: mgr inż. Piotr Kontowicz	Grupa II 14 czerwca 2024 r., piątek godz. 18:00 – 21:00 15 czerwca 2024 r., sobota godz. 10:00 – 15:00 16 czerwca 2024 r., niedziela godz. 10:00 – 15:00
3.	25 maja 2024 r., sobota, godz. 10:00 – 15:00 • **Bezpieczeństwo sieci domowej.** • **Bezpieczne korzystanie z komputera** • **Bezpieczne obchodzenie się z danymi** Prowadzący: mgr inż. Piotr Kontowicz	Grupa III 28 czerwca 2024 r., piątek godz. 18:00 – 21:00 29 czerwca 2024 r., sobota godz. 10:00 – 15:00 30 czerwca 2024 r., niedziela godz. 10:00 – 15:00
4.	26 maja 2024 r., niedziela, godz. 10:00 – 12:00 • **Aktualizacje** • **Niebezpieczeństwa związane z USB** • **Bezpieczeństwo urządzeń mobilnych** Prowadzący: mgr inż. Piotr Kontowicz	Grupa IV 5 lipca 2024 r., piątek godz. 18:00 – 21:00 6 lipca 2024 r., sobota godz. 10:00 – 15:00 7 lipca 2024 r., niedziela godz. 10:00 – 15:00
5.	1 czerwca 2024 r., sobota, godz. 10:00 – 15:00 • **Niebezpieczeństwa AI** • **Bezpieczeństwo w mediach społecznościowych** • **Kryptowaluty** • **Steganografia w służbie bezpieczeństwa** Prowadzący: mgr inż. Piotr Kontowicz	Grupa V 12 lipca 2024 r., piątek godz. 18:00 – 21:00 13 lipca 2024 r., sobota godz. 10:00 – 15:00 14 lipca 2024 r., niedziela godz. 10:00 – 15:00
6.	2 czerwca, niedziela, godz. 12:00 – 13:00 • Egzamin końcowy Prowadzący: mgr inż. Piotr Kontowicz	

Opis modułów szkolenia z podstaw cyberbezpieczeństwa		
1.	Dlaczego smartphone to szatan? Piotr Konieczny, niebezpiecznik.pl	Prelekcja „Dlaczego smartphone to szatan” opisuje szereg funkcji smartfonów, które można wykorzystać w "złośliwy" sposób. Uczulamy na to, jak twórcy aplikacji mobilnych mogą "po cichu" wykradać dane od niczego nieświadomych użytkowników. W trakcie prezentacji pokazujemy realne ataki na telefony komórkowe i najpopularniejsze aplikacje. Poza zwróceniem uwagi na problemy dotyczące wykorzystania Wi-Fi, Bluetooth i "gospodarowania" uprawnieniami w aplikacjach otrzymasz informacje z zakresu: • jak podnieść bezpieczeństwo swojego telefonu? • jak chronić swoją prywatność jeśli korzystamy ze smartfona? • na jakie ataki uważać i czego pod żadnym pozorem nie robić? • jak bezpiecznie wykorzystać smartfona w środowisku firmowym? • na co uważać w trakcie wyjazdów służbowych • jak można kogoś inwigilować przez telefon komórkowy (i co zrobić, aby nie stać się ofiarą podsłuchu)?
2.	Hasła	• Dowiesz się: czym są hasła, poznasz przykłady silnych i słabych haseł, • Nauczysz się: ○ budowania haseł (błędy w tworzeniu haseł, dobre praktyki) ○ technik pamięciowych dla tworzenia i zapamiętania haseł ○ Hasła oparte na frazach (passphrases) ○ bezpiecznego zmieniania haseł ○ korzystania z menadżerów haseł ○ sprawdzania danych z wycieków ○ logowania wieloskładnikowego (sms, aplikacje generujące kody, tokeny, klucze u2f, biometria) ○ wprowadzenia koncepcji haseł jednorazowych ○ wprowadzenia koncepcji passwordless • Zobaczysz przykład łamania hasła, którego nagranie zamieścimy na platformie eNauka.
3.	Sieci	• Poznasz podstawowe urządzenia sieciowe i pojęcia związane z sieciami i ich bezpieczeństwem • Nauczysz się: ○ Jak zadbać o bezpieczeństwo domowej sieci, ○ Jak bezpiecznie dodać urządzenia IoT do swoje sieci ○ Dowiesz się czy VPN faktycznie poprawia bezpieczeństwo ○ Zobaczysz jak łatwo hasło do sieci może zostać złamane ○ Dowiesz się czy korzystanie z otwartych sieci bezprzewodowych jest bezpieczne
4.	Bezpieczeństwo korzystania z komputera	• Poznasz podstawowe pojęcia związane z zagrożeniami z którymi spotykasz się na co dzień podczas korzystania z komputera oraz dowiesz się jak zadbać o swoje bezpieczeństwo. • Nauczysz się: ○ jak rozpoznawać phishing, ○ wysyłać szyfrowane wiadomości email, ○ Wybierać odpowiedni komunikator ○ Jak tworzyć szyfrowane kontenery i zewnętrzne dyski
5.	Bezpieczeństwo obchodzenia się z danymi	• Poznasz podstawy zabezpieczania danych w podczas ich przechowywania • Nauczysz się: ○ bezpiecznie niszczyć dokumenty elektroniczne i papierowe, ○ wybierać odpowiedniego dostawcę usług chmurowych.

6.	Bezpieczeństwo urządzeń mobilnych	• Poznasz zagrożenia występujące podczas korzystania z urządzeń mobilnych oraz metody ochrony przed nimi jak i minimalizowania ryzyka. • Nauczysz się: ○ zabezpieczać swoje urządzenia mobilne, ○ w bezpieczny sposób instalować aplikacje na urządzeniach mobilnych.
7.	Niebezpieczeństwa sztucznej inteligencji (AI)	• Poznasz jak możesz wykorzystać sztuczną inteligencję w codziennym życiu. Dowiesz się jak przestępcy mogą wykorzystywać narzędzia sztucznej inteligencji do przeprowadzania ataków. • Nauczysz się: ○ korzystać z narzędzi wyposażonych w sztuczną inteligencję, ○ podniesiesz swoją świadomość jak przestępcy mogą wykorzystać sztuczną inteligencję do przeprowadzania ataków.
8.	Bezpieczeństwo w mediach społecznościowych	• Poznasz zagrożenia występujące w mediach społecznościowych. • Nauczysz się: ○ chronić swoją tożsamość w mediach społecznościowych
9.	Kryptowaluty	• Dowiesz się czym są kryptowaluty, oraz poznasz mechanizmy oszustów związanych z kryptowalutami.
10.	Steganografia w służbie bezpieczeństwa	• Poznasz czym jest steganografia i jak możesz z niej skorzystać. • Nauczysz się: ○ oznaczać dokumenty tak, aby udowodnić ich pochodzenie w przypadku kradzieży, ○ dowiesz się jak możesz wykorzystać techniki steganografii w różnych scenariuszach.

Warsztaty live z podstaw testowania web aplikacji		

1.	Konfiguracja oraz zapoznanie ze środowiskiem pracy	• Poznasz podstawowe narzędzia pozwalające na tworzenia środowiska pracy, dowiesz się warunki muszą zostać spełnione aby móc badać bezpieczeństwo aplikacji.
		• Nauczysz się:
		  ○ konfigurować i tworzyć własne bezpieczne środowisko pracy
		  ○ dowiesz się na co zwracać uwagę i jak wybierać obiekty swoich badań

2.	Przedstawienie podstawowych narzędzi pracy	• Poznasz narzędzia wspomagające testowanie bezpieczeństwa aplikacji.
		• Nauczysz się:
		  ○ konfigurować przeglądarkę internetową do pracy z zewnętrznymi narzędziami,
		  ○ korzystać a BurpSuite,
		  ○ Poznasz przydatne wtyczki do przeglądarek

3.	Zapoznanie z aplikacją – czyli rekonesans	• Poznasz zasady przeprowadzania rekonesansu aplikacji. • Nauczysz się: ○ metodycznego zapoznawania się z aplikacjami i wybierania miejsca które jest potencjalnie warte przetestowania.

4.	Zarządzenie sesją użytkownika	• Poznasz zasady bezpiecznego zarządzania sesją użytkownika oraz popularne błędy występujące w tym mechanizmie. Również poruszone będę elementy związane z mechanizmami logowania, tworzenia kont jak i resetowania hasła.
		• Dowiesz się:
		  ○ Czym są ciasteczka,
		  ○ Co to jest JWT,
		  ○ Jakie błędy może popełnić programista lub projektant aplikacji i jak je wykorzystać.

5.	XSS	• Poznasz czym jest podatność Cross-site scripting i jak ją możesz wykorzystać.
		• Nauczysz się:
		  ○ wyszukiwać miejsca podatne na atak XSS,
		  ○ wykradać ciasteczka sesyjne,
		  ○ Rozpoznawać rodzaje podatności XSS: Persistent, Reflected, DOM Based.

6.	SQL injection	• Poznasz podstawy języka SQL, poznasz podstawowe rodzaje podatności związanych z wykorzystaniem języka SQL w web aplikacjach.
		• Nauczysz się:
		  ○ wykorzystywać podatność SQL podczas testowania bezpieczeństwa web aplikacji,
		  ○ korzystać z narzędzi automatyzujących ataki

7.	XML	• Poznasz zasady budowania dokumentów XML oraz podatności związane z przetwarzaniem i obsługą tych dokumentów w web aplikacjach. • Nauczysz się: ○ wykorzystywać dokumenty XML do przeprowadzania podstawowych ataków: XML External Entity, Remote Code Execution.
8.	OWASP Top Ten	• Poznasz czym jest organizacja OWASP, czym jest dokument OWASP Top Ten, do kogo jest kierowany i przez kogo tworzony. Zostaną też omówione klasy podatności wymienione w ostatnio opublikowanej wersji.