Tytuł projektu: Clickjacking w aplikacjach webowych: demonstracja ataku i mechanizmów obrony (X-Frame-Options, CSP frame-ancestors)

Skład zespołu:

- Mateusz Aleksander [**maleksander@student.agh.edu.pl**]

- Kinga Surma [**ksurma@student.agh.edu.pl**]

Numer grupy i nazwa kierunku

- Numer grupy laboratoryjnej: **2**

- Kierunek: **Teleinformatyka**

Cel projektu (dlaczego temat jest ważny)

Pokażemy, w jaki sposób atak **clickjacking** pozwala nakłonić użytkownika do wykonania niechcianej akcji na stronie ofiary osadzonej w ukrytej ramce (iframe). Zademonstrujemy realne ryzyko dla aplikacji webowych (np. zmiana ustawień konta) oraz proste i skuteczne mechanizmy obrony konfigurowane po stronie serwera: nagłówki X-Frame-Options oraz Content-Security-Policy z dyrektywą frame-ancestors. Uzasadnieniem wyboru jest powszechność błędu (brak nagłówków) oraz duża wartość edukacyjna - uczestnicy od razu widzą efekt „przed/po".

Przedmiot demonstracji (co dokładnie pokażemy)

Zbudujemy kontrolowane środowisko z dwiema prostymi stronami: „ofiara" (form. zmiany e-maila) i „atakujący" (przynęta z ukrytą ramką). Pokażemy, że klik użytkownika w widoczny element trafia w przycisk ofiary w iframe. Następnie włączymy ochronę: X-Frame-Options (DENY/SAMEORIGIN) oraz CSP frame-ancestors ('none'/'self'/lista dozwolonych originów). Dodatkowo przedstawimy wariant ochrony selektywnej tylko dla ścieżek wrażliwych (/sensitive/*) i omówimy różnice XFO vs CSP.

Zakres demonstracji (jak będzie przeprowadzona)

1) **Krótkie wprowadzenie:** wytłumaczzenie znaczenia ataku i sposobów przeciwdziałania (mechanizm iframes, realne incydenty).

2) **Część praktyczna prezentacji:** uruchomienie dwóch lokalnych serwerów (Python), wykonanie ataku clickjacking, a następnie stopniowe twardnienie nagłówkami (XFO, CSP) i obserwacja efektu w devtools.

3) **Wariant selektywny:** nagłówki tylko dla /sensitive.

4) **Cześć praktyczna dla grupy:** zadania związane z wprowadzaniem albo weryfikowaniem zabezpieczeń przed atakiem i krótki quiz (5 pytań). Całość mieści się w 1,5 h (~60 min praktyki).