SKRYPT ODCINKA NR 1

ABSTRAKT:

W pierwszym odcinku poznamy hakera o imieniu Buggy i nawiążemy z nim dialog, w trakcie którego usłyszymy historię jednego z przeprowadzonych przez niego ataków. Buggy wykorzystuje w nim błędną implementację mechanizmu kontroli dostępu w aplikacji webowej by dostać się do funkcjonalności administratora pozwalającej na wgrywanie licencji. Wgrywane licencje są przesyłane w formacie XML. Nieprawidłowa konfiguracja parsera okazuję się być podatna na atak XXE, który przy braku zabezpieczenia połączeń wychodzących, pozwala mu finalnie na pobranie wewnętrznych plików organizacji.

Odcinek jest oparty o kill-chain składający się z następujących podatności:

1. Nieprawidłowa kontrola dostępu
2. XML External Entity
3. Nieprawidłowa konfiguracja połączeń wychodzących.

Zagadnienia poruszane w odcinku

- Błędy kontroli dostępu
  - Na czym polegają i jak wyglądają błędy kontroli dostępu?
  - Czym jest uwierzytelnienie, a czym autoryzacja?
  - Jakie ryzyka niosą za sobą błędy kontroli dostępu?
  - Różnice między błędami kontroli dostępu do funkcji i do zasobów.
  - Przykłady najczęstszych błędów kontroli dostępu.
  - Przykłady najczęstszych błędnych implementacji poprawek.
  - Co jest ważne przy poprawnej kontroli dostępu?
- Podatności XML

    - Na czym polega i jak wygląda atak XML External Entity (XXE)?
    - Na czym polega i jak wygląda atak XML Bomb?
    - Jakie ryzyka niosą za sobą ataki XXE oraz XML Bomb?
    - W jaki sposób atakujący wykorzystują niepoprawne implementacje parserów XML?
    - Domyślne konfiguracje parserów nie zawsze są poprawnie skonfigurowane?
    - Co powinna zawierać bezpieczna konfiguracja parsera XML?
- Połączenia wychodzące
    - Skutki braku kontroli połączeń wychodzących.
    - Poprawna konfiguracja połączeń wychodzących.
- Wstęp do modelowania zagrożeń
    - Czym jest modelowanie zagrożeń i jakie niesie korzyści?
    - Przykład krótkiego modelowania zagrożeń.
    - Zestaw przykładowych pytań, nad którymi warto się zastanowić w trakcie modelowania zagrożeń.

Odcinek zawiera ćwiczenia, które pomogą zrozumieć poruszane zagadnienia oraz pozwolą na trwalsze przyswojenie materiału:

ĆWICZENIE 1: Błędy kontroli dostępu do funkcji oraz zasobów

Ćwiczenie, w którym uczestnik na podstawie np. opisu sytuacji, przykładowych żądań, odpowiedzi HTTP, które napotkaliśmy w trakcie testów będzie musiał zdecydować czy dany przykład dotyczy błędu kontroli dostępu do funkcji czy do zasobu.

Rezultat ćwiczenia:

- Zobaczenie realnego przykładu błędu kontroli dostępu.
- Zrozumienie w jaki sposób błędy kontroli dostępu są wykorzystywane i na czym polegają.
- Odróżnianie błędów kontroli dostępu do funkcji oraz do zasobów.

ĆWICZENIE 2:Przegląd przykładowych payloadów wykorzystujących nieprawidłową konfigurację parsera XML stosowanych przez atakującego

Ćwiczenie, w którym uczestnik będzie musiał wybrać jeden z gotowych payloadów pozwalający na wykonanie konkretnej akcji np. pobrania pliku, wywołania niedostępności.

Rezultat ćwiczenia:

- Utrwalenie w świadomości skutków nieprawidłowej konfiguracji parsera XML.
- Zobaczenie realnego przykładu XXE, XML BOMB.
- Zrozumienie w jaki sposób może zostać wykorzystana nieprawidłowa konfiguracja parsera XML.

ĆWICZENIE 3: Rozpoznawanie nieprawidłowych konfiguracji parserów XML

Ćwiczenie, w którym uczestnik widząc przykładową konfigurację parsera XML, będzie musiał zdecydować, czy jest ona podatna czy bezpieczna.

Rezultat ćwiczenia:

- Uświadomienie, że nie każda dostępna konfiguracja jest bezpieczna przy domyślnych ustawieniach.
- Zrozumienie kluczowych elementów wpływających na bezpieczeństwo parsera XML.
- Umiejętność rozpoznawania niebezpiecznych konfiguracji parsera XML.

ĆWICZENIE 4: Próba samodzielnego modelowania zagrożeń

Ćwiczenie, w którym uczestnik zaznajomi się z podstawami modelowania zagrożeń i zobaczy w jaki sposób może wyglądać krótkie modelowanie zagrożeń. Następnie będzie miał możliwość przeprowadzić je samodzielnie korzystając przy tym z przygotowanych przykładowych pytań.

Rezultat ćwiczenia:

- Zrozumienie podstaw, celu oraz tego w jaki sposób wygląda modelowanie zagrożeń.
- Zaznajomienie z podstawowymi terminami.

- Zachęcenie do zastanowienia nad projektowanymi komponentami wewnątrz firmy

Na końcu odcinka znajdzie się Quiz pozwalający na powtórkę najważniejszych zagadnień poruszanych w module pierwszym.

PODSUMOWANIE

Po obejrzeniu odcinka uczestnik:

- Rozumie i potrafi zidentyfikować zagrożenia związane z błędami kontroli dostępu.
- Rozumie i potrafi zidentyfikować zagrożenia związane z nieprawidłową konfiguracją XML.
- Rozumie podstawy modelowania zagrożeń.
- Zna kluczowe zasady bezpieczeństwa dotyczące kontroli dostępu, parserów XML oraz połączeń wychodzących.