

Skanowanie aplikacji webowych

http



Skanowanie aplikacji webowych

Gartner podaje, że 75% ataków następuje w warstwie aplikacji. Oznacza to, że aplikacje webowe są najbardziej podatną na ataki warstwą środowiska IT. Skanuj swoje aplikacje webowe i API pod kątem stale rosnącej liczby podatności. Wykrywamy podatności 10 najważniejszych typów OWASP, w tym niewłaściwe konfiguracje, słabe hasła oraz niezabezpieczone dane systemowe i osobowe we wszystkich typach aplikacji.

KLUCZOWE CECHY

Znajdź słabe punkty, które odpowiadają za podatność

Stale, zautomatyzowane skanowanie aplikacji webowych umożliwia wykrycie podatności związanych z niewłaściwymi konfiguracjami systemowymi, słabymi hasłami oraz niezabezpieczonymi danymi systemowymi i osobowymi.



Automatyczne i ciągłe

W ciągu miesiąca pojawiają się tysiące nowych podatności. Zaplanowane i ciągłe skanowanie pozwala szybko wykryć nowe luki.



Systematyczne i proaktywne

Nasza platforma stanowi doskonałą podstawę do systematycznego zarządzania cyberbezpieczeństwem.



Pełne pokrycie

Obsługujemy każdy rodzaj aplikacji webowych, zarówno publicznych jak i lokalnych. Intranet, strony komercyjne, portale i inne.



Oparte na ryzyku

Nie zgub się wśród dużej ilości danych. Nasza platforma pomoże Ci określić, jakie luki w zabezpieczeniach należy naprawić w pierwszej kolejności, dzięki wielu zautomatyzowanym i prostym narzędziom.

ZGODNOŚĆ Z PRZEPISAMI

Przygotuj się na przyszłe wymogi

Wraz z rosnącą liczbą zagrożeń pojawiają się nowe wymogi prawne, normy i certyfikaty. Pomagamy spełniać istniejące i przyszłe wymogi.



OWASP TOP 10



RODO



PDPA



NIS

SKUTECZNY SKANER

OWASP TOP 10

Nasz skaner aplikacji internetowych wykrywa podatności w Twoich aplikacjach internetowych w szerokim zakresie.

- ✓ 10 najważniejszych podatności OWASP.
- ✓ Podatności w REST API.
- ✓ Duża liczba popularnych podatności w aplikacjach webowych.
- ✓ Kilka tysięcy podatności w konkretnych CMS, takich jak WordPress.

SZCZEGÓŁY TECHNICZNE

Cechy i funkcje

Nasz produkt do skanowania aplikacji webowych zawiera szereg skutecznych funkcji, które pomogą Ci odnieść sukces.

- ✓ Skanowanie aplikacji webowych wymagających uwierzytelnienia.
- ✓ Skanowanie lokalnej infrastruktury chmurowej, AWS.
- ✓ Wykrywanie przestarzałych i podatnych na ataki komponentów JavaScript.
- ✓ Wykrywanie nieprawidłowej konfiguracji i uprawnień dostępu aplikacji webowych.
- ✓ Wykrywanie niezabezpieczonych danych osobowych, numerów kart kredytowych i haseł.
- ✓ Wykrywanie niezabezpieczonych danych o systemie.
- ✓ Ostrzeżenie, że certyfikaty SSL wygasły, wkrótce wygasną lub są podatne na ataki.
- ✓ Fuzz testing – wykrywanie nieracjonalnych lub nieoczekiwanych działań aplikacji internetowej.
- ✓ Automatyczna identyfikacja serwerów internetowych, języków programowania i baz danych.
- ✓ Automatyczna aktualizacja bazy danych podatności.
- ✓ Wysoka wykrywalność.
- ✓ Stałe monitorowanie.
- ✓ SAML 2.0 Single Sign-On.
- ✓ Kontrola dostępu oparta na rolach (RBAC).
- ✓ Pełne wsparcie IPv6.

SPOSÓB WDROŻENIA

Dostępność w chmurze i lokalnie

Nasza platforma może być bezpiecznie użytkowana na dwa sposoby. Jako usługa chmurowa, dzięki kilku globalnym centrom danych lub zainstalowana lokalnie, w ramach własnej infrastruktury i magazynu danych. Po prostu wybierz opcję, która najbardziej pasuje do Twojej organizacji.



Chmura

Bezpieczne zarządzanie i przechowywanie w chmurze. Wybierz fizyczne centrum danych, które Ci odpowiada. Rozpocznij pracę w ciągu kilku minut.



Lokalnie

Instalacja w ramach własnej infrastruktury, wykorzystanie lokalnego magazynu danych. Automatyczne aktualizacje oprogramowania i testów podatności.

O FIRMIE HOLM SECURITY

Unikalne trójwarstwowe zarządzanie podatnościami

Holm Security umożliwia wykrywanie podatności, ocenę ryzyka i ustalenie priorytetów wśród działań naprawczych dla każdego zasobu w Twojej infrastrukturze. Oferujemy platformę typu „wszystko w jednym”, obejmującą trzy warstwy, ze wszystkimi niezbędnymi narzędziami – niezależnie od tego, czy jest to kolejne rozwiązanie do zarządzania podatnościami, czy wdrażasz je po raz pierwszy.

