Sprint

Łączymy Technologie

AUDYTY I TESTY BEZPIECZEŃSTWA

TESTY APLIKACJI WEBOWYCH

Aplikacje webowe są szczególnie narażone na różne formy ataków hakerskich. Celem testów penetracyjnych jest praktyczna ocena bieżącego stanu bezpieczeństwa systemu w szczególności wykrycie wszystkich podatności i odporności na próby przełamania zabezpieczeń.

Wykonujemy testy penetracyjne aplikacji webowych oraz stron internetowych z wykorzystaniem najnowszych technologii.

Dysponujemy narzędziami i umiejętnościami, które pozwalają na kompleksowy audyt bezpieczeństwa Twojej firmy. Oferujemy zarówno testy infrastruktury sieciowej, aplikacji webowych, stron internetowych, social engineering, OSINT, jak i usługi specjalne tj. 0day.

cybersecurity@sprint.pl

RODZAJE TESTÓW

Stress Testy – z wykorzystaniem technik DoS, DDoS, mają za zadanie sprawdzenie przepustowości sieci oraz stopień odporności serwerów i innych urządzeń skojarzonych z daną aplikacją czy stroną internetową.

Testy bazy danych – z wykorzystaniem technik SQL Injection oraz błędów wersji. Zidentyfikowanie rodzaju i wersji bazy danych często wskazuje na niezaktualizowane bazy danych, dla których sam producent przedstawia szereg miejsc newralgicznych związanych z lukami bezpieczeństwa. Ponadto wykorzystując strukturalny język zapytań do baz danych, przeprowadzany jest szereg testów, których zadaniem jest dostęp do nieautoryzowanych danych lub manipulacja bazą danych przez tworzenie nowych rekordów, lub usuwanie istniejących itd.

Testy mobilne – skupiają się wokół aplikacji mobilnych zarówno pod względem testowanego oprogramowania, jak i technik smishingowych/vishingowych.

Testy aplikacji – testy webowe sprawdzają nie tylko bezpieczeństwo, ale również funkcjonalność oraz optymalność danych witryn czy aplikacji. W skład takich testów wchodzi:

1. Kompletne sprawdzenie linkowania (zewnętrznego i wewnętrznego) oraz MailTo.
2. Testy formularzy – związane często z testami baz danych, ale również podatności na takie ataki jak: przechwytywanie sesji, plików cookies, Clickjacking, XSS, HTML Injection, CSS injection itp.
3. Testy kompatybilności przeglądarki – wykorzystujące różne możliwości działania przeglądarek, dodatków – wskazujemy ewentualne nieprawidłowości w działaniu danej aplikacji lub strony na podstawie konkretnych ustawień przeglądarki.
4. Testy certyfikatów, szczególnie prawidłowego skonfigurowania SSL.
5. Testy transakcji – weryfikują proces rezerwacji lub płatności krok po kroku w celu wykrycia nieprawidłowości w czasie transakcji.
6. Host Header Attack – testy na różnym etapie działania aplikacji lub strony mające za zadanie przesłania specjalnie spreparowanego nagłówka w celu zmuszenia serwera do niepożądanego działania.
7. Atak wektorowy – specjalny rodzaj ataku półautomatycznego wykorzystującego wiele podatności związanych z działaniem konkretnej aplikacji/strony.

TESTY INFRASTRUKTURY

Testy zewnętrzne – czyli takie, w których próbujemy uzyskać nieautoryzowany dostęp do danych Twojej firmy, korzystając z sieci zewnętrznej poprzez próby ataku na sieci bezprzewodowe oraz przez Internet. A może jesteś właścicielem sieci kiosków informacyjnych w galerii handlowej lub maszyn do ticketowania? Tak, takie również testujemy.

Testy wewnętrzne – takie, w których podłączeni do sieci wewnętrznej zbieramy informacje dotyczące działających w niej urządzeń – ich słabych punktów czy błędów w konfiguracji.

Testy penetracyjne są automatyczne, półautomatyczne i manualne w zależności od celów testowych.

SOCIAL ENGINEERING

Szczególny rodzaj testowania, który opiera się na testach miękkich związanych ze słabością zasobów ludzkich.

Scenariusze tych testów są niejawne i rozłożone w czasie w zależności od stopnia zintensyfikowania tychże testów. Chcesz sprawdzić, czy Twoi pracownicy poprzez nieuwagę lub brak znajomości przepisów mogą przekazać dostęp do danych, lub urządzeń Twojej firmy? Te testy są właśnie dla Ciebie.

0 DAY

Usługa polegająca na wykryciu podatności przed publikacją aktualizacji przez producenta.

Poprzez zastosowanie najnowszych technologii i pracy wielu specjalistów możemy zaproponować Państwu usługę najbardziej pożądaną przez właścicieli dużych firm i ogromnych korporacji. To nie tylko audyt bezpieczeństwa, to przede wszystkim wysiłek włożony w analizę kodu aplikacji webowych, stron internetowych czy sposobów działania urządzeń sieciowych w celu znalezienia luki w bezpieczeństwie, jeszcze nieuwzględnionej przez producenta.

Proces ten zajmuje w zależności od zamówienia od 2 do 4 tygodni. Zamawiający jest zobowiązany zorganizować dostęp do zwirtualizowanej przestrzeni testowej.

ZAUFAJ NAM, PODNIEŚ POZIOM BEZPIECZEŃSTWA TWOJEJ ORGANIZACJI

- doświadczeni i wykwalifikowani pentesterzy
- certyfikaty GLP/GCP i FDA
- dobór odpowiednich technologii i narzędzi
- sprawdzone procedury testowania
- certyfikaty ISO 27001, AQAP 2210, AQAP 2110

OLSZTYN

ul. Jagiellończyka 26
10-062 Olsztyn

tel.: +48 89 522 11 00
fax: +48 89 522 11 25

olsztyn@sprint.pl

GDAŃSK

ul. Budowlanych 64E
80-298 Gdańsk

tel.: +48 58 340 77 00
fax: +48 58 340 77 01

gdansk@sprint.pl

WARSZAWA

ul. Inflancka 4
00-189 Warszawa

tel.: +48 22 826 62 77
fax: +48 22 827 61 21

warszawa@sprint.pl

BYDGOSZCZ

ul. Przemysłowa 15
85-758 Bydgoszcz

tel.: +48 52 365 01 01
fax: +48 52 365 01 11

bydgoszcz@sprint.pl

KAŻDY DZIEŃ
PRZYNOSI NOWE WYZWANIA

WYBIERZ PARTNERA,
KTÓRY POMOŻE CI
IM SPROSTAĆ

Chcesz wiedzieć więcej?
Chętnie odpowiemy na wszystkie pytania.

cybersecurity@sprint.pl

www.sprint.pl

www.linkedin.com/company/sprintsa

www.twitter.com/sprint_sa

www.facebook.pl/sprintsa