

WebService
Grupa SOLIDEX®



audyty
bezpieczeństwa
systemów IT

audyty
bezpieczeństwa

more than software...

O Webservice

Jesteśmy integratorem systemów informatycznych. Od 2003 roku należymy do Grupy SOLIDEX - wiodącego integratora systemów sieciowych. Tworzymy i wdrażamy kompleksowe rozwiązania informatyczne. Nasi specjaliści łączą doświadczenie biznesowe, głęboką wiedzę informatyczną oraz unikalne umiejętności projektowania architektury informacyjnej oraz użytecznych interfejsów graficznych.

more than software...

Unikalną cechą naszej metodologii jest przeprowadzanie testów penetracyjnych metodą półautomatyczną. W przeciwieństwie do znacznej części naszej konkurencji nie poprzestajemy na uruchomieniu automatycznych skanerów bezpieczeństwa i wygenerowaniu z nich raportów. Wykonując testy, nasz audytor działa jako potencjalny hacker – planuje i wykonuje drogę ataku, wspierając się ściśle kontrolowanymi przez siebie narzędziami wspomagającymi.

Bezpieczeństwo zasobów sieciowych

W ostatnich latach obserwuje się lawinowy wzrost ilości błędów bezpieczeństwa wykrywanych w aplikacjach webowych. W obecnej chwili wiele niezależnych źródeł podaje, iż średnio 8 na 10 portali webowych posiada poważne luki bezpieczeństwa. Słaby stan bezpieczeństwa tego typu aplikacji potwierdzają również nasze wewnętrzne badania, którym poddajemy największe portale w Polsce oraz znane portale z branży finansowej. Stan bezpieczeństwa znacznej części tych systemów można określić jako niezadowolający.

Dodatkowym czynnikiem zwiększającym ryzyko pomyślnego ataku hackerskiego jest fakt, iż ataki na aplikacje webowe należą do grupy ataków wykonywanych najczęściej. Wyniki badań przeprowadzonych przez Gartner Group mówią, iż ponad 70% wszystkich ataków hackerskich odbywa się właśnie w warstwie aplikacyjnej.

Błędy bezpieczeństwa w aplikacjach webowych pozwalają atakującemu uzyskać takie korzyści jak:

- * nieograniczony dostęp do bazy danych w trybie do zapisu i odczytu (umożliwia to np. umieszczenie kompromitujących informacji w portalu czy odczytanie poufnych danych)
- * nieograniczony dostęp do administracji aplikacji
- * dostęp do shell-a w systemie operacyjnym i eskalacja ataku w głąb infrastruktury
- * przejęcie dostępu do kont użytkowników bez znajomości haseł
- * wykorzystanie serwera jako zombie host do ataków na inne serwery w Internecie
- * wykorzystywanie skompromitowanych systemów do wyludzenia istotnych informacji (np. numerów kart kredytowych)

W wyniku tego typu ataków cierpi poważnie cenna reputacja firmy, a jak można się domyślić, niekiedy atak przenosi się na bezpośrednie, wymierne straty atakowanego podmiotu.

Jako środek zaradczy oferujemy wykonanie audytu bezpieczeństwa aplikacji. W zależności od krytyczności danego rozwiązania audyt może przyjąć postać od wariantu podstawowego aż do wariantu pełnego (z badaniem infrastruktury oraz kodu źródłowego). Zakres audytu jest ustalany z Klientem każdorazowo – w zależności od charakteru audytowanej aplikacji, oraz konkretnych wymagań ze strony Zamawiającego.

„[...] ataki na aplikacje webowe należą do grupy ataków wykonywanych najczęściej.”

„Korzystamy z metodologii: OWASP, CIS, WASC, Rekomendacje GINB D.”

W wyniku audytu dostarczamy raport zawierający opis przeprowadzonych testów, dokładne wskazanie znalezionych podatności wraz z określeniem typu oraz stopnia krytyczności, oraz rekomendacje naprawy.

Nasza metodologia

Unikalną cechą naszej metodologii jest przeprowadzanie testów penetracyjnych metodą półautomatyczną. W przeciwieństwie do znacznej części naszej konkurencji nie poprzestajemy na uruchomieniu automatycznych skanerów bezpieczeństwa i wygenerowaniu z nich raportów.

Wykonując testy, nasz audytor działa jako potencjalny hacker – planuje i wykonuje drogę ataku, wspierając się ściśle kontrolowanymi przez siebie narzędziami wspomagającymi. Dodatkowo łącząc kompetencje programistyczne z kompetencjami bezpieczeństwa, jest w stanie przewidzieć słabe punkty aplikacji na podstawie nawet wstępnego badania.

Taka metoda daje znakomite efekty o czym świadczy wykrycie przez nas wysoce krytycznych luk bezpieczeństwa (np. SQL injections) w wielu serwisach bankowych, serwisach finansowych, czy popularnych polskich portalach.

Wyróżniającą nas cechą jest również fakt, iż jako audytorów zatrudniamy jedynie osoby pracujące u nas na pełen etat oraz w wysokim stopniu dbamy o poufność dotyczącą szczegółów wykonywanych prac. Każda zatrudniona u nas osoba podpisuje stosowne oświadczenie o poufności, a w przypadku wykonywania audytu praktykujemy dodatkowo podpisanie dokumentu NDA na piśmie – czyżnie firma-firma.

Dzięki standardom bezpieczeństwa obowiązującym w Grupie SOLIDEX, świadczymy usługi związane z dostępem do danych osobowych (GIODO) czy też objętych tajemnicą bankową. Realizując nasze prace często nawiązujemy bezpośrednie połączenie do sieci bankowych.

Oferta Webservice:

Nasza oferta obejmuje audyty bezpieczeństwa w zakresie :

- * Oprogramowania webowego (praktycznie wszystkie znaczące technologie: ASP.NET/Java/PHP/ASP/Python). Audyty wykonujemy metodą blackbox i/lub whitebox (analiza kodu źródłowego).
- * Systemów operacyjnych (Windows Server 2003, Linux, FreeBSD, OpenBSD, Solaris 10, AIX, HP-UX).
- * Baz danych (Microsoft SQL Server , Oracle, MySQL, PostgreSQL).
- * Usług systemu operacyjnego (serwery webowe, serwery aplikacyjne, serwery pocztowe, serwery ftp, itd.).
- * Testów wydajnościowych oprogramowania webowego (stress testy, symulacja korzystania z aplikacji przez określoną liczbę użytkowników).
- * Testów przywracania z backupu oraz poprawności działania mechanizmów typu failover.
- * Infrastruktury sieciowej (routery, firewalle, IDS-y).

Wykonując audyty bezpieczeństwa opieramy się o uznane w świecie bezpieczeństwa rekomendacje i metodologie (np. OWASP, CIS, WASC, Rekomendacje GINB D).

W przypadku zainteresowania naszą ofertą prosimy o kontakt e-mailowy: security@webservice.pl

more than software...

WebService
Grupa SOLIDEX®

www.webservice.eu

WebService Sp. z o.o.; ul. Lea 124, 30-133 Kraków; tel. +48 (12) 637 34 32, fax +48 (12) 637 26 96