(Nie)bezpieczeństwo aplikacji internetowych

Nie ma wątpliwości, że bezpieczeństwo aplikacji internetowych jest tematem aktualnym i wartym opublikowania. Dla wszystkich zainteresowanych stawka jest wysoka: dla firm, które czerpią coraz większe dochody z handlu internetowego, dla użytkowników, którzy ufają aplikacjom internetowym zawierającym poufne informacje, oraz dla przestępców, którzy mogą zarobić duże pieniądze na kradzieży danych płatniczych lub przejmowaniu kont bankowych. Reputacja odgrywa kluczową rolę. Niewiele osób chce prowadzić interesy z niezabezpieczoną witryną, więc niewiele organizacji chce ujawniać szczegóły dotyczące własnych luk w zabezpieczeniach lub naruszeń. W związku z tym uzyskanie wiarygodnych informacji o stanie bezpieczeństwa aplikacji internetowych nie jest dziś łatwym zadaniem. Pokrótce przyjrzymy się, jak ewoluowały aplikacje internetowe i jakie korzyści zapewniają. Przedstawiamy kilka wskaźników dotyczących podatności w obecnych aplikacjach internetowych, zaczerpniętych z bezpośrednich doświadczeń autorów, pokazujących, że większość aplikacji nie jest bezpieczna. Opisujemy główny problem bezpieczeństwa, z jakim borykają się aplikacje internetowe - użytkownicy mogą je dowolnie dostarczać dane wejściowe - oraz różne czynniki, które przyczyniają się do ich słabej pozycji w zakresie bezpieczeństwa. Na koniec opisujemy najnowsze trendy w bezpieczeństwie aplikacji internetowych i ich rozwój w najbliższej przyszłości.

Ewolucja aplikacji internetowych

W początkach Internetu sieć WWW składała się wyłącznie z witryn internetowych. Były to zasadniczo repozytoria informacji zawierające dokumenty statyczne. Przeglądarki internetowe zostały wynalezione jako sposób pobierania i wyświetlania tych dokumentów. Przepływ interesujących informacji był jednokierunkowy, od serwera do przeglądarki. Większość witryn nie uwierzytelniała użytkowników, ponieważ nie było takiej potrzeby. Każdy użytkownik był traktowany w ten sam sposób i otrzymał te same informacje. Wszelkie zagrożenia bezpieczeństwa wynikające z hostingu strony internetowej były związane w dużej mierze z lukami w oprogramowaniu serwera WWW (których było wiele). Jeśli atakujący włamał się na serwer sieciowy, zwykle nie uzyskałby dostępu do żadnych poufnych informacji, ponieważ informacje przechowywane na serwerze były już publicznie dostępne. Przeciwnie, atakujący zazwyczaj modyfikuje pliki na serwerze, aby zamazać zawartość witryny lub wykorzystać pamięć masową i przepustowość serwera do dystrybucji „warez". Dziś World Wide Web jest prawie nie do poznania ze swojej wcześniejszej formy. Większość witryn internetowych to w rzeczywistości aplikacje. Są wysoce funkcjonalne i opierają się na dwukierunkowym przepływie informacji między serwerem a przeglądarką. Wspierają rejestrację i logowanie, transakcje finansowe, wyszukiwanie i tworzenie treści przez użytkowników. Treść prezentowana użytkownikom jest generowana dynamicznie w locie i często jest dostosowana do każdego konkretnego użytkownika. Wiele przetwarzanych informacji jest prywatnych i bardzo wrażliwych. Dlatego bezpieczeństwo jest dużym problemem. Nikt nie chce korzystać z aplikacji internetowej, jeśli wierzy, że jego informacje zostaną ujawnione nieuprawnionym podmiotom. Aplikacje internetowe niosą ze sobą nowe i znaczące zagrożenia bezpieczeństwa. Każda aplikacja jest inna i może zawierać unikalne luki w zabezpieczeniach. Większość aplikacji jest opracowywana wewnętrznie - wiele z nich przez programistów, którzy mają tylko częściową wiedzę na temat problemów związanych z bezpieczeństwem, które mogą pojawić się w tworzonym przez nich kodzie. Aby zapewnić swoją podstawową funkcjonalność, aplikacje internetowe zwykle wymagają połączenia z wewnętrznymi systemami komputerowymi, które zawierają bardzo wrażliwe dane i mogą wykonywać zaawansowane funkcje biznesowe. Piętnaście lat temu, jeśli chciałeś dokonać przelewu, odwiedziłeś swój bank, a kasjer wykonał przelew za Ciebie; dziś możesz odwiedzić aplikację internetową i samodzielnie wykonać transfer. Osoba atakująca, która włamuje się do aplikacji sieci Web, może być w stanie ukraść dane osobowe, dokonać oszustwa finansowego i wykonać złośliwe działania przeciwko innym użytkownikom.

Wspólne funkcje aplikacji internetowych

Aplikacje internetowe zostały stworzone po to, aby wykonywać praktycznie każdą użyteczną funkcję, którą można zaimplementować online. Oto kilka funkcji aplikacji internetowych, które zyskały na znaczeniu w ostatnich latach:

* Zakupy (Amazon)

* Serwisy społecznościowe (Facebook)

* Bankowość (Citibank)

* Wyszukiwarka internetowa (Google)

* Aukcje (eBay)

* Hazard (Betfair)

* Dzienniki internetowe (Blogger)

* Poczta internetowa (Gmail)

* Informacje interaktywne (Wikipedia)

Aplikacje dostępne za pomocą przeglądarki komputerowej coraz częściej pokrywają się z aplikacjami mobilnymi, do których dostęp uzyskuje się za pomocą smartfona lub tabletu. Większość aplikacji mobilnych korzysta z przeglądarki lub dostosowanego klienta, który wykorzystuje do komunikacji z serwerem interfejsy API oparte na protokole HTTP. Funkcje i dane aplikacji są zazwyczaj współużytkowane przez różne interfejsy, które aplikacja udostępnia na różnych platformach użytkowników. Oprócz publicznego Internetu, w organizacjach szeroko zaadoptowano aplikacje webowe wspierające kluczowe funkcje biznesowe. Wiele z nich zapewnia dostęp do bardzo wrażliwych danych i funkcji:

* Aplikacje HR umożliwiające użytkownikom dostęp do informacji płacowych, przekazywanie i otrzymywanie informacji zwrotnych o wydajności oraz zarządzanie procedurami rekrutacyjnymi i dyscyplinarnymi.

* Interfejsy administracyjne do kluczowej infrastruktury, takiej jak serwery WWW i pocztowe, stacje robocze użytkowników i administracja maszynami wirtualnymi.

* Oprogramowanie do współpracy służące do udostępniania dokumentów, zarządzania przepływem pracy i projektami oraz śledzenia problemów. Tego typu funkcje często wiążą się z krytycznymi kwestiami bezpieczeństwa i nadzoru, a organizacje często całkowicie polegają na kontrolkach wbudowanych w ich aplikacje internetowe.

* Aplikacje biznesowe, takie jak oprogramowanie do planowania zasobów przedsiębiorstwa (ERP), które wcześniej były dostępne za pomocą zastrzeżonej aplikacji typu „gruby klient”, są teraz dostępne za pomocą przeglądarki internetowej.

* Usługi programowe, takie jak poczta e-mail, które pierwotnie wymagały oddzielnego klienta poczty e-mail, są teraz dostępne za pośrednictwem interfejsów internetowych, takich jak Outlook Web Access.

* Tradycyjne aplikacje biurowe, takie jak edytory tekstu i arkusze kalkulacyjne, zostały przeniesione do aplikacji internetowych za pośrednictwem usług, takich jak Google Apps i Microsoft Office Live.

We wszystkich tych przykładach, to, co jest postrzegane jako „wewnętrzne" aplikacje, jest coraz częściej hostowane zewnętrznie, ponieważ organizacje przenoszą się do zewnętrznych dostawców usług, aby obniżyć koszty. W tych tak zwanych rozwiązaniach chmurowych funkcje i dane o znaczeniu krytycznym dla firmy są udostępniane szerszemu gronu potencjalnych napastników, a organizacje w coraz większym stopniu polegają na integralności zabezpieczeń, które są poza ich kontrolą. Szybko zbliża się czas, kiedy jedynym oprogramowaniem klienckim, którego będzie potrzebowała większość użytkowników komputerów, jest przeglądarka internetowa. Różnorodny zakres funkcji zostanie zaimplementowany przy użyciu wspólnego zestawu protokołów i technologii, a tym samym odziedziczy charakterystyczny zakres typowych luk w zabezpieczeniach.

Korzyści z aplikacji internetowych

Nietrudno zrozumieć, dlaczego aplikacje internetowe cieszą się tak dramatycznym wzrostem popularności. Kilka czynników technicznych współpracowało z oczywistymi zachętami komercyjnymi, aby napędzać rewolucję, która nastąpiła w sposobie korzystania z Internetu:

* HTTP, podstawowy protokół komunikacyjny używany do uzyskiwania dostępu do sieci WWW, jest lekki i bezpołączeniowy. Zapewnia to odporność w przypadku błędów komunikacji i pozwala uniknąć konieczności utrzymywania przez serwer otwartego połączenia sieciowego dla każdego użytkownika, jak miało to miejsce w przypadku wielu starszych aplikacji klient/serwer. HTTP może być również proxy i tunelowany przez inne protokoły, co pozwala na bezpieczną komunikację w dowolnej konfiguracji sieci.

* Każdy użytkownik internetu ma już zainstalowaną przeglądarkę na swoim komputerze i urządzeniu mobilnym. Aplikacje internetowe dynamicznie wdrażają swój interfejs użytkownika w przeglądarce, unikając konieczności rozpowszechniania i zarządzania oddzielnym oprogramowaniem klienckim, jak miało to miejsce w przypadku aplikacji pre-web. Zmiany w interfejsie muszą zostać wprowadzone tylko raz na serwerze i od razu zaczynają obowiązywać.

* Dzisiejsze przeglądarki są wysoce funkcjonalne, umożliwiając tworzenie bogatych i satysfakcjonujących interfejsów użytkownika. Interfejsy internetowe wykorzystują standardowe elementy sterujące nawigacją i wprowadzaniem danych, które są od razu znane użytkownikom, co pozwala uniknąć konieczności poznawania sposobu działania poszczególnych aplikacji. Skrypty po stronie klienta umożliwiają aplikacjom przekazywanie części przetwarzania po stronie klienta, a możliwości przeglądarek można rozszerzać w dowolny sposób za pomocą technologii rozszerzeń przeglądarki, gdy jest to konieczne.

* Podstawowe technologie i języki używane do tworzenia aplikacji internetowych są stosunkowo proste. Dostępna jest szeroka gama platform i narzędzi programistycznych, które ułatwiają tworzenie zaawansowanych aplikacji przez stosunkowo początkujących, a duża ilość kodu open source i innych zasobów jest dostępna do włączenia do niestandardowych aplikacji.

Bezpieczeństwo aplikacji internetowych

Podobnie jak w przypadku każdej nowej klasy technologii, aplikacje internetowe przyniosły ze sobą nowy zakres luk w zabezpieczeniach. Zestaw najczęściej spotykanych defektów ewoluował nieco z biegiem czasu. Pojawiły się nowe ataki, które nie były brane pod uwagę podczas tworzenia istniejących aplikacji. Niektóre problemy stały się mniej rozpowszechnione, ponieważ wzrosła ich świadomość. Opracowano nowe technologie, które wprowadziły nowe możliwości eksploatacji. Niektóre kategorie usterek w dużej mierze zniknęły w wyniku zmian wprowadzonych w oprogramowaniu przeglądarki internetowej. Najpoważniejsze ataki na aplikacje internetowe to te, które ujawniają poufne dane lub

uzyskują nieograniczony dostęp do systemów zaplecza, na których działa aplikacja. Tego rodzaju głośne kompromisy nadal występują często. Jednak dla wielu organizacji każdy atak, który powoduje przestój systemu, jest zdarzeniem krytycznym. Ataki typu „odmowa usługi" na poziomie aplikacji mogą służyć do osiągnięcia takich samych wyników, jak tradycyjne ataki polegające na wyczerpywaniu zasobów na infrastrukturę. Jednak często są one używane z bardziej subtelnymi technikami i celami. Mogą być wykorzystywane do zakłócania działania konkretnego użytkownika lub usługi w celu uzyskania przewagi konkurencyjnej w stosunku do innych użytkowników w sferze handlu finansowego, gier, licytacji online i rezerwacji biletów. W trakcie tej ewolucji w wiadomościach utrzymywały się kompromisy znanych aplikacji internetowych. Nie ma poczucia, że skręcono za róg i że te problemy z bezpieczeństwem zanikają. Pod pewnymi względami bezpieczeństwo aplikacji internetowych jest obecnie najważniejszym polem bitwy między atakującymi a osobami dysponującymi zasobami komputerowymi i danymi do obrony i prawdopodobnie pozostanie nim w przewidywalnej przyszłości.

„Ta witryna jest bezpieczna"

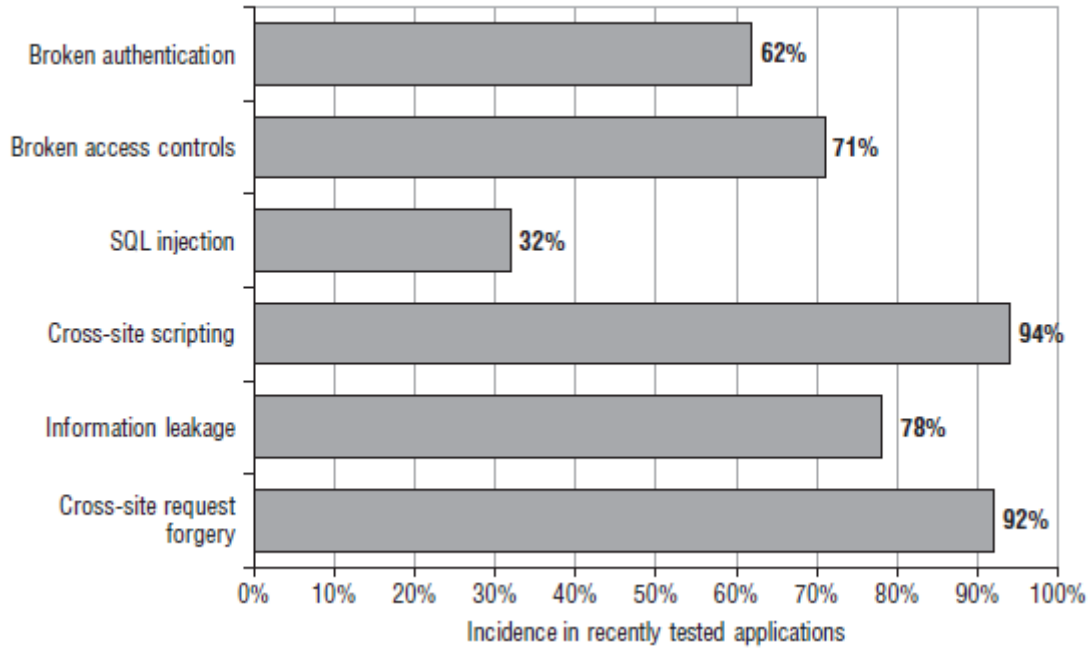
Istnieje powszechna świadomość, że bezpieczeństwo jest problemem dla aplikacji internetowych. Zapoznaj się ze stroną FAQ typowej aplikacji, a będziesz mieć pewność, że jest ona w rzeczywistości bezpieczna. Większość aplikacji twierdzi, że są bezpieczne, ponieważ używają protokołu SSL. Na przykład:

Ta strona jest całkowicie bezpieczna. Został zaprojektowany do korzystania z 128-bitowej technologii Secure Socket Layer (SSL), aby uniemożliwić nieautoryzowanym użytkownikom przeglądanie jakichkolwiek informacji. Możesz korzystać z tej strony mając pewność, że Twoje dane są u nas bezpieczne.

Użytkownicy są często nakłaniani do weryfikacji certyfikatu witryny, podziwiania stosowanych zaawansowanych protokołów kryptograficznych i na tej podstawie powierzania jej swoich danych osobowych. Coraz częściej organizacje przytaczają również zgodność ze standardami Payment Card Industry (PCI), aby zapewnić użytkowników, że są bezpieczni. Na przykład:

Bezpieczeństwo traktujemy bardzo poważnie. Nasza strona internetowa jest codziennie skanowana, aby zapewnić zgodność z PCI i ochronę przed hakerami. Możesz zobaczyć datę ostatniego skanu na poniższym logo i masz gwarancję, że korzystanie z naszej strony internetowej jest bezpieczne.

W rzeczywistości większość aplikacji internetowych nie jest bezpieczna, pomimo powszechnego stosowania technologii SSL i regularnego skanowania PCI. Rysunek pokazuje, jaki procent aplikacji testowanych w latach 2007 i 2011 został wykryty przez niektóre popularne kategorie podatności:



* Uszkodzone uwierzytelnianie (62%) - ta kategoria luk obejmuje różne defekty w mechanizmie logowania aplikacji, które mogą umożliwić osobie atakującej odgadnięcie słabych haseł, przeprowadzenie ataku typu brute-force lub ominięcie logowania.

* Uszkodzone kontrole dostępu (71%) - dotyczy to przypadków, w których aplikacja nie zapewnia odpowiedniej ochrony dostępu do swoich danych i funkcji, potencjalnie umożliwiając atakującemu przeglądanie poufnych danych innych użytkowników przechowywanych na serwerze lub wykonywanie uprzywilejowanych działań.

* Wstrzyknięcie SQL (32%) - ta luka umożliwia atakującemu przesłanie spreparowanych danych wejściowych, aby zakłócić interakcję aplikacji z bazami danych zaplecza. Atakujący może być w stanie pobrać dowolne dane z aplikacji, ingerować w jej logikę lub wykonać polecenia na samym serwerze bazy danych.

* Cross-site scripting (94%) - ta luka umożliwia atakującemu atakowanie innych użytkowników aplikacji, potencjalnie uzyskując dostęp do ich danych, wykonując w ich imieniu nieautoryzowane działania lub przeprowadzając inne ataki przeciwko nim.

* Wyciek informacji (78%) - dotyczy to przypadków, w których aplikacja ujawnia poufne informacje, które mogą być przydatne osobie atakującej podczas ataku na aplikację, poprzez wadliwą obsługę błędów lub inne zachowanie.

* Cross-site request forgery (92%) - ta usterka oznacza, że użytkownicy aplikacji mogą zostać nakłonieni do wykonania niezamierzonych działań na aplikacji w ramach ich kontekstu użytkownika i poziomu uprawnień. Luka umożliwia szkodliwej witrynie odwiedzanej przez ofiarę użytkownika interakcję z aplikacją w celu wykonania działań, których użytkownik nie zamierzał.

SSL to doskonała technologia, która chroni poufność i integralność danych przesyłanych między przeglądarką użytkownika a serwerem sieciowym. Pomaga bronić się przed podsłuchiwaniem i może zapewnić użytkownikowi tożsamość serwera WWW, z którym ma do czynienia. Nie powstrzymuje

jednak ataków, które są bezpośrednio wymierzone w składniki serwera lub klienta aplikacji, jak robi to większość udanych ataków. W szczególności nie zapobiega żadnej z wymienionych luk w zabezpieczeniach ani wielu innym, które mogą narazić aplikację na krytyczny atak. Niezależnie od tego, czy używają SSL, większość aplikacji internetowych nadal zawiera luki w zabezpieczeniach.

Główny problem bezpieczeństwa: użytkownicy mogą przesyłać dowolne dane wejściowe

Podobnie jak w przypadku większości aplikacji rozproszonych, aplikacje internetowe napotykają podstawowy problem, który muszą rozwiązać, aby były bezpieczne. Ponieważ klient jest poza kontrolą aplikacji, użytkownicy mogą przesyłać dowolne dane wejściowe do aplikacji po stronie serwera. Aplikacja musi zakładać, że wszystkie dane wejściowe są potencjalnie złośliwe. Dlatego musi podjąć kroki w celu zapewnienia, że osoby atakujące nie będą mogły użyć spreparowanych danych wejściowych do złamania zabezpieczeń aplikacji, zakłócając jej logikę i zachowanie, uzyskując w ten sposób nieautoryzowany dostęp do jej danych i funkcji. Ten podstawowy problem przejawia się na różne sposoby:

* Użytkownicy mogą ingerować w dowolne dane przesyłane między klientem a serwerem, w tym parametry żądań, pliki cookie i nagłówki HTTP. Wszelkie kontrole bezpieczeństwa zaimplementowane po stronie klienta, takie jak sprawdzanie poprawności danych wejściowych, można łatwo obejść.

* Użytkownicy mogą wysyłać żądania w dowolnej kolejności i mogą przesyłać parametry na innym etapie niż oczekuje aplikacja, więcej niż raz lub wcale. Wszelkie założenia deweloperów dotyczące sposobu interakcji użytkowników z aplikacją mogą zostać naruszone.

* Użytkownicy nie są ograniczeni do korzystania z przeglądarki internetowej w celu uzyskania dostępu do aplikacji. Liczne powszechnie dostępne narzędzia działają razem z przeglądarką lub niezależnie od niej, pomagając w atakowaniu aplikacji internetowych. Narzędzia te mogą wysyłać żądania, których zwykle nie wysyła żadna przeglądarka, i mogą szybko generować ogromną liczbę żądań w celu znalezienia i wykorzystania problemów.

Większość ataków na aplikacje internetowe polega na wysyłaniu danych wejściowych do serwera, które są tak spreparowane, aby spowodować zdarzenie, którego nie oczekiwał ani nie chciał projektant aplikacji. Oto kilka przykładów przesyłania spreparowanych danych wejściowych, aby osiągnąć ten cel:

* Zmiana ceny produktu przesyłana w ukrytym polu formularza HTML w celu dokonania oszukańczego zakupu produktu za niższą kwotę

* Modyfikowanie tokena sesji przesyłanego w pliku cookie HTTP w celu przejęcia sesji innego uwierzytelnionego użytkownika

* Usunięcie pewnych parametrów, które normalnie są przesyłane w celu wykorzystania luki logicznej w przetwarzaniu aplikacji

* Zmiana niektórych danych wejściowych, które będą przetwarzane przez wewnętrzną bazę danych w celu wstrzyknięcia złośliwego zapytania do bazy danych i uzyskania dostępu do poufnych danych

Nie trzeba dodawać, że SSL nie robi nic, aby powstrzymać atakującego przed przesłaniem spreparowanych danych wejściowych do serwera. Jeśli aplikacja korzysta z SSL, oznacza to po prostu, że inni użytkownicy w sieci nie mogą przeglądać ani modyfikować przesyłanych danych atakującego. Ponieważ atakujący kontroluje jej koniec tunelu SSL, może przez ten tunel wysłać do serwera wszystko, co chce. Jeśli którykolwiek z wcześniej wspomnianych ataków zakończy się sukcesem, aplikacja jest zdecydowanie podatna na ataki, niezależnie od tego, co może powiedzieć jej FAQ.

Kluczowe czynniki problemu

Podstawowy problem bezpieczeństwa, z którym borykają się aplikacje internetowe, pojawia się w każdej sytuacji, w której aplikacja musi akceptować i przetwarzać niezaufane dane, które mogą być złośliwe. Jednak w przypadku aplikacji internetowych kilka czynników połączyło się, aby zaostrzyć problem i wyjaśnić, dlaczego tak wiele aplikacji internetowych w dzisiejszych czasach tak słabo radzi sobie z tym problemem.

Słabo rozwinięta świadomość bezpieczeństwa

Chociaż świadomość problemów związanych z bezpieczeństwem aplikacji internetowych wzrosła w ostatnich latach, pozostaje ona słabiej rozwinięta niż w starszych obszarach, takich jak sieci i systemy operacyjne. Chociaż większość osób zajmujących się bezpieczeństwem IT ma rozsądne pojęcie o podstawach zabezpieczania sieci i wzmacniania hostów, nadal istnieje powszechne zamieszanie i błędne przekonanie na temat wielu podstawowych koncepcji związanych z bezpieczeństwem aplikacji internetowych. Praca programisty aplikacji internetowych w coraz większym stopniu polega na łączeniu dziesiątek, a nawet setek pakietów innych firm, które mają na celu oderwanie programisty od podstawowych technologii. Często spotyka się doświadczonych programistów aplikacji internetowych, którzy robią główne założenia dotyczące bezpieczeństwa zapewnianego przez ich środowisko programistyczne i dla których wyjaśnienie wielu podstawowych rodzajów wad jest objawieniem.

Niestandardowy rozwój

Większość aplikacji internetowych jest opracowywana wewnętrznie przez własny personel organizacji lub zewnętrznych wykonawców. Nawet jeśli aplikacja korzysta z dobrze ugruntowanych komponentów, są one zazwyczaj dostosowywane lub łączone za pomocą nowego kodu. W tej sytuacji każda aplikacja jest inna i może zawierać własne, unikalne wady. Stoi to w kontraście do typowego wdrożenia infrastruktury, w którym organizacja może zakupić najlepszy w swojej klasie produkt i zainstalować go zgodnie ze standardami branżowymi.

Zwodnicza prostota

Dzięki dzisiejszym platformom aplikacji internetowych i narzędziom programistycznym początkujący programista może w krótkim czasie stworzyć potężną aplikację od podstaw. Istnieje jednak ogromna różnica między tworzeniem kodu, który jest funkcjonalny, a kodem bezpiecznym. Wiele aplikacji internetowych jest tworzonych przez osoby o dobrych intencjach, którym po prostu brakuje wiedzy i doświadczenia, aby określić, gdzie mogą pojawić się problemy z bezpieczeństwem. Znaczącym trendem w ostatnich latach jest stosowanie frameworków aplikacji, które dostarczają gotowe komponenty kodu do obsługi wielu wspólnych obszarów funkcjonalności, takich jak uwierzytelnianie, szablony stron, tablice ogłoszeń oraz integracja ze wspólnymi komponentami infrastruktury zaplecza. Przykładami takich struktur są Liferay i Appfuse. Produkty te umożliwiają szybkie i łatwe tworzenie działających aplikacji bez konieczności technicznego zrozumienia sposobu działania aplikacji lub potencjalnych zagrożeń, które mogą zawierać. Oznacza to również, że wiele firm korzysta z tych samych frameworków. Tak więc wykryta luka wpływa na wiele niepowiązanych aplikacji.

Szybko zmieniający się profil zagrożeń

Badania nad atakami na aplikacje internetowe i zabezpieczeniami nadal są prężnie rozwijającym się obszarem, w którym nowe koncepcje i zagrożenia powstają szybciej niż ma to miejsce obecnie w przypadku starszych technologii. Szczególnie po stronie klienta powszechne jest, że zaakceptowana ochrona przed konkretnym atakiem jest podważana przez badania, które demonstrują nową technikę

ataku. Zespół programistów, który rozpoczyna projekt z pełną wiedzą o bieżących zagrożeniach, mógł utracić ten status do czasu ukończenia i wdrożenia aplikacji.

Ograniczenia zasobów i czasu

Większość projektów tworzenia aplikacji internetowych podlega ścisłym ograniczeniom czasowym i zasobowym, wynikającym z ekonomii wewnętrznego, jednorazowego tworzenia. W większości organizacji zatrudnianie wyspecjalizowanej wiedzy w zakresie bezpieczeństwa w zespołach projektowych lub programistycznych jest często niewykonalne. A ze względu na poślizg projektu, testowanie bezpieczeństwa przez specjalistów jest często pozostawiane na bardzo późnym etapie cyklu życia projektu. W równoważeniu konkurencyjnych priorytetów potrzeba stworzenia stabilnej i funkcjonalnej aplikacji w terminie zwykle przesłania mniej namacalne względy bezpieczeństwa. Typowa mała organizacja może być skłonna zapłacić tylko za kilka osobodni czasu konsultacji w celu oceny nowej aplikacji. Szybki test penetracyjny często wykryje nisko wiszący owoc, ale może ominąć bardziej subtelne luki, których identyfikacja wymaga czasu i cierpliwości.

Zaawansowane technologie

Wiele z podstawowych technologii stosowanych w aplikacjach internetowych powstało, gdy krajobraz sieci WWW był bardzo inny. Od tego czasu zostały wyparte daleko poza cele, dla których zostały pierwotnie wymyślone, takie jak użycie JavaScript jako środka transmisji danych w wielu aplikacjach opartych na AJAX. Zgodnie z oczekiwaniami dotyczącymi funkcjonalności aplikacji webowych szybko ewoluowały, technologie wykorzystywane do realizacji tej funkcjonalności pozostały w tyle, a stare technologie zostały rozszerzone i przystosowane do nowych wymagań. Nic dziwnego, że doprowadziło to do powstania luk w zabezpieczeniach, ponieważ pojawiają się nieprzewidziane skutki uboczne.

Rosnące wymagania dotyczące funkcjonalności

Aplikacje są projektowane przede wszystkim z myślą o funkcjonalności i użyteczności. Niegdyś statyczne profile użytkowników zawierają teraz funkcje sieci społecznościowych, umożliwiające przesyłanie zdjęć i edycję stron w stylu wiki. Kilka lat temu projektant aplikacji mógł zadowolić się zaimplementowaniem wyzwania nazwy użytkownika i hasła w celu stworzenia funkcjonalności logowania. Nowoczesne witryny mogą obejmować odzyskiwanie hasła, odzyskiwanie nazwy użytkownika, podpowiedzi do hasła oraz opcję zapamiętania nazwy użytkownika i hasła podczas przyszłych wizyt. Taka witryna bez wątpienia byłaby promowana jako posiadająca wiele funkcji bezpieczeństwa, ale każda z nich jest tak naprawdę funkcją samoobsługową, zwiększającą powierzchnię ataku witryny.

Nowa granica bezpieczeństwa

Przed pojawieniem się aplikacji internetowych wysiłki organizacji mające na celu zabezpieczenie się przed zewnętrznymi atakami koncentrowały się w dużej mierze na obwodzie sieci. Obrona tego obwodu wiązała się z umocnieniem i załataniem usług potrzebnych do ujawnienia i zaporą dostępu dla innych. Aplikacje internetowe zmieniły to wszystko. Aby aplikacja była dostępna dla jej użytkowników, zapora obwodowa musi zezwalać na połączenia przychodzące do serwera za pośrednictwem protokołu HTTP lub HTTPS. Aby aplikacja działała, serwer musi mieć możliwość połączenia się z obsługującymi ją systemami zaplecza, takimi jak bazy danych, komputery mainframe oraz systemy finansowe i logistyczne. Systemy te często leżą u podstaw operacji organizacji i znajdują się za kilkoma warstwami zabezpieczeń na poziomie sieci. Jeśli w aplikacji internetowej istnieje luka, osoba atakująca w publicznym Internecie może być w stanie złamać podstawowe systemy zaplecza organizacji wyłącznie poprzez przesłanie spreparowanych danych ze swojej przeglądarki internetowej. Dane te przechodzą

przez wszystkie zabezpieczenia sieciowe organizacji, w taki sam sposób, jak zwykły, łagodny ruch do aplikacji internetowych. Skutkiem powszechnego wdrażania aplikacji internetowych jest przesunięcie granic bezpieczeństwa typowej organizacji. Część tego obwodu jest nadal zawarta w zaporach ogniowych i hostach bastionowych. Ale znaczna jej część jest teraz zajęta przez aplikacje internetowe organizacji. Ze względu na różnorodne sposoby, w jakie aplikacje internetowe odbierają dane wejściowe użytkownika i przekazują je do wrażliwych systemów zaplecza, są one potencjalnymi bramami dla szerokiej gamy ataków, a ochrona przed tymi atakami musi być zaimplementowana w samych aplikacjach. Pojedyncza linia wadliwego kodu w jednej aplikacji internetowej może narazić wewnętrzne systemy organizacji na podatność. Co więcej, wraz z rozwojem aplikacji typu mash-up, widżetów innych firm i innych technik integracji międzydomenowej, granica bezpieczeństwa po stronie serwera często wykracza daleko poza samą organizację. Niejawne zaufanie pokładane jest w usługach aplikacji i usług zewnętrznych. Opisane wcześniej statystyki dotyczące występowania luk w tej nowej granicy bezpieczeństwa powinny dać każdej organizacji chwilę do namysłu.

UWAGA: Dla atakującego organizację uzyskanie dostępu do sieci lub wykonanie arbitralnych poleceń na serwerach może nie być tym, co chce osiągnąć. Często, a być może zazwyczaj, to, czego naprawdę chce osoba atakująca, to wykonanie pewnych działań na poziomie aplikacji, takich jak kradzież danych osobowych, transfer środków lub dokonywanie tanich zakupów. A przeniesienie granicy bezpieczeństwa do warstwy aplikacji może znacznie pomóc napastnikowi w osiągnięciu tych celów. Załóżmy na przykład, że atakujący chce „włamać się" do systemów banku i ukraść pieniądze z kont użytkowników. W przeszłości, zanim bank wdrożył aplikację internetową, osoba atakująca mogła potrzebować znaleźć lukę w publicznie dostępnej usłudze, wykorzystać ją, aby uzyskać dostęp do strefy DMZ banku, przeniknąć zaporę sieciową ograniczającą dostęp do jego systemów wewnętrznych, mapować sieć, aby znaleźć komputer typu mainframe, odszyfrować tajemniczy protokół używany do uzyskania do niego dostępu i odgadnąć niektóre dane uwierzytelniające, aby się zalogować. Jeśli jednak bank wdroży teraz podatną na ataki aplikację internetową, atakujący może po prostu osiągnąć ten sam wynik poprzez modyfikację numeru rachunku w ukrytym polu formularza HTML.

Drugi sposób, w jaki aplikacje internetowe przeniosły granicę bezpieczeństwa, wynika z zagrożeń, z którymi borykają się sami użytkownicy, gdy uzyskują dostęp do podatnej na ataki aplikacji. Złośliwy atakujący może wykorzystać niegroźną, ale podatną na ataki aplikację internetową, aby zaatakować każdego odwiedzającego ją użytkownika. Jeśli ten użytkownik znajduje się w wewnętrznej sieci firmowej, atakujący może wykorzystać przeglądarkę użytkownika do przeprowadzenia ataku na sieć lokalną z zaufanej pozycji użytkownika. Bez jakiejkolwiek współpracy ze strony użytkownika atakujący może być w stanie wykonać dowolne działanie, które użytkownik mógłby wykonać, gdyby sam był złośliwy. Wraz z rozprzestrzenianiem się technologii rozszerzeń przeglądarki i wtyczek znacznie zwiększył się zasięg ataku po stronie klienta. Administratorzy sieci znają pomysł uniemożliwiania swoim użytkownikom odwiedzania złośliwych witryn internetowych, a sami użytkownicy końcowi stopniowo stają się coraz bardziej świadomi tego zagrożenia. Jednak natura luk w zabezpieczeniach aplikacji internetowych oznacza, że podatna aplikacja może stanowić nie mniejsze zagrożenie dla swoich użytkowników i ich organizacji niż strona internetowa, która jest jawnie złośliwa. W związku z tym nowa granica bezpieczeństwa nakłada na wszystkich właścicieli aplikacji obowiązek dbania o ochronę swoich użytkowników przed atakami na nich dostarczanymi za pośrednictwem aplikacji. Kolejnym sposobem częściowego przeniesienia granicy bezpieczeństwa na stronę klienta jest szerokie wykorzystanie poczty e-mail jako rozszerzonego mechanizmu uwierzytelniania. Ogromna liczba dzisiejszych aplikacji zawiera funkcje „zapomnianego hasła", które umożliwiają atakującemu wygenerowanie wiadomości e-mail umożliwiającej odzyskanie konta na dowolny zarejestrowany adres, bez konieczności podawania jakichkolwiek innych informacji specyficznych dla użytkownika. Dzięki temu osoba atakująca, która włamuje się na konto poczty internetowej użytkownika, może

łatwo eskalować atak i włamać się na konta ofiary w większości aplikacji internetowych, w których zarejestrowana jest ofiara.

Przyszłość bezpieczeństwa aplikacji internetowych

Ponad dziesięć lat po ich powszechnym przyjęciu aplikacje internetowe w Internecie nadal są pełne luk w zabezpieczeniach. Zrozumienie zagrożeń bezpieczeństwa, z jakimi borykają się aplikacje internetowe, oraz skuteczne sposoby ich radzenia sobie z nimi są wciąż słabo rozwinięte w branży. Obecnie niewiele wskazuje na to, że czynniki problemowe opisane w tym rozdziale znikną w najbliższej przyszłości. To powiedziawszy, szczegóły krajobrazu bezpieczeństwa aplikacji internetowych nie są statyczne. Mimo że wciąż pojawiają się stare i dobrze zrozumiane luki w zabezpieczeniach, takie jak wstrzykiwanie SQL, ich rozpowszechnienie stopniowo maleje. Ponadto, przypadki, które pozostały, stają się coraz trudniejsze do odnalezienia i wykorzystania. Nowe badania w tych obszarach koncentrują się na opracowaniu zaawansowanych technik atakowania bardziej subtelnych przejawów luk w zabezpieczeniach, które kilka lat temu można było łatwo wykryć i wykorzystać tylko za pomocą przeglądarki. Drugim widocznym trendem jest stopniowe odwracanie uwagi od ataków po stronie serwera aplikacji do tych, które są skierowane do użytkowników aplikacji. Ten ostatni rodzaj ataku nadal wykorzystuje defekty w samej aplikacji, ale zazwyczaj wiąże się z pewnego rodzaju interakcją z innym użytkownikiem, aby złamać jego postępowanie z podatną aplikacją. Jest to trend, który został powtórzony w innych obszarach bezpieczeństwa oprogramowania. W miarę dojrzewania świadomości zagrożeń bezpieczeństwa wady po stronie serwera są pierwszymi, które należy dobrze zrozumieć i usunąć, pozostawiając po stronie klienta kluczowe pole bitwy w miarę postępu procesu uczenia się. Ze wszystkich ataków opisanych w tej książce te na innych użytkowników ewoluują najszybciej i były przedmiotem większości badań w ostatnich latach. Różne najnowsze trendy w technologii nieco zmieniły krajobraz aplikacji internetowych. Powszechna świadomość tych trendów istnieje za pomocą różnych, dość mylących słów, z których najważniejsze to:

* Web 2.0 - termin ten odnosi się do większego wykorzystania funkcji, które umożliwiają udostępnianie treści i informacji generowanych przez użytkowników, a także do zastosowania różnych technologii szeroko obsługujących tę funkcjonalność, w tym asynchronicznych żądań HTTP i integracji międzydomenowej.

* Przetwarzanie w chmurze - termin ten odnosi się do większego korzystania z usług zewnętrznych dostawców różnych części stosu technologicznego, w tym oprogramowania aplikacji, platform aplikacji, oprogramowania serwera WWW, baz danych i sprzętu. Odnosi się to również do zwiększonego wykorzystania technologii wirtualizacji w środowiskach hostingowych.

Podobnie jak w przypadku większości zmian technologicznych, trendy te przyniosły ze sobą nowe ataki i odmiany istniejących ataków. Nie znosząc szumu, poruszone kwestie nie są tak rewolucyjne, jak mogą się początkowo wydawać. W tej książce przeanalizujemy implikacje bezpieczeństwa tych i innych najnowszych trendów w odpowiednich lokalizacjach. Pomimo wszystkich zmian, które zaszły w aplikacjach internetowych, niektóre kategorie „klasycznych” luk w zabezpieczeniach nie wykazują oznak zmniejszania się. Wciąż pojawiają się w prawie takiej samej formie, jak w pierwszych dniach sieci. Obejmują one wady logiki biznesowej, nieprawidłowe stosowanie kontroli dostępu i inne problemy projektowe. Nawet w świecie skręcanych ze sobą komponentów aplikacji i wszystkiego jako usługi te ponadczasowe problemy prawdopodobnie pozostaną szeroko rozpowszechnione.

Streszczenie

W ciągu nieco ponad dekady sieć WWW przekształciła się z czysto statycznych repozytoriów informacji w wysoce funkcjonalne aplikacje, które przetwarzają wrażliwe dane i wykonują potężne działania o

rzeczywistych konsekwencjach. Podczas tego rozwoju kilka czynników połączyło się, aby doprowadzić do słabego stanu bezpieczeństwa większości dzisiejszych aplikacji internetowych. Większość aplikacji boryka się z podstawowym problemem związanym z bezpieczeństwem, w którym użytkownicy mogą wprowadzać dowolne dane wejściowe. Każdy aspekt interakcji użytkownika z aplikacją może być złośliwy i powinien być tak traktowany, chyba że udowodniono inaczej. Niewłaściwe rozwiązanie tego problemu może narazić aplikacje na ataki na wiele sposobów. Wszystkie dowody dotyczące obecnego stanu bezpieczeństwa aplikacji internetowych wskazują, że chociaż niektóre aspekty bezpieczeństwa rzeczywiście uległy poprawie, wyewoluowały całkowicie nowe zagrożenia, aby je zastąpić. Ogólny problem nie został rozwiązany na żadną znaczącą skalę. Ataki na aplikacje internetowe nadal stanowią poważne zagrożenie zarówno dla organizacji, które je wdrażają, jak i użytkowników uzyskujących do nich dostęp.