Rodzaje ataków na stronę internetową

1. SQL Injection

Ta metoda jest obecnie bardzo często wykorzystywana, ponieważ większość witryn korzysta z SQL – do komunikacji z bazą danych. Przykładami takowego rozwiązania (oprogramowania) są: Microsoft SQL Server, PostgreSQL czy MySQL.

SQL injection polega na „wstrzyknięciu" kodu SQL na stronę internetową tak, aby został on uruchomiony. Haker zamieszcza go np. w polu formularza logowania do konta.

Dzięki czemu strona, która docelowo ma tam sczytać dane logowania, uruchamia kod. W ten sposób osoba nieuprawniona może uzyskać dostęp do wybranej aplikacji lub bazy danych.

2. Brutalny atak

Niski poziom bezpieczeństwa danych logowania to dobra wiadomość dla osób, które mają zamiar przeprowadzić atak hakerski na stronę internetową.

W takim przypadku mogą oni wykorzystać oprogramowanie, które generuje nieskończone wersje haseł oraz loginów, by trafić na właściwą kombinację.

W ten sposób omijają zabezpieczenia. Aby uchronić się przed tego rodzaju atakami hakerskimi, bardzo istotne jest nie tylko dbanie o wysokie bezpieczeństwo danych logowania administratorów strony.

Tego samego należy także wymagać od użytkowników witryny, aby haker nie był w stanie uzyskać dostępu do witryny przez ich słabo zabezpieczone konta.

3. Atak DoS/DDoS (Denial of Service)

Kolejnym rodzajem ataku hakerskiego jest DoS/DDoS. Skrót DDoS znaczy Distributed Denial of Service. W skrócie ma on na celu doprowadzenie do crashu, wyłączenia serwera. Aby przeprowadzić tego rodzaju atak na stronę,

wykorzystuje się głównie boty. Wysyłają one liczne i ciągle powtarzające się zapytania do serwera (hostingu).

W końcu serwer nie jest w stanie ich przetworzyć, więc dochodzi do wyłączenia. Atak DoS jest stosunkowo łatwy i szybki do przeprowadzenia.

Warto zauważyć, że w postaci botów haker często wykorzystuje inne komputery, do których dostęp uzyskał dzięki złośliwemu oprogramowaniu. Właściciele zainfekowanych urządzeń zwykle w ogóle o tym nie wiedzą.

4. Cross Site Scripting (XSS)

Atak XSS to jeden z najtrudniejszych ataków hakerskich na stronę www, z jakim może przyjść Ci się zmierzyć. Jego skuteczność wynika z tego, w jaki sposób działa. Większość ataków XSS wykorzystuje złośliwe skrypty JavaScript, które są zamieszczone w linkach.

Gdy dana osoba klika taki link, uruchamia kod, który jest w stanie przejąć sesję na stronie, uzyskać dostęp do konta, czy nawet zmienić reklamy wyświetlane na witrynie.

Hakerzy zazwyczaj zamieszczają takie złośliwe linki na forach internetowych, serwisach społecznościowych czy w innych miejscach, które generują dużo ruchu, a pozwalają jednocześnie na w miarę łatwe zamieszczanie swoich treści.

Aby zapobiec takim atakom, konieczne jest kontrolowanie tego, jakie treści są zamieszczane przez użytkowników witryny.

5. Kradzież plików cookie

Dane osobowe mają dużą wartość, dlatego często to one są celem ataków hakerskich na strony www. Pliki cookie są zwykle przechowywane w przeglądarce internetowej i zawierają w sobie informacje na temat użytkownika, jego dane logowania, czy historię przeglądania.

Jako że często dane te są zapisane w postaci czystego tekstu, za pomocą addonów do przeglądarek internetowych haker może stosunkowo łatwo

uzyskać do nich dostęp. Gdy już to zrobi, będzie w stanie podszywać się pod osobę, której dane wykradł.

6. Phishing

W przypadku tego rodzaju ataku hakerskiego na stronę wykorzystuje się niewiedzę lub częstą naiwność ludzi. Jej celem jest kradzież informacji potrzebnych do logowania, szczegółów kart kredytowych czy innych wrażliwych danych.

W tym celu haker podszywa się pod jedną ze stron w komunikacji internetowej – jako przykład weźmy tutaj bank.

Próba wyłudzenia informacji często sprowadza się do wysyłania maili czy SMS-ów do użytkowników danego banku z prośbą o podanie, czy „potwierdzenie" pewnych danych.

Użyte wiadomości przekierowują na stronę, która podszywa się pod prawdziwą witrynę instytucji – wygląda w zasadzie identycznie, a jej adres będzie zwykle bardzo podobny.

Niczego niepodejrzewające osoby „zweryfikują" na prośbę pewne dane, czy też wykonają normalną próbę logowania. W ten sposób haker uzyska dostęp do konta bankowego.

Choć o phishingu mówi się od jakiegoś czasu, to jednak dalej wiele osób pada ofiarą takich ataków. Aby temu zapobiec, konieczne jest informowanie użytkowników swojej strony choćby o tym, że nigdy nie będziesz ich prosić mailowo o podanie pewnych wrażliwych danych.

Dzięki temu będą bardziej ostrożni, gdy otrzymają tego typu zapytania od niedoszłych złodziei.