10

SERVER-SIDE REQUEST FORGERY

Podatność typu *Server-Side Request Forgery* (*SSRF*) pozwala atakującemu na manipulację żądaniami serwera. Podobnie jak podatność cross-site request forgery (CSRF), SSRF nadużywa innego systemu, aby wykonać niezamierzone akcje. Podczas gdy CSRF wykorzystuje innego użytkownika, SSRF wykorzystuje serwer docelowej aplikacji. Tak samo jak CSRF, podatności SSRF mogą być różne w skutkach i sposobach wykonania. Sam jednak fakt, że możesz wysyłać żądania z docelowego serwera do innych serwerów, nie oznacza, że aplikacja jest podatna. Aplikacje mogą umyślnie zezwalać na takie zachowanie. Z tego powodu ważne jest, aby zademonstrować możliwości wykorzystania, które otwiera znaleziony SSRF.

Demonstracja zagrożeń podatności SSRF

W zależności od tego, w jaki sposób witryna jest zorganizowana, serwer podatny na SSRF może wykonywać żądania HTTP do wewnętrznej sieci albo na zewnętrzny adres. Zdolność podatnego serwera do wykonywania żądań decyduje o tym, co można zrobić ze znalezionym SSRF-em.

Niektóre większe strony internetowe mają zapory, które blokują zewnętrzny ruch przed dostępem do wewnętrznych serwerów: na przykład witryna ma ograniczoną liczbę publicznych serwerów, które przyjmują żądania HTTP od odwiedzających. Następnie wysyłają otrzymane żądania na pozostałe serwery, które są już poza dostępem publicznym. Częstym przykładem jest serwer z bazą danych, będący zazwyczaj niedostępny dla internetu. Kiedy logujesz się na stronę, która komunikuje się z serwerem bazy danych, przesyłasz nazwę użytkownika i hasło przez standardowy formularz internetowy. Następnie witryna, która otrzyma Twoje żądanie, wykonuje swoje własne żądanie do serwera z bazą danych przy użyciu podanych przez Ciebie danych. Potem serwer z bazą danych wyśle odpowiedź do serwera aplikacji, a ten przekaże informacje do Ciebie. Podczas tego procesu często nie zdajesz sobie sprawy z tego, że zewnętrzny serwer bazy danych w ogóle istnieje.

Podatne serwery, które pozwalają atakującemu kontrolować żądania do wewnętrznych serwerów, mogą doprowadzić do ujawnienia prywatnych informacji. Na przykład, jeżeli w poprzednim przykładzie istniałby SSRF, to mógłby on pozwolić atakującemu przesyłać żądania do serwera bazy danych i uzyskać informacje, do których nie powinien mieć dostępu. Podatności SSRF dostarczają atakującym możliwość komunikacji z wewnętrzną siecią.

Załóżmy, że znalazłeś SSRF, jednak podatna strona nie ma wewnętrznych serwerów lub serwery te nie są dostępne przez podatność. W takim przypadku sprawdź, czy możesz wykonywać żądania do zewnętrznych stron z podatnego serwera. Jeżeli uda Ci się wykorzystać docelowy serwer tak, aby komunikował się z twoim własnym serwerem, możesz użyć żądanych informacji, aby poznać szczegóły oprogramowania, z którego korzysta docelowa aplikacja. Być może będziesz też w stanie kontrolować odpowiedź.

Na przykład możliwe jest konwertowanie zewnętrznych żądań na wewnętrzne, pod warunkiem, że podatny serwer śledzi przekierowania – trik, który pokazał mi Justin Kennedy. W niektórych przypadkach strona nie pozwoli na dostęp do wewnętrznych adresów IP, ale nawiąże połączenie z zewnętrznymi witrynami. Jeśli tak będzie, możesz zwrócić odpowiedź HTTP z kodem 301, 302, 303 lub 307, które oznaczają przekierowanie. Ponieważ masz kontrolę nad odpowiedziami, możesz skierować serwer na wewnętrzny adres IP, aby przetestować, czy prześledzi on odpowiedź 301 i wykona żądanie HTTP do wewnętrznej sieci.

Alternatywą jest użycie odpowiedzi z własnego serwera, aby sprawdzić obecność innych podatności, takich jak SQLi albo XXS, tak jak zostało to