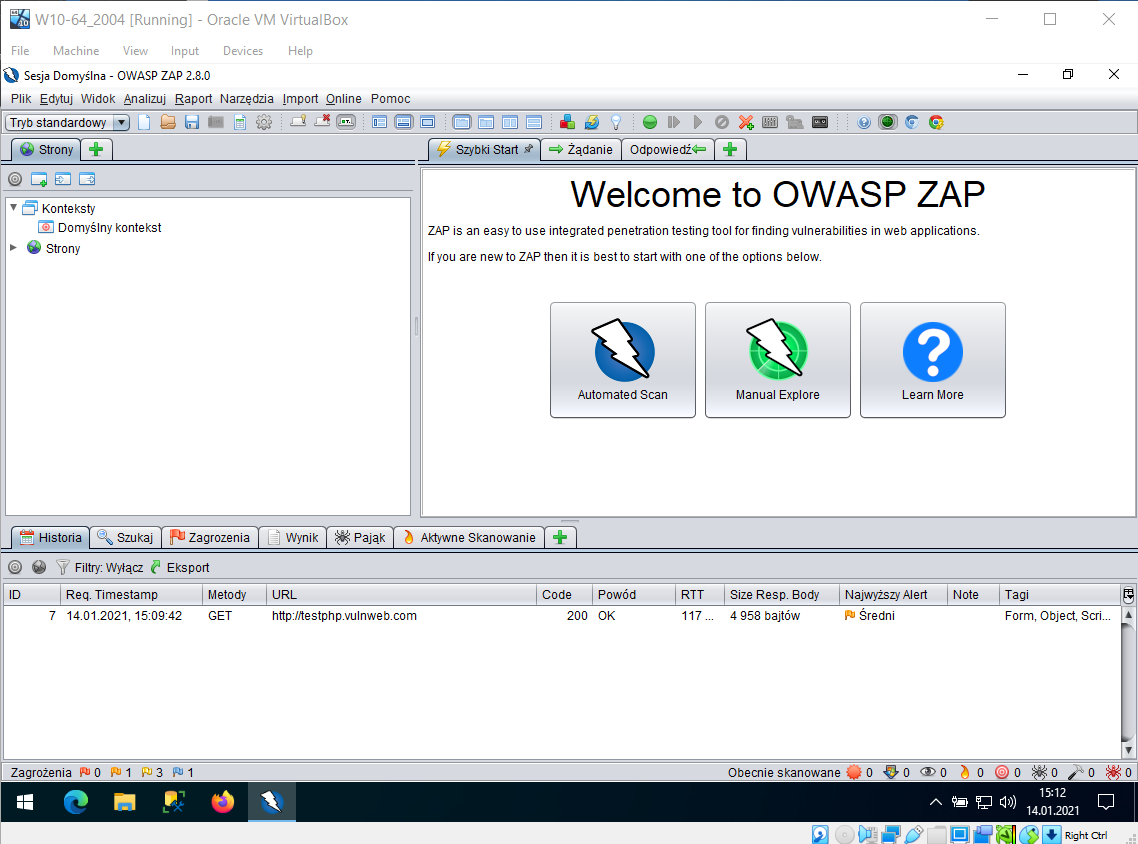
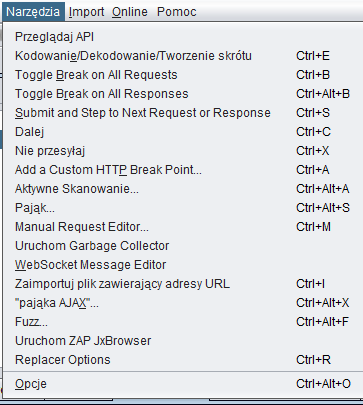
**Główne okno**

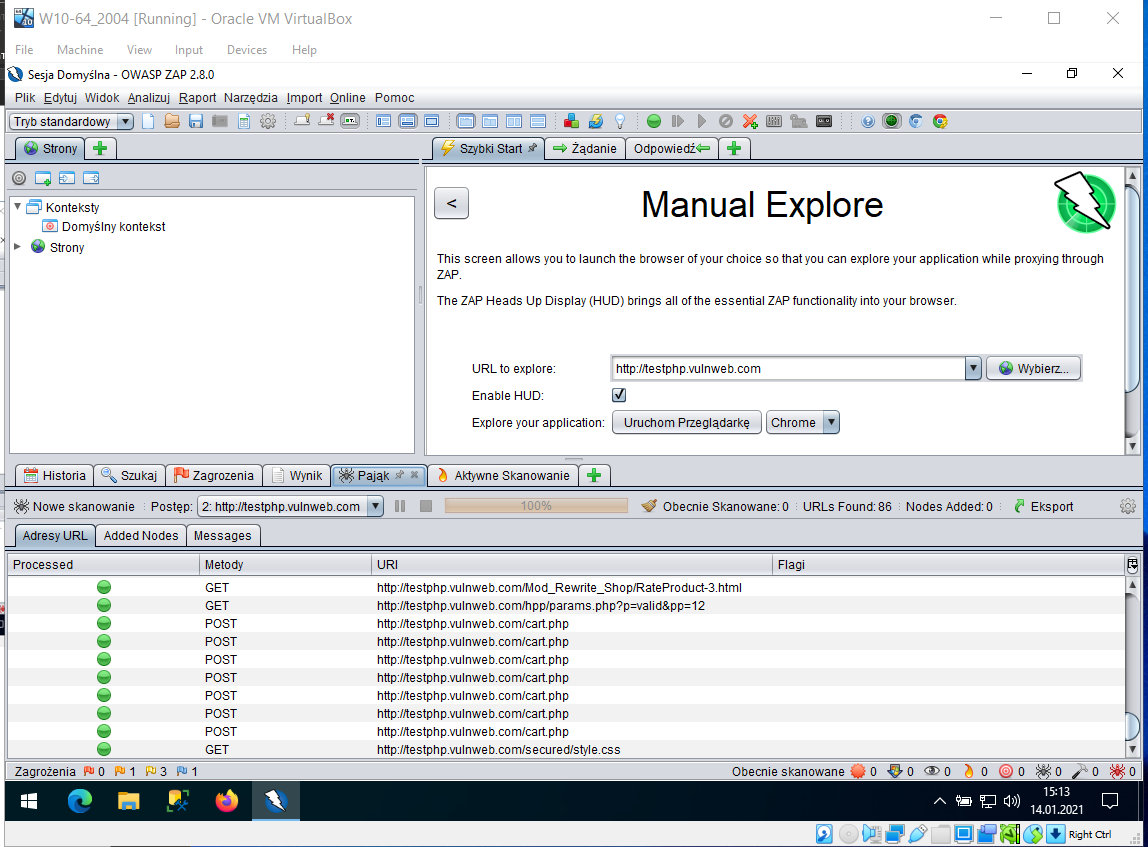
Przy otwieraniu aplikacji widzimy główny ekran.

W pasku menu na górze wybieramy punkt Narzędania, dalej Aktywne skanowanie.

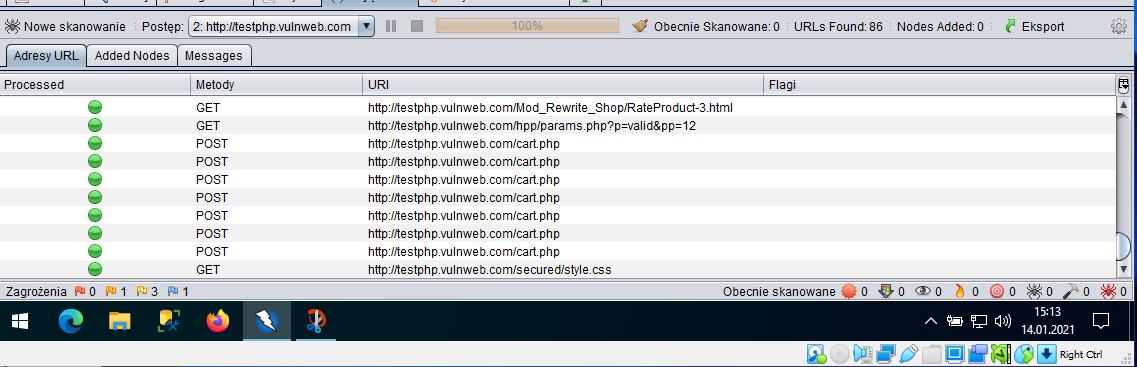


**Pająk**

Także możemy wybrać opcje tylko pająka, żeby sprawdził wszystkie strony i linki, zawierające się na stronie.

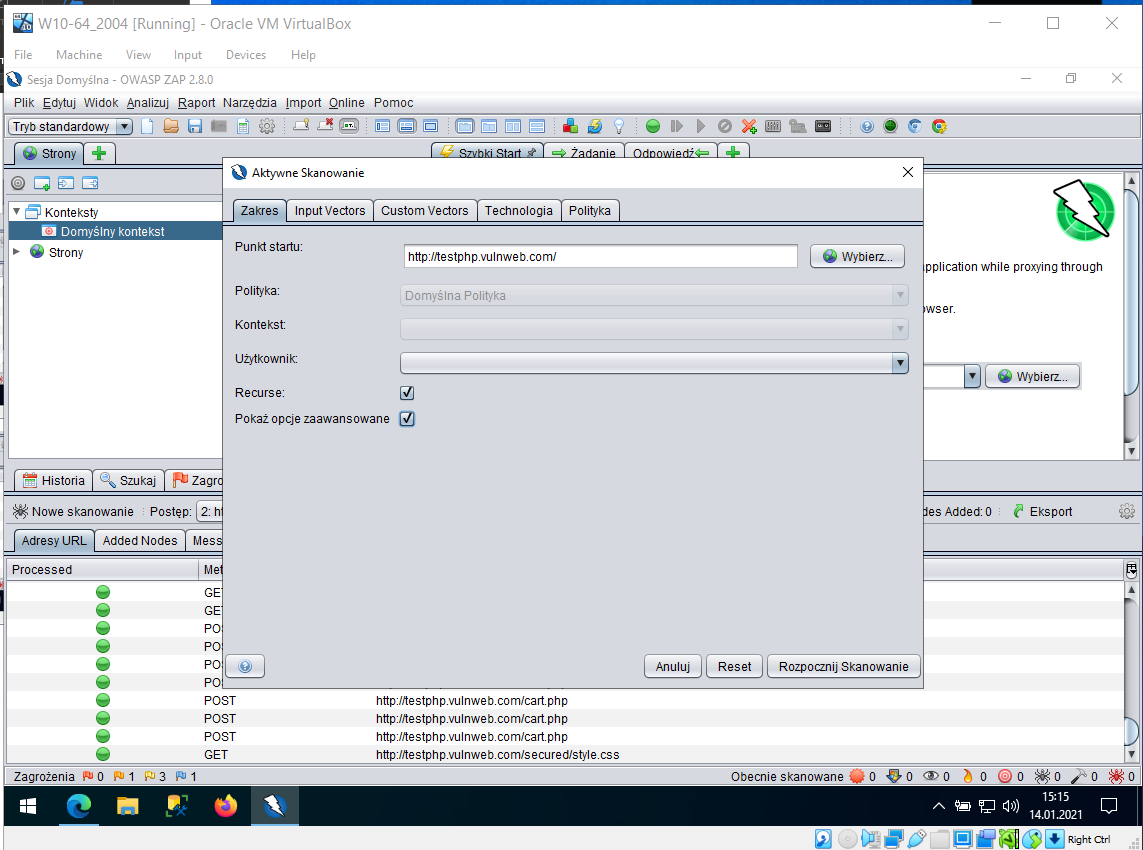


Możemy widać spis tych stron.



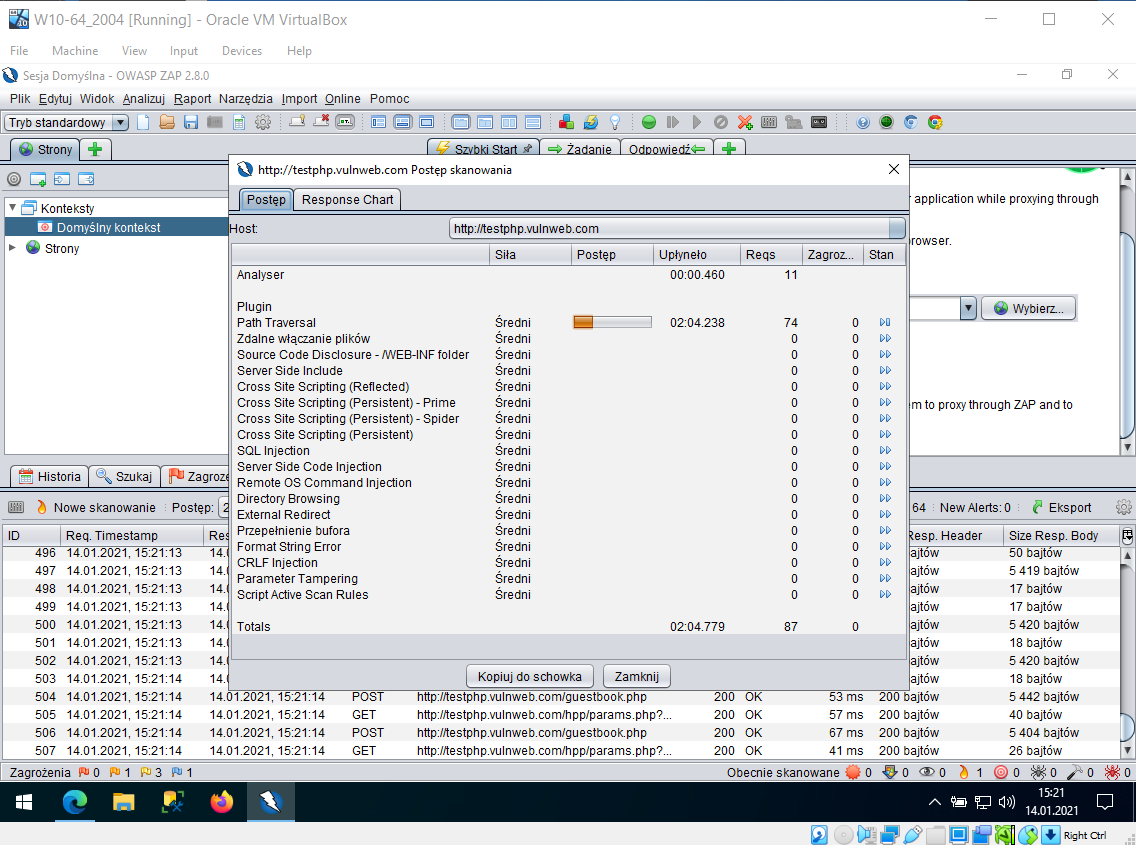
**Aktywne skanowanie**

W oknie Aktywnie Skanowanie wprowadzamy URL naszej strony http://testphp.vulnweb.com

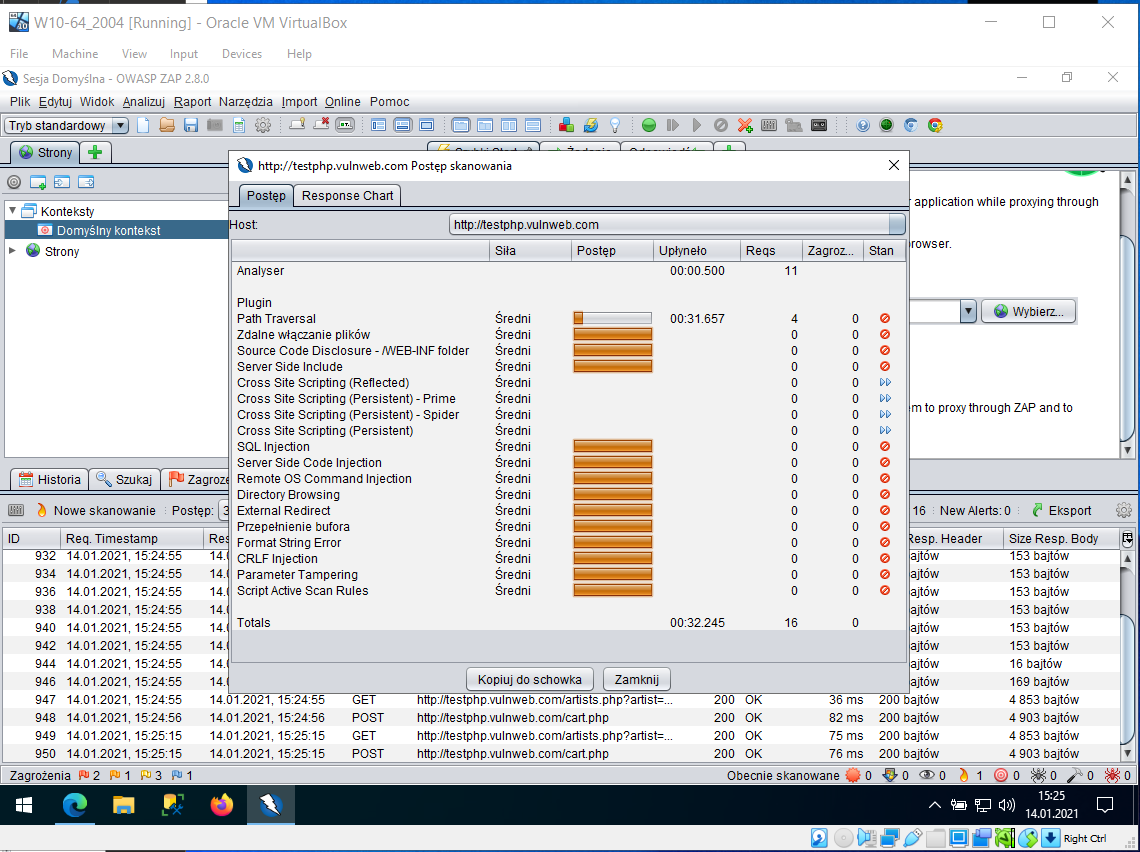


Dalej wybieramy Rozpocznij Skanowanie.

Przy otwieraniu okna Postępu skanowania widzimy szystkie typy skanowań. Możemy ominąć niepotrzebne klikając na odpowiednią ikonę po prawej stronie.

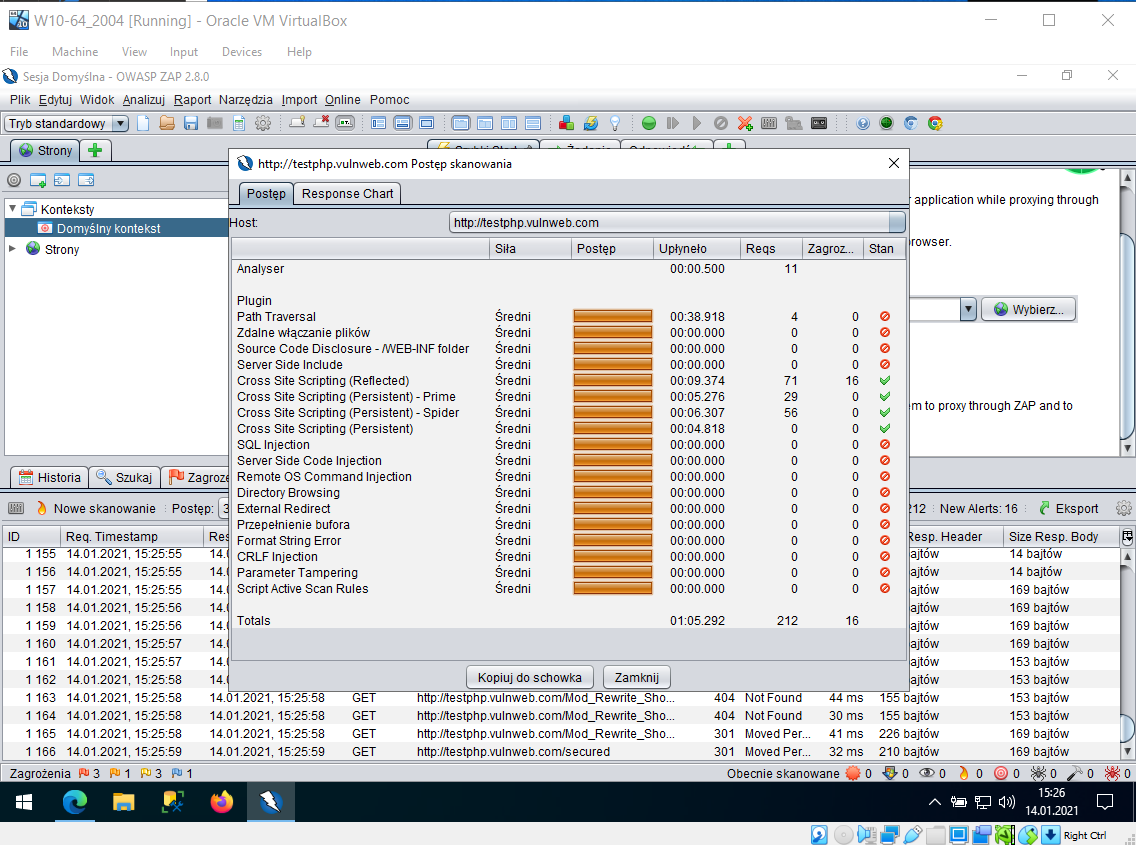


Po ominięciu nipotrzebnych typów skanowań zostawiamy tylko potrzebne dla XSS.



**Tworzenie raportu**

Po niektorzym czasie widzimy, że skanowanie już jest skończone. Żeby wygenerować raport wybieramy punkt Raport, dalej wygeneruj Raport HTML w górnym menu.



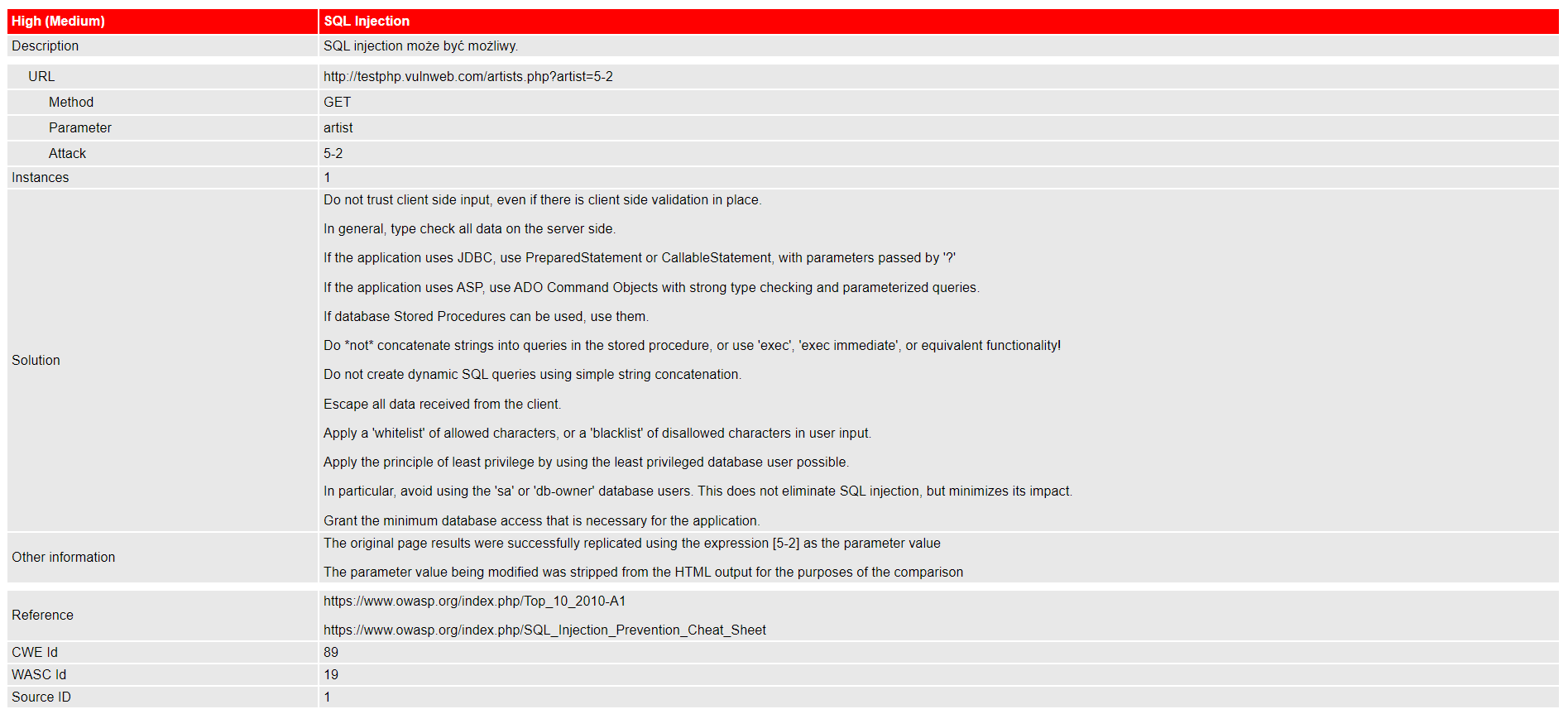
**Zagrożenie typu High**

W raporcie widzimy typy zagrożeń. Dla przykładu weźmę typ High SQL Injection.

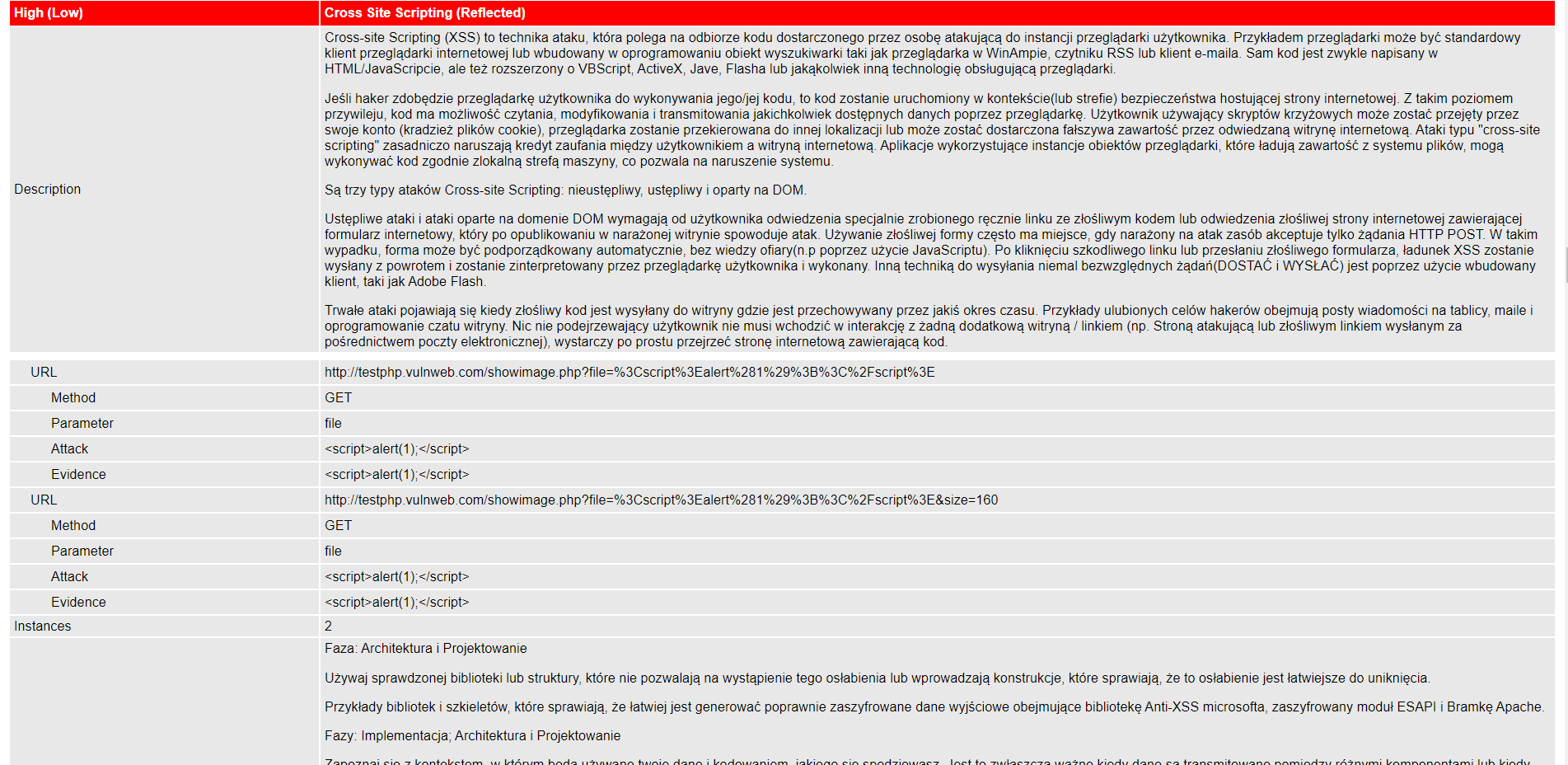
Zagrożenie wynika na stronie <http://testphp.vulnweb.com/artists.php?artist=5-2>, przy wprowadzeniu danych użytkownikiem.

Aby usunąć zagrożenie tego typu na serwerze potrzebujemy sprawdzać dane wprowadzone przez użytkowników i tylko po tym sprawdzeniu robić żądanie do bazy danych. Dla każdej bazy danych są swoje funkcje do sprawdzenia takich rzeczy.

Wybrałem problem tego typu, bo jest najpopularniejszy. Często programiści nie pamiętają o nim i pomijają sprawdzenie wprowadzonych danych użytkownikiem.



Jeszcze jeden przykład zagrożenia typu High.



Cross-site Scripting (XSS) to technika ataku, która polega na odbiorze kodu dostarczonego przez osobę atakującą do instancji przeglądarki użytkownika. Przykładem przeglądarki może być standardowy klient przeglądarki internetowej lub wbudowany w oprogramowaniu obiekt wyszukiwarki taki jak przeglądarka w WinAmpie, czytniku RSS lub klient e-maila. Sam kod jest zwykle napisany w HTML/JavaScripcie, ale też rozszerzony o VBScript, ActiveX, Jave, Flasha lub jakąkolwiek inną technologię obsługującą przeglądarki.

**Aby usunąć zagrożenie tego typu, należy:**

- Faza architektury i projektowania:

Używaj sprawdzonej biblioteki lub struktury, które nie pozwalają na wystąpienie tego osłabienia lub wprowadzają konstrukcje, które sprawiają, że to osłabienie jest łatwiejsze do uniknięcia.

- Faza implementacji, architektury i projektowania:

Zapoznaj się z kontekstem, w którym będą używane twoje dane i kodowaniem, jakiego się spodziewasz. Jest to zwłaszcza ważne kiedy dane są transmitowane pomiędzy różnymi komponentami lub kiedy generowane są dane wyjściowe, które zawierają wielokrotne szyfrowanie w tym samym czasie, tak jak strony internetowe albo kilkuczęściowe wiadomości e-mail. Zbadaj wszystkie przewidywane protokoły komunikacyjne i reprezentacje danych, aby określić wymagane strategie kodowania.

Jeśli możliwe, używaj wymodelowane mechanizmy automatycznie wymuszające oddzielenie danych i kodu. Te mechanizmy mogą być w stanie zapewnić odpowiednie cytowanie, kodowanie i sprawdzanie poprawności automatycznie, zamiast polegać na programistach, aby zapewnić tę możliwość w każdym punkcie, w którym generowane są dane wyjściowe.

**Zagrożenie typu Medium**

Wykryte zostało zagrożenie typu Medium X-Frame-Options Header Not Set. Ta wada była na różnych stronach naszej witryny.

Aby usunąć zagrożenie tego typu musimy upewnić się, że jest ustawione na wszystkich stronach internetowych ta opcja. Większość nowoczesnych przeglądarek internetowych obsługuje nagłówek HTTP X-Frame-Options. Upewnij się, że jest ustawiony na wszystkich stronach internetowych zwracanych przez twoją witrynę (jeśli oczekujesz, że strona będzie otoczona tylko stronami na twoim serwerze (np. Jest częścią zestawu FRAMESET), wtedy będziesz chciał użyć SAMEORIGIN, w przeciwnym razie jeśli nigdy nie spodziewasz się strony aby została umieszczona w ramce, użyj opcji ODMOWA. ZEZWÓL-OD pozwala określonym witrynom na umieszczenie strony internetowej w ramce w obsługiwanych przeglądarkach internetowych).