Testing for Client-side (İstemci Tarafı için Test)

Summary (Özet)

İstek tarafı SQL enjeksiyonu, bir uygulama Web SQL Veritabanı teknolojisini uyguladığında ve girişi düzgün bir şekilde doğrulamadığında veya sorgu değişkenlerini parabriyalet etmediğinde ortaya çıkar. Bu veritabanı, JavaScript (JS) API aramaları kullanılarak manipüle edilir. `openDatabase()`, mevcut bir veritabanı oluşturan veya açar.

Test Objectives (Test Hedefleri)

Aşağıdaki test senaryosu, uygun girdi doğrulamasının gerçekleştirildiğini doğrulayacaktır. Uygulama savunmasızsa, saldırgan veritabanında depolanan bilgileri okuyabilir, değiştirebilir veya silebilir.

How To Test (Nasıl Test Edilir)

Identify the Usage of Web SQL DB (Web SQL DB Kullanımını Belirleyin)

Test edilen uygulama Web SQL DB'yi uygularsa, aşağıdaki üç arama istemci tarafı çekirdeğinde kullanılacaktır:

- `openDatabase()`
- `transaction()`
- `executeSQL()`

Aşağıdaki kod, API'lerin uygulanmasının bir örneğini göstermektedir:

```
var db = openDatabase(shortName, version, displayName, maxSize);

db.transaction(function(transaction) {
   transaction.executeSql('INSERT INTO LOGS (time, id, log) VALUES (?, ?, ?)', [dateTime, id, log]);
});
```

Web SQL DB Injection (Web SQL DB Enjeksiyonu)

Kullanımını onayladıktan sonra `executeSQL()` Saldırgan, uygulanmasının güvenliğini test etmeye ve doğrulamaya hazırdır.

Web SQL DB'nin uygulaması SQLite'ın sözdizibine dayanmaktadır.

Bypassing Conditions (Koşulları atlamak)

Aşağıdaki örnek, bunun müşteri tarafında nasıl istismar edilebileceğini göstermektedir:

```
// URL example: https://example.com/user#15
var userId = document.location.hash.substring(1,); // Grabs the ID without the hash → 15

db.transaction(function(transaction){
   transaction.executeSQL('SELECT * FROM users WHERE user = ' + userId);
});
```

Tüm kullanıcılar için bilgi iade etmek için, yalnızca saldırgana karşılık gelen kullanıcı yerine, aşağıdakiler kullanılabilir: `15 OR 1=1` URL parçasında.

Ek SQL Enjeksiyon yükleri için SQL Injection senaryosu için Test bölümüne gidin.

Remediation (Düzeltme)

SQL Injection'ın Düzeltme Bölümü için Test'ten aynı iyileştirmeyi takip edin.

References (Referanslar)

- W3C Web SQL Veritabanı
- Apple'ın JavaScript Veritabanı Öğretici
- Öğreticiler noktası HTML5 Web SQL Veritabanı
- Portswigger'ın Client-Side SQL Injection