記事
Hiroshi Sato · 2020年12月16日 2m read

SQLインジェクションに対する対策

これはInterSystems FAQ サイトの記事です。

SQLインジェクションに関しては、様々なWebサイトで対策等が公開されていますが、InterSystems SQLを使ったアプリケーションでも、他のRDBMSと同様にそれらの対策を適切に実施することで、SQLインジェクションは防げると考えられます。

さらに、InterSystems Data Platform(以下IRIS)の場合、一般的なRDBMSに比較して、SQLインジェクションを実行しづらい、幾つかの施策が組み込まれています。

1. InterSystems SQLでは、一度のリクエストで複数個のSQL文は実行できませんので、セミコロン（;）の後ろに悪意のあるコマンドを入力時に追加するというテクニックが使えません。
2. IRISは、SQLアクセスだけではなく、オブジェクトアクセスも提供しています。 更新処理を、オブジェクトアクセスで実装することで、一般ユーザに対するSQL文による更新処理を禁止することにより、SQL文のインジェクションによるアプリケーションが予期していないデータベースの改竄を防ぐことができます。
3. IRISのWeb技術であるCSPでは、urlのクエリ文字列は、全て暗号化できるので、クエリ文字列から、インジェクションの手がかりを得るなどのテクニックが使用しづらいです。
4. IRISのセキュリティモデルでは、ユーザだけではなくアプリケーションにデータベースへのアクセス権限を付与することができます。 そして、ユーザには、アプリケーションの実行の権限だけを与えて、データベースへの読み書きの権限を制限することができます。

これらにより、悪意のあるユーザがデータベースそのものを直接アクセスする機会をさらに狭めることができます。

#SQL #Caché #Ensemble #InterSystems IRIS #InterSystems IRIS for Health

ソースURL:
https://jp.community.intersystems.com/post/sql%E3%82%A4%E3%83%B3%E3%82%B8%E3%82%A7%E3%82%AF%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E5%AF%BE%E7%AD%96