NoSQL, No Injection !?

By. Kuon

Agenda

- ✓ What is NoSQL ?
- ✓ Types of NoSQL
- ✓ Who use NoSQL concept?
- ✓ NoSQL Architecture
- ✓ Security Problem
- ✓ Prevention and Detection !?

What is NoSQL ?

- ✗ No SQL (statement)
- ✗ No SQL Injection

- ✓ Not only a SQL
- ✓ Non-RDBMS
  - Semi-structured
  - Schema-less

Types of NoSQL

1. Key-value based
2. Column-based
3. Document-based
4. Graph-based
5. Object-based
6. …

Why NoSQL

1. Performance
2. Scalability

Who use NoSQL concept?

1. Cloud Computing
   - **(SaaS Security)**

2. SNS

3. Portal Website

✓ Mixed Databases

NoSQL Architecture

1. Web Application & Web Service

2. Client Library
   - ✓ The key factor
   - ✓ Query-method

3. NoSQL Database

NoSQL Vulnerabilities

1. Connection Pollution
2. JSON Injection
3. View Injection
4. Key Bruteforce

NoSQL Vulnerabilities

1. Connection Pollution
   - ✓ RESTful
   - ✓ Cross-Database/-Pool Access
   - ✓ CouchDB's Global and DB Handler

   Ex:

   - NoSQL.connect("http://".$Pool."/HIT2010/")
   - NoSQL.connect("http://POOL/".$Database)

Document-based Problem (CouchDB)

2. JSON Injection（Data）
   - ✓ DRY（Don't Repeat Yourself）
   - ✓ The weakness is String type
     - Using Collection type
   - ✓ escapeJSON()/unescapeJSON()
     - When handling tainted strings

Document-based Problem (CouchDB)

3. View Injection（Application）
   - ✓ CouchDB's view is using SpiderMonkey as Scripting Engine
     - ✓ What is “View”? CouchApp ☺
   - ✓ Predefined View and Temporary View
     - ✓ Evil Map/Reduce

Key-Value based Problem

4. Key Bruteforce
   - ✓ Schema-free ☺
   - ✓ How to make faster attacks?
     - ✓ Depends on implementation of client library & architecture
     - ✓ CHALLENGE : Can I make context-sensitive attack?

http://IP/app/action?key=1aD33rSq

Ex:

- $value = NoSQL.Get($key)

Key-Value based Problem

4. Key Bruteforce Prevention (Application-level)
   - ✓ Key Size
   - ✓ Key Space
   - ✓ Unpredictable Key Generation
   - ✓ Challenge-based

NoSQL vs. WAS

1. Unknown Error Message
   - ✓ Logic-based Blind Injection when XQL is exist
   - ✓ Time-based Differential Attack?

2. Different Types of Attack Payload
   1. Languages
   2. Schema-less
      - **Redefine Attack Surface**

        (Entry Point Sensitive than RDBMS)

3. Different Concepts of Attack

NoSQL vs. SCA

1. Checking by Data Flow，but **Diversity**
   - ✓ Unsupported Client Library

NoSQL vs. WAF

1. Key Bruteforce is not Injection Attack
   - ✓ Block by Access Threshold

2. URL Integrity Check (ex: Add Token)
   - ✓ Transparency

   Ex:

   http://IP/app/action?key=1aD33rSq**[HMAC($key)]**

   http://IP/app/action?key=1aD33rSq**&OTPtoken=sdfg23s0**

THANK YOU

Kuon@chroot.org