

PROJECT 9

SQL Injection dengan WebGoat

Kebutuhan Sistem

- Sistem Operasi Windows 7, XP atau lainnya.
- Sudah terinstal Java dan WebGoat seperti pada Project 9

String SQL Injection

1. Jalankan Webgoat seperti pada project 8, sehingga akan tampil halaman utama WebGoat pada jendela Web Browser.
2. Di bagian kiri pada jendela WebGoat, click "**Injection Flaws**".
3. Pada bagian "Injection Flaws", click "**String SQL Injection**", seperti terlihat di bawah ini.

The screenshot shows the OWASP WebGoat v5.4 interface in a Microsoft Internet Explorer browser. The address bar shows the URL: `http://localhost:8080/WebGoat/attack?Screen=36&menu=1100`. The page title is "String SQL Injection". The interface includes a navigation menu on the left with categories like "Introduction", "General", "Access Control Flaws", "AJAX Security", "Authentication Flaws", "Buffer Overflows", "Code Quality", "Concurrency", "Cross-Site Scripting (XSS)", "Improper Error Handling", and "Injection Flaws". Under "Injection Flaws", there are sub-links for "Command Injection", "Numeric SQL Injection", "Log Spoofing", "XPath Injection", "String SQL Injection", and "LAB: SQL Injection". The main content area has a "Solution Videos" section with text explaining SQL injection attacks and a "General Goal(s)" section with a form that says "Enter your last name: [Your Name] [Go!]" and a "Restart this Lesson" button. The bottom of the page has a navigation bar with buttons for "Hints", "Show Params", "Show Cookies", "Lesson Plan", "Show Java", and "Solution".

4. Click tombol **Lesson Plan** pada bagian atas. Maka akan muncul penjelasan dari pelajaran tersebut. Baca. Kemudian click tulisan yang berwarna abu-abu "**Close this window**" pada kotak text bagian bawah.
5. Kerjakan latihan. Jika bingung, gunakan tombol **Hints** atau tombol "**Solution Videos**" (bisa juga didownload di elearning).
6. Ketika telah menyelesaikan pelajaran (lesson), maka akan Nampak tanda centang hijau di sisi kiri, seperti terlihat di gambar.

Internationalization is not available for this lesson

Logout ?

Add Data with SQL Injection

OWASP WebGoat V5.3

Hints Show Params Show Cookies Lesson Plan Show Java Solution

Restart this Lesson

Solution Videos

The form below allows a user to view salaries associated with a userid (from the table named **salaries**). This form is vulnerable to String SQL Injection. In order to pass this lesson, use SQL Injection to add a record to the table.

Enter your userid:

USERID	SALARY
jsmith	20000

Created by Chuck Willis **MANDIANT**
INTELLIGENT INFORMATION SECURITY

OWASP Foundation | Project WebGoat | Report Bug

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Command Injection
Numeric SQL Injection
Log Spoofing
XPath Injection
LAB: SQL Injection
Stage 1: String SQL Injection
Stage 2: Parameterized Query #1
Stage 3: Numeric SQL Injection
Stage 4: Parameterized Query #2
String SQL Injection
Modify Data with SQL Injection
Add Data with SQL Injection
Database Backdoors
Blind Numeric SQL Injection
Blind String SQL Injection

Pelajaran SQL Injection yang lain

- Lakukan dua hal lain dengan cara yang sama (solusi bisa lihat di **WEB.pdf** yang sudah diupload di elearning atau videonya):

Modify Data with SQL Injection

Add Data with SQL Injection

- Jika sudah selesai, maka kalian bisa melihat tiga tanda centang hijau di sisi kiri, seperti gambar di bawah ini.
- Simpan gambar kirim dengan nama **NamaKamu_Proj9**.
- Upload melalui elearning.



Internationalization is not available for this lesson

OWASP WebGoat V5.3

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Command Injection
Numeric SQL Injection
Log Spoofing
XPath Injection
LAB: SQL Injection
Stage 1: String SQL Injection
Stage 2: Parameterized Query #1
Stage 3: Numeric SQL Injection
Stage 4: Parameterized Query #2
String SQL Injection
Modify Data with SQL Injection
Add Data with SQL Injection
Database Backdoors

Last modified 31-10-12