Analysis of the Havij SQL Injection tool

By bferrite

Published: 2015-05-14 · Archived: 2026-04-05 12:56:10 UTC

Havij, an automatic SQL Injection tool, is distributed by **ITSecTeam**, an Iranian security company. The name Havij means “carrot”, which is the tool’s icon.

The tool is designed with a user-friendly GUI that makes it easy for an operator to retrieve the desired data. Such ease of use may be the reason behind the transition from attacks deployed by code-writing hackers to those by non-technical users.

Havij was published during 2010, and since its, release several other automatic SQL Injection tools (such as **sqlmap**) were introduced. However, Havij is still active and commonly used by both penetration testers and low level hackers.

Havij traffic is easily identified by its user agent:

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij

Check Point’s IPS protection which detects SQL Injection attempts using this tool, “*Havij Automated SQL Injection tool*”, has detected attacks toward 30% of the monitored customers in Chek Point’s Managed Security Service.

Review of the connections’ details indicates that the majority of the detected attacks included the input ***999999.9***, usually used to scan a website for an injection vulnerability. Most of the queries had the following structure:
SELECT * FROM table_example WHERE ID = 999999.9

Error messages are not hidden. Therefore, if an error is received, the source knows the website is vulnerable to injection attempts.

Another method used by Havij is “attempting” to convert something to integer values which can’t be converted. For example, the DB name (usually a string):

SELECT * FROM table_example WHERE ID = CONVERT (int, db_name()) and 1=1

The ensuing error message exposes the DB name:

Conversion failed when converting the nvarchar value ‘BadWebsite’ to data type int.

Havij attempts to extract the tables and columns names in a similar manner

Once Havij is served with a vulnerable website, it enables the attacker to analyze the site and bring back the DB name, tables’ names and the actual data. Once the schema is received, the attacker can choose the specific columns they would like to obtain (see example below).

As Havij scans for several SQLi vulnerabilities, it is detected by other IPS protections as well. This gives us another clue on what the scanning tool looks for, namely:

- SQL Servers MySQL Vendor-specific SQL Injection
- SQL Servers Time-based SQL Injection
- SQL Servers Stack Query SQL Injection
- SQL Servers SQL Injection Evasion Techniques
- SQL Servers UNION Query-based SQL Injection

Based on the attacks detected against Managed Service customers, it seems the majority of the attacks originated from IP addresses registered in the United States, as seen in the graph below.

The easy-to-operate program, together with the free version and quick analysis, makes Havij one of the most common tools for automated SQL Injection and vulnerability assessments.
Tools such as Havij are changing the landscape of cyber attacks, as attackers no longer require the resources once needed to deploy attacks. This may also mean that not all attacks will necessarily carry information disclosure or damage – they sometimes only serve to pass a boring afternoon for a high-school kid, playing with a cool tool they found online.
