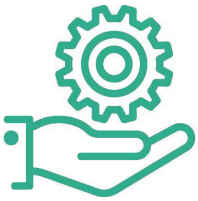
DATA-CORE SYSTEMS

Security Automation Offerings

About Security Automation



Security automation is the machine-based execution of security tasks with little to no human intervention. Automated security tasks involve everything from detecting, investigating, preventing, resolving and securing cyber-related threats. This is important regarding the overall security health of your organization's cyber properties.

The goal of automating security tasks is to make the process more streamlined so that your security team no longer has to sift through threats one by one and address them every time they come in. We can help measure security vulnerabilities through different types of assessments.

Types of Assessments

Web Application Vulnerability Assessment

Web vulnerabilities are weaknesses or misconfigurations in a website or web application's code that allows a hacker to gain control of your site. To mitigate these vulnerabilities, we can analyze and understand the security requirements, compliance and policies. Assessments are performed using automated tools and manual attack methods as per business requirements.

Types of Web Vulnerabilities

- SQL Injections / No-SQL Injections
- Cross Site Scripting (XSS)
- Broken Authentication & Session Management
- Sensitive Data Exposure
- Browser Cache Directive
- Parameter Fuzzing
- Security Misconfiguration
- Content Security Policy Header Missing
- Cross-Site Request Forgery (CSRF)

Database Vulnerability Assessment

Database vulnerabilities are weaknesses on a server or database that can be breached by hackers. Assessments for these vulnerabilities are performed using tools such as Azure Security Center for SQL Server and the like for other databases for cloud or on-premise. We perform both manual analysis and do checks using automation tools to assess the vulnerabilities. We use Microsoft Security Center to check for vulnerabilities.

Types of Database Vulnerabilities:

- Default, blank, and weak username/password
- SQL injections
- Extensive user and group privileges
- Privilege escalation
- Denial-of-service attack
- Unencrypted sensitive data at rest and in motion

Business Logic Vulnerability Assessment

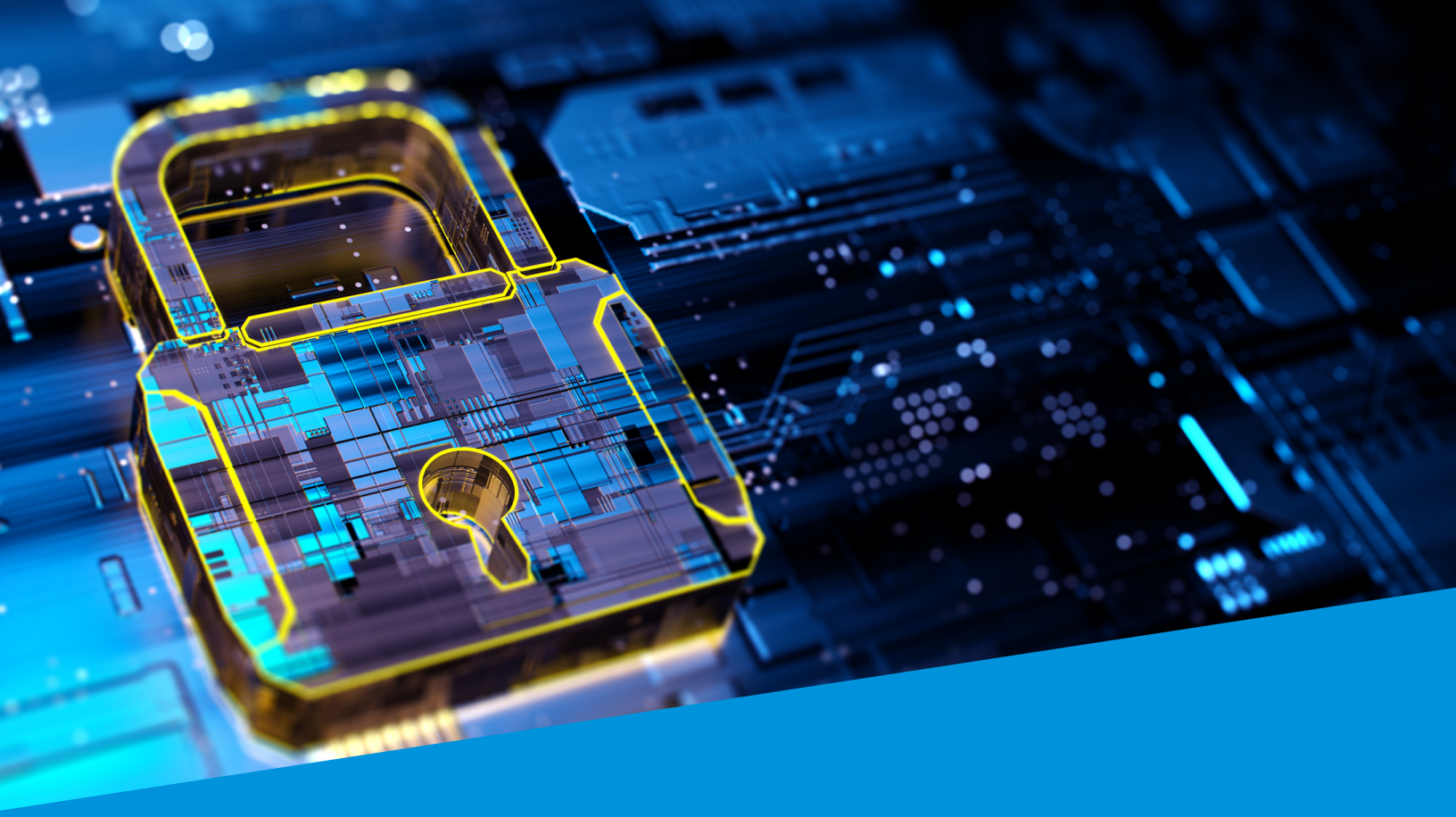
Business logic vulnerabilities are defects in the design and implementation of an application that allows hackers to manipulate the workflow behavior. We provide a complete & unique solution for assessing these vulnerabilities using 2 simple steps:

1. Review & analysis of business logic & process to identify weaknesses and prepare relevant use cases.
2. Use cases are then fed into a process automation framework and workflows are created to assess business logic vulnerabilities for complex to enterprise level applications.

Types of Business Logic Vulnerabilities:

- Role Based Access Control
- Vertical Privilege Escalation
- Horizontal Privilege Escalation
- Context-Dependent Access Controls
- Access Control Vulnerabilities in Multi-Step Processes

***For All Processes:** Data-Core interprets the results and provides remediation recommendations. We create a plan for vulnerability mitigation and repeat the scans until all vulnerabilities no longer appear on the reports.



Contact us today to get started on your securtiy automation journey.

dcs@datacoresystems.com
www.datacoreautomation.com

Tel: 215 243 1990
Toll Free: 877 327 4838
Fax: 215 243 1978

DATA-CORE SYSTEMS