



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

API Testing

API security testing entails testing the endpoints of an Application Program Interface (API) for security, correctness, and reliability, to ensure it complies with security best practices.



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



SNAPSEC.CO



WHO IS IT FOR?

- Any organisation running REST, GraphQL, and SOAP.
- Companies with their API integrated in their web application.
- Companies who have separate API as a service to their customers.



WHAT WE TEST?

- OWASP TOP 10
- Input Fuzzing
- API Logic Testing
- Excessive Role Based Testing



BENEFITS?

- Identify and fix Authorization and authentication vulnerabilities.
- Security compliance and reporting analytics that give real-time awareness of threats associated with your APIs.
- Identify missing API service method configurations.
- OWASP 10 Covers majority of the modern day web API vulnerabilities.



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Mobile Application Penetration Testing

Mobile app penetration testing exposes vulnerabilities in the cyber security posture of a mobile application, especially the case for applications that handle sensitive data and functionality.



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



SNAPSEC.CO



WHO IS IT FOR?

- Organisations who develop mobile applications that deal with sensitive information and functionalities related to the customers.
- Companies with SaaS mobile applications.
- Companies with their API integrated in their web application.



WHAT WE TEST?

- Architecture and Design issues
- Data Storage and privacy issues
- Misconfiguration Issues
- Authentication and Authorization issues
- Communication
- Underlying API issues



BENEFITS?

- Enables secure extension of business applications.
- Help meet regulatory and compliance requirements.
- Identification of exploitable security issues.
- Discover Security issues in the Underlying APIs consumed by the APP
- Customized reports will help you take both strategic and tactical decisions

**SNAPSEC.CO**

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Web Application Vulnerability Assessment and Penetration Testing (VAPT)

A Vulnerability Assessment is a quick automated examination of network devices, servers, and systems to identify fundamental vulnerabilities and configuration issues. A Penetration Test is an in-depth expert-driven activity focused on pinpointing various potential routes an attacker could use to break into the network

**SUPPORT@SNAPSEC.CO**
SALES@SNAPSEC.CO**SNAPSEC.CO**

WHO IS IT FOR?

- Businesses or organizations that want to find and eliminate security weaknesses in their Web-Apps, Publicly facing systems, and Networks that could potentially cause financial and reputational damages to the organization



WHAT WE TEST?

- Recon
- Injection Attacks
- Broken Authentication and Session Management
- Sensitive Data Exposure
- Server Side Misconfiguration
- Insufficient Security Configurability
- Unpatched Service
- Default Credentials



BENEFITS?

- Advantages of Analyzing Your IT Infrastructure
- Help meet regulatory and compliance requirements.
- Identification of exploitable security issues.
- Prioritize fixes with indepth report details
- Discover Backdoors and Miss-configurations



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Vulnerability Scanning

A vulnerability scan is automated high-level test that looks for potential security vulnerabilities in target assets, This includes scanning Internal & External Infrastructure of the company.



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



SNAPSEC.CO



WHO IS IT FOR?

- Companies which often push code to their production servers and application, because every time a code on the server changes, It affects the Application logic.



WHAT WE TEST?

- External Network
- Internal Network
- Tech Stack
- Applications



BENEFITS?

- Reduce the attack surface of your organisation.
- Quick & frequent vulnerability scanning
- Contributes to meeting data protection requirements and facilitating the security of processing
- Once configured, can be run as a repeatable process, providing ongoing, updated assurance



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Continuous Security Testing

Our Continuous Security Testing (CST) service gives you visibility of potential vulnerabilities, across your infrastructure, 365 days all around the year because traditional pentesting is not enough for large applications that are changing often.



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



SNAPSEC.CO



WHO IS IT FOR?

- Organisations who want to continually test their applications and infrastructure to keep a strict eye on any new vulnerabilities introduced to their network or application.



WHAT WE TEST?

- Architecture and Design issues
- Data Storage and privacy issues
- Misconfiguration Issues
- Authentication and Authorization issues
- Communication
- Underlying API issues



BENEFITS?

- Continues surveillance on your application and network security.
- Continuous Attack Surface Management.
- Balanced Vulnerability Reporting.
- Cost Efficiency.



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Access Control Model Evaluation (Role Based Testing)

We make sure to test your Access control for all kind of escalations that are possible, Plus out f uses their specially crafted (Forward | Backward) Approached to test your Access control Model



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



SNAPSEC.CO



WHO IS IT FOR?

- SaaS business which are using any Role-based or Access-Control technologies.
- Application which allows their customers to invite new members.
- Applications that allows to create teams and have different roles to different members.



WHAT WE TEST?

- Role Based Access Control (RBAC)
 - Identify BAC(broken access control issues)
 - Permission Overrides Issues
 - IDORS
 - Authorization issues
- Missing Permission checks



BENEFITS?

- Identify privilege escalation in your web-app/Api.
- Get full insights on your access control models.
- Identify permission overrides in your web-app/Api.
- Customized reports will help you understand the privileges set around different roles in the application.



SNAPSEC.CO

FIND YOUR WEAKNESSES, BEFORE THE BAD GUYS DO.

Infrastructure Penetration Testing

Infrastructure penetration test uncovers vulnerabilities residing within your infrastructure with a detailed attack narrative to properly assess the impact of each finding. With a manual focus, our services begin with the latest tools and technologies and leverage them to identify improvements in even the most sophisticated environments.



SUPPORT@SNAPSEC.CO
SALES@SNAPSEC.CO



[SNAPSEC.CO](https://www.snapsec.co)



WHO IS IT FOR?

- Infrastructure testing is for organisations who wish to gain a real-world view of their security posture in terms of their -
- infrastructure, This service allows them to keep good track of their externally facing servers, devices, domains, Ip's, Application and Services running on the staging and production systems



WHAT WE TEST?

- Unpatched Services
- Default/Weak Configuration issues
- Input Fuzzing
- OWASP TOP 10
- Relative CVE's
- Service Related Flaws
- External Network scanning
- Cryptographic Flaws
- 3rd party Attacks



BENEFITS?

- Identifying potential areas that are vulnerable to data compromise and disclosure.
- Identify Unpatched domains and servers.
- Incorrectly configured database servers.
- Identify server/application vulnerable to default credential attacks.
- Validation of high-severity results through manual verification process