# AINA

## Breach Simulator

Real-World Cybersecurity Training in a Fully Controlled Environment

Powered by Rocheston

# Welcome to AINA

Rocheston AINA Breach Simulator brings together realism, safety, and precision in one complete cybersecurity training platform. It is built for both professionals and students who want to experience real-world attacks in a fully controlled lab setting.

AINA gives users the freedom to launch and observe web application breaches without any risk to live systems, making it a reliable and practical tool for cybersecurity learning and enterprise validation.

### 100+ Vulnerable Apps

Realistic targets across banking, e-commerce, healthcare, and more

### Live Telemetry

Real-time monitoring of every attack step and outcome

### Complete Safety

Sandboxed environment with kill switches and rate limits

### Detailed Reports

Exportable documentation with MITRE ATT&CK mappings

# Platform Features

## Extensive Target Library

The simulator operates within Rose X OS and comes with a large collection of more than 100 intentionally vulnerable web applications. These cover a wide range of industries and use cases — banking, e-commerce, universities, hotels, healthcare, gaming, and more. Each site contains realistic weaknesses such as SQL injection, XSS, CSRF, SSRF, IDOR, and file inclusion.

## Deterministic Simulation

Users can select which targets to test, choose their MITRE ATT&CK tactics, and launch the simulation. Every run is deterministic, meaning it follows exactly what the user configures — no random actions, no guesswork. This ensures consistent, reproducible training scenarios.

## Real-Time Monitoring

During each exercise, AINA streams live telemetry, showing every step, status, and result in real time. You can see the tactics used, the point of entry, and the impact as it unfolds. This visual feedback transforms abstract concepts into tangible cybersecurity understanding.

## Comprehensive Reporting

When the run finishes, the simulator automatically generates detailed reports with timestamps, success and failure data, and tactic mappings, all in a clear, exportable format. These reports can be used for training records, SOC analysis, or compliance documentation.

# Who Benefits from AINA?

## RCCE Students

AINA is the perfect bridge between theory and hands-on experience. It allows learners to practice real attack techniques, observe telemetry, understand response behavior, and gain a true understanding of how web vulnerabilities work in practice.

- Hands-on practice with real attack vectors
- Safe environment for experimentation
- Build job-ready cybersecurity skills

## Enterprise Teams

For enterprise teams, AINA becomes a validation tool—used to measure detection speed, incident handling, and defensive capability across multiple simulated scenarios.

- Test SOC detection capabilities
- Validate security controls
- Measure incident response effectiveness

## Key Benefits

### Time Savings

Eliminates hours of manual lab setup, allowing focus on actual learning and analysis

### Measurable Results

Generate exportable reports for training records and compliance documentation

### Scalable Platform

From individual learners to enterprise-wide security validation programs

# Safety & Control

AINA was designed to make cybersecurity education visual, interactive, and measurable. The system is fully governed by strict safety controls to ensure every simulation remains secure.

### Sandboxed Environment

All simulations run in completely isolated environments with no access to production systems or live data

### Global Kill Switch

Instant termination capability allows administrators to stop any simulation immediately if needed

### Rate Limiting

Built-in controls prevent resource exhaustion and ensure fair usage across all users

### Dry-Run Preview

Review simulation parameters and expected outcomes before execution to prevent mistakes

## Enterprise-Grade Security

Every aspect of AINA has been designed with security in mind. From the isolated execution environment to comprehensive audit logging, the platform ensures that training exercises never pose a risk to real systems or data. Organizations can confidently deploy AINA knowing that their security posture remains intact while their teams gain invaluable hands-on experience.

# Transform Your Cybersecurity Training

With AINA, breach simulation is no longer limited to elite red teams or expensive enterprise systems. It's now accessible, structured, and measurable, ready to transform how cybersecurity training is delivered.

Every launch demonstrates Rocheston's commitment to redefining how cybersecurity professionals learn, test, and evolve in a constantly changing digital world. The platform bridges the gap between theoretical knowledge and practical application, providing learners with the experience they need to succeed in real-world scenarios.

## Ready to Get Started?

Experience the future of cybersecurity training with AINA Breach Simulator

**100+**

Vulnerable Applications

**Real-Time**

Telemetry & Monitoring

**100%**

Safe & Sandboxed

Whether you're an aspiring cybersecurity professional looking to build practical skills or an enterprise team seeking to validate your defensive capabilities, AINA provides the comprehensive, realistic training environment you need. The platform's combination of safety, realism, and measurability makes it an essential tool for modern cybersecurity education and validation.

# Rocheston

Empowering the next generation of cybersecurity professionals through innovative training platforms and real-world simulation technology

AINA Breach Simulator

Powered by Rose X OS