

# RAMPART™ RED TEAM REPORT FINDINGS

Enhancing Application Security with Robust Detection and Blocking Capabilities

The Rampart™ Red Team Report presents the findings of a comprehensive assessment conducted on the Miniblog.Core application, utilizing the Rampart application security tool. The objective of the assessment was to evaluate the capabilities of Rampart in detecting and blocking both known and unknown vulnerabilities, as well as malicious behaviors while maintaining the intended functionality of an application. This case study highlights the key findings and implications of the report.

## KEY FINDINGS

### Successful Detection and Blocking of Previously Unknown Vulnerabilities:

Rampart demonstrated its effectiveness in detecting and blocking previously unknown vulnerabilities.

### Detection of In-Scope Vulnerabilities:

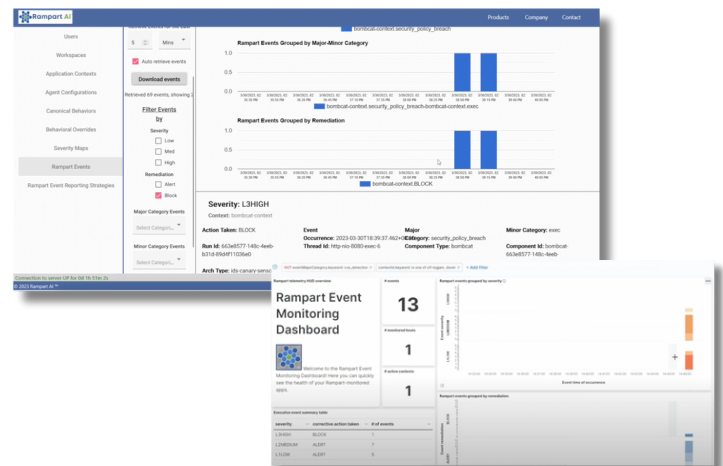
All vulnerabilities within the defined scope of the assessment were effectively detected and blocked by Rampart. These included simulated known vulnerabilities, as well as an additional previously unknown vulnerability discovered during the testing process. The successful identification of these vulnerabilities underscores Rampart's ability to provide comprehensive protection against a range of potential threats.

### Preservation of Application Functionality:

Rampart's implementation did not result in any noticeable loss of functionality. Despite actively detecting and blocking malicious behaviors, the fortified application continued to operate as intended. This highlights the seamless integration of Rampart within the existing application infrastructure and its capacity to safeguard against threats without compromising user experience.

### Prevent the triggering of a backdoor during both soft-enforce and hard-enforce modes:

Rampart successfully prevented the backdoor logic from running, ensuring that no root access was granted to potential attackers. This demonstrates Rampart's potential to proactively protect applications against unauthorized access and maintain the integrity of sensitive data.



## AT A GLANCE

### Detect & Block

- Previously unknown vulnerabilities
- All in-scope vulnerabilities
- Prevents triggering of backdoors in both soft-enforce and hard-enforce modes

### Application Functionality

- Application operates as intended
- Seamless integration
- Safeguard against threats without compromising user experience