Introduction to the OWASP Top 10 – 2021

Risk A9: Security Logging and Monitoring Failures

Key Concepts

Key Concept 1: Event Logging

- Provides a standard, centralized way of recording important software events
- Records events from various sources and stores them, typically, in a single collection, called an event log

Key Concept 2: Event Monitoring

- The process of collecting, analyzing, and signaling event occurrences
- The process of collecting events in our event log
- Collected for future analysis

Key Concept 3: Security Logging and Monitoring

- This is the process of logging and monitoring events that can impact the confidentiality, integrity, or availability of our software
- Not a specific risk leading to compromised software

Additional Information

A9 is unique in that it is not a specific risk that leads to compromised software. Good security logging and monitoring processes help us resolve information security incidents, perform forensic investigations, and (among other things) protect our applications from future attacks.

Event logging provides a standard, centralized way of recording important software events. This process records events from various sources and stores them (typically) in a single collection called an event log. As an example, think of the Operating System (O/S) of the computer, from which you are viewing this training. This (O/S) has an event log, where important things happening are collected and stored.

Event Monitoring is the process of collecting, analyzing, and signaling event occurrences. Think of event collection as the process of collecting events in our event log. We do not just collect events for the sake of it; we collect them knowing that they will be analyzed in future.

Combining the previous two terms, Security Logging and Monitoring is the process of logging and monitoring events that can impact the confidentiality, integrity, or availability of our software.

Definition

Having auditable events, warnings and errors within our web application or API, which are not adequately logged.

To have adequate logging, developers and security staff must work together

- Agree on a security centric logging standard
  - Developers know exactly what needs to be logged
  - Security teams need to monitor logs for suspicious activity
- A proper logging infrastructure is necessary to securely collect and store logs
  - Having adequate logging infrastructure is a *prerequisite* to be able to analyze the logs

Additional Information

The definition of A9 of 2021 – Security Logging and Monitoring Failures – is having auditable events, warnings, and errors within our web application or API that are not adequately logged.

To have adequate logging, developers and security staff must work together and agree on a security centric logging standard. Having a logging standard will enable developers to know exactly what events they need to log. Inversely, security teams need to be able to monitor logs for suspicious activity. It is important to have auditable events on actions, such as logins, failed logins, and high-value transactions, and similar.

The proper logging infrastructure is necessary to securely collect and store logs. Having adequate logging infrastructure is a prerequisite to be able to analyze the logs collected. As one example, developers need to have understood what a brute force attack on the login page would look like from a login perspective. This will then enable security teams to build alerts when such brute force attacks take place.

Example

To demonstrate our good and bad example, consider our application has a set of actions, that only an administrator of the web application can perform. Following secure development practices, we check that our user has indeed permission to access the specific administrative action.

Bad Example

```
if (!user.hasAccess("ADMIN_ACTION")) {
 //quietly deny access
}
```

Good Example

```
if (!user.hasAccess("ADMIN_ACTION")) {
 //deny access and log
 log.event(Event.SECURITY, Event.CRITICAL,
          "User attempted to access admin  action without permission");
}
```

Additional Information

In our bad example, despite checking the correct permissions are in place, we deny access and not log anything relating to this failed access attempt. A normal user attempted to access something meant for the administrator has no event logged.

In our good example, for the invalid access attempt, we want to log that the user attempted to access the specific admin action, without having the permission to do so.

Challenges

- Developers are unaware of the security events that they need to log
  - Appropriate alerting thresholds and response escalation processes are not in place, or effective
  - Leads to applications that cannot detect, escalate, or alert for attacks or suspicious activity

- Incident response/security operations teams do not know enough about how the application is working and what should be logged
  - Security staff may not have the development experience to know how suspicious activities need to be logged
  - Security staff may not have the deep experience with how exactly how complex software is supposed to work properly

Additional Information

We now understand how the risk of security logging and monitoring failures can materialize, let us look at why this is a common issue.

Developers are often unaware of the security events that need to be logged. This can be because appropriate alerting thresholds and response escalation processes have not been defined. It could also be because response escalation processes might be in place but are not effective. This can lead to web applications or APIs that cannot detect, escalate, or alert on attacks or suspicious activity.

Incident response and security operations teams might not know enough about how the application is logging. When developing software, we often forget how suspicious activities need to be logged. Security logging and monitoring requires us to think of what actions are important within our web application or API.

This requires further analysis and time to develop best logging and reporting for suspicious activities or attacks.

Logging and monitoring can be challenging to test, often involving interviews, or asking if attacks were detected during a penetration test.

Best Protection Strategies

BEST

Build a secure logging infrastructure for collection and storage of logs long term

Ensure all authentication and access control events, both failed and successful, are logged

Standardize machine-readable formats for events and alerts

Test incident response based on logging events

Additional Information

Above you have some of the best protection strategies against A9 of Top 10 – Security Logging and Monitoring Failures.