Security Logging and Monitoring Report

Chameleon Security Team

Authors:

Name:	Student ID:	Team:
Rewniz Patell	221267802	Chameleon Security
Usman Tariq	(s)217034263	Chameleon Security

Table of Contents

Summary:

This report was written and researched by Rewniz Patell and Usman Tariq from the Chameleon Security Team. This report involves introducing the concepts of security logging and monitoring, the importance of effective security logging for web applications and websites, and the significance of ensuring that proper monitoring protocols are in place to suggest solutions based on log activity. Additionally, the importance of security logging and monitoring is showcased within the OWASP top ten most common web application threats, and how certain attacks could be conducted, and become successful if inadequate security logging and monitoring is implemented. Additionally, the report provides solutions and preventions of failures, and applies these to the Chameleon Organization infrastructure, and how these could be implemented within Chameleon systems to ensure that Chameleon Security and data would not be compromised by an attacker, or important systems do not fail to function due to high internet traffic attacks. Furthermore, it was concluded that if Chameleon was to expand its web applications and store customer data, proper regulatory standards for security logging and monitoring would need to be implemented to ensure that the organization meets governmental standards.

Introduction:

Security logging and monitoring is a two-part process that is utilized to monitor security events within a system or technology infrastructure. Security events are when there is a change in normal behavior within a cyber security system. Security events could include a lapse in security due to a server powering off or not functioning properly, an employee flagging a suspicious spam email, or an employee downloading a authorized software to a company device. Security events can be positive, such as an employee downloading an authorized software or negative, such as an employee downloading an unauthorized and potentially malicious software [1].

Security logging is the first part of the security logging and monitoring process and involves logging all security events in order to keep tabs on security events, and potential threats or vectors that could be exploited. The second part of the process is the monitoring of security events. This involves members of an organization examining the logged events, and investigating whether the event could be malicious or harmful to the organization, or whether an unauthorized may have access to the company infrastructure. If this is the case, the logged security event would be flagged, and then further investigated before taking necessary measures [2].

Security logging and monitoring is vital to organizations to ensure that they are aware of potential attacks, or vectors of attacks. Therefore, effective logging and monitoring is extremely important. Logging and monitoring protocols should have methods to weed out unnecessary information such as non-security events or non-critical events. Effective logging should focus on

- logging any scanning or reconnaissance from attackers such as port scanning, or IP scanning
- analyzing potential packages or packets that have exploits,
- monitoring organization devices to ensure malware is not installed or executed
- mitigating control of potential attackers, by having failsafe measures
- monitoring privileges to avoid privilege exploitation or escalation
- logging and analyzing when potential attackers gain access to a server or system, and effectively take back control of the environment

Importance of Security Logging and Monitoring:

Ineffective security logging can cause negative security events or major attacks to not be logged within a database, causing a scenario where the organization is unable to correctly and accurately monitor security threats or attacks conducted against their systems. Furthermore, logging too many unnecessary events can cause clutter within the database, meaning that the security analysts would be unable to filter out unnecessary security events with important and potentially harmful security events. Additionally, ineffective monitoring can cause situations where important security events are logged within the database, but the organization does not have the required resources, manpower or mitigation strategies to monitor, analyze and take effective action to mitigate attacks or exploit vectors. As a result, effective security logging and monitoring is important to any organization's infrastructure and data.

The Open Worldwide Application Security Project (OWASP) is an online community that produces tools, documentation, articles and research into web application security, IoT and system security. In 2021, OWASP released a standard awareness document for developers of web applications to educate the community on web application security and emerging web application security risks [3]. The document included a list of the top ten web application security risks, ranging from the most common reported risk in web development security, all the way to the tenth most common reported risk. At ninth was security logging and monitoring failures. This moved up one spot from the previous top ten report, indicating that security logging and monitoring failures are becoming increasingly prevalent within the web application industry.

The OWASP top ten report includes failures such as high-value bank transactions, multiple successive failed logins not being reported, errors generating unclear or no log messages, logs only being stored locally and not backed up, application logs and APIs not being monitored, penetration testing and scans (such as OWASP ZAP) don't trigger alerts or logs, improper logging that does not provide context or meaningful information, and no detection or alerts for active attacks [4].

Prevention of Failures and Solutions:

To prevent failures such as the ones previously listed, developers can implement strategies to mitigate these failures and provide effective security logging and monitoring. Prevention methods include,

- Ensuring all login, access control, server-side input validation failures are logged, so that they can be monitored.
- Ensure that all logs are stored correctly and backed-up, not just locally stored. Data recovery of logs and RAID configuration could be considered to avoid data loss and ensure data recovery is achievable. Additionally, ensuring that logs are held for a long enough time that delayed analysis can be conducted, or analysts are able to pull dated logs to compare with analyzed logs for context.
- Ensure user validation and encoding of log data, to avoid injections or attacks on the logging and monitoring infrastructure. This would help to ensure that attackers are not able to delete or modify logs to cover their methodologies and attack vectors.
- Ensure that high-value banking transactions are logged, in scenarios where they need to be analyzed.
- Ensure permissions for employees and members are assigned effectively, so that logs can't be deleted or modified if employee credentials are compromised by an attacker. This can be done by ensuring that most employees have privileges to only add logs, and few required employees have the privilege to modify or delete logs after analysis.
- Establish correct protocols to security events, to ensure that once a security event is logged and analyzed, effective reporting and action can be taken.
- Documentation of all analyzing and monitoring, so that members can understand previous security events and understand action that was taken to mitigate risks in the past.

[5].

Solutions for the Chameleon Organization:

The Chameleon Organization has multiple websites with front-end functionality such as the Chameleon Website, the MOP platform and the Chameleon Security website. Ensuring that proper security logging and monitoring is conducted within these websites is vital to ensure that attackers do not cause issues to the website or attempt to compromise the system. Ensuring that user validation is built into the websites, detailed and concise logging, and occasional monitoring from the security team and the website development team would help to ensure that solutions and mitigations are conducted when there is a potentially serious security threat. Firstly, ensuring that proper logging is conducted when there are security events such as numerous login attempts, attempted injection attacks, and documentation of security events would help to ensure that there is adequate logging of these security events. Additionally, monitoring these logs and suggesting solutions to ensure that the security of the websites and platforms is paramount, to ensure that malicious attackers do not gain access or conduct damaging attacks to the Chameleon infrastructure.

Furthermore, if Chameleon web applications expand in the coming years, or if Chameleon products become frequently used by Deakin University Students (such as the Ontrack project, or Deakin Blackboard), implementing security logging and monitoring would become increasingly important. With more students using these systems, they would naturally become more likely to be targeted by attackers, as more internet traffic is moving between these systems and its users. Additionally, if these websites and the organization stores customer or user data such as passwords, emails, student enrollment information and other identifiable information, it would become increasingly important to ensure that security measures are in place to protect that data from malicious attackers. Implementing effective security logging and monitoring measures would be of paramount importance when customer data is stored, as the organization and Deakin would need to meet customer data security guidelines and standards. Additionally, Australian Government does have security and event logging policies for websites that store a moderate to large amount of customer data, to ensure that websites and organizations adequately protect user data and credentials. While not necessary to implement in the present due to the Chameleon projects currently not storing data, it may become necessary in the future as these web applications expand. Guidelines such as ISM-0585; Revision: 5 standards would need to be met to effectively log important details for the event log to be useful, and ISM-1906; Revision: 0 guidelines would need to be met to ensure that event logs are analyzed in a timely manner where internet facing servers and infrastructure is implemented within the organization [6].

Conclusion:

Security logging and monitoring is an important component of developing and maintaining web applications. Security logging and monitoring failures are becoming increasingly common, with the OWASP top ten researching that these failures are among the biggest contributors of web application flaws. Implementing measures to avoid common logging and monitoring failures would ensure that web applications developed by Chameleon Security are adequately protected, and the security standard is maintained to safeguard website systems and data. Furthermore, if Chameleon platforms do expand and store customer data, it would be required for the organization to follow all security logging and monitoring guidelines set by the Australian Government and other relevant regulatory standards.

References (IEEE):

[1] J. Miller (2019) BitLyft 'Security Incident vs Event : What's the Difference' [Website]. Available: https://www.bitlyft.com/resources/security-incident-vs-event-what-is-the-difference

[2] J. Miller (2019) BitLyft 'What is Security Logging and Monitoring' [Website]. Available: https://www.bitlyft.com/resources/what-is-security-logging-and-monitoring

[3] The Open Worldwide Application Security Project (OWASP) (2021) 'OWASP Top Ten' [Website]. Available: https://owasp.org/www-project-top-ten/

[4] The open Worldwide Application Security Project (OWASP) (2021) 'A09:2021 – Security Logging and Monitoring Failures' [Website]. Available: https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/

[5] J. Clements. Foresite Cybersecurity (Unknown date) 'OWASP Top Ten: #9 Security Logging and Monitoring Failures' [Website]. Available: https://foresite.com/blog/owasp-top-ten-9-security-logging-and-monitoring-failures/

[6] Cyber.Gov. Australian Cyber Security Centre (Unknown date) 'Guidelines for System Monitoring' [Website]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring