OWASP Top 10:2021

A09:2021 – Security Logging and Monitoring Failures

Jalaj Bhaskar
@ Null : Delhi Chapter
Airtel Center, Gurgaon
4th November 2023

Jalaj@null:~$ whoami

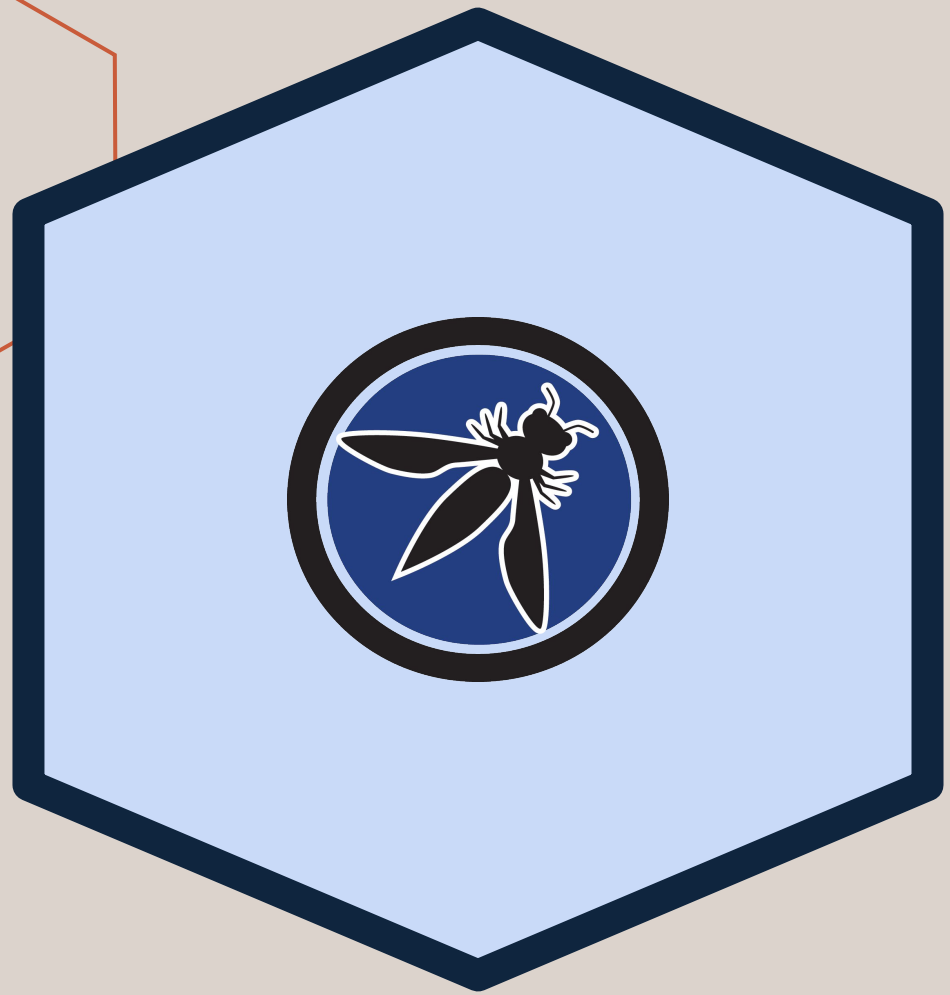
- Cybersecurity Geek
- Blue Team’er (SOC Analyst)
- Exploring the world of IR and Threat Hunting
- CRAC Learning
- MMA and Bikes
- Have a question / want to connect ?
  - Telegram : @senditfast

Agenda


Introduction
A09
Failures and Attacks
Prevention
Conclusion and QnA

OWASP Top 10:2021

The OWASP Top 10 is a de facto industry standard that provides a list of the 10 Most Critical Web Application Security Risks



1. Broken Access Control
2. Cryptographic Failure
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. **Security Logging and Monitoring Failures**
10. Server-Side Request Forgery (SSRF)

Security Logging and Monitoring Failures

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

There isn't much CVE/CVSS data for this category, but **detecting and responding to breaches is critical.** Still, it can be very impactful for accountability, visibility, incident alerting, and forensics.

➔ Mapped CWEs

- CWE-117 Improper Output Neutralization for Logs
- CWE-223 Omission of Security-relevant Information
- CWE-532 Insertion of Sensitive Information into Log File
- CWE-778 Insufficient Logging

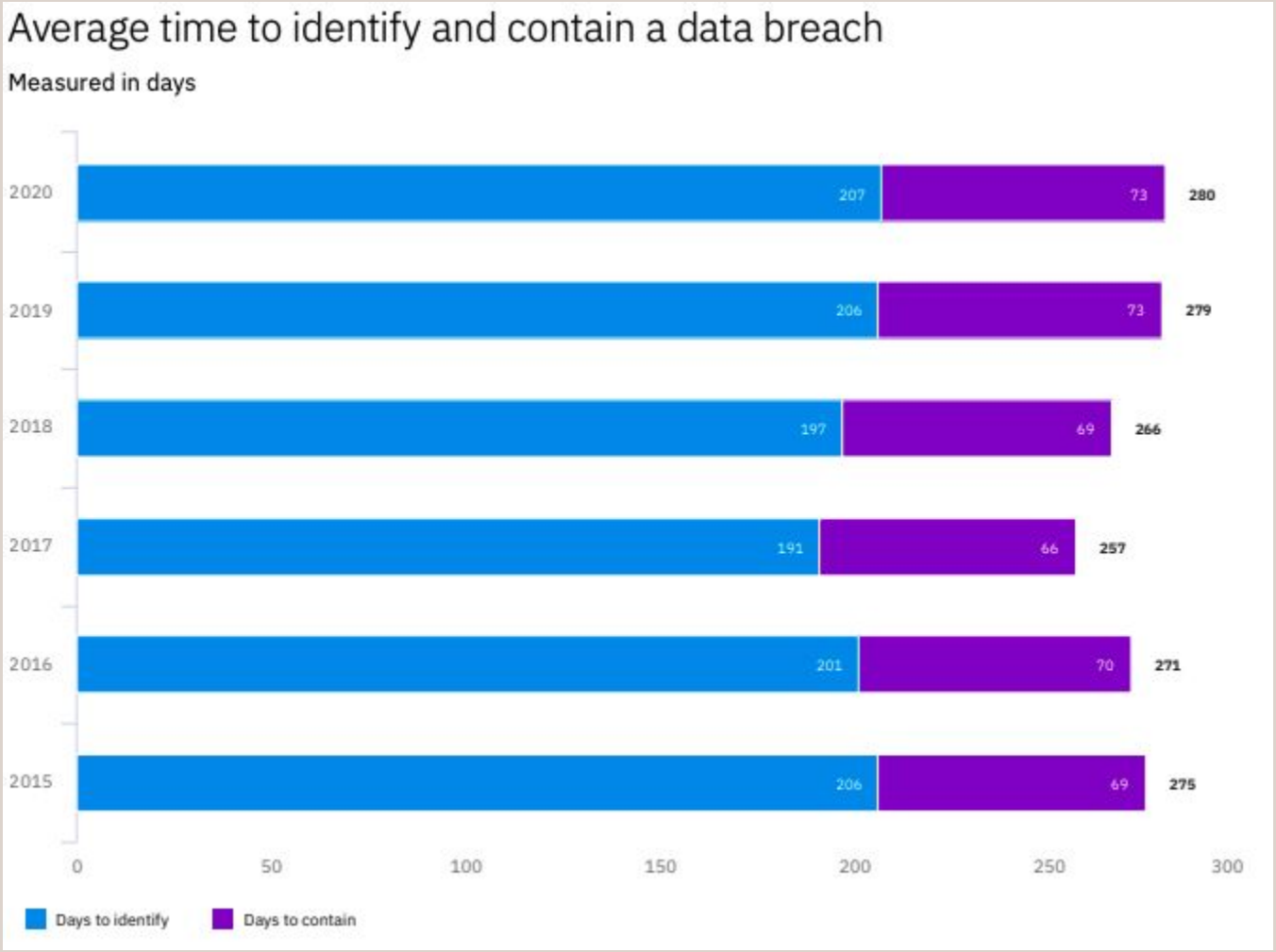

SANS Cyber Defense
@SANSDefense
"Sunlight is the best disinfectant. Malware festers in the darkness." - @eric_conrad
Don't miss more gems of wisdom like this at the #BlueTeamSummit: sans.org/u/1paL
8:01 PM · Jun 12, 2023 · 668 Views

```
::ffff:115.110.154.68 - - [17/Dec/2022:14:02:44 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-version HTTP/1.1" 200 20 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-version HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/languages HTTP/1.1" 200 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/products/search?q= HTTP/1.1" 200 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:56 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 624 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:56 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:56 +0000] "GET /api/Quantitys/ HTTP/1.1" 200 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:44:56 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:03 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/user/whoami HTTP/1.1" 200 11 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/user/whoami HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "POST /rest/user/login HTTP/1.1" 200 834 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/user/whoami HTTP/1.1" 200 134 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/user/whoami HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/products/search?q= HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /api/Quantitys/ HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:18 +0000] "GET /rest/basket/1 HTTP/1.1" 200 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:29 +0000] "GET /rest/saveLoginIp HTTP/1.1" 200 344 "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:45:29 +0000] "GET /rest/products/search?q= HTTP/1.1" 304 - "http://3.110.234.194:81/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"

::ffff:115.110.154.68 - - [17/Dec/2022:15:47:11 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://3.110.234.194:81/?user=(%20!%20)%3C/span%3E%20Warning:"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
::ffff:115.110.154.68 - - [17/Dec/2022:15:47:11 +0000] "GET /rest/admin/application-version HTTP/1.1" 304 - "http://3.110.234.194:81/?user=(%20!%20)%3C/span%3E%20Warning:" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36"
```

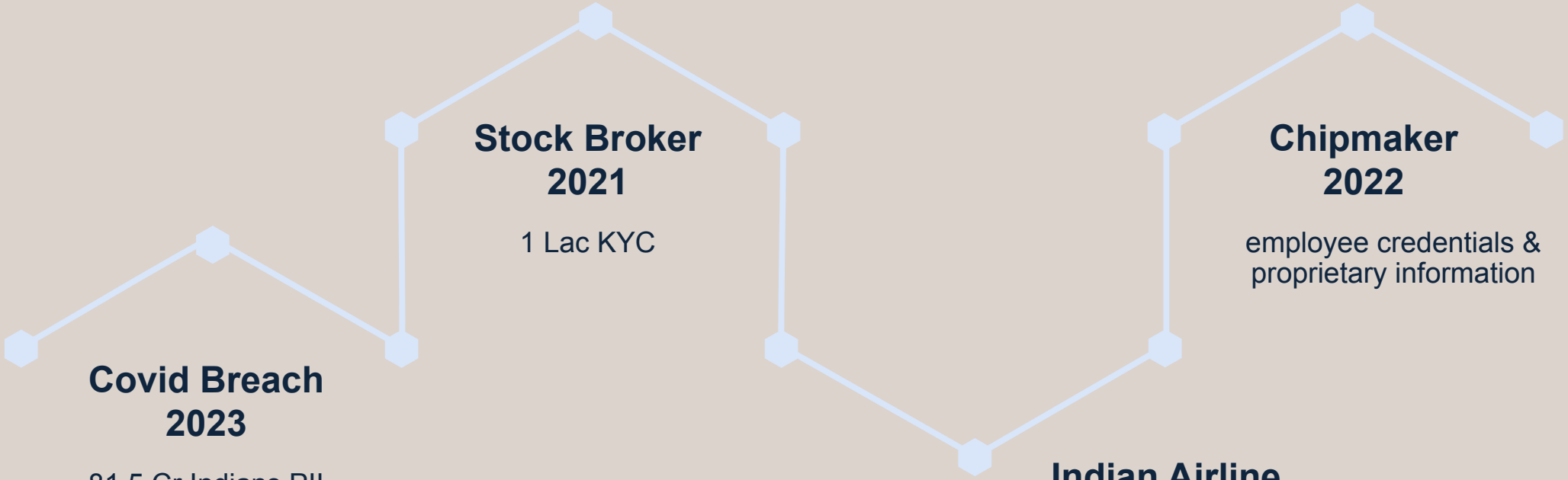
"...the goal of logging is to be able to alert on specific security events..."

- **High value transactions** are not logged.
- **Unclear** log messages.
- Logs **not monitored** for suspicious activity.
- Alerting **thresholds** and response escalation processes are not in place.
- Alert for active attacks in real-time or **near real-time**.



Application Logging Vocabulary Cheat Sheet 🔗

Attacks



Covid Breach
2023

81.5 Cr Indians PII

Stock Broker
2021

1 Lac KYC

Indian Airline
2021

45 Lac PII

Chipmaker
2022

employee credentials &
proprietary information

Prevention

1. Ensure **proper logging of failures with user context** for suspicious account identification and retention for forensic analysis.
2. Generate log data in easily **consumable formats** for log management solutions.
3. **Encode log data correctly** to prevent injections or attacks on the logging system.
4. Implement audit trails for **high-value transactions** with integrity controls to prevent tampering or deletion.
5. Establish effective monitoring and alerting to **quickly detect and respond** to suspicious activities.
6. Develop an **incident response plan**, following recognized frameworks like NIST 800-61r2 or later, to handle security incidents.

Thank you,
Any Questions ?

Resources