



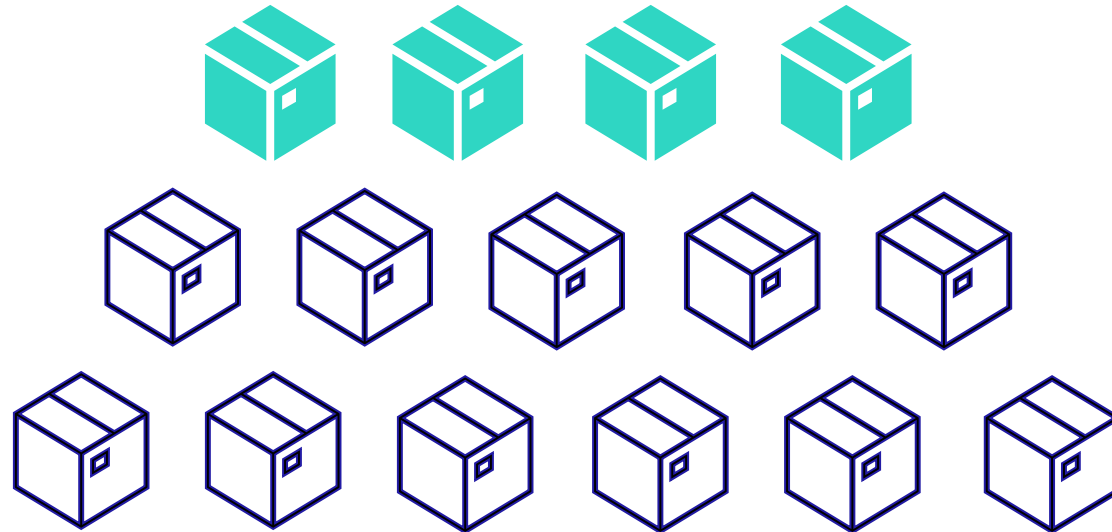
# Why Securing Your Open Source Components Is Critical for AppSec Success

Matt Stanchek

Fortify on Demand Architect

# The Use of Open Source

A modern application can include Open Source software as more than 50% of its total codebase



# Security Risks from Using Open Source

- Vulnerabilities in Open Source components are inherited by your application
- Many Open Source components use *other* Open Source components as dependencies
- Vulnerabilities are public
- Exploits are public

# Open Source, Open Exploit

The image shows a screenshot of the Exploit Database website and a National Vulnerability Database (NVD) entry for CVE-2017-5638. The Exploit Database entry is for "Struts2/XWork < 2.2.0 - Remote Command Execution".

**Exploit Database Entry:**

- EDB-ID:** 14360
- CVE:** 2010-1870
- Author:** MEDER KYDYRALIEV
- Type:** REMOTE
- Platform:** MULTIPLE
- Exploit:** Download icon / Code icon
- EDB Verified:** ✗

**NVD Entry (CVE-2017-5638):**

- Severity:** CVSS Version 3.x: 10.0 CRITICAL; CVSS Version 2.0: 10.0 CRITICAL
- Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- Current Description:** The Jakarta Multipart parser in Apache Struts 2.2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd=string.
- QUICK INFO:**
  - CVE Dictionary Entry:** CVE-2017-5638
  - NVD Published Date:** 03/10/2017
  - NVD Last Modified:** 03/03/2018
  - Source:** MITRE

**Exploit Database Comment:**

Friday, July 9, 2010  
CVE-2010-1870: Struts2/XWork remote command execution  
Update Tue Jul 13 2010: Added proof of concept

Apache Struts team has announced uploaded but has not released, due to an unreasonably prolonged voting process for a new version of the framework which fixes vulnerability that I've reported to them on May 31st 2010. Apache Struts team is ridiculously slow in releasing the fixed version and all of my attempts to expedite the process have failed.

**Introduction**  
Struts2 is Struts + WebWork. WebWork in turn uses XWork to invoke actions and call appropriate setters/getters based on HTTP parameter names, which is achieved by treating each HTTP parameter name as an OGNL statement. OGNL (Object Graph Navigation Language) is what turns:

```
user.address.city=Bishkek&user['favoriteDrink']=kumys
```

into

# OWASP Top 10

## *A9:2017-Using Components with Known Vulnerabilities*

*Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application.*

*If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.*

*Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.*

T10 OWASP Top 10 Application Security Risks – 2017	
<b>A1:2017-Injection</b>	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
<b>A2:2017-Broken Authentication</b>	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
<b>A3:2017-Sensitive Data Exposure</b>	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
<b>A4:2017-XML External Entities (XXE)</b>	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
<b>A5:2017-Broken Access Control</b>	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
<b>A6:2017-Security Misconfiguration</b>	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
<b>A7:2017-Cross-Site Scripting (XSS)</b>	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
<b>A8:2017-Insecure Deserialization</b>	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
<b>A9:2017-Using Components with Known Vulnerabilities</b>	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
<b>A10:2017-Insufficient Logging &amp; Monitoring</b>	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

# Legal Risks from Using Open Source

- Some Open Source licenses are more restrictive than others
- Several licenses have “interesting” requirements
- Patent trolls



# Demonstration

# Wrap Up

- Bill of Materials (BoM)
- Issue transparency
- Seamless experience





**Thank You.**



MICRO<sup>®</sup>  
FOCUS