PRESENTATION ON “VULNERABLE AND OUTDATED COMPONENTS”

Course: CSC 577 - Enterprise Security Management

Presented by:
Md Kausar Hamid Miji
South Dakota School of Mines and Technology

AGENDA

- Introduction to OWASP
- What is OWASP Top 10
- The Open-Source Ecosystems
- Overview of Vulnerable and Outdated Components
- Impact of Vulnerable and Outdated Components
- Ways of mitigation
- Examples
- A simple XSS Demo
- Conclusion

WHAT IS OWASP?

OWASP

Open Web Application Security Project

OWASP is an international non-profit organization whose mission is to secure web.

OWASP provides tools, resources, education, training and community events to developers, hackers, and technologists.

OWASP Top 10

Webgoat

Zed Attack Proxy (ZAP)

Web Security and Testing Guide

Juice Shop

Mobile Security Testing Guide

Mobile App Security Requirements and Verification

OWASP PROJECTS

What is in OWASP TOP 10

OWASP TOP 10 WAS FIRST RELEASED IN 2003…LATEST 2021…

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A4:2017-XML External Entities (XXE)
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

THE OPEN-SOURCE ECOSYSTEMS

10+ Million GitHub code repositories

2500 public binary repositories

Different packaging systems for same function

Different coordinates systems and level of granularity

Ref. WebGoat

OVERVIEW OF VULNERABLE AND OUTDATED COMPONENT

- What is Vulnerable and Outdated Component?
- A vulnerable and outdated component is a software component that is no longer being supported by the developer, making it susceptible to security vulnerabilities. Many times, a component has known vulnerabilities that don't get fixed due to a lack of maintainer.

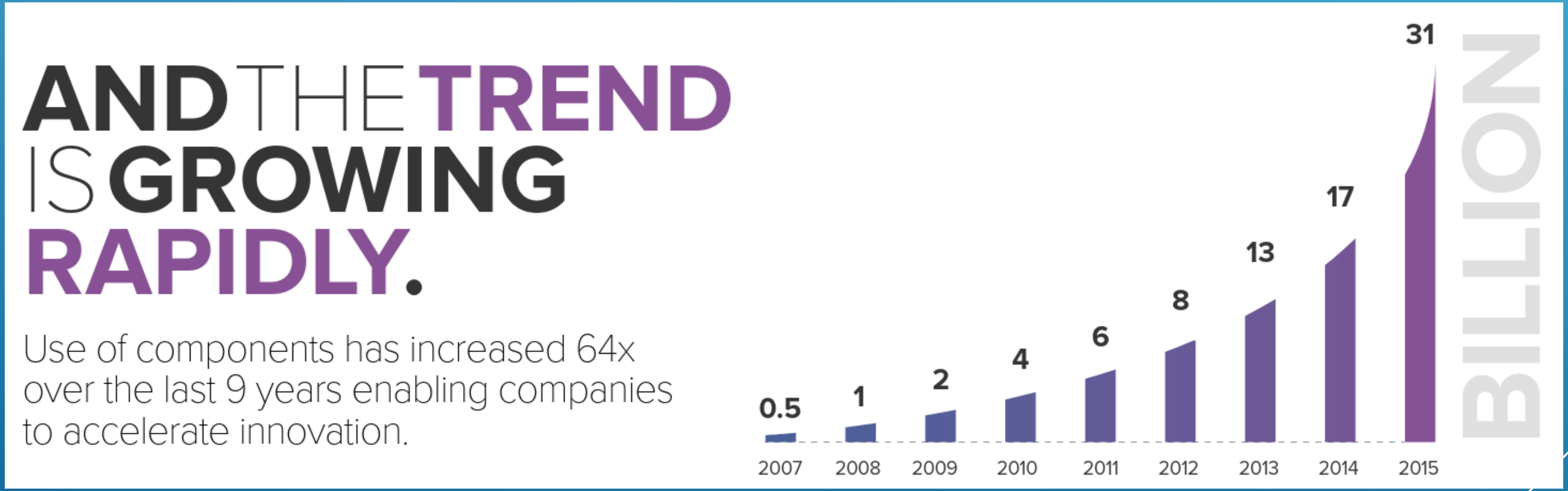


Fig: Software Supply Chain 2016

Ref. Software Supply Chain & snyk.io

OVERVIEW OF VULNERABLE AND OUTDATED COMPONENT

- What is Vulnerable and Outdated Component?

According to software supply chain 2016 by sonatype.com:

- Not all components are created equal.
  - ✓ 10,000 new component versions per day
  - ✓ Developers create 1,000 new open-source projects per day
  - ✓ Each company downloaded 229,898 component per year!

6.8% of components used in applications have at least one known security vulnerability

Parts age and grow stale. Older components in apps have 3x rate of vulnerabilities.

Ref. Software Supply Chain 2016

OVERVIEW OF VULNERABLE AND OUTDATED COMPONENT

According to Software supply chain report 2022:

- 14% of all monthly downloads are vulnerable.
- 4.5% of the vulnerable dependencies have no version with available fix, which means that 95.5% of known-vulnerable downloads had a non-vulnerable option available.

Only category to not have any Common Vulnerability and Exposures (CVEs) mapped to the included CWE

Default exploits/impact weight is 5.0

- Vulnerable Components are a known issue that we struggle to test and assess risk

Ref. OWASP TOP 10 and Software Supply Chain Report 2022

OVERVIEW OF VULNERABLE AND OUTDATED COMPONENT

- When we are vulnerable?

- When the versions of all components used in both client-side and server-side is unknown.
  - Components: Directly used and nested dependencies.
- If the software is vulnerable, unsupported, or out of date.
  - The OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- If regular scanning for vulnerabilities are not done and do not keep update to security bulletins related to the components used.

Ref. OWASP TOP 10

OVERVIEW OF VULNERABLE AND OUTDATED COMPONENT

- When we are vulnerable?

- If we do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion.
  - This commonly happens in environments when patching is a monthly or quarterly task under change control, leaving organizations open to days or months of unnecessary exposure to fixed vulnerabilities.
- If the compatibility of updated, upgraded, or patched libraries are not tested.
- If the components' configurations are insecure.
  - A05:2021-Security Misconfiguration

Ref. OWASP TOP 10

IMPACT OF VULNERABLE AND OUTDATED COMPONENT

- What can go wrong?

- The impact of this type of vulnerability varies considerably depending on the type of vulnerability that the outdated/vulnerable component is. At worst it can result in the complete loss of data integrity, data confidentiality and system availability.

Ref. OWASP TOP 10

WAYS OF MITIGATION

Knowing the Open-Source Software "Bill of Materials"

Questions we should know the answer to:

- How do we know what open-source components are in our applications?
  - How do we know what versions of open-source components we are using?
- How do we discover and define the risk of open-source components?
  - How do we associate a specific risk to a specific version of an open-source component?
- How do we know when a component releases a new version?

Ref. OWASP TOP 10

WAYS OF MITIGATION

Knowing the Open-Source Software "Bill of Materials" (OSS-BOM)

Questions we should know the answer to:

- How do we know if a new vulnerability is found on what was previously a "good" component?
- How do we know if we are using the authentic version of an open-source component?

Tools Used to Generate OSS-BOM

Syft by Anchore	Snyk	FOSSA	Microsoft
SPDX SBOM Generator	Tern Project	TauruSeer	Mend

Ref. WebGoat, csoonline.com and mergebase.com

WAYS OF MITIGATION

Identifying Security Information of the Open-Source Modules

- **Is my component exploitable?**
- **Is my component an authentic copy?**
  - **Do I understand why my component is modified?**

Identifying License Information Overload of the Open-Source Modules

- **Can I use this component within the context of distribution of my software?**
- **Are there license incompatibilities?**
- **If using a modified component, did I address additional license obligations?**

Ref. WebGoat

WAYS OF MITIGATION

Identifying Architecture Information of the Open-Source Modules

- **Is my component old or is it stable**
- **Is my component unpopular**
- **Was my lack of upgrade a deliberate choice or a lack of knowledge**

Ref. WebGoat

WAYS OF MITIGATION

Applying Patch Management Process

After identifying OSS-BOM:

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies using tools like versions, OWASP Dependency Check, retire.js, etc. Continuously monitor sources like CVE and NVD for vulnerabilities in the components.
- Use software composition analysis tools to automate the process. Subscribe to email alerts for security vulnerabilities related to components you use.

Ref. OWASP TOP 10

EXAMPLES

- New Linux malware uses 30 plugin exploits to backdoor WordPress sites

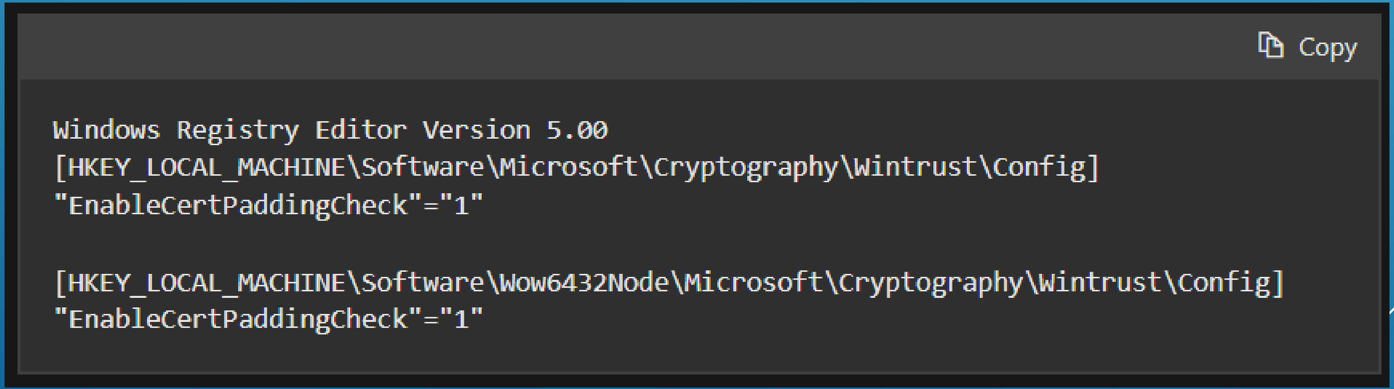
- Affected Components: WP Live Chat Support Plugin, Easysmtp, Thim Core, Google Code Inserter etc.
- Security Issue: Infected pages act as redirectors to a location of the attacker's choosing, so the scheme works best on abandoned sites. These redirections may serve in phishing, malware distribution, and malvertising campaigns to help evade detection and blocking. That said, the operators of the auto-injector might be selling their services to other cybercriminals.
- Countermeasure: Update to the latest available version the themes and plugins running on the site and replace those that are no longer developed with alternatives that being supported.

Ref. bleecpingcomputer.com

EXAMPLES

- 10-year-old Windows bug with 'opt-in' fix exploited in 3CX attack

- Affected Components: Windows OS (WIN_CERTIFICATE structure)
- Security Issue:: Cannot identify malicious dll or exe file execution as the d3dcompiler_47.dll uses Microsoft's Digital Signature
- Countermeasure: Microsoft made it optional fix as it would invalidate legitimate, signed executables that stored data in the signature block of an executable.



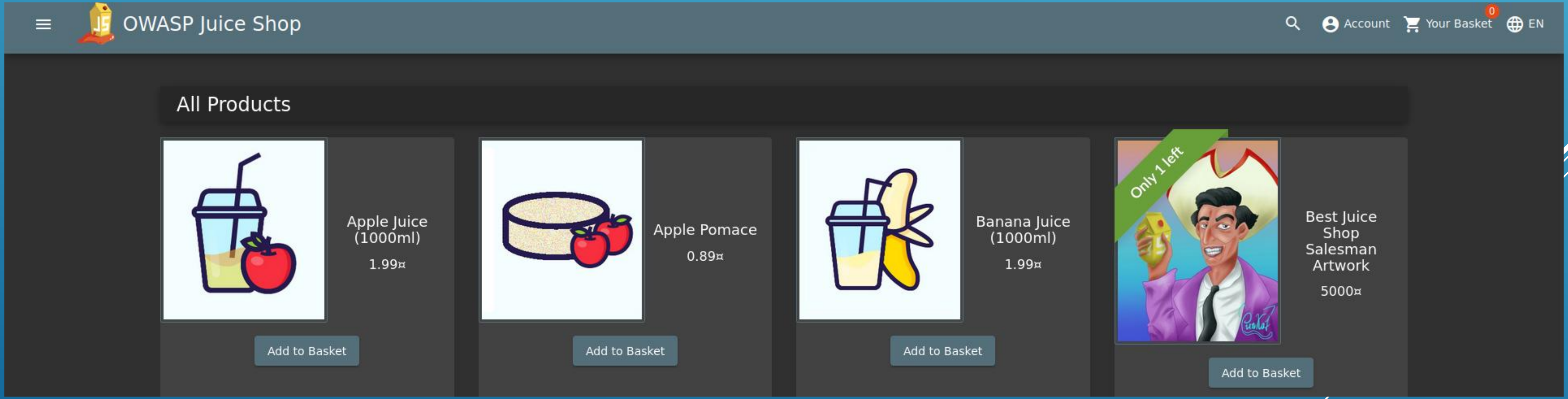
```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"

[HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config]
"EnableCertPaddingCheck"="1"
```

Ref. bleecpingcomputer.com & Microsoft

A SIMPLE XSS DEMO

DOM Based XSS in Web Juice

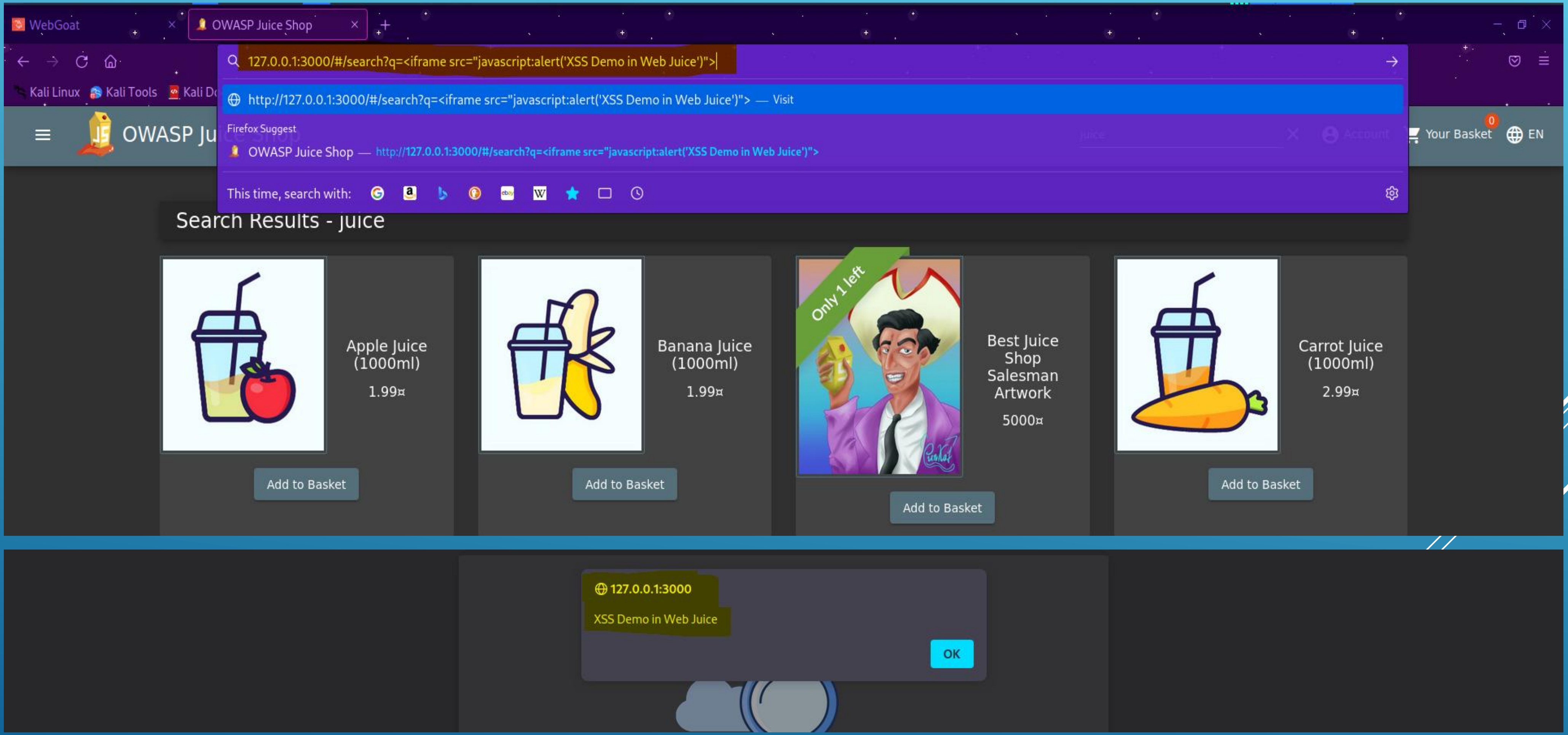
DOM Based XSS: This attack uses malicious code to modify the DOM elements/environment in the client-side script. In this attack, the payload is placed on the server-side.



Ref. Web Juice

A SIMPLE XSS DEMO

DOM Based XSS in Web Juice



```
127.0.0.1:3000/#/search?q=<iframe src="javascript:alert('XSS Demo in Web Juice')">
```

WebGoat
OWASP Juice Shop
Kali Linux
Kali Tools
http://127.0.0.1:3000/#/search?q=<iframe src="javascript:alert('XSS Demo in Web Juice')"> — Visit
Firefox Suggest
OWASP Juice Shop — http://127.0.0.1:3000/#/search?q=<iframe src="javascript:alert('XSS Demo in Web Juice')">
This time, search with:
Your Basket
EN
Search Results - juice
Apple Juice (1000ml) 1.99¤
Banana Juice (1000ml) 1.99¤
Only 1 left
Best Juice Shop Salesman Artwork 5000¤
Carrot Juice (1000ml) 2.99¤
Add to Basket
127.0.0.1:3000
XSS Demo in Web Juice
OK

Ref. Web Juice

CONCLUSION

Main takeaways from this presentation:

1. Basic knowledge about outdated and vulnerable components.
2. Reasons behind the generation of outdated and vulnerable components.
3. Ways of mitigation of vulnerable and outdated components.

Ref. Web Juice

QUESTION AND ANSWER

THANK YOU ALL.