



42036 - CYBER SECURITY FOR MOBILE PLATFORMS

LAB 5: NVD, COW, SQLITE INJECTION

Tutor: Ngoc LE

Outline:



1

NVD, what is it?

2

COW, SQL injection

3

The overview of Lab 5

1. NVD, what is it? [1]

The NVD is the U.S. government repository of standards-based vulnerability management data



General +
Vulnerabilities +
Vulnerability Metrics +
Products +
Configurations (CCE)
Contact NVD
Other Sites +
Search +

JSON 1.1 Vulnerability Feed Announcement

CVSS Version 3.1 Support Coming Soon!

XML Vulnerability Feeds Retirement

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Last 20 Scored Vulnerability IDs & Summaries

CVSS Severity

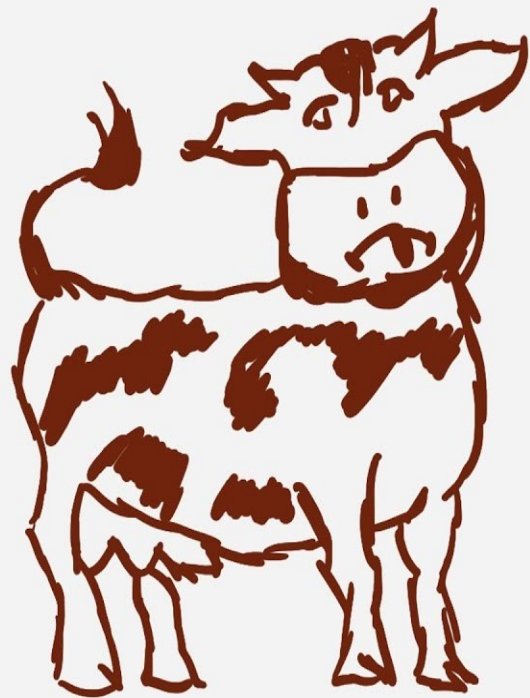
CVE-2019-8041 — Adobe Acrobat and Reader versions , 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap ove... read CVE-2019-8041
Published: August 20, 2019; 04:15:18 PM -04:00

CVE-2019-8042 — Adobe Acrobat and Reader versions, 2019.012.20035 and earlier, 2019.012.20035 and earlier, 2017.011.30142 and earlier, 2017.011.30143 and earlier, 2017.011.30142 and earlier, 2015.006.30497 and earlier, and 2015.006.30498 and earlier have a heap over... read CVE-2019-8042
Published: August 20, 2019; 04:15:18 PM -04:00

V3: **9.8 CRITICAL**
V2: **7.5 HIGH**

V3: **9.8 CRITICAL**
V2: **7.5 HIGH**

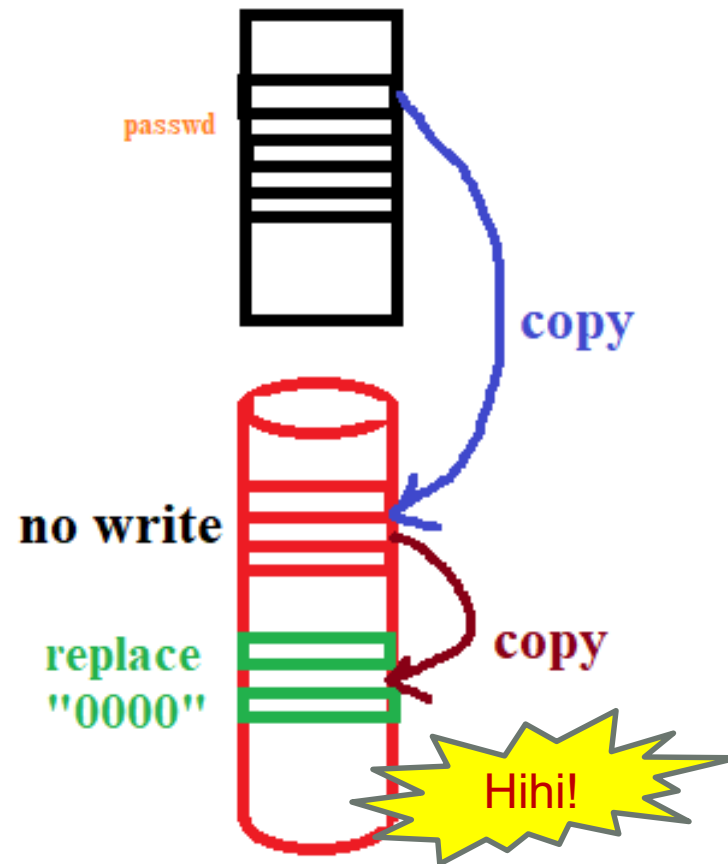
2. Dirty COW attack [2]



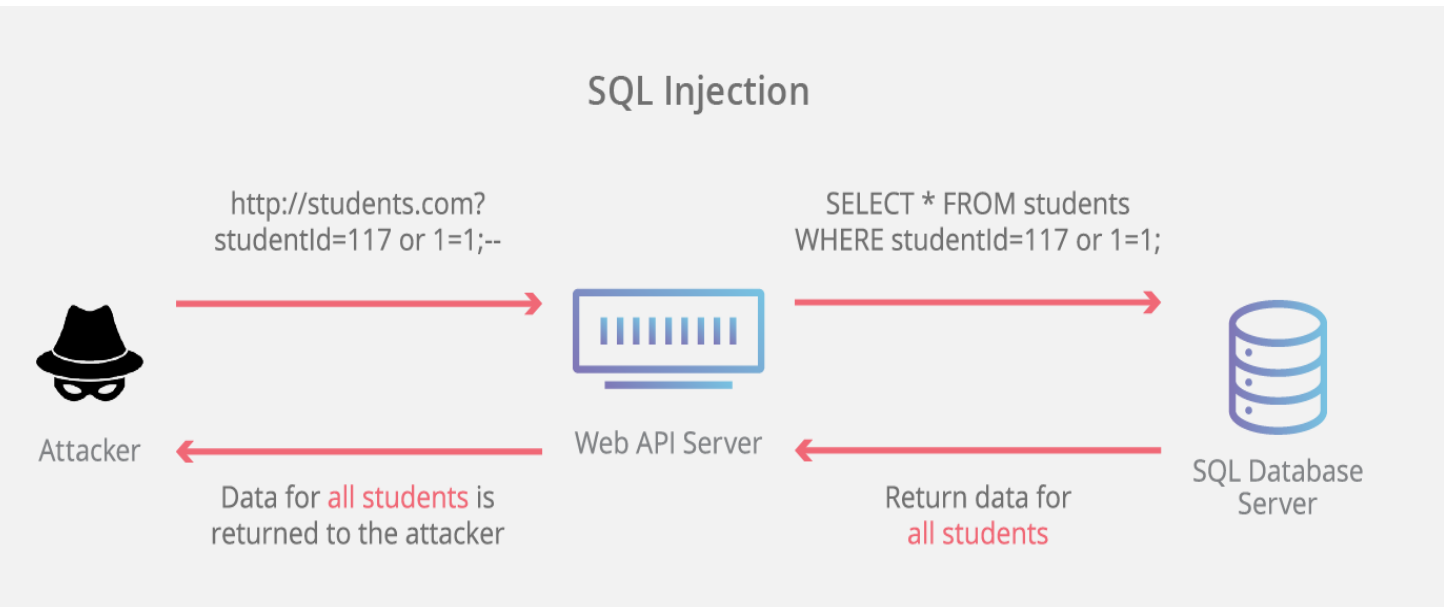
DirtyCOW

CVE-2016-5195

Linux root exploit

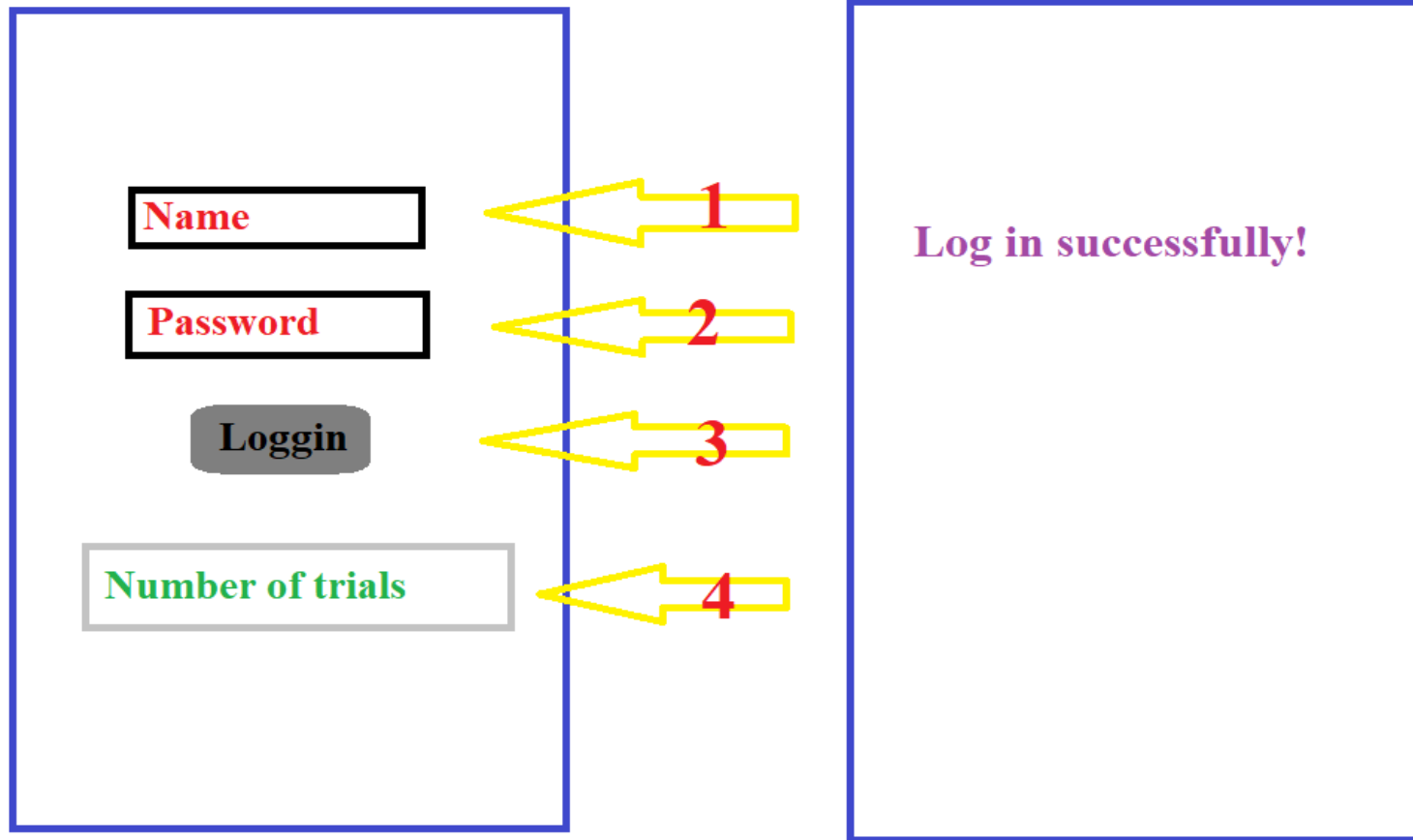


2. SQL injection [3]



[3] <https://www.cloudflare.com/learning/security/threats/sql-injection/>

2. Simple log in app



3. Over view of Lab 5

- ✓ **Task 1:** NVD, what is it
- ✓ **Task 2:** Copy on write attack
- ✓ **Task 3:** SQL injection attack
- ✓ **Task 4:** Simple log in app
- ✓ **Task 5:** Suggest creating SQLite injection app

THANK YOU!

Question & Answer