

Skillsoft Course Player - Google Chrome

cdn2.percipio.com/rustici/us/custom-content/147e488c-8636-4ca5-9e78-72945e613cf2/rustici/course-packages/courses/2547ebcc-7922-4113-96d0-e098098fe628/0/Content/ria\_V3\_1\_4520/in...

Open Menu Panel Third-party APIs and Components Save and Exit

## Third-party APIs and Components

Dan Lachance

skillsoft

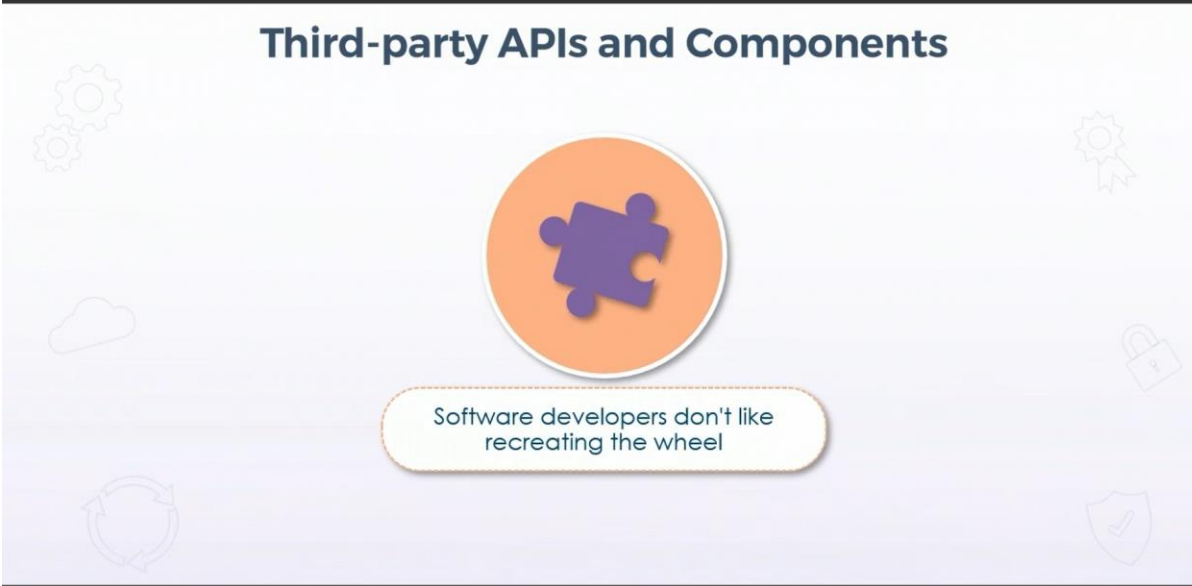
00:04 03:03

Type here to search

31°C 10:43 07-05-2024

Third-party APIs and Components

## Third-party APIs and Components



Software developers don't like recreating the wheel

00:41 02:27

Previous Topic Next Topic

CC AD

## Software Dependencies

- **Modules/libraries**
- **Plug-ins/add-ons**
- **Stability**
- **Security**
  - No back doors
  - Not infected
- **Timely software update availability**



Third-party APIs and Components

## Know What Is Being Used



Developers must fully understand components they use, including version numbers

Components must be kept patched

02:25



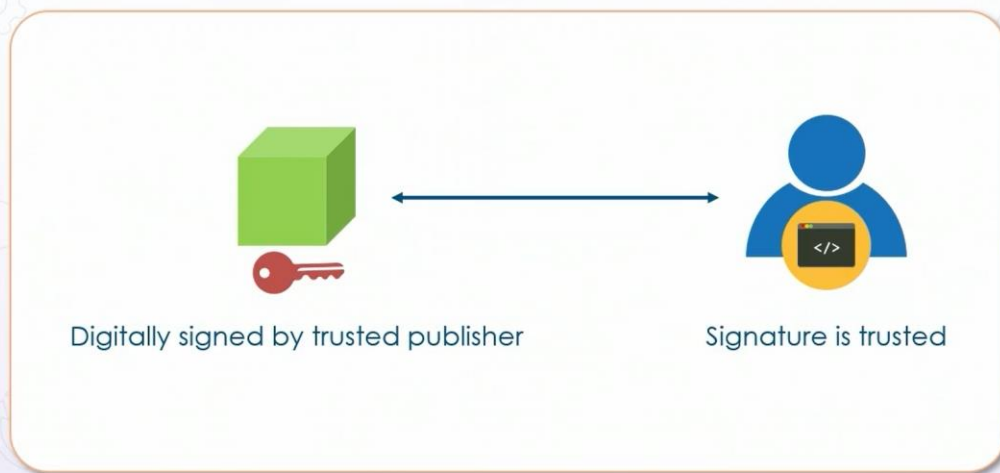
◀ Previous Topic

Next Topic ▶



00:43

## Signed Scripts, Code, and Packages



---

## Buffer Overflows

Dan Lachance

skillsoft<sup>®</sup>

## Buffer Overflows



Programming error - lack of checking memory allocation for variables

## Buffer Overflow Types



Stack overflow

Heap overflow

Integer overflow

Unicode overflow

## Metasploit HTTP Buffer Overflow Exploits

```
012-02-27    normal    Yes    Sysax 5.53 SSH Username Buffer Overflow
419  exploit/windows/telnet/gamsoft_telnet_username 2
000-07-17    average    Yes    GAMSoft TelSrv 1.5 Username Buffer Overflow
420  exploit/windows/tftp/opentftp_error_code 2
008-07-05    average    No    OpenTFTP SP 1.4 Error Packet Overflow
421  exploit/windows/tftp/quick_tftp_pro_mode 2
008-03-27    good        No    Quick FTP Pro 2.1 Transfer-Mode Overflow
422  exploit/windows/tftp/threectftpsvc_long_mode 2
006-11-27    great        No    3CTftpSvc TFTP Long Mode Buffer Overflow
423  exploit/windows/vnc/winvnc_http_get 2
001-01-29    average    No    WinVNC Web Server GET Overflow
424  exploit/windows/vpn/safenet_ike_11 2
009-06-01    average    No    SafeNet SoftRemote IKE Service Buffer Overflow
425  payload/osx/x64/meterpreter/bind_tcp
normal        No    OSX Meterpreter, Bind TCP Stager
426  payload/osx/x64/meterpreter/reverse_tcp
normal        No    OSX Meterpreter, Reverse TCP Stager
```

Buffer Overflows

## Buffer Overflow Attacks



Attacker supplies more than 3 characters, which could include code to be executed remotely on the server

```
void readstring()
{
    char stringvar[3];
    gets(stringvar);
    printf("%s", stringvar);
    return;
}
```

02:56



Previous Topic

Next Topic



03:56

## Buffer Overflow Attacks



Attacker supplies more than 3 characters, which could include code to be executed remotely on the server

```
void readstring()
{
    char stringvar[3];
    gets(stringvar);
    printf("%s", stringvar);
    return;
}
```

## Buffer Overflow Results



Remote access to server memory contents

Overwritten executable code can produce incorrect results

Overwritten executable code can crash the server

## Heartbleed Bug

