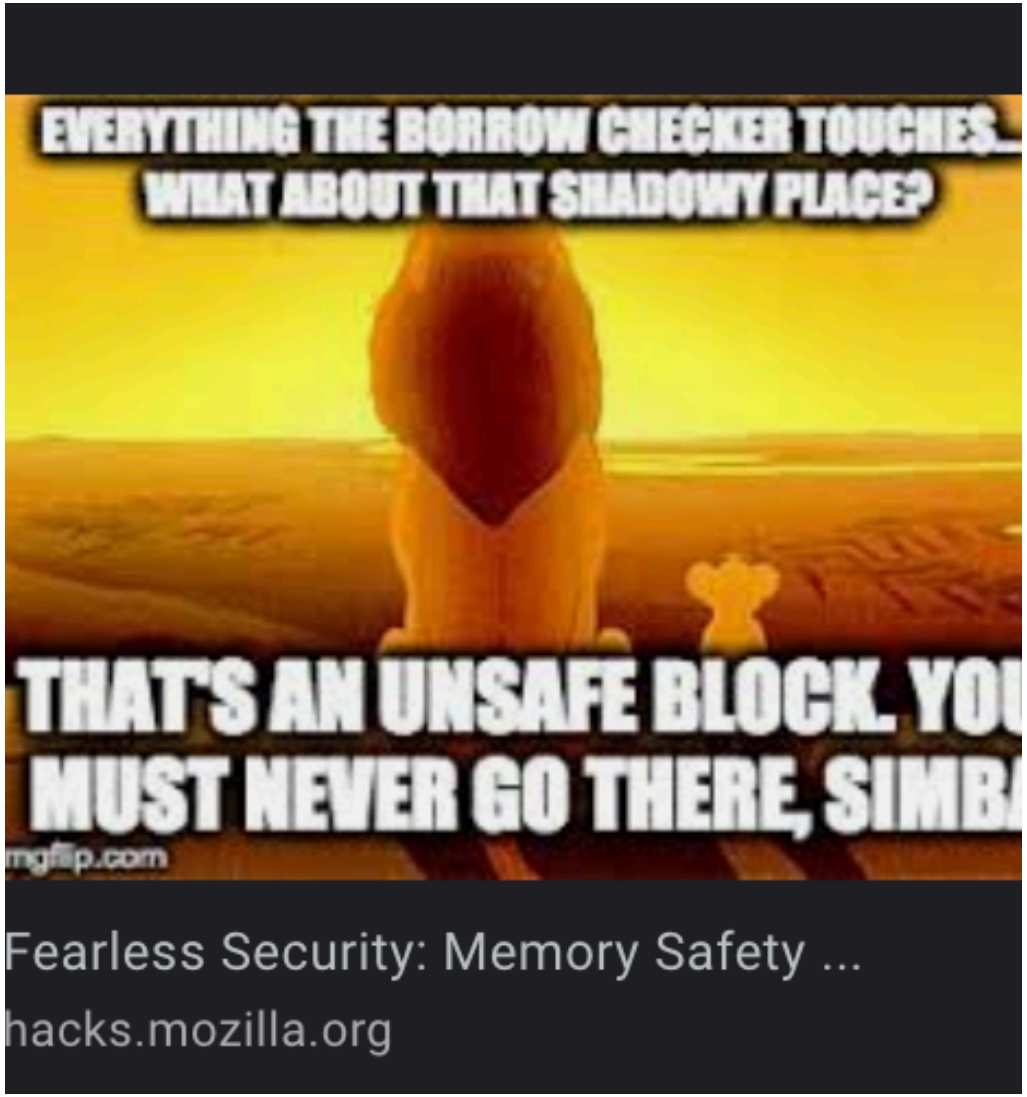
COS30015 – Lab 3

Buffer Overflow

Presented by Jamie Ooi

Thursday 18 August, 2022



SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 3 Background

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾ NVD

Go to for: CVSS Scores CPE Info

Search CVE List | Downloads | Data Feeds | Update a CVE Record | Request CVE IDs

TOTAL CVE Records: 158840

HOME > CVE > SEARCH RESULTS

Search Results

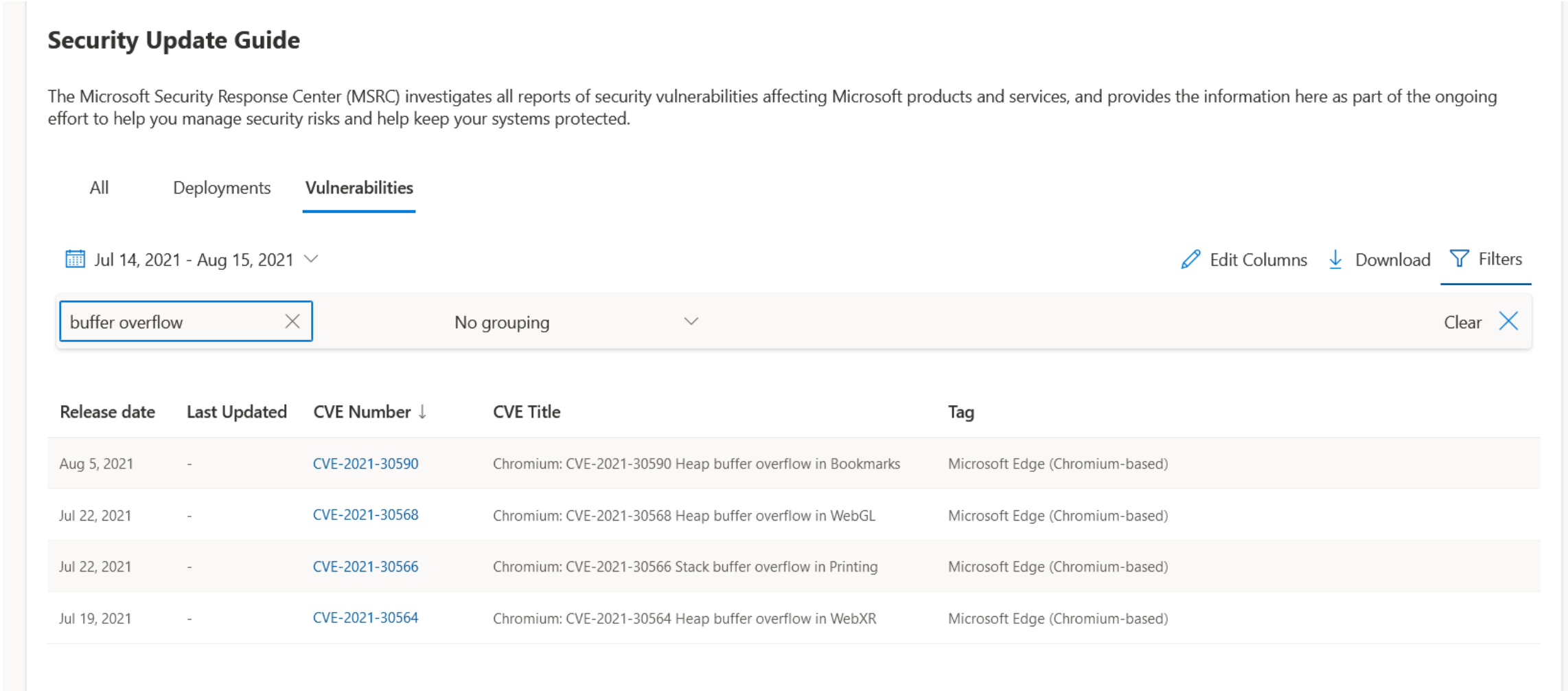
There are **11869** CVE Records that match your search.

- **11869 Buffer Overflow vulnerabilities identified since 1999**
- **396 August 2021**

Name	Description
CVE-2021-38614	** UNSUPPORTED WHEN ASSIGNED ** Polipo through 1.1.1, when NDEBUG is used, allows a heap-based buffer overflow during parsing of a Range header. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2021-38592	Wasm3 0.5.0 has a heap-based buffer overflow in op_Const64 (called from EvaluateExpression and m3_LoadModule).
CVE-2021-38526	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects RAX35 before 1.0.3.94, RAX38 before 1.0.3.94, and RAX40 before 1.0.3.94.
CVE-2021-38525	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 before 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40.
CVE-2021-38524	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects MK62 before 1.0.6.110, MR60 before 1.0.6.110, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.32, RAX50 before 1.0.2.32, RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, and RBS750 before 3.2.16.6.
CVE-2021-38523	NETGEAR R6400 devices before 1.0.1.70 are affected by a stack-based buffer overflow by an authenticated user.
CVE-2021-38522	NETGEAR R6400 devices before 1.0.1.52 are affected by a stack-based buffer overflow by an authenticated user.

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 3 Background



Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.

All Deployments **Vulnerabilities**

Jul 14, 2021 - Aug 15, 2021 Edit Columns Download Filters

buffer overflow No grouping Clear

Release date	Last Updated	CVE Number ↓	CVE Title	Tag
Aug 5, 2021	-	CVE-2021-30590	Chromium: CVE-2021-30590 Heap buffer overflow in Bookmarks	Microsoft Edge (Chromium-based)
Jul 22, 2021	-	CVE-2021-30568	Chromium: CVE-2021-30568 Heap buffer overflow in WebGL	Microsoft Edge (Chromium-based)
Jul 22, 2021	-	CVE-2021-30566	Chromium: CVE-2021-30566 Stack buffer overflow in Printing	Microsoft Edge (Chromium-based)
Jul 19, 2021	-	CVE-2021-30564	Chromium: CVE-2021-30564 Heap buffer overflow in WebXR	Microsoft Edge (Chromium-based)

COS30015 IT Security – Lab 3 Background

Buffer Overflow – Hall of Fame

1988 – Morris Worm MIT Buffer Overflow of fingerd

- Coding mistake instructing the worm to replicate itself
- Severely impacting the Internet at that time

2001 – Code Red Buffer Overflow on IIS Server

- Used the 'N' character to overflow the buffer

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

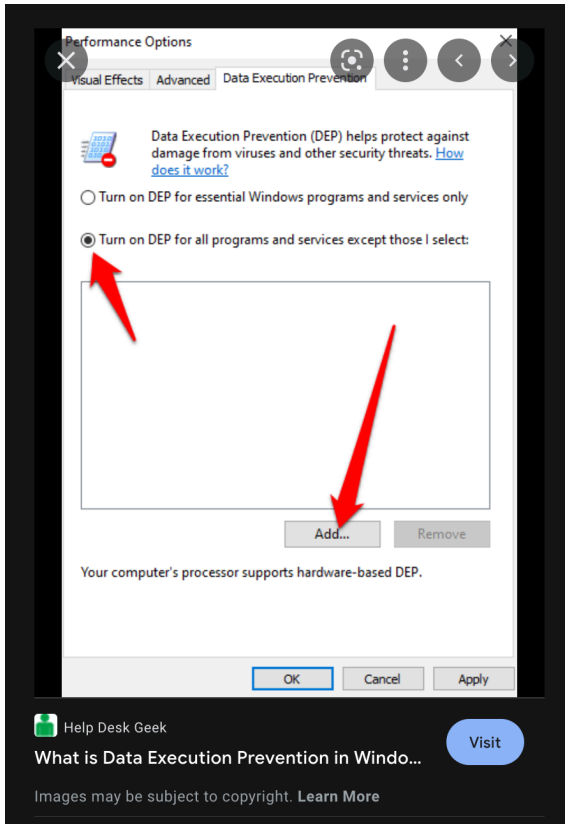
2003 – SQL Slammer Buffer Overflow on Microsoft SQL Server UDP Port 1434

- Crashed routers and slowed the Internet down significantly

COS30015 IT Security – Lab 3 Background

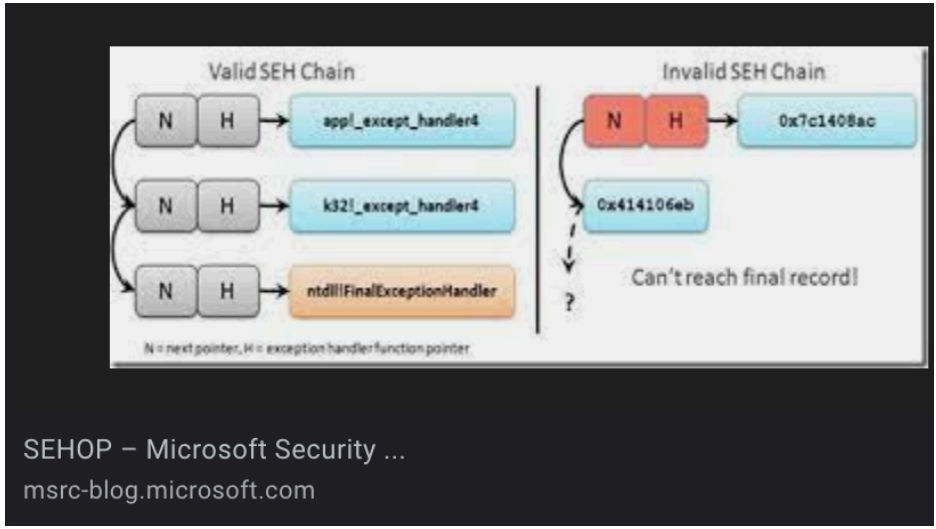
Windows Built-in Prevention

- Data Execution Prevention (DEP)



- Address Space Layout Randomization (ASLR)

- Structured Exception Handling Overwrite Protection (SEHOP)

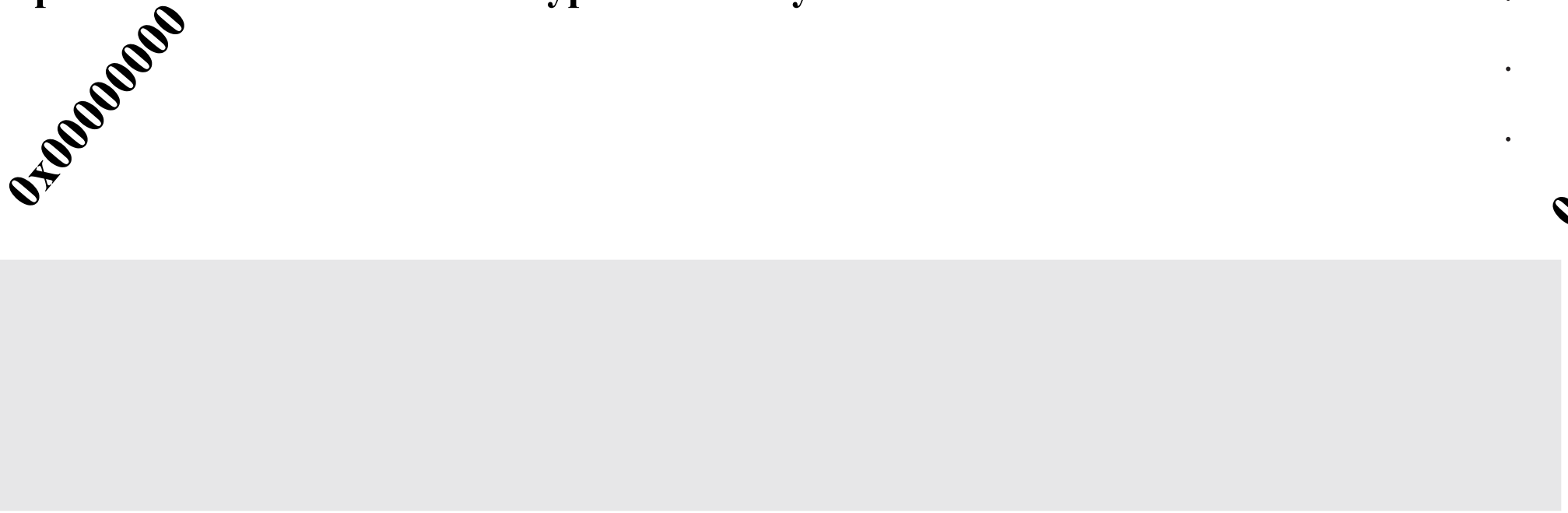


SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 3 Background

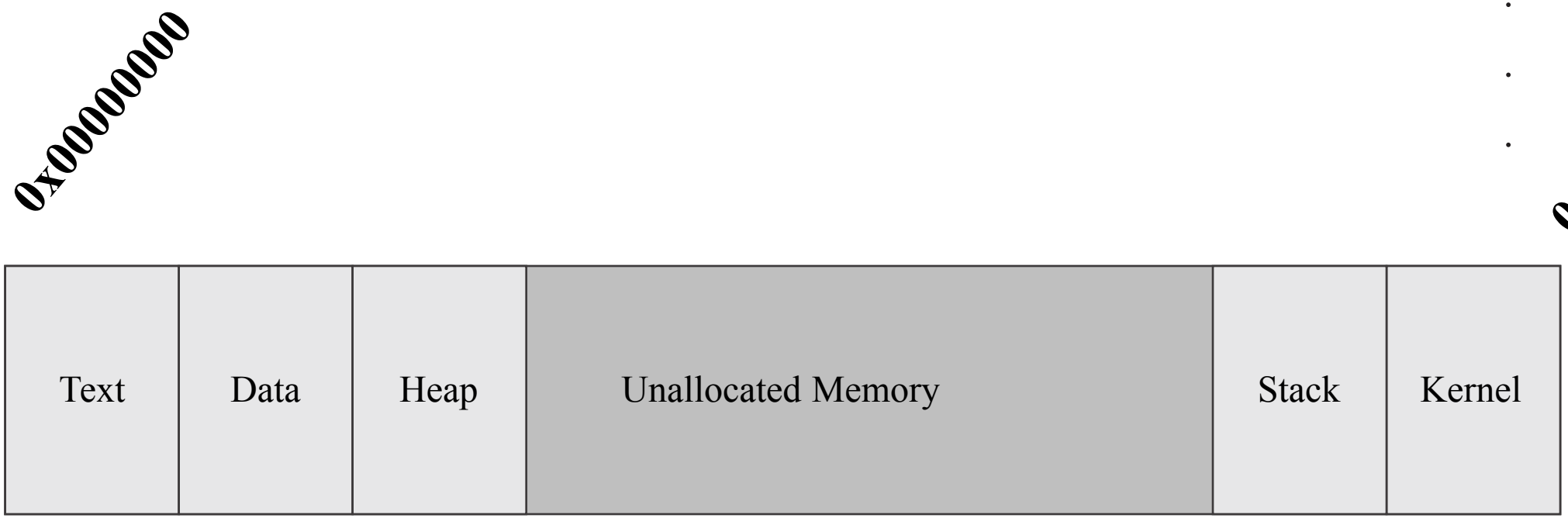
Buffer Overflow Explained

Here is a picture of the construct of a typical memory



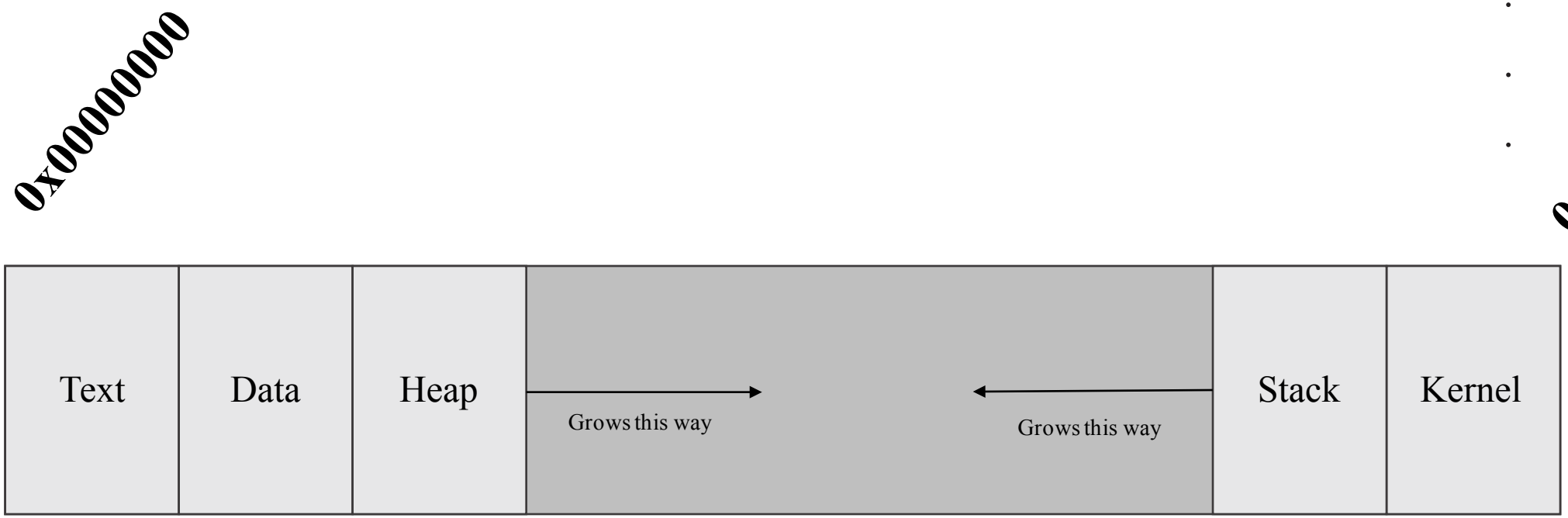
COS30015 IT Security – Lab 3 Background

Buffer Overflow Explained



COS30015 IT Security – Lab 3 Background

Buffer Overflow Explained



COS30015 IT Security – Lab 3 Background

Buffer Overflow Explained

```
…
add_three_numbers(int a, int b, int c);
…
```

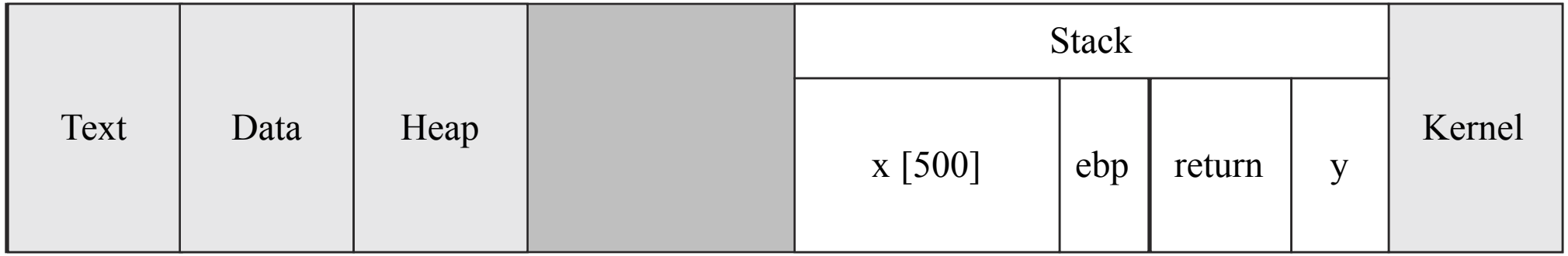
COS30015 IT Security – Lab 3 Background

Buffer Overflow Explained

```
void broken_function(char *y) {
  char x[500];
  strcpy(y, x);
}
```

0x00000000

0xffffffff



COS30015 IT Security – Lab 3 Background

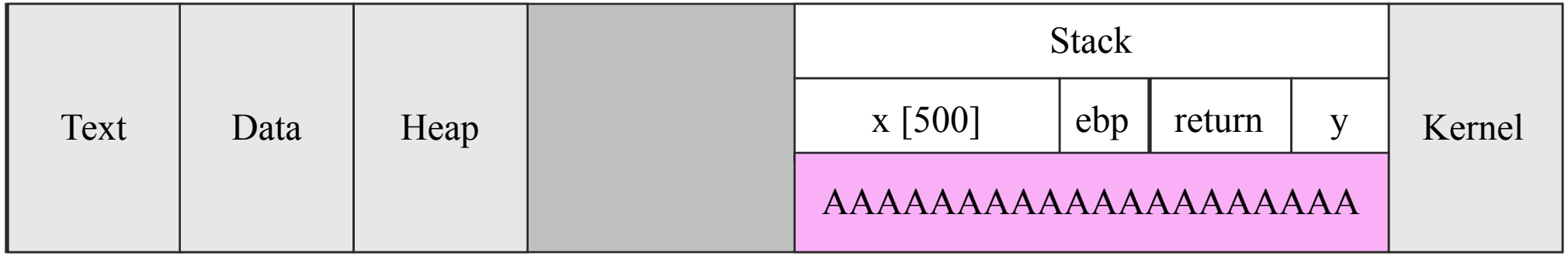
Buffer Overflow Explained

```
void broken_function(char *y) {
  char x[500];
  strcpy(y, x);
}
```

Y = 1000 A's

0x00000000

0xffffffff



COS30015 IT Security – Lab 3 Background

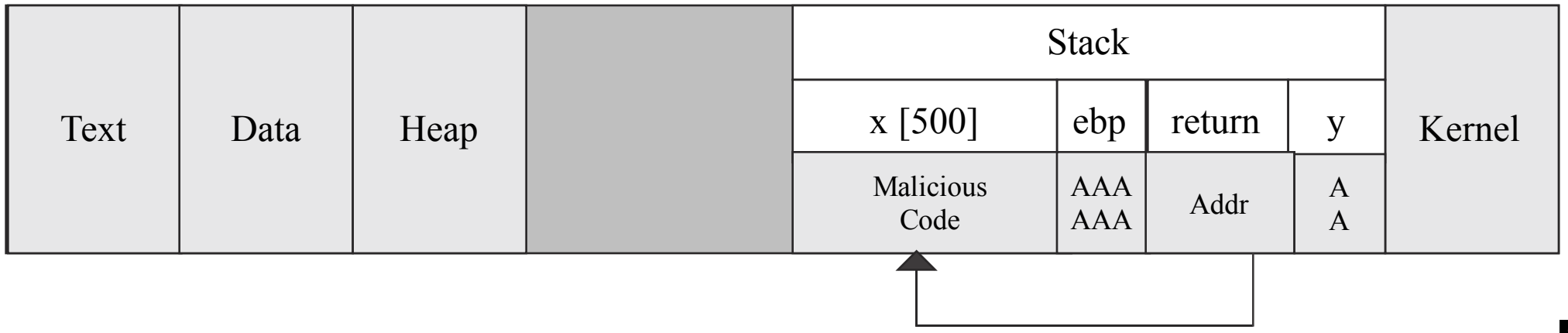
Buffer Overflow Explained

```
void broken_function(char *y) {
  char x[500];
  strcpy(y, x);
}
```

0x00000000

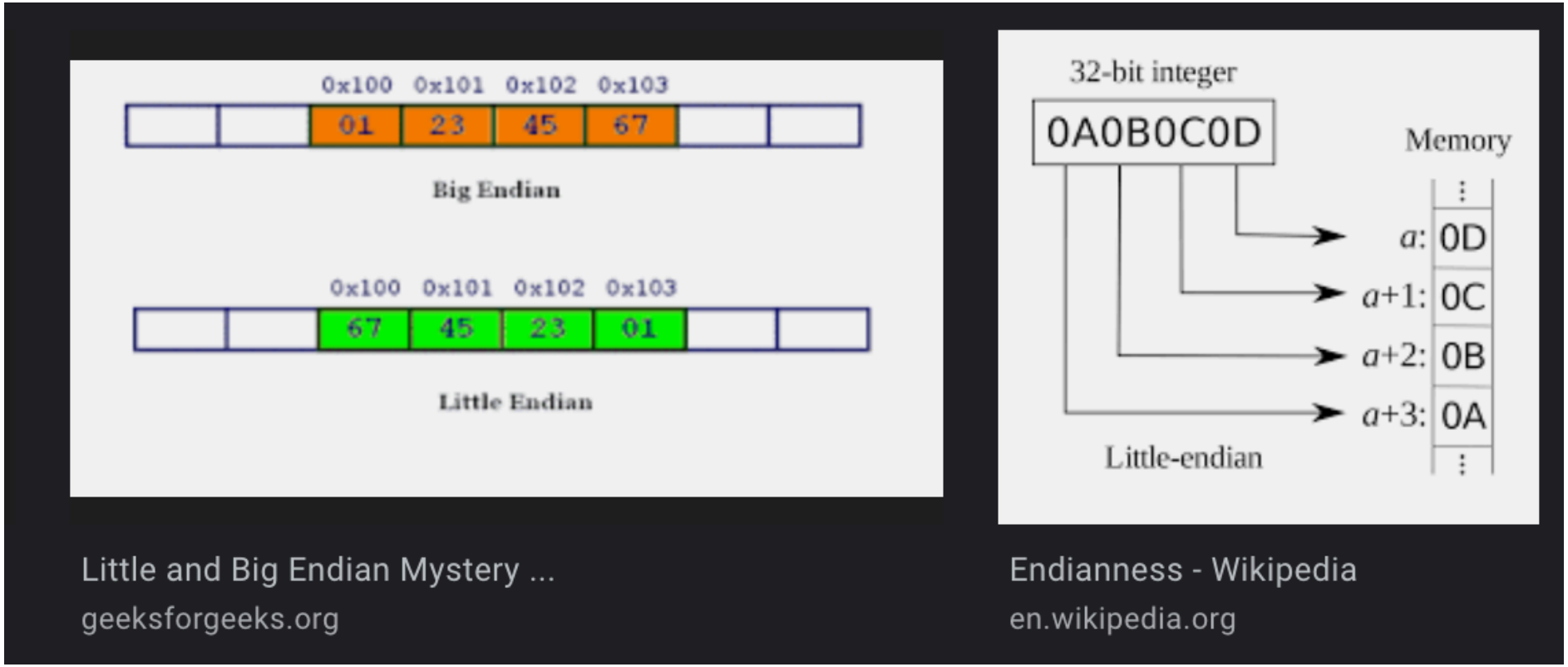
Y = Malicious Code+AAAAs+Address

Y = NOPSLED+Malicious Code+NOPs+Address



COS30015 IT Security – Lab 3 Background

Endianness



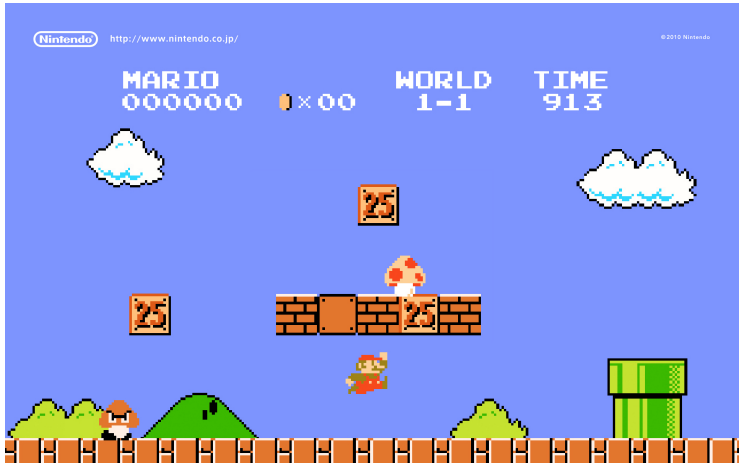
COS30015 IT Security – Lab 3 Background

Shellcode Examples

Run calc.exe
(Execution)

Source: https://www.shpock.com/en-gb/i/WuYZ_c2JekmqBcDl/olympia-desktop-retro-calculator/

User -> Root
(Privilege Escalation)



Source: https://www.yesvegetarian.com/super-mario-eats-mushrooms-to-grow-and-have-power-why-should-you-too/

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 3 Background

Download and have **three** Virtual Machines (Kali, Cysca2014, Win95) up and running ☺

Questions ?

Email: jooi@swin.edu.au
Linkedin: https://www.linkedin.com/in/jamie-ooi-15297b98/

Thursday 18 August, 2022

Reminder:
Assignment 1 is due in 3 weeks!