CIS3165 – WEB SECURITY

BY PELIN

1. WEB SECURITY FUNDAMENTALS

WHAT IS SECURITY

Generally security is The state of being protected or safe from harm

in context of websites security is keeping a web server and its applications protected or safe from harm.

Websites are public and high profile

Need to first be aware of the dangers

Awareness + protection = security

WHAT IS SECURITY

Security is a deep topic

General principles to follow

Most common attacks

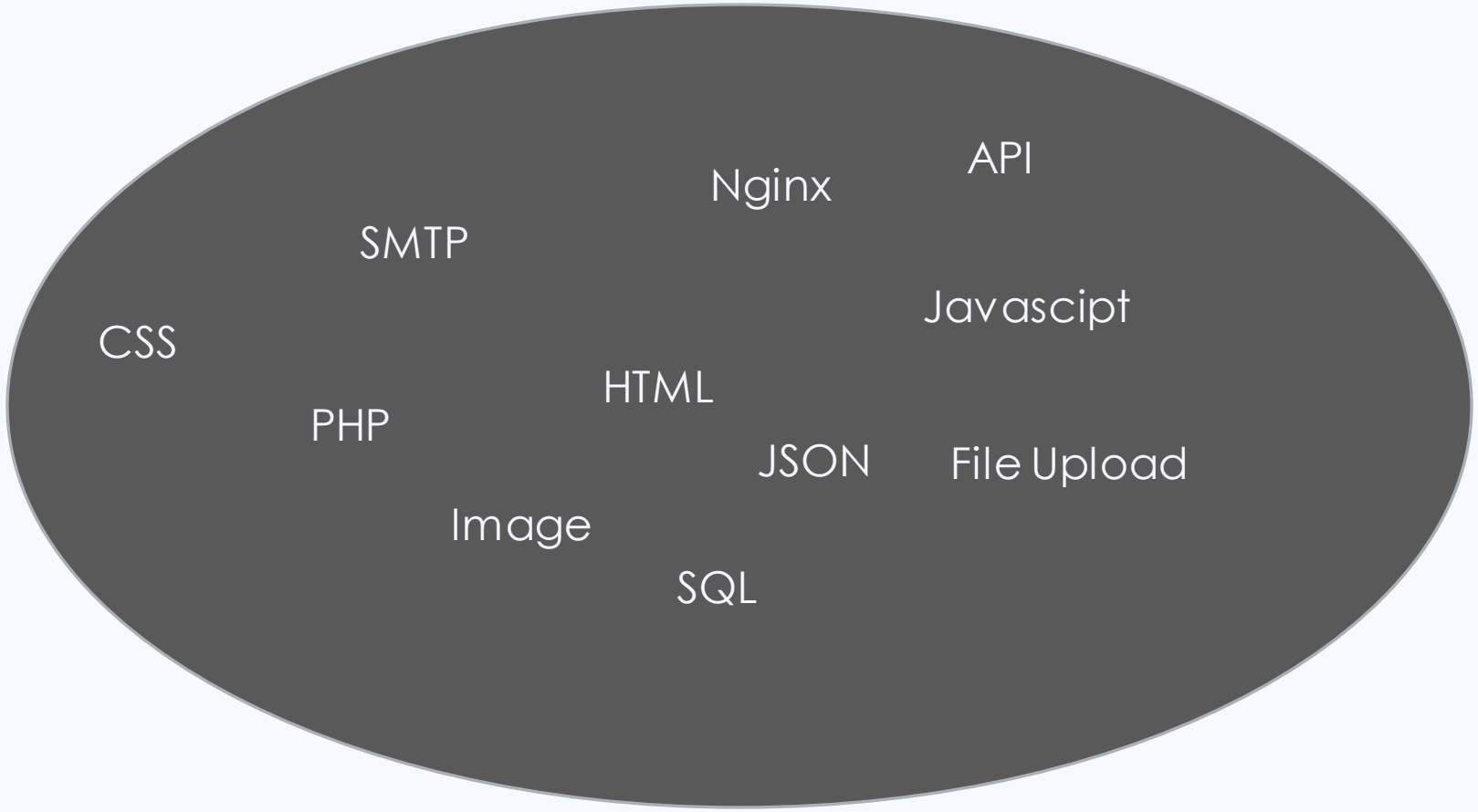
Useful strategies

WHY SECURITY MATTERS

Just because the development of a simple website is easy it should not undermine security issues.

The more technologies you use to more complex it will become to secure

WHY SECURITY MATTERS



MALICIOUS SOFTWARE

Malicious software:

Email spam

Spyware

Sending web requests

Scanning for vulnerabilities

Data crunching

Backdoor for future access

BOTNETS

Botnets:

- Sizes are measured in hundreds-thousands or millions
- Wait quietly for instructions
- Rented out for profit
- Can be used for any purpose

WHY CARE?

Lost of control

You become part of the problem

Can get your server flagged

Public embarrassment

Costs money

theft

WHAT IS A HACKER?

Security professionals classify hackers into two categories:

White hat hacker and **black hat hacker**

White hat hacker: curious user that mean no harm, just want to build something new and exercise their creativity.

Black hat hacker: someone who uses your web server in a way that you did not intend

BLACK HAT HACKERS

Curious users

Thrill seekers

Trophy hunters

Script kiddies

Political activists

professionals

TOTAL SECURITY IS UNACHIEVABLE

"the only secure computer is one that's unplugged, locked in a safe place and buried 20 feet under the ground in a secret location … and I'm not even too sure about that one" - Dennis Hughes, FBI

THREATS & VULNERABILITIES

A threat occurs when vulnerability exists in a system or a network

vulnerability may not exist, but a system is always open to threats

Vulnerability is a flaw or loophole in a system or program that facilitates an attacker to enter a security system

- Known
- Unknown (zero-day exploits)

Types of threats:

- **Accidental threats**
- **Malicious threats**
- **Authorization threats**
- **Application threats**
- **Privacy threats**
- **Access control threats**

To be discussed in the common threats section

ZERO-DAY EXPLOITS

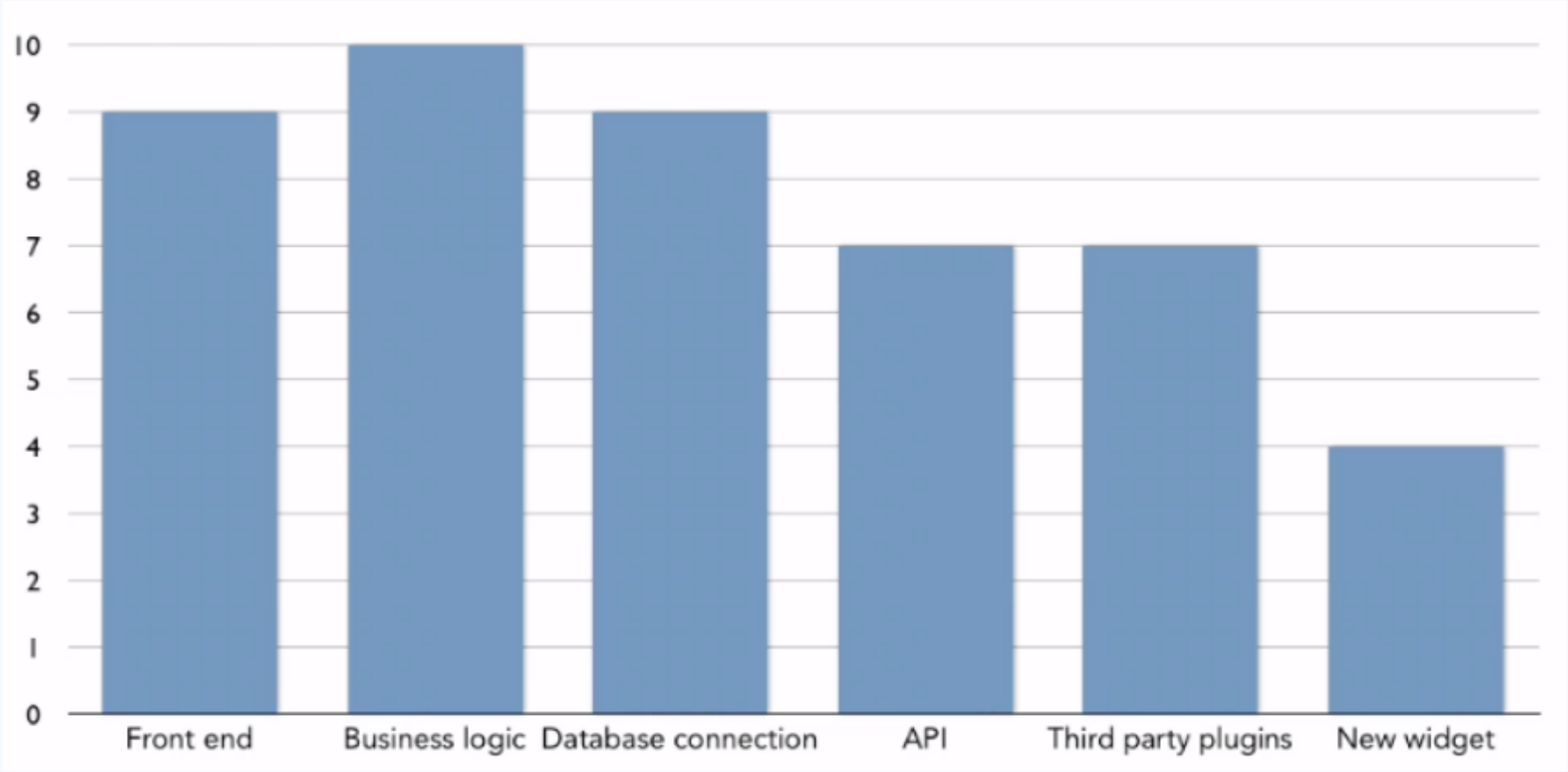
These are newly discovered vulnerabilities

Security vulnerabilities known only to hackers

Kept secret or traded

Developer has had "zero days" of awareness

WEAKEST LINK



HOW MUCH SECURITY

Should match your needs and goals

Execute the security you need really well

Re-evaluate periodically

ASPECTS OF WEB SECURITY

Three areas that need to be secured:

- A client
- A server
- A network

Two important aspects to consider:

- Defining the purpose of the security (CIAA)
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
- Establishing security equation

DEFINING THE PURPOSE

Confidentiality: refers to securing critical information from disclosure to unauthorized users.

Integrity: implies ensuring that information is not modified by unauthorized users.

Availability: implies that the data or information is available for use whenever the need arises

Authentication: ensuring that an individual who is trying to access a resource on the Web is who he or she claims to be.

It also implies ensuring that only authorized individuals are permitted to access information

ESTABLISHING SECURITY EQUATION

A **security equation** involves identifying the critical information that needs to be secured and the level to which it should be secured.

The following factors should be considered while determining a security equation:

- **The tangible value of the information**
  - the actual value of the information that an organization wants to secure
- **The perceived value of the information**
  - the gain that a user would derive upon attaining the information through unfair means
- **The cost of securing the information**
  - the total resources, monetary or nonmonetary, invested in deploying measures to secure information
- **The cost if security is breached:**
  - includes the cost that an intruder would have to incur to break into a system and access the information.

DEFINING THE SECURITY EQUATION

An organization should ensure that the cost of securing information is less than or equal to the tangible value of information.

The cost of breaching information should be greater than the perceived value of information

THE SECURITY MINDSET

Everyone, all the time

Weakest link in your security is your level of security

Average users have to be mindful of security

May require an education plan

THE SECURITY MINDSET

Decision makers have to be mindful of security

Security may require time and money

Allocate for security in project timeliness

Understand security impact of choices

Take any raised security concerns seriously

REGULAR SECURITY REVIEWS

Review all technologies in use (hardware and software)

Review code in use and still in development

Review procedures

Review access privileges

Educate and re-educate

BETTER DEVELOPERS

Fully learn technologies

Better programmers write more secure programs

Write software tests for common security concerns

WRITE A SECURITY POLICY

Communicates how information assets are protected

Rules or guidelines

Keep it simple, clear and easy to follow

Involve all stakeholders

Review periodically – security concerns change

SECURITY POLICY

Define the scope of the policy

Identify and classify data to be protected or controlled

Map the interaction of people and systems

Define the handling procedures for each type of data

Designate user or department responsibilities

THANK YOU