Introduction to Web Vulnerabilities and Hardening

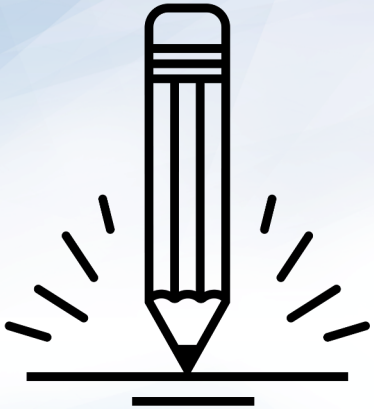
Cybersecurity

Web Vulnerabilities and Hardening

Class Objectives

By the end of today's class, we'll be able to:

- Hack some stuff
- Talk about the "kill chain," "cyber kill chain," and the "hybrid kill chain" like a smart person
- Refer to the OWASP top 10 knowledgeably
- Identify and differentiate between client- and server-side attacks.
- Use social media, WHOIS, and Wafw00f to gather information that informs attack options.



Activity: Executing Exploits

In this activity, you will use OWASP's Broken Web Apps to demonstrate the various ways a website can be exploited.

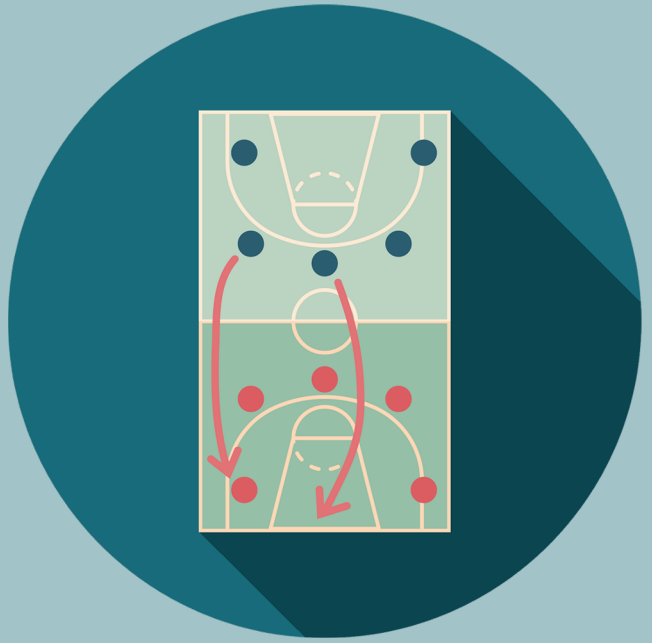
Suggested Time:
45 Minutes

Offense Informs Defense

Throughout this unit, we will act out examples of malicious attacks to show how various hacks and exploits work and how we can better defend against them.

It is important to note that the skills we learn in offensive security units should only be used ethically and with permission.

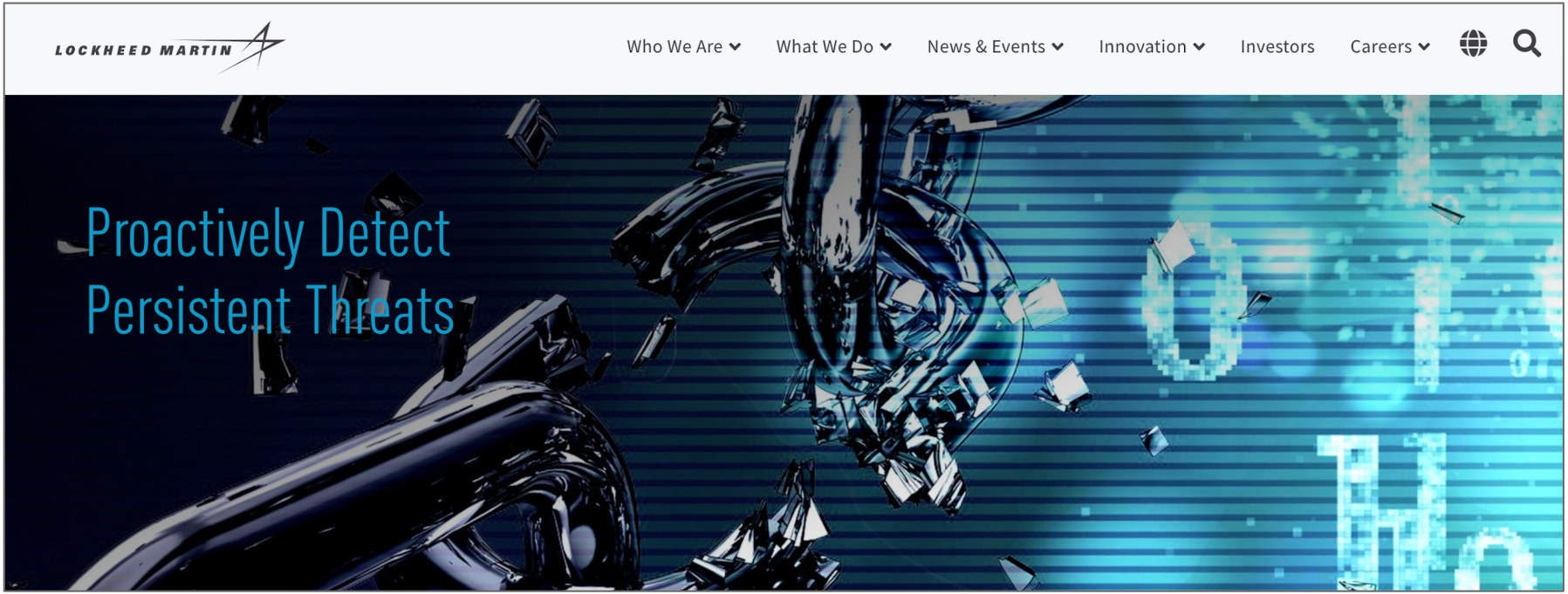
The actions and intents of criminal hackers, hacktivists and other malicious actors that we mimic for demonstrations are in no way condoned or encouraged.



Intro to Web Vulnerabilities and the OWASP Top 10

The Cyber Kill Chain

Lockheed Martin, an aerospace and defense company, developed another form of layered defense: the cyber kill chain.

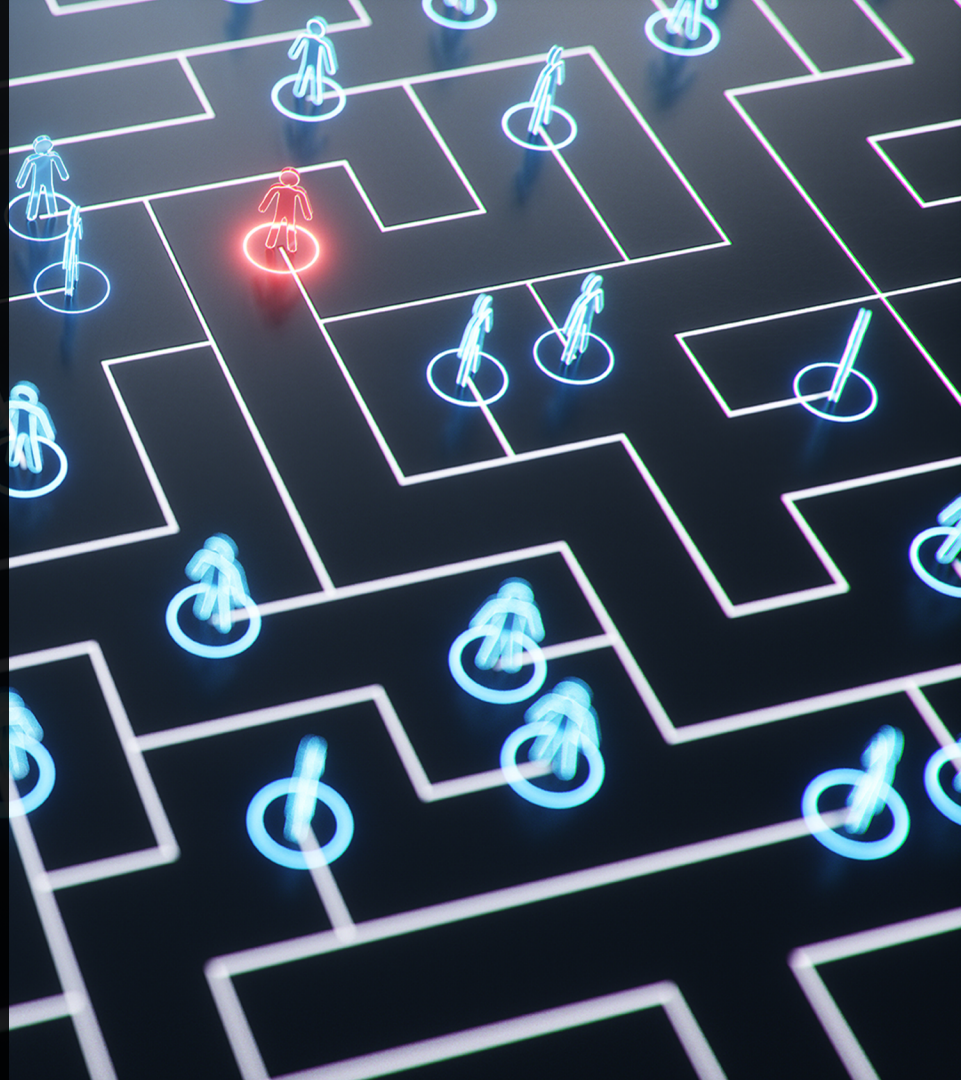


lockheedmartin.com

The cyber kill chain is an "intelligence-driven defense framework" designed to identify and prevent cyber intrusions.

The Cyber Kill Chain

This framework enhances visibility into an attack by improving a security analyst's understanding of an adversary's tactics, techniques, and procedures. It does this by allowing the observation of an attack as it progresses through each stage of the kill chain.



The Hybrid Kill Chain

A derivative of Lockheed Martin's cyber kill chain. The hybrid kill chain has been adapted to apply more directly to web server infrastructure.

Who cares about the Kill Chain?

It’s just a model, don’t confuse it with reality.

If you think attackers always behave this way, you’re deluded.

Who cares about the Kill Chain?

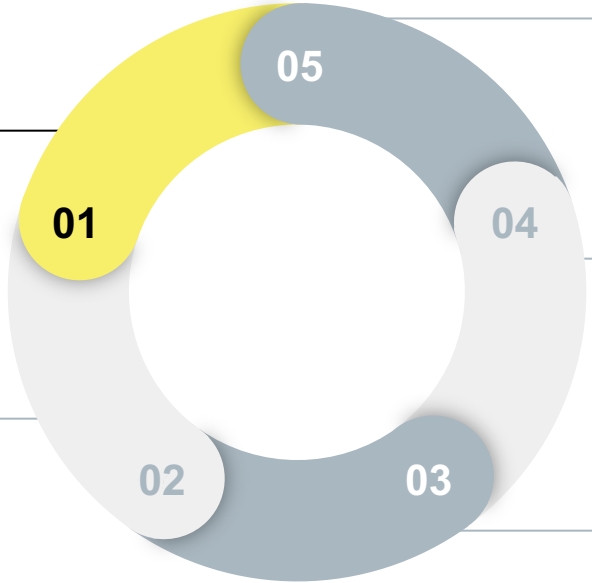
One useful concept: Attackers do have to get multiple things right in order to accomplish anything more than vandalism, and that gives you a chance to detect and intervene.

The Hybrid Kill Chain

It includes the following stages:

Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.



Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

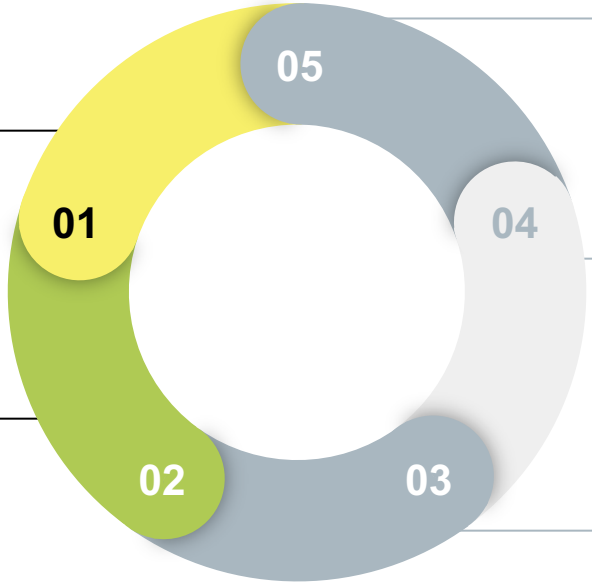
Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

The Hybrid Kill Chain

It includes the following stages:

Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.



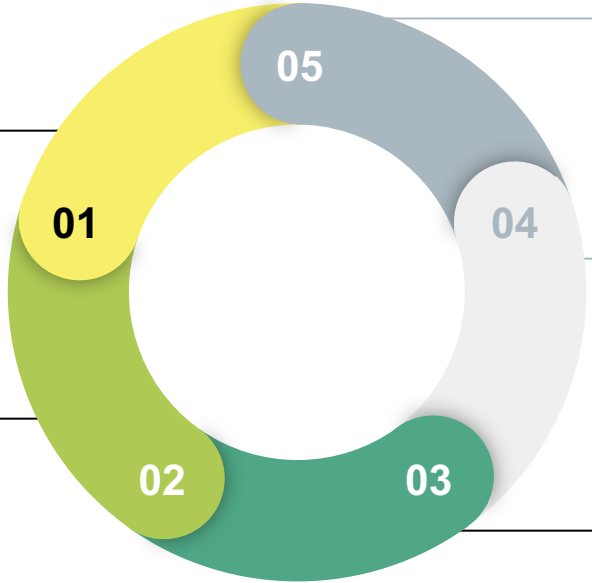
Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

The Hybrid Kill Chain

It includes the following stages:



Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.

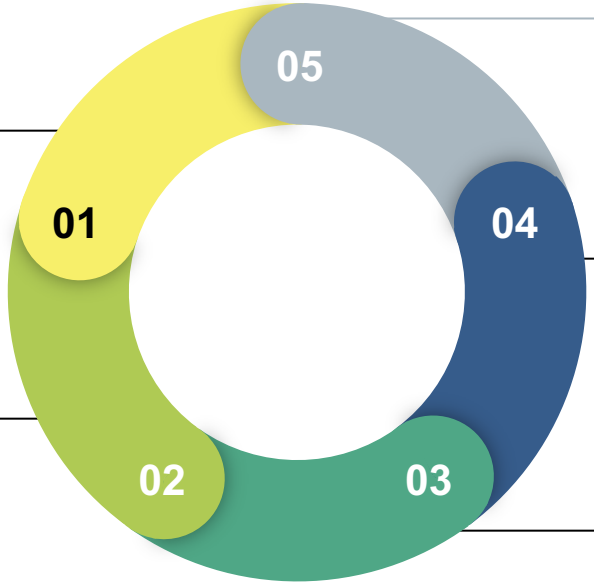
Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

The Hybrid Kill Chain

It includes the following stages:



Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.

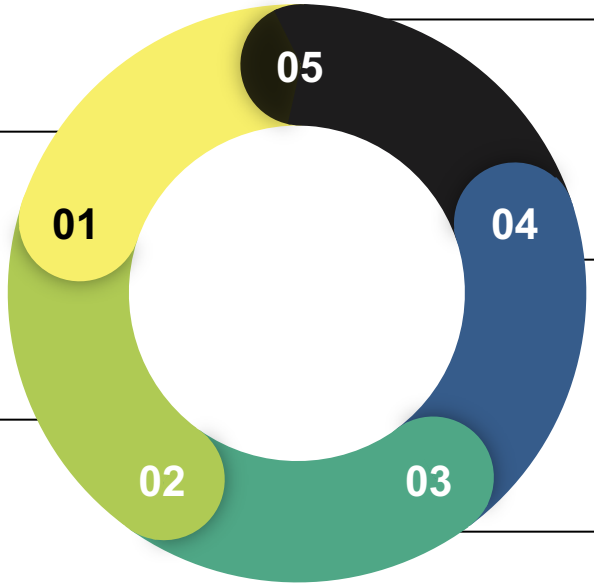
Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

The Hybrid Kill Chain

It includes the following stages:



Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.

Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

Web Vulnerabilities and the Business

Previously we learned that cybersecurity is often considered an obstacle for business operations. This is because enforcing good cybersecurity practices can cause production delays and increase budgets.

Web Vulnerabilities and the Business

Results of complacency and relaxed security to maximize profit can include:

01

A defaced web page containing malicious content or links to inappropriate sites, ultimately damaging a company's reputation.

02

A compromised web server used to download malicious software to anyone visiting the webpage.

03

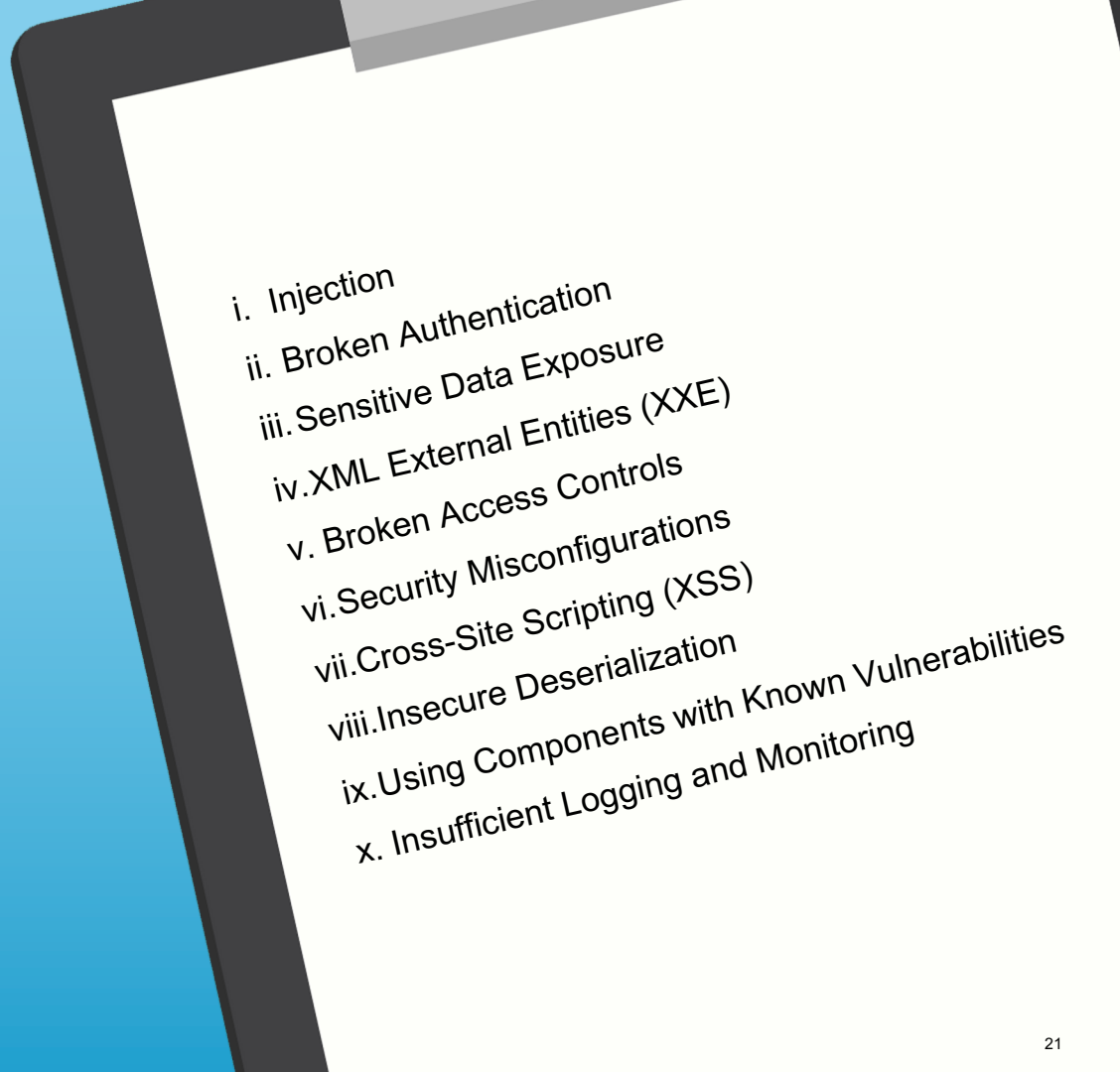
Compromised data used to commit fraudulent activities, leading to loss of business or lawsuits.

OWASP Top 10

The OWASP Top 10 is widely considered to represent the most prevalent security risks facing web applications today.

OWASP Top 10

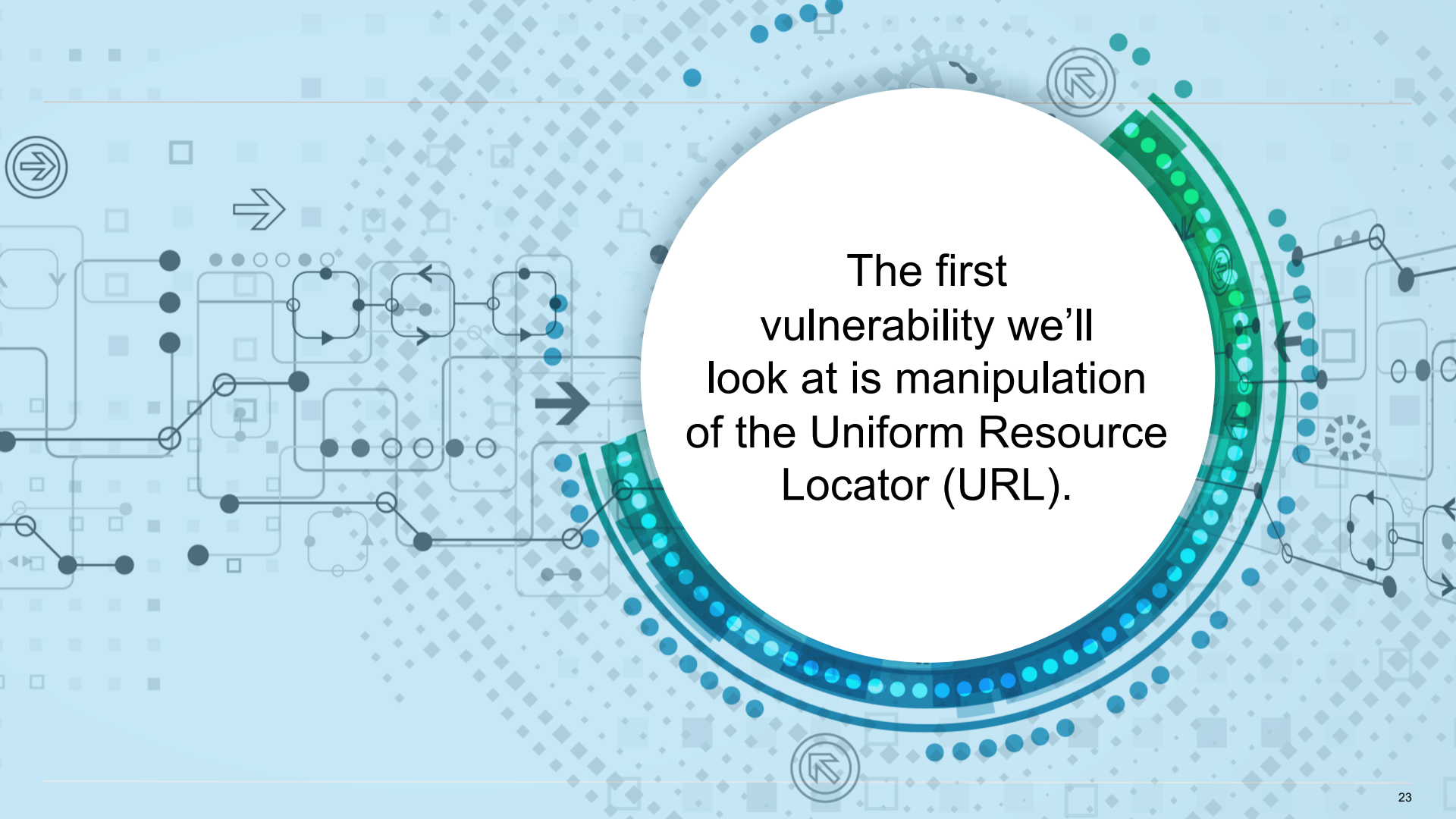
The current list includes:



OWASP Top 10

TL;DR this is how people actually get pwned, not how people theoretically get pwned

https://www.cloudflare.com/learning/security/threats/owasp


The first vulnerability we'll look at is manipulation of the Uniform Resource Locator (URL).

The URL

Uniform Resource Locators are the standardized naming convention for referencing documents that are accessible over the internet.

A web address is essentially a ~~unique~~ reference to an online resource.

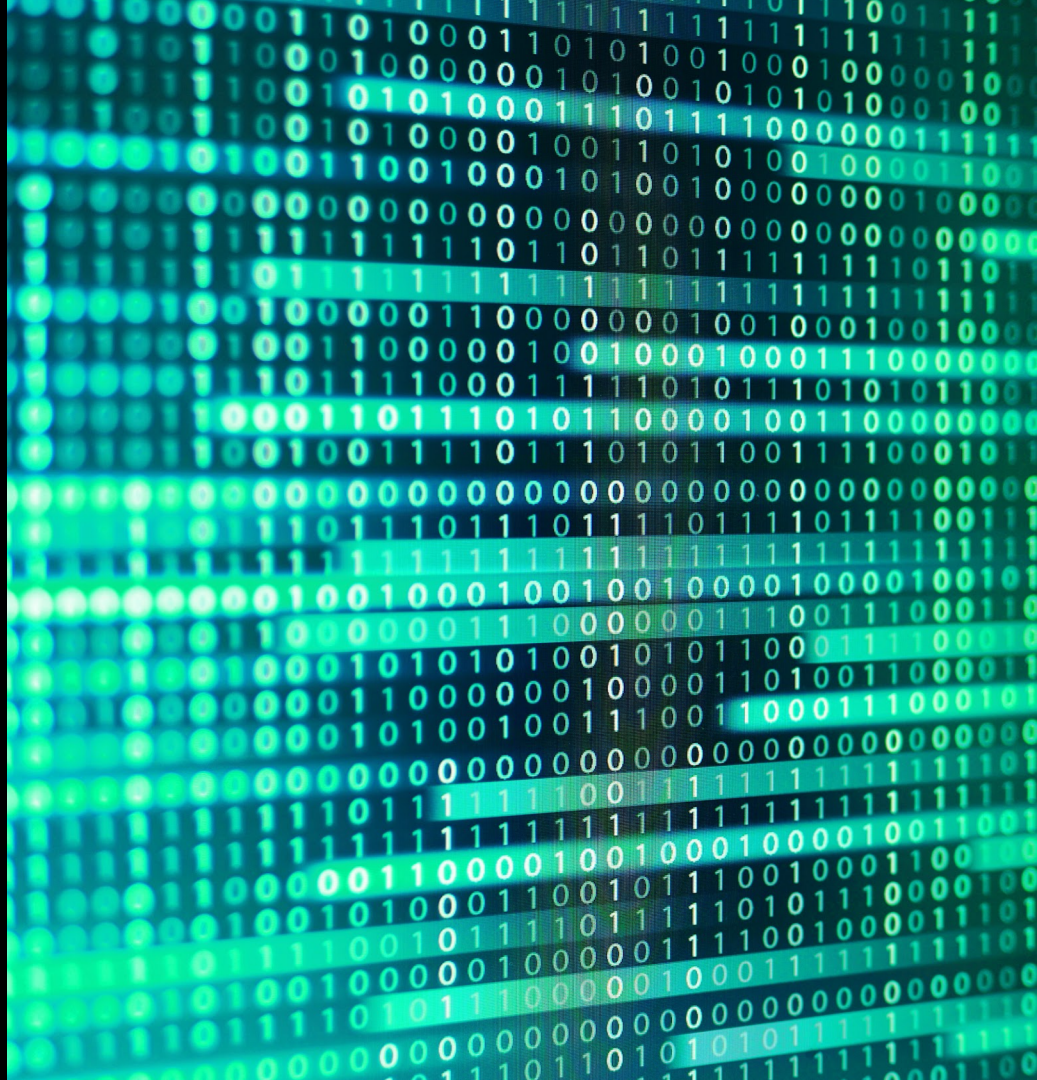
The URL is the gateway to the web. URLs can trivially be manipulated, which makes certain attacks possible.

We got to prove that point when we did the “Parameter Tampering” attack in our lab.

Since no mechanism prevents tampering with URLs, developers need to check validity in their application code. Very often, they don’t.

Web Server Infrastructure

In order to have any chance at all to secure a web infrastructure, knowing the basic mechanics is necessary. Way too many people operate web infrastructures without this understanding, and security suffers.



Components of a model Web Infrastructure

Let’s consider the security properties of five components. (there are many more)

01 **Client**

02 **Firewall**

03 **Web Server**

04 **Web Application**

05 **Database**

Components of a model Web Infrastructure

a.k.a. Treasure Map

01 **Client – Bug potential: High**

02 **Firewall – Bug potential: Low**

03 **Web Server – Bug potential: Low**

04 **Web Application – Bug potential: Insanely great**

05 **Database – Bug potential: Low**

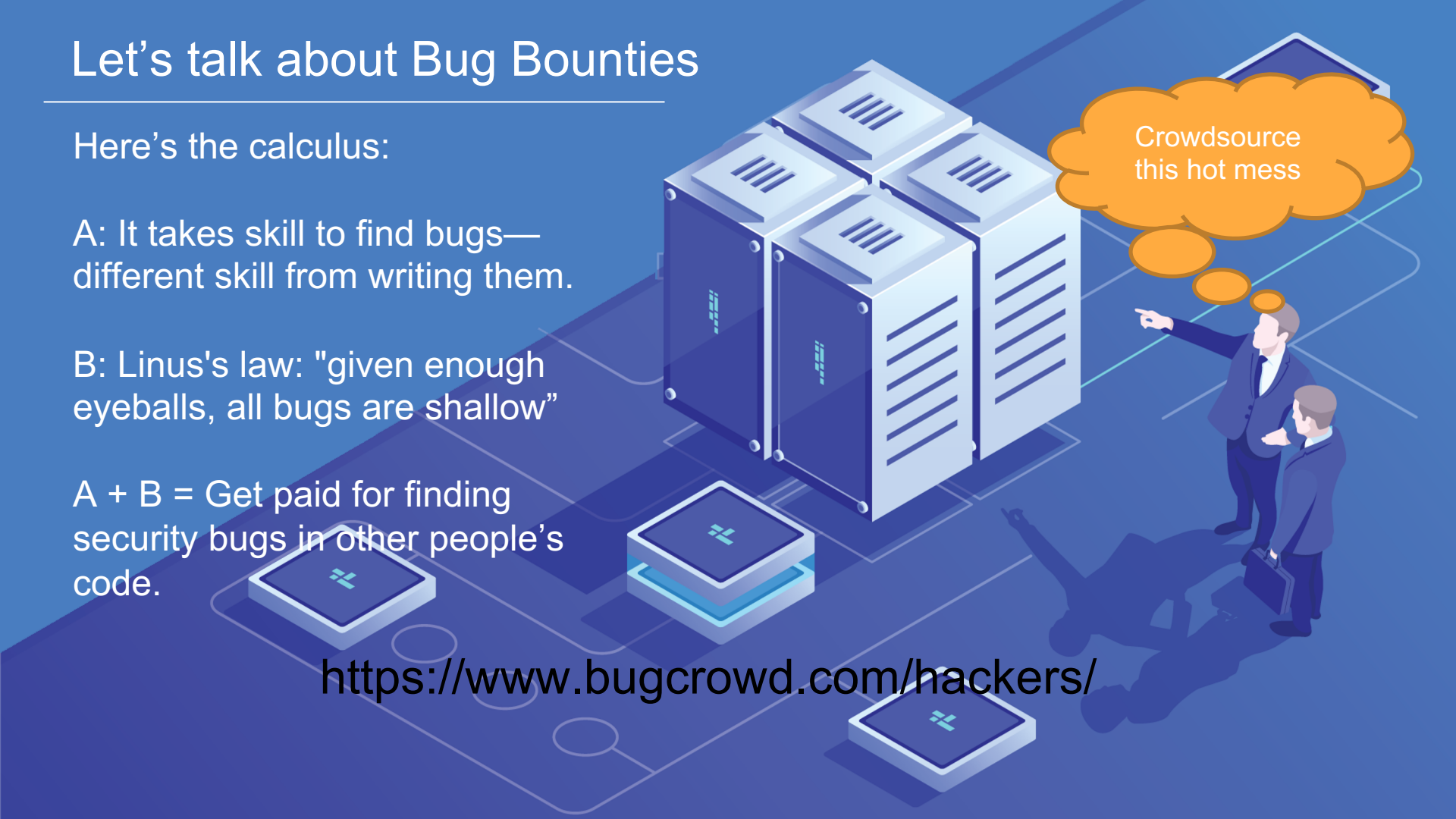
Let’s talk about Bug Bounties

Here’s the calculus:

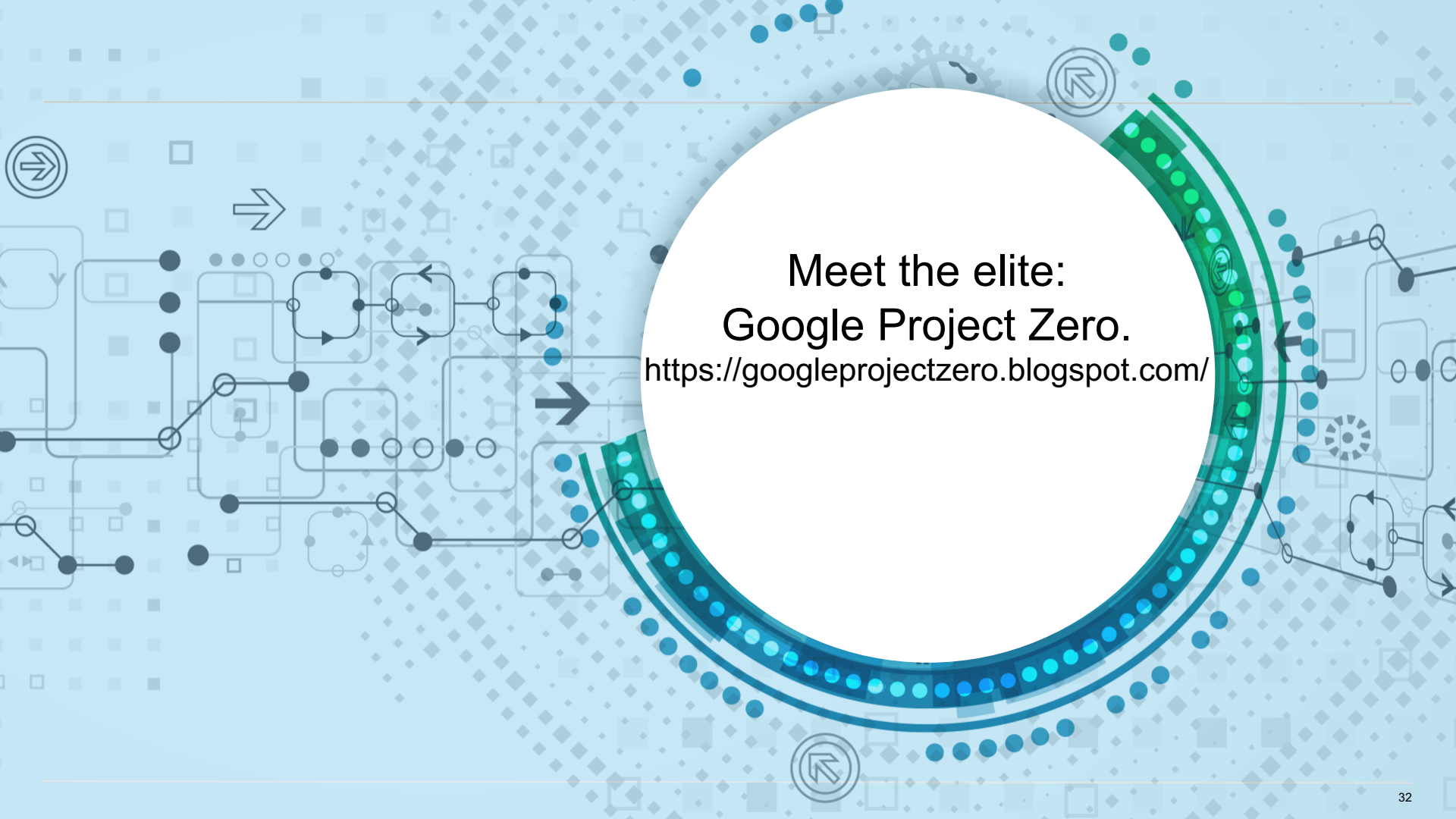
A: It takes skill to find bugs—different skill from writing them.

B: Linus's law: "given enough eyeballs, all bugs are shallow”

A + B = Get paid for finding security bugs in other people’s code.

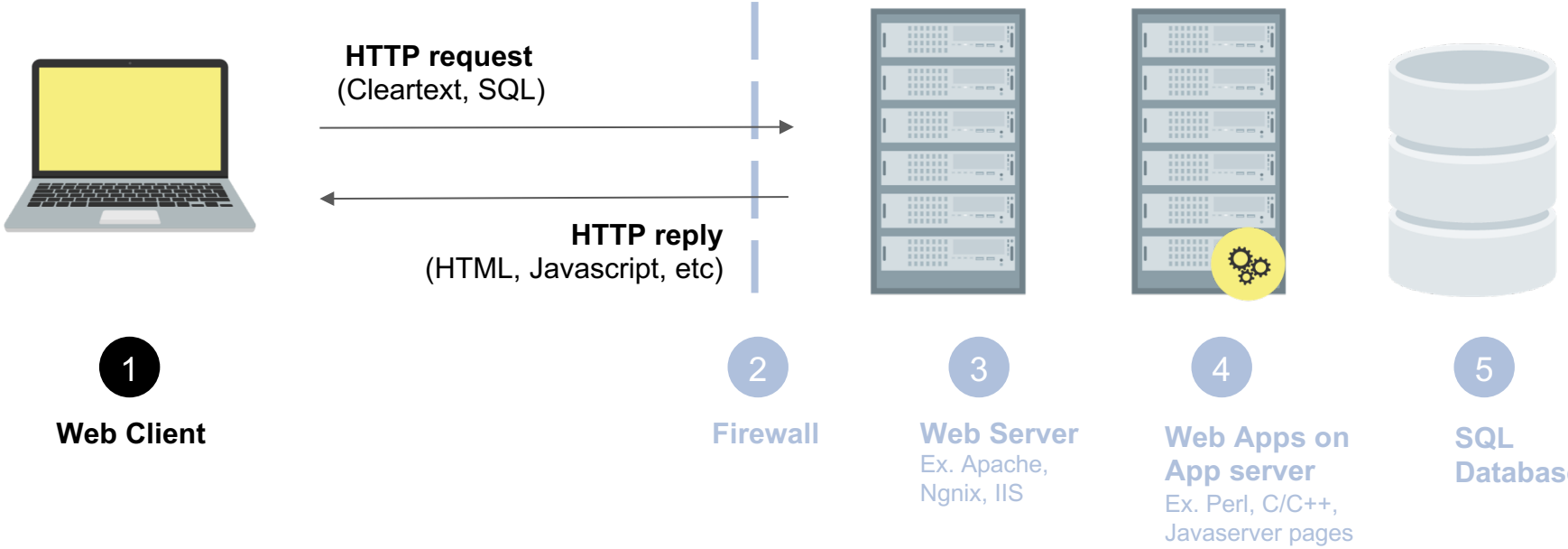


https://www.bugcrowd.com/hackers/


Meet the elite:
Google Project Zero.
https://googleprojectzero.blogspot.com/

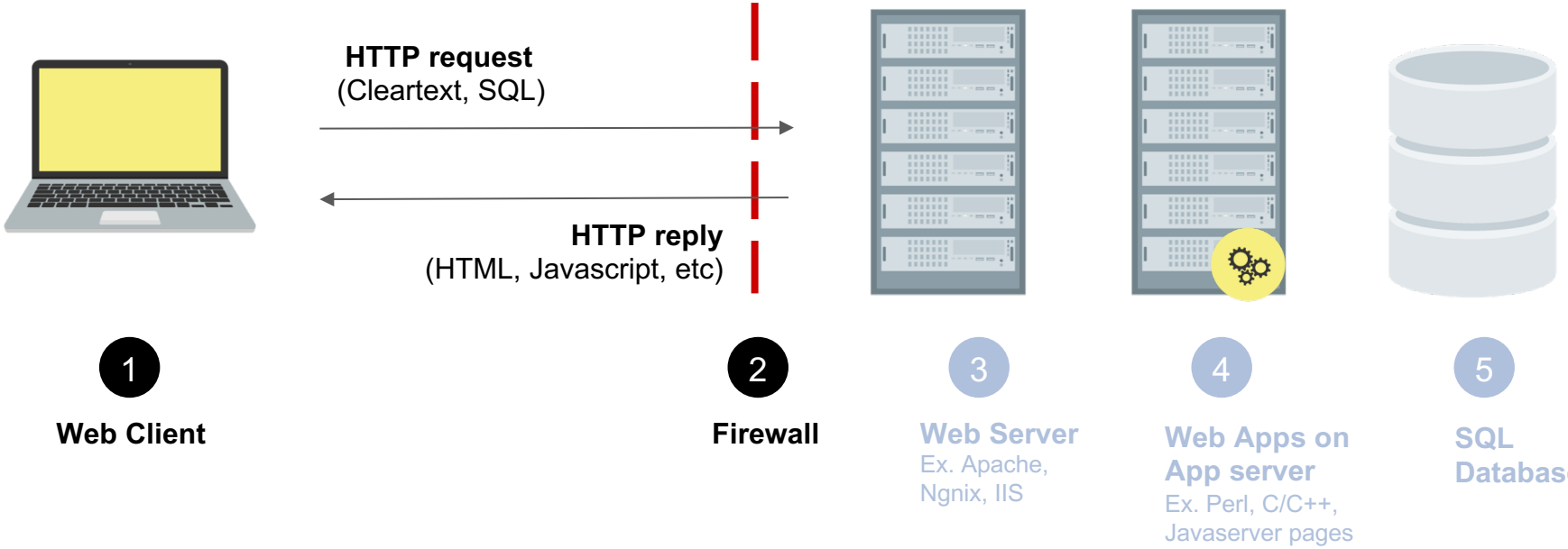
Components of Web Infrastructure: Client

A thing that makes requests.



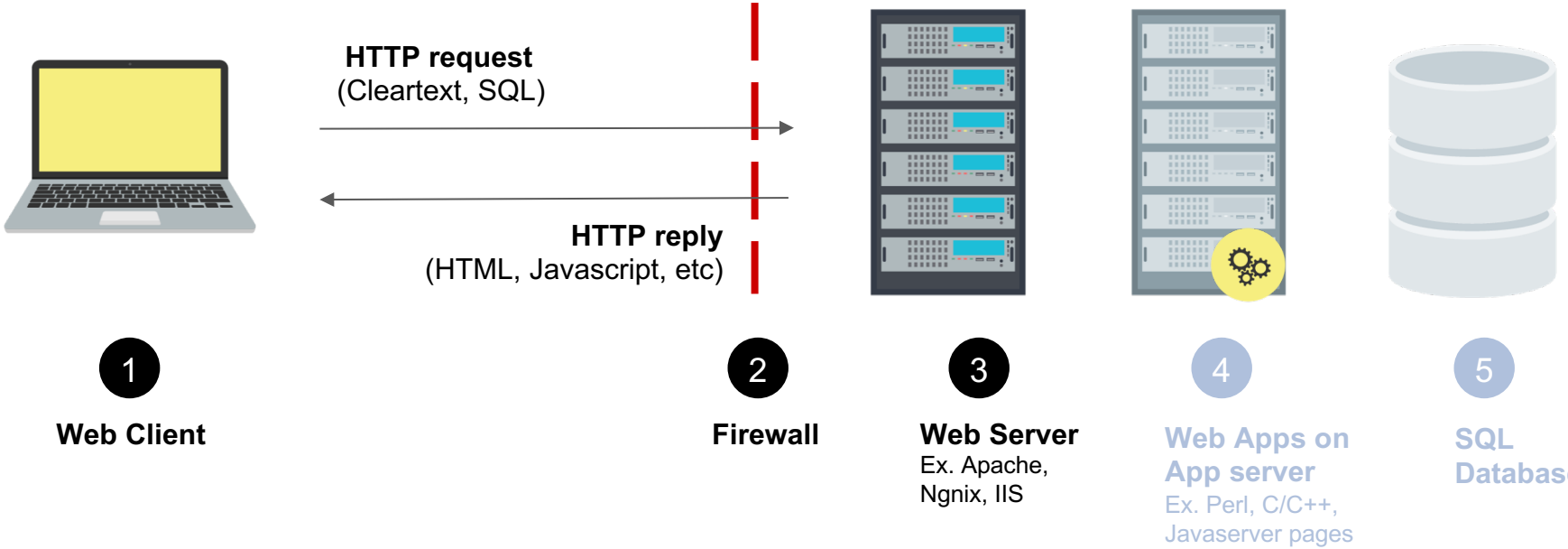
Components of Web Infrastructure: Firewall

A thing that enforces rules, probably to protect the application sitting behind it.



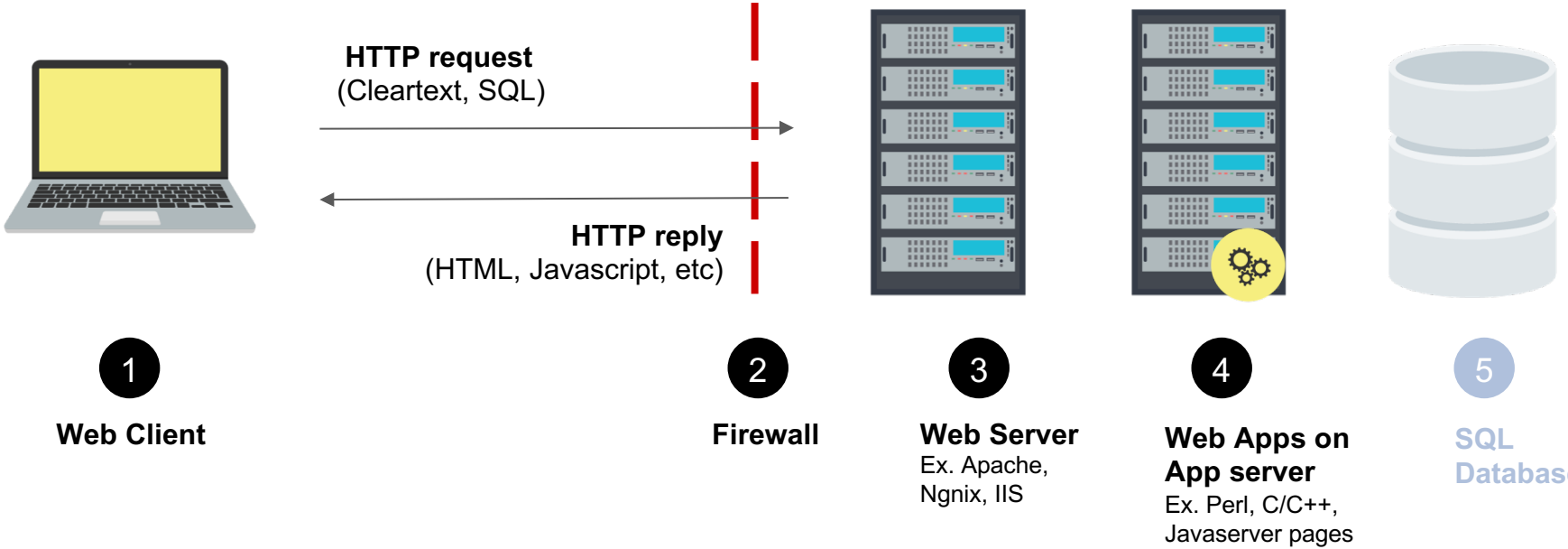
Components of Web Infrastructure: Web Server

An httpd service, such as Apache, Nginx, or IIS, that responds to a client's requests for resources.



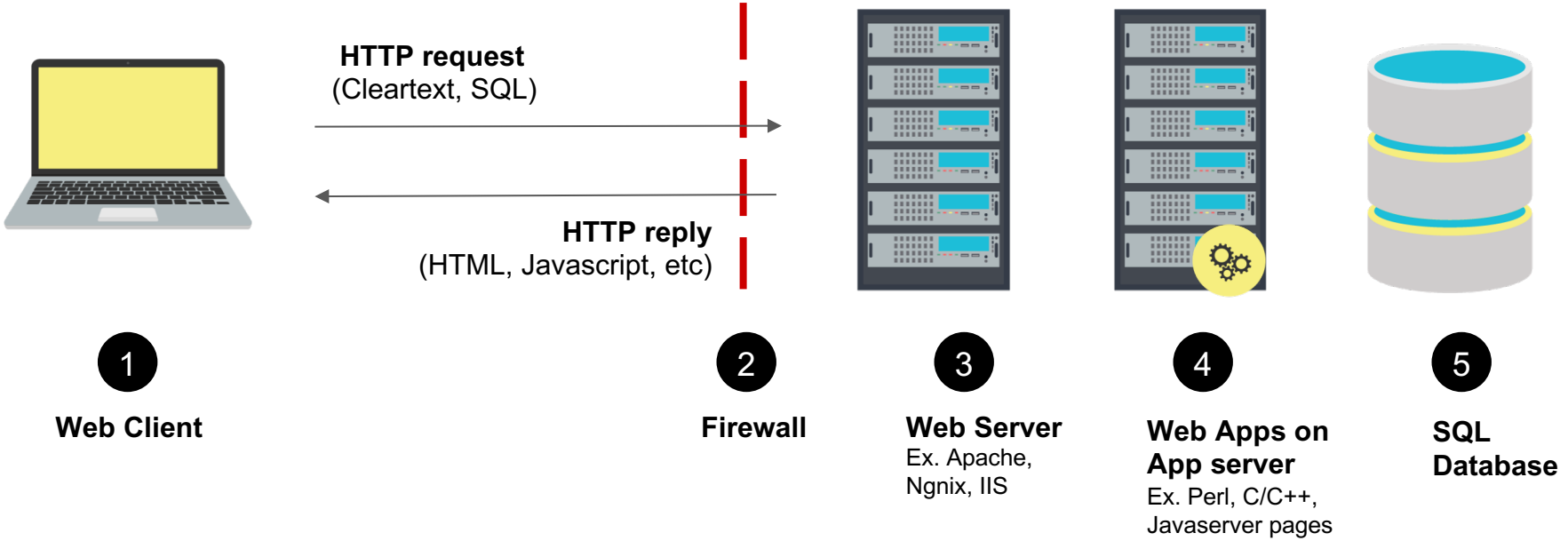
Components of Web Infrastructure: Web Application

Code that does some useful work. It probably has bugs!



Components of Web Infrastructure: Database

Storage for structured (indexed for retrieval) data like customer names, addresses, account numbers, and credit card info.



Client-Side and Server-Side Attacks

Components of a model Web Infrastructure

Remember this from 5 minutes ago?

01 **Client – Bug potential: High**

02 **Firewall – Bug potential: Low**

03 **Web Server – Bug potential: Low**

04 **Web Application – Bug potential: Insanely great**

05 **Database – Bug potential: Low**

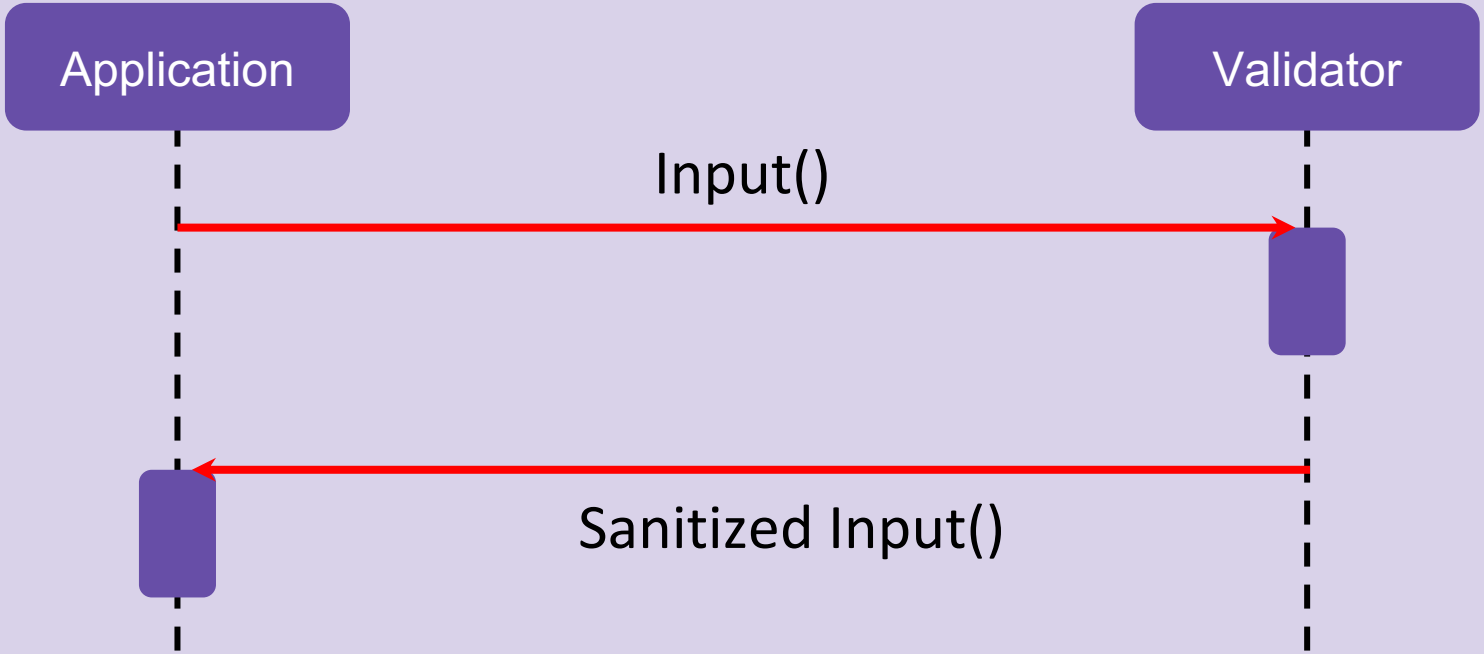
today’s globally connected cyber community

Don’t Trust User Input

And that includes the entire URL

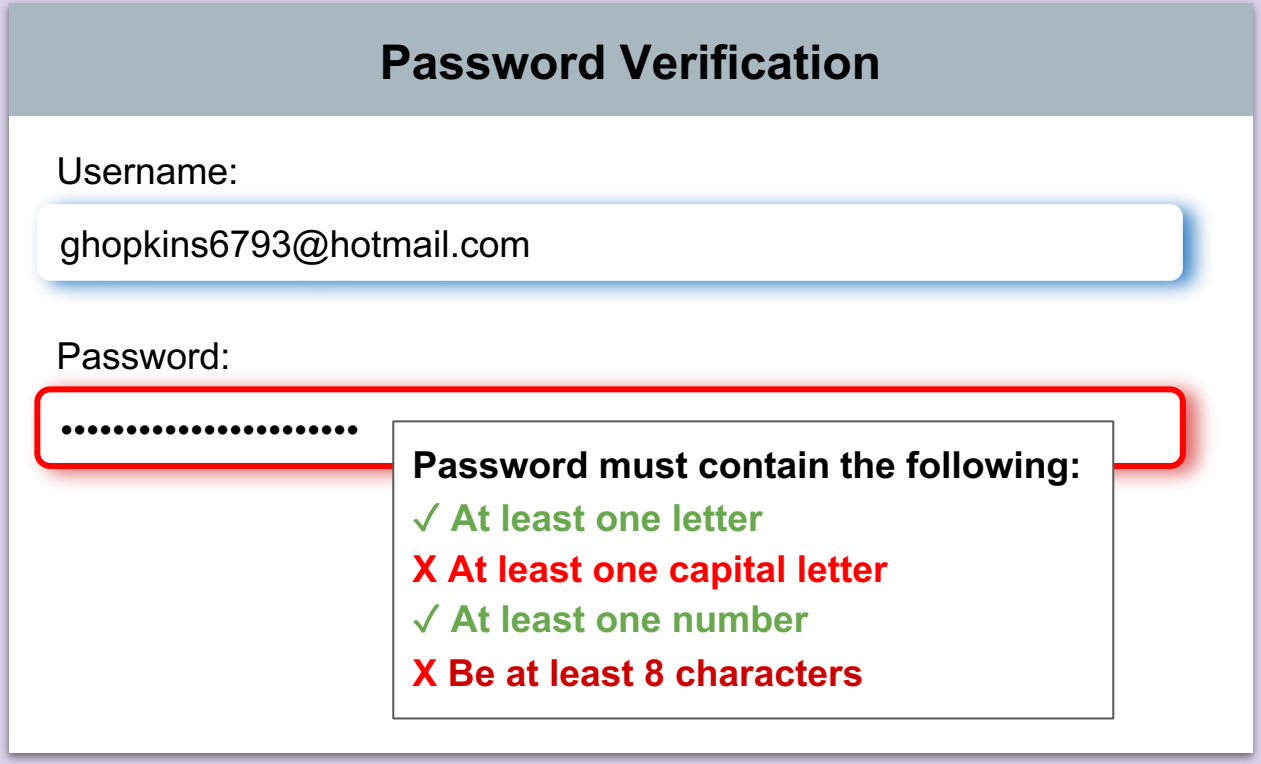
Risk Mitigation: Input sanitization

Web application (preferably server-side) actively modifies user input to an acceptable format or blocks the user's request.



Risk Mitigation: Input validation

Checks that user input is in an acceptable format.



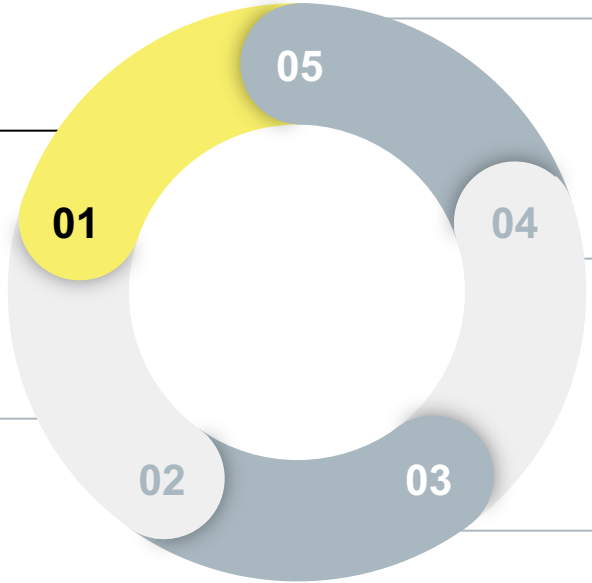
Reconnaissance and Information Gathering

The Hybrid Kill Chain

It includes the following stages:

Reconnaissance
Information gathered against a target

Weaponization
Preparation of offensive operations against specific targets using information gathered during reconnaissance.



Exfiltration
Ultimate goal. The exfiltration of private, sensitive data that the target considers critically sensitive.

Exploitation
Active compromise of adversary's apps, servers, or network, and averting physical, logical, or administrative controls.

Delivery
Launch of the operation. Attacks carried out based on Red Team offensive strategies.

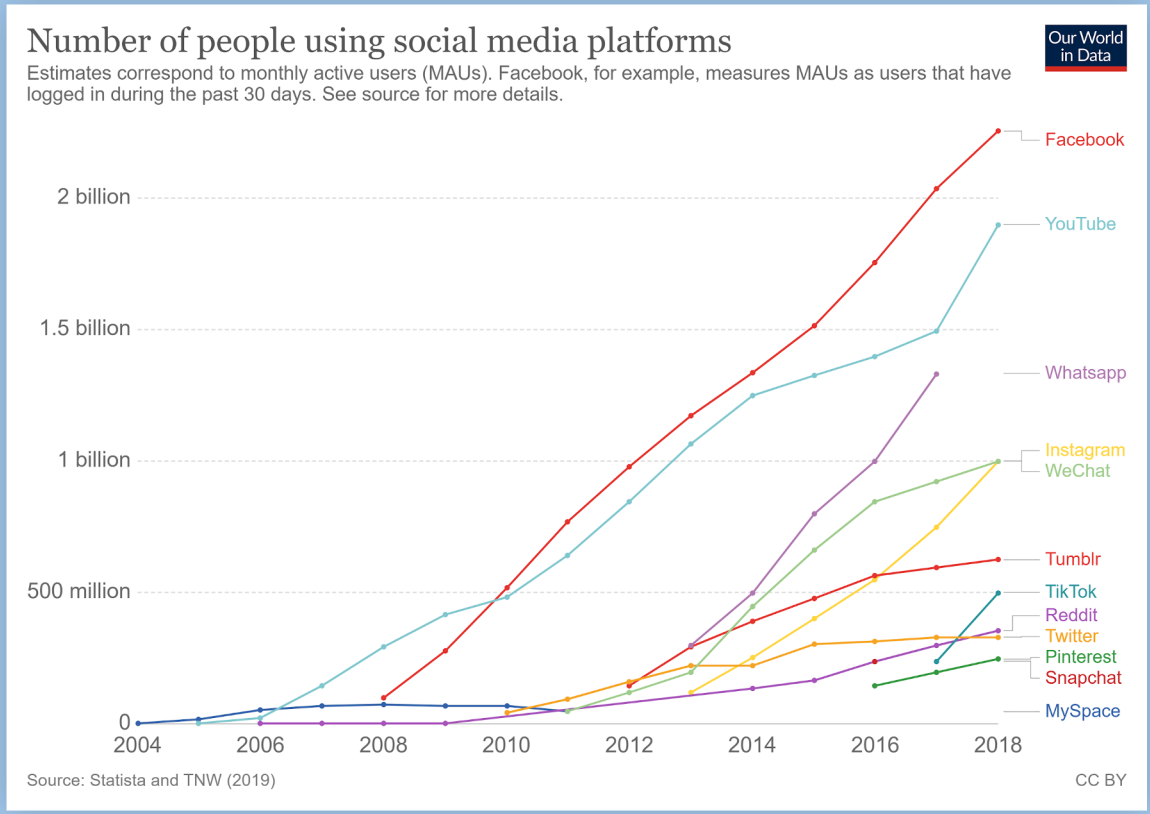
Reconnaissance

Facebook is the most popular online social media platform used today.

It can be thought of as an information wholesaler, making it incredibly desirable to attackers.

Reconnaissance

While not on the list, LinkedIn and its 500+ million users provide a wealth of information that can be used against employers and companies.



Reconnaissance

Social media has proven a profitable and effective way to build communities and engage customers. But to securely operate social media accounts, businesses must train employees to ensure they **do not**:

					
Engage with suspicious posts.	Share passwords.	Click on ads.	Use social media on public Wifi.	Use the same password for extended periods of time.	Follow accounts or people you don't know or haven't vetted.

Social Engineering

The attack surface is amplified for attackers who cross-reference information gathered from LinkedIn and Facebook, allowing them to carry out various social engineering attacks.

LinkedIn

- Types of hardware and software
- used by a company
- First and last names of employees
- Employee position information
- Length of employment
- Prior work history
- Education
- Skills and endorsements
- Previous projects

Facebook

- Names of friends and family
- Favorite hobbies
- Vacation spots
- Favorite books and movies
- Favorite foods, drinks and restaurants

Hackers also use more advanced forms of information gathering.

Web crawlers

Web crawlers, also known as spiders and spiderbots, index sites to help search engines find content.

Web crawlers: robots.txt file

01

To hide information from web crawlers, such as sensitive web server information, website owners can use the robots.txt file.

02

But excluding directories and pages indicates that they likely contain critical, sensitive data. This makes them attractive targets.

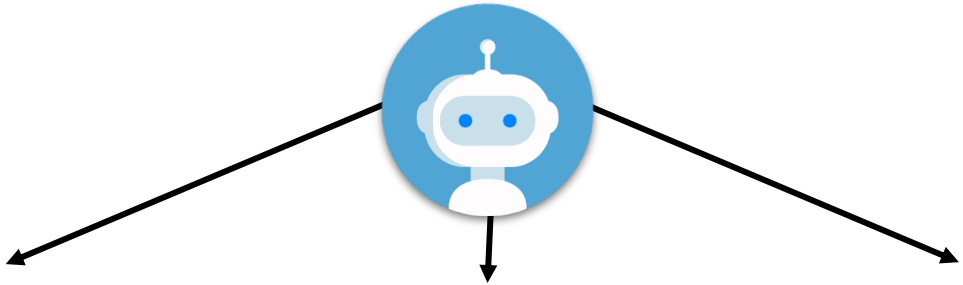
03

Experienced criminal hackers will attempt to harvest the robots.txt file to retrieve private data, such as content management system information and root directory structure.

robots.txt

A bot wants to visit the following URL: http://www.example.com/welcome.html

Prior to visiting the URL, it first checks http://www.example.com/robots.txt
It might receive any of the following responses:



User-agent: *
Disallow: /
Excludes all bots (indicated by the * wildcard symbol) from the entire server as indicated by disallowing access to the / root directory

User-agent: *
Disallow: /cgi-bin/
Disallow: /tmp/
Disallow: /user/
Excludes all bots from specific directories.

User-agent: BadBot
Disallow: /
Excludes a single bot (BadBot) from the entire server.

Bots

Two important security implications that organizations must consider when using **/robots.txt** files:

01 Malicious Bots

Bots can ignore your **robots.txt** file. Especially malware robots, which scan the web searching for security vulnerabilities.

02 “Don’t Look Here!”

robots.txt is available to the public.

Be aware that files that have been disallowed may be seen as opportunities to find important sensitive data. Otherwise they wouldn’t have been disallowed in the first place.

WHOIS

Another effective reconnaissance tool is the WHOIS protocol. WHOIS is a query and response protocol used for querying the WHOIS database.

As you may recall from earlier units, a WHOIS database stores registered user information including IP address blocks, domain names, email and street addresses, and phone numbers.

Whois Demo

We'll demonstrate using the WHOIS database with the following scenario:

A hacktivist is trying to infiltrate the local newspaper's network, The Sacramento Bee, in order to deface their home web page.

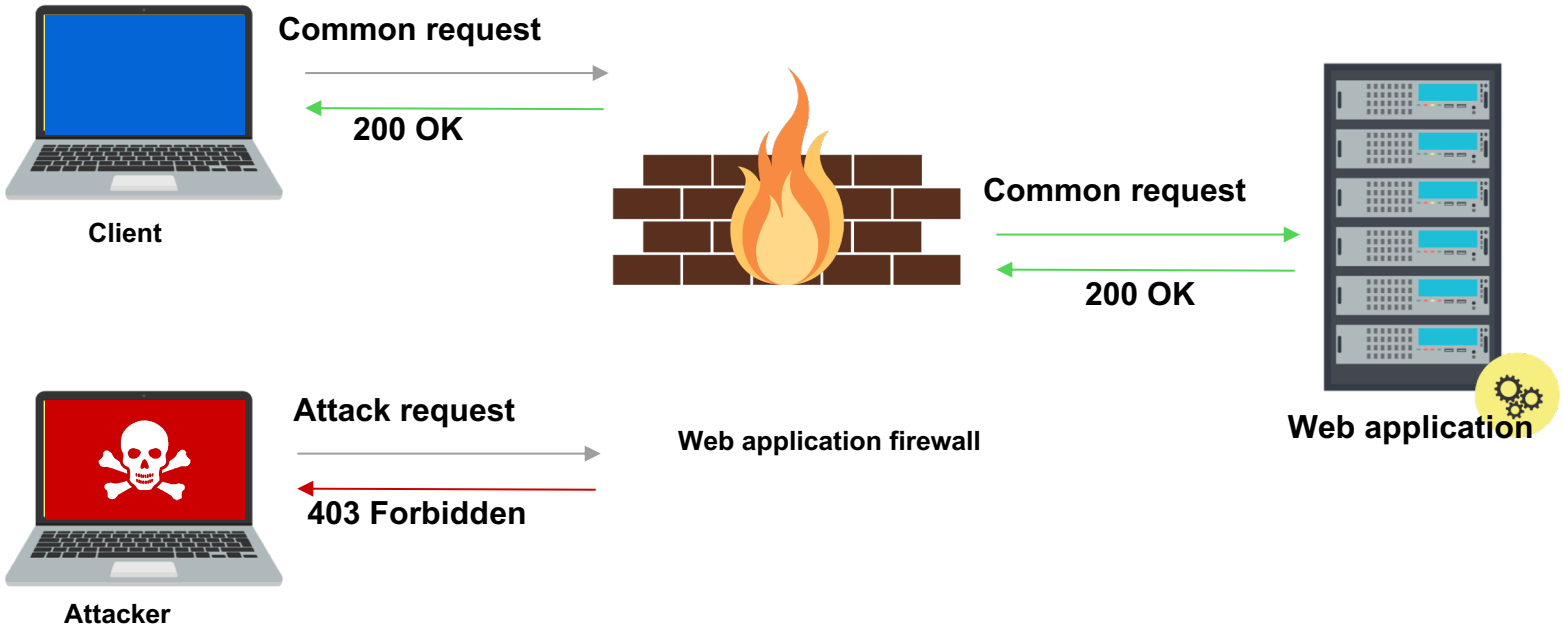
The hacktivist is upset about a recently published op-ed article that favors a view they oppose.

They've decided to produce a phishing email to collect personal data from the newspaper's website registrant by falsely stating that their domain name
will be taken offline due to non-payment.

We will use a WHOIS registration database query to find registered user information, such as emails and phone numbers.

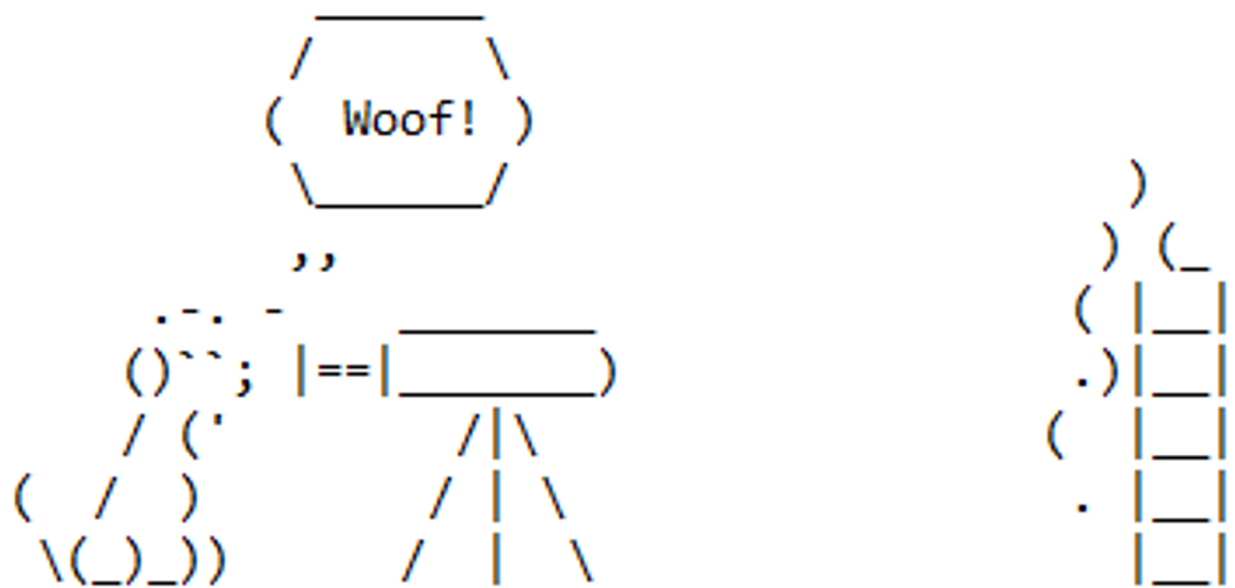
Web Application Firewalls

Web application firewalls (WAFs) are designed to defend against different types of HTTP attacks and various query types, such as SQLi and XSS.



Wafw00f

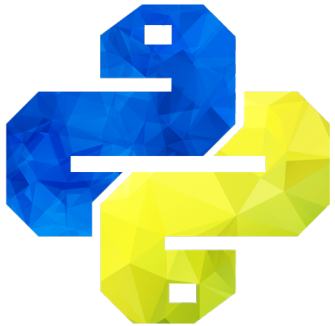
Wafw00f is an open source command-line WAF utility focused on web-based attacks that occur at the application layer.



Wafw00f

01 Python

It is written in Python and automates a carefully crafted set of procedures to determine if a website sits behind a web application firewall.



02 Vulnerabilities

Although WAFs are used to harden web server infrastructure, they do come with vulnerabilities of their own.

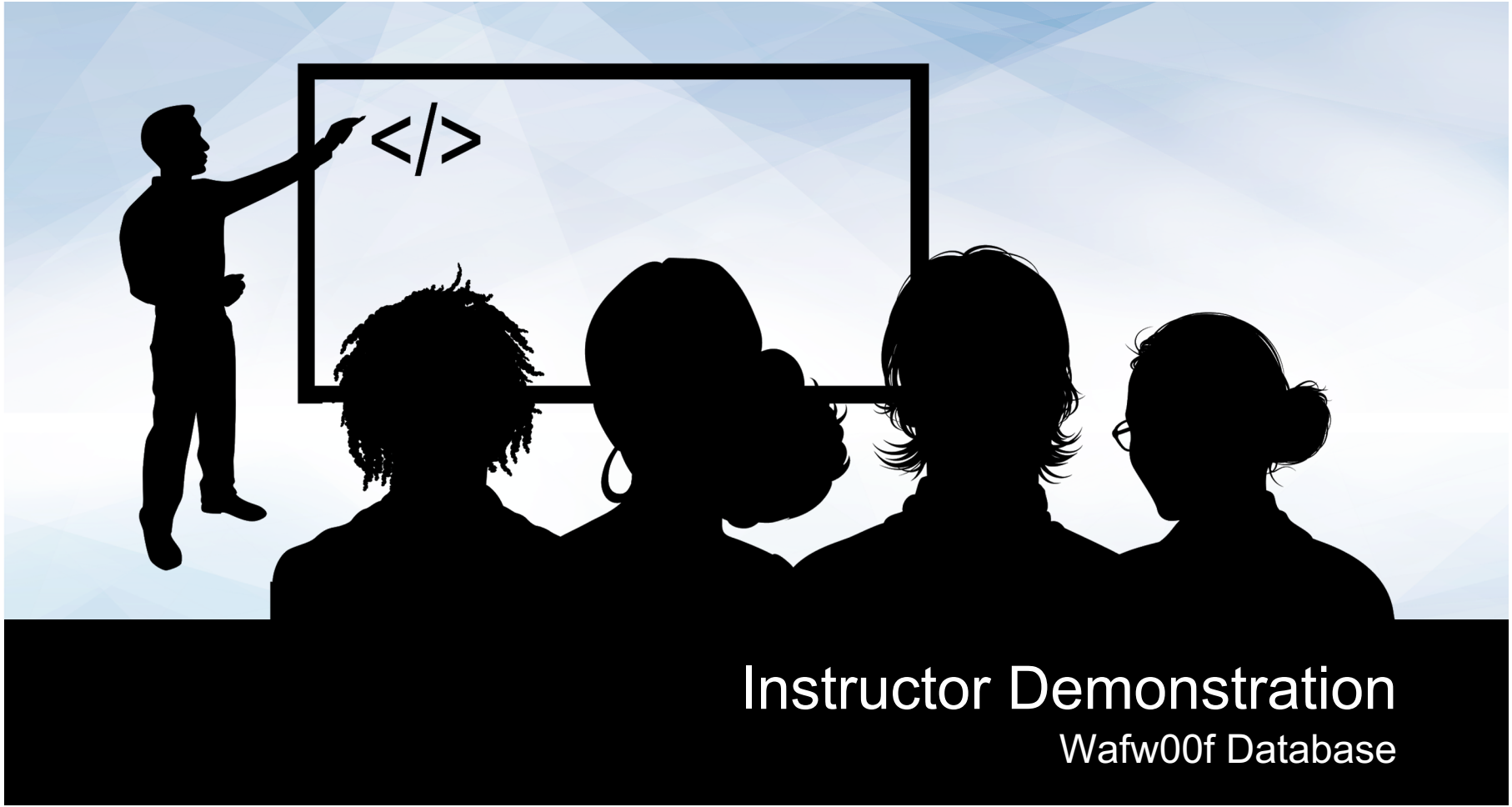
Wafw00f Demonstration

We'll demonstrate Wafw00f using the following scenario:

You're a criminal hacker looking to exploit any web vulnerability on a web site.

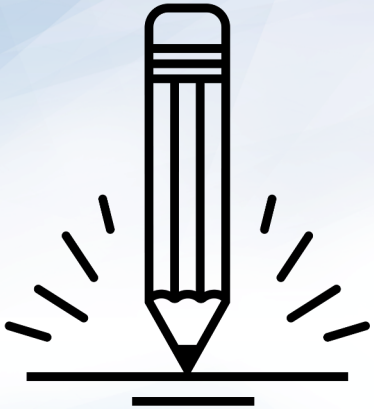
Before you can launch an attack, you need to know if the website is protected by a web application firewall and if so, what kind.

The results of this information gathering process will indicate the types of attacks that are available to you.



Instructor Demonstration

Wafw00f Database



Activity: Information Supermarket

In this activity, you will research how to mitigate data sourcing from web vulnerabilities that resulted in a surge of social engineering attacks.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Executing Attacks


The End.