# Workshops

Workshops all explained in text

- Introduction to Cyber Security
- Introduction to web

# Introduction to Cyber Security

The slides for this workshop can be found here

## Introduction

Consider the following four sentences, which ones would you consider 'hacking'?

- A security specialist finds a command injection vulnerability, allowing them to execute arbitrary system commands.
- A speedrunner discovers a new glitch, allowing them skip several levels ahead.
- A teenager asks chatGPT a question starting with “Please pretend to be my deceased grandma…”, resulting in an answer with detailed instructions on the production of napalm.
- A student borrows a course book from the library for the entire semester, paying $50 in late fees instead of buying the book for $300.

In essence, every one of them can be considered to be 'hacking'. Hacking is the process of finding creative, often unintended, ways of bypassing intended restrictions. But lets start off with a story that most people would associate with hacking.

## Saudi Aramco

Saudi Aramco is one of the largest companies in the world when measured by revenue. It does this by supplying nearly 15% of the worlds global oil and natural gas needs.

On the Wednesday morning of the 15th, 2012, employees were greeted with the image of a burning U.S flag on all the computers in the system. Hackers had managed to compromise the entire administrative network of Saudi Aramco, installing a wiper virus known as "Shamoon" on all computers, crippling the company. While the pumps themselves remained unaffected the company could no longer manage, distribute and sell the oil, causing millions in financial damage.

What happened? Well, the hackers had initially gained access through a phishing email, a user had downloaded a malicious file believing it to be a C.V. giving the hackers access. From there the hackers spent months expanding their access, gaining access to more machines, networks and accounts, until finally they deployed their malware.

# Why care

Over the next few weeks we will be giving several workshops on different aspects of cyber security. Each of these workshops will be more technical, focused on giving a basis for that particular aspect. We won't be teaching you how to be a master at hacking, partially because this would take far more time than these workshops last, but mostly because we are not masters at it ourselves. Instead, we will be focusing on giving you a basis to get started on, to then hopefully go out and learn more on your own.

In the workshops we will mostly be covering offensive cyber security, for example we will describe how to identify and exploit a particular vulnerability. Even if you don't have any interest in working in cyber security, most of you will likely end up building IT systems for companies. If we go back to the story of Saudi Aramco, everyone in your company will probably get training about not clicking strange links, plugging in strange USB sticks, etc. But you will be the ones that build the systems within the network, the systems that the hackers will target after they have infected a computer, the ones they will target to try to expand their access.

# StudSec

So now onto us, who are we? StudSec is an informal group that is part of STORM working with VuSec focussing on helping people get into cyber security. We have a discord (which will be linked at the end), CTF challenges, a wiki and we try to meetup once every two weeks to socialize and hack. We also participate in CTF competitions occasionally, under the name "vubar".

# Workshops

As mentioned we're planning to give several workshops, here is a quick overview of the ones we're planning to give in the coming weeks as well as tentative dates. We will be announcing them in the discord in advance. All workshops are interactive, and exercises will be provided.

## Web

In pure technical terms, web is focused on the security of systems interacting through the HTTP/HTTPS protocols. In more normal terms, this means everything revolving the websites we use every day. The servers serving the content and the browsers rendering them.

## Pwn

Pwn, also referred to as binary exploitation is the exploitation of lower level programs. Programs like C and C++ are memory unsafe, this means the programmer interacts directly with the computers memory, which can result in significantly faster programs but also brings a lot of security considerations.

## Crypto

Crypto, short for cryptography, focusses on the integrity and confidentiality of data. When you send a message over Whatsapp you want to be sure that the receiver and only the receiver reads your message, and that the receiver knows you were the one that sent it.

## Reversing

Reverse engineering, as the name implies, works backwards. Instead of writing a program, we take an existing program and try to understand how it works.

## Forensics

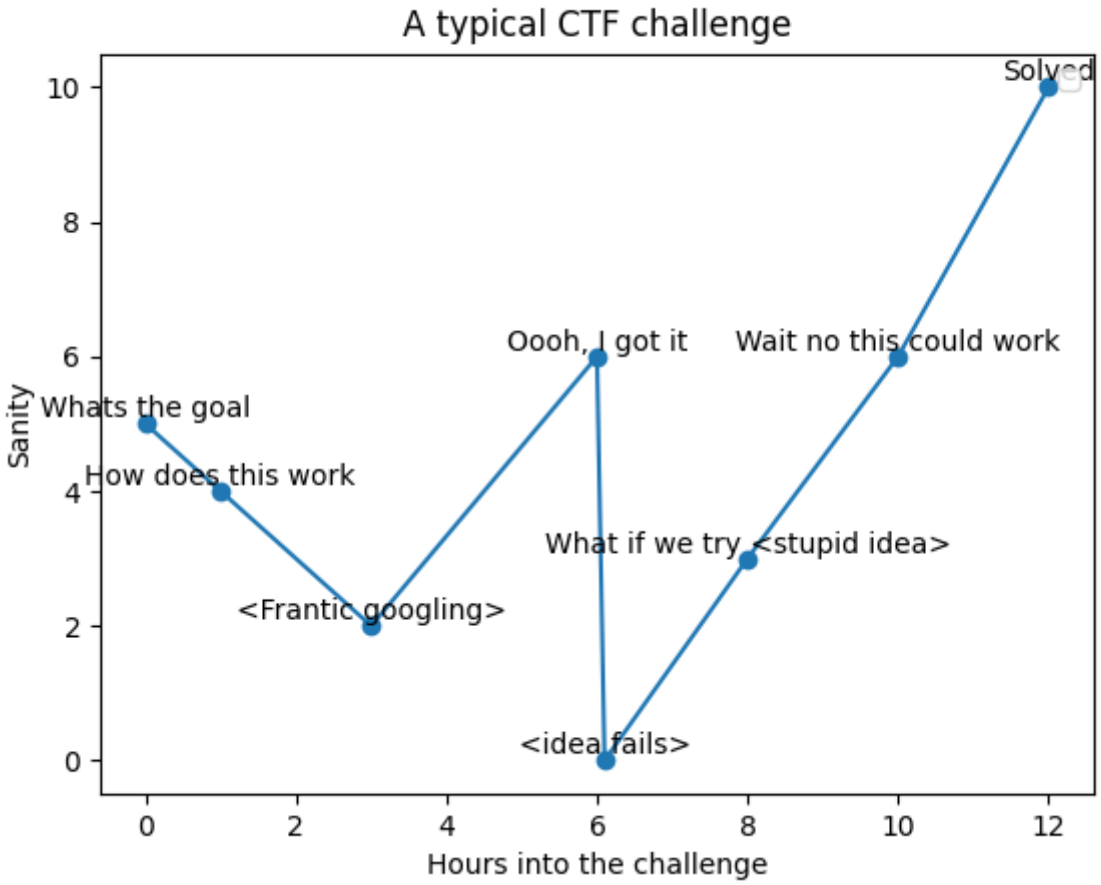
After a system has been hacked it is crucial to understand how the system was hacked, and what the hackers have done with this access, this is what forensics focusses on.

# Competitive Hacking - Capture the flag (CTF)

Capture the flag (CTF) is a specific type of hacking competition. These events are designed to serve as an educational exercise to give participants experience in dealing with real-world hacking situations. They are usually set up as a series of challenges, with each challenge involving a flag to capture. These flags are often hidden or protected in some manner, requiring the contestants to use various hacking skills to access them.

CTF competitions are global and take multiple forms; they may involve attack-defense style challenges, the most common being the Jeopardy style where multiple-choice questions are used. Other forms include King of the Hill and mixed competitions which have a combination of various styles.

When trying to find bugs, either in the real world or in CTF categories it will likely be a lot of frustrating failures. Regardless of skill a typical CTF challenge will go like this. There will be a lot of failed ideas, a lot of mistakes made, and that's part of the learning process.




# Cybersecurity

Cybersecurity refers to the practice of safeguarding information and its interconnected systems from unauthorized intrusion and disruption. As a broad-spectrum discipline, it encompasses a multitude of processes dedicated to maintaining and improving the security of information. The key adversary in this context is hacking. As these threats constantly evolve, so too do the protective measures against them, creating a perpetual cycle within the cybersecurity arena. This vast field of cybersecurity is further divided into specialized domains, each requiring an expert team to ensure comprehensive and effective protection, as depicted in the given diagram.


# Architecture and engineering.

The field of architecture and engineering encompasses a complex array of considerations that primarily revolve around balancing resources and managing risks. To illustrate, let's consider a simple residential building - a house. A house's design isn't simply about aesthetics or comfort; it also must consider the potential risks and safeguards necessary to protect its inhabitants. Here, the concept of security management comes in. Let's consider the installation of smoke detectors as an example.

In a small house, if only one smoke detector is available, it's typically installed in the kitchen, a high-risk area for fire generation. Nonetheless, even with this prevention measure, there's still the lingering threat that a fire could break out in the bedroom and potentially engulf the entire house before the smoke detector in the kitchen is set off.

This example demonstrates the complexities of architecture and engineering, where resources must be balanced, and safety risks need to be strategically managed. The primary focus lies not only in creating functional and appealing structures but also in ensuring the safety and security of its occupants against unpredictable or potentially overlooked hazards.  In this way, architecture and engineering are a constant play of compromises and decisions, aiming to achieve the best possible outcome within the available resources and constraints.

# Digital Forensics and Incident Response (DFIR)

Digital Forensics and Incident Response (DFIR) is a specific field of cybersecurity that involves collecting and analyzing computer systems and networks to uncover, understand and prevent incidents of security breaches.

DFIR is essential for a number of reasons, primarily because it aids in identifying exactly what went wrong when a security breach occurs. By accurately pinpointing the cause of the breach, improvements can be made to prevent such incidents from happening again in the future, and assist in tracing back the origin of the breach.

Let's illustrate DFIR with an example scenario using the given logs:

```
21:32:00 - User realuser logged in pc101.mycompany.com
21:32:15 - Application "SDClient.exe" started..
21:32:45 - access randomdomain.com/antivirusCheck
21:33:34 - User realuser started "Spotify.exe" on pc101
21:34:00 - Access google.com/upgradeRam
21:34:30 - NewFile: upgraderam.exe
21:35:12 - EventLogs: Administration Rights granted to upgraderam.exe
21:36:29 - Network logs: credential bruteforcing
21:36:48 - User realuser initiated system scan with "AVG.exe"
21:37:30 - access youtube.com/howToCookPasta
21:38:00 - User realuser started "Excel.exe" on pc101
22:01:00 - Network error occurred - Error 404 on stackoverflow.com
22:02:12 - User realuser logged off pc101.mycompany.com
```

Analyzing these logs, we can observe that the user 'realuser' logged in at 21:32:00, following which a number of applications started, and some internet access occurred. At 21:34:30, 'upgraderam.exe' was downloaded, and thereafter, administration rights were granted to this file, which appears suspicious.

The logs further show that around 21:36:29, there were attempts at credential bruteforcing, which is a method used in hacking, indicating a security compromise. The subsequent detection of a network error at 22:01:00 provides additional evidence that a security incident may have occurred.

This example showcases how DFIR allows for detailed scrutiny of security incidents, providing insights into what went wrong, thereby enabling cybersecurity experts to devise effective countermeasures and strategies for future protection.

## Hardware & Physical Security

While cybersecurity predominantly concerns itself with virtual threats and intrusions, it's crucial to remember that hardware and physical security are equally significant aspects of a comprehensive security strategy. Physical devices like servers, personal computers, and internet of things (IoT) devices present a tangible threat surface that can be physically tampered with or damaged. Several physical security measures can be employed to safeguard machines and equipment, such as robust locking mechanisms on server room doors, surveillance cameras, and man-traps, which allow only one person to pass through an area at a time. Other protocols include requiring identification keycards for access and monitoring via alarms and security personnel.

Among these measures, a critical consideration is the secure handling of removable media like USBs, which can potentially carry and introduce harmful malware into systems. Controls may involve prohibiting the use of personal removable media, regularly scanning authorized media for threats and ensuring effective destruction of data when no longer in use. A lot of such equipment which can be used to bypass measures can be found online, and it is recommended you take a brief look for example at hak5 which is a popular vendor.

In the realm of IoT devices, the threat can also come from reverse engineering wherein, a device is physically infiltrated to understand its inner workings, extract binary data, or create unauthorized reproductions. Manufacturers need to implement secure design and coding practices, encryption, and regular security updates to ensure the resilience of IoT devices against such physical attacks.

In conclusion, while the virtual world may seem like the most prominent battlefield for information security, the tangible, physical aspect should not be overlooked. The interplay between hardware and software security is key to a robust and effective security strategy.

# Further Reading

We have a little library for ebooks in progress so tune in!

## Cool videos

- I'll Let Myself In: Tactics of Physical Pen Testers
- You’re Probably Not Red Teaming... And Usually I’m Not, Either - SANS ICS 2018
- BREAKING in BAD (I’m the one who doesn’t knock) - Jayson Street
- DEFCON - The Full Documentary
- DEF CON 17 - That Awesome Time I Was Sued For Two Billion Dollars
- DEF CON 18 - Zoz - Pwned By The Owner: What Happens When You Steal A Hacker's Computer
- DEF CON 18 - Chris Paget - Practical Cellphone Spying
- DEF CON 19 - Deviant Ollam - Safe to Armed in Seconds
- DEF CON 21 - ZOZ - Hacking Driverless Vehicles
- DEF CON 22 - Metacortex and Grifter - Touring the Darkside of the Internet. An Introduction to Tor
- DEF CON 22 - Deviant Ollam & Howard Payne - Elevator Hacking - From the Pit to the Penthouse
- DEF CON 22 - Zoz - Don't Fuck It Up!
- DEF CON 23 - Robinson and Mitchell - Knocking my neighbors kids cruddy drone offline
- DEF CON 23 - Van Albert and Banks - Looping Surveillance Cameras through Live Editing

- DEF CON 23 - Chris Rock - I Will Kill You
- DEF CON 24 - Chris Rock - How to Overthrow a Government
- DEF CON 24 - Weston Hecker - Hacking Hotel Keys and Point of Sale Systems
- DEF CON 24 - int0x80 - Anti Forensics AF
- DEF CON 25 - Roger Dingledine - Next Generation Tor Onion Services
- DEF CON 26 - smea - Jailbreaking the 3DS Through 7 Years of Hardening

## Cool Youtube Channels

LiveOverflow

John Hammond

Ippsec

Computerphile

PwnFunction

DAY[0]

Nahamsec

Professor Messer

The Cyber Mentor

DEFCONConference

Hacksplained

HackerSploit

Open Security Training

Seytonic

Tib3rius

Tech Raj

Tom Scott

247CTF

# Conclusion

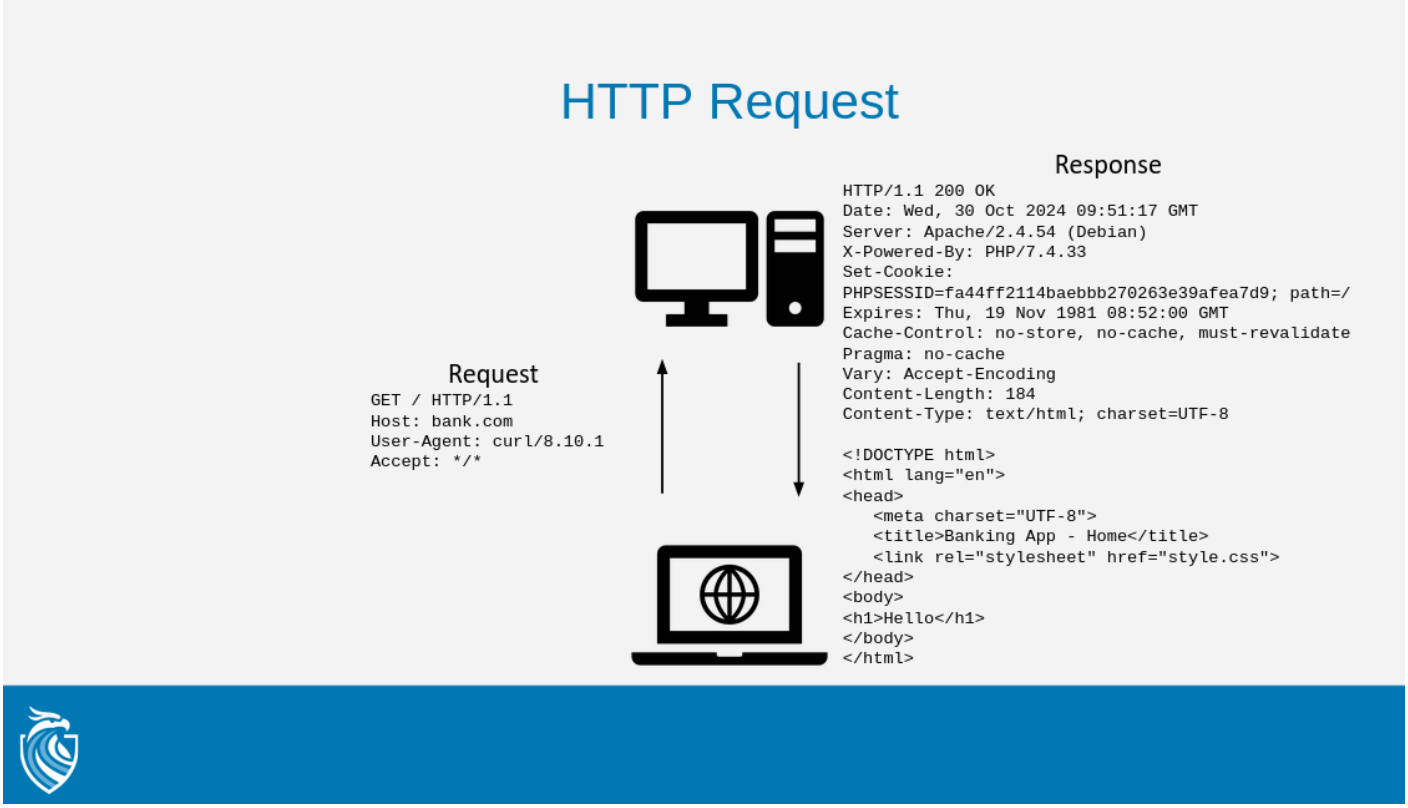
Overall, Cybersecurity is fun! If you have any questions feel free to post them on discord at any time :). Feel free to practice on our ctf.studsec.nl platform!

# Introduction to web

The slides can be found here, technical files for the workshop can be found here

## The modern web

When you open up your browser and go to a website, what happens? Well, after a bunch of networking steps are taken your computer sends a HTTP request to the website, specifically the web server. This server is a different computer that is running the website. The web server then processes the HTTP request and sends back an HTTP response, the overall interaction looks like this:

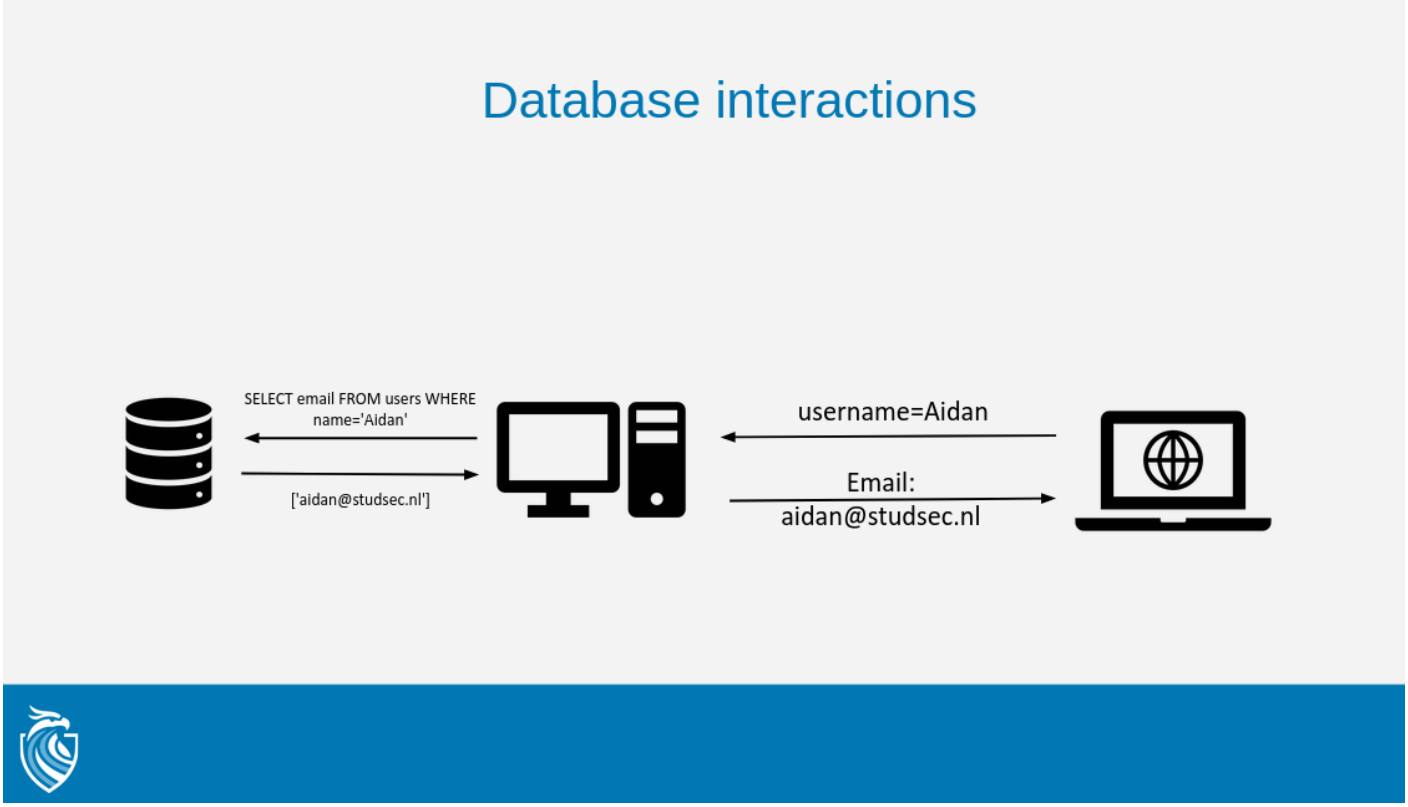



The first part is called the HTTP headers, these are key value pairs ending on a newline. After the newline comes the optional HTTP body, which can be seen in the response sent back by the server.

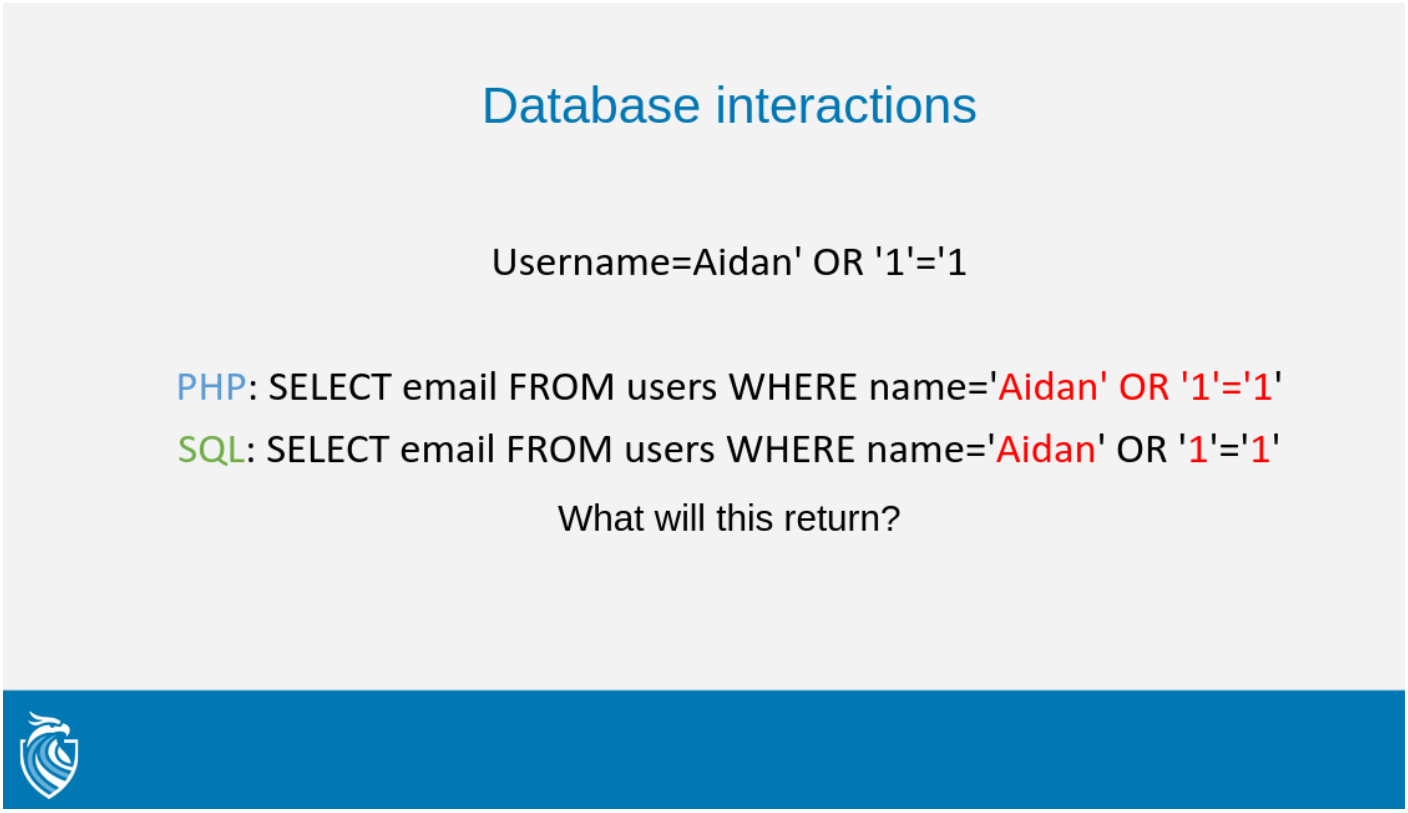
However, nowadays the interaction is often not as simple as that. The web server in turn might interact with other servers to process the HTTP request. One of these servers might be a database.

## A simple search engine

Suppose our website implements a search feature, that allows users to search entries in a database. The web server processes the users HTTP request and then uses it to query the database. The result is then sent back to the user, the overall interaction will look like:




Here you will notice the request sent to the database from the web server, "SELECT email FROM users WHERE name='Aidan'", this is an SQL query that will return all users who's name is "Aidan". But what happens when we add an apostrophe in our username query? And what if we then add some SQL after that? The result can be seen in the following image, note that variables are highlighted in red.



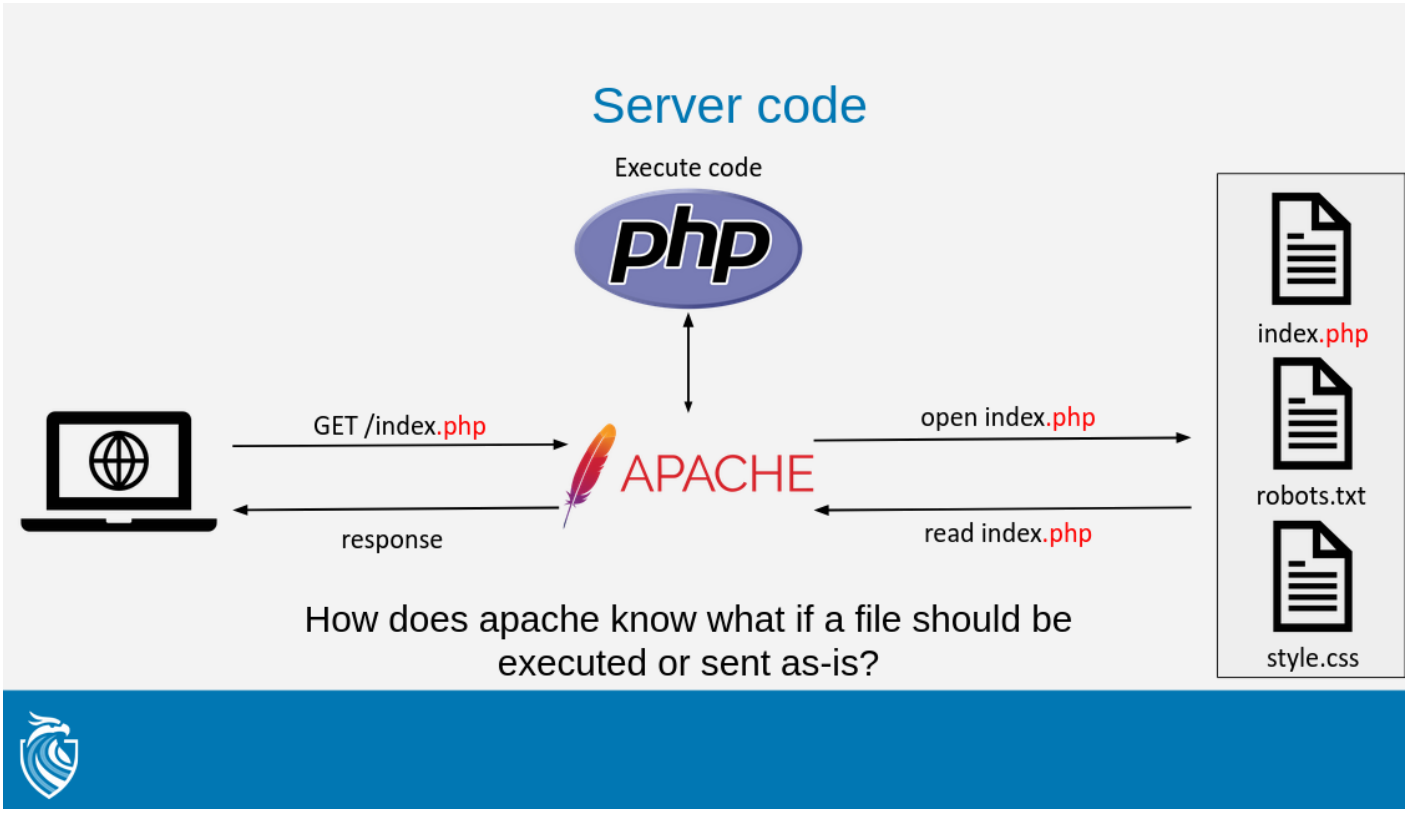

Here the web server (PHP) is asking for the email address of all users whose name is "Aidan' OR '1'='1". However, SQL will interpret the same string as "Give me the email of all users where the name is 'Aidan' or all users where 1=1", this will always be the case, meaning the database will return all entries.

Why is this a problem, we are supposed to  query the database right? Correct, but we are only allowed to get the "email" field of all users, by adding our own SQL we can get *all* information in the database, including possibly sensitive information like passwords.

# Uploading a file

Lets now turn our attention to the web server itself. Originally most websites were based on a folder structure, where each file could be accessed as a web page. This worked brilliantly for simply sharing and displaying files, where code (if any) would be run on the computer accessing the files. However, more complex systems, such as logging a user in or searching a database also required code to run on the web server.

One way this was implemented is with PHP, existing files could define PHP code that would be run on the server when the page was accessed. To distinguish between code that was intended to run on the server and normal text the web server looks at the file extension, a ".php" file will first execute the PHP code and then send the result to the client.




So far so good, but what if a website allows you to upload files? Say a profile picture or as personal storage, how does the web server know the difference between the original files and files that a user uploaded? Well, it doesn't, if a user manages to upload a file with a ".php" extension then they are able to run PHP code on the web server. This is a big problem, as it allows a user to run any command on the server as if it were their own computer, essentially giving them full control over the web server.