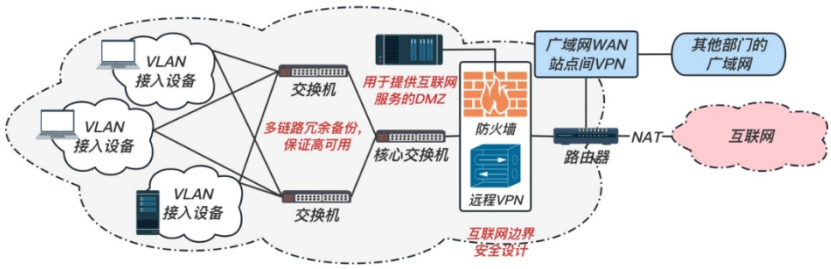
Elements of information security:

- Confidentiality: to ensure that information is not leaked to unauthorized people, even if the information is intercepted, the information expressed is not understood by non-authorized people→ **encryption**.
- Integrity: Prevents information from being tampered with by unauthorized people.
- Availability: Ensures that information can be used properly by authorized users. ▪ Controllability
- Non-repudiation: Provide a basis and cell for investigating security issues that arise. Detection and prosecution of malicious persons.

Response to risk: defense, detection, response

In the case of a completely closed internal grid where communication with the Internet is not considered, we need to consider:

- Strict access control should be applied to different workers by assigning them different identification; more stringent identification and multi-factor authentication are required for important and sensitive information about the service center (management systems, databases, etc. within the enterprise).
- Assign different sub-grid divisions to different departments and continue to divide VLANs within sub-grids to control access, reduce the ineffective use of bandwidth by intra-domain multicast, and minimize the scope of ARP-type attacks;
- It is necessary to encrypt the transmitted information in the intranet to prevent information leakage;
- All sections, at least the important ones, require a diary to record all user behaviors and provide a clue for troubleshooting after the fact.



As shown in the figure above, the following security risks may exist at the border of the interconnected grid:

- DoS attacks from the Internet (strategy: ***Anti-DDoS, WAF***);
- Encryption of plain files in HTTP protocol transfers (policy: ***HTTPS TLS/SSL***);
- If there is a Web application, then you need to consider the problem of various types of non-legal information being written in, such as SQL, XSS, etc. (strategy: troubleshoot the code, **validate the in/output**)
- VPN access should also be controlled at a finer level for different VPN users (policy: **configure different *VPNs***).
- .....

About the password:

- If the attacker uses force, we can set the number of attempts to block the account after a certain number of password entries.
- Change passwords regularly, do not set simple passwords.

- For high-privileged accounts, multi-factor authentication is required to avoid massive losses if a single authentication fails

---

How should organizations with remote workers secure their data?

- **Protect data in transit and at rest**. Access control and encryption are key technologies for data protection, and in addition, data transmitted over the Web, including the Internet, should be encrypted using HTTPS, VPN, or other methods.

  > Access control and encryption are the key technologies for protecting data. Additionally, data passing over networks, including the Internet, should be encrypted with HTTPS, a VPN, or another method.
  > Additionally, data passing over networks, including the Internet, should be encrypted with HTTPS, a VPN, or another method.

- **Protecting Staffed Endpoints**. Remote staffed endpoint devices must be protected from network attacks, as malware infections can lead to data leakage. At a minimum, the network should be protected at the endpoint of the device.
  Anti-malware software can be installed on devices. Loss of devices is even more common, which is another reason why device encryption is so important.

  > ***Protect employee endpoints***. Remote worker endpoint devices must be protected against cyberattacks, as malware infections can lead to data breaches. Lost devices are even more common, which is another reason why device encryption is so important. Lost devices are even more common, which is another reason why device encryption is so important.

- **We prevent account takeover practices such as phishing attacks**. The company must enforce a strict password policy. No one should be able to guess any employee's password, and passwords should be able to withstand most machine attacks. If possible, companies should implement two-factor authentication for each corporate application used.

  > Companies must enforce a strong password policy. No one should be able to guess any employee's password, and the password should be able to withstand most bot attacks. ***No one should be able to guess any*** employee's password, and the password should be able to withstand most bot attacks. No one should be able to guess any employee's password, and the password should be able to withstand most bot attacks.

DoS

What is a *DDoS* attack?

A Distributed Denial of Service (DDoS) attack is the destruction of a destination server by flooding it or its surrounding infrastructure with massive amounts of interconnected web traffic,
Malicious behavior in the normal flow of traffic to a service or network.

> A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a floo d of Internet traffic.

DDoS attacks utilize multiple compromised computer systems as a source of attack traffic to achieve the attack effect. The machines utilized can include computers as well as other network resources such as IoT

devices.

> DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

In general, a DDoS attack is akin to a highway traffic jam, preventing regular vehicles from reaching their intended destination.

Principles of *DDoS* Attacks

DDoS attacks are performed on computer networks connected to the Internet.

> DDoS attacks are carried out with networks of Internet-connected machines.

These grids consist of computers and other devices, such as IoT devices, that are infected with malware so that they can be remotely controlled by an attacker. These individual devices
A machine is called a人(或僵尸) and a group of machines is called a grid of rigidities.

> These networks consist of computers and other devices (such as IoT devices) which have been infected with malwares, allowing them to be controlled These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.

Once a rigid grid is established, an attacker can launch an attack by sending remote commands to each machine.

> Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a dead grid targets a victim's server or network, each machine sends requests to the target IP address, which can overwhelm the server or network and cause a denial of service for normal traffic.

> When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Since every machine is a legitimate Internet device, it may be difficult to distinguish between attack traffic and normal traffic.

> Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

DDoS Attacks at the Application Layer

Attack Objectives

This type of attack is sometimes referred to as a Layer 7 DDoS attack (referring to Layer 7 of the OSI model), and its goal is to exhaust the resources of the destination.

> Sometimes referred to as a Application Layer DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the target's resources to create a denial-of-service. 's resources to create a denial-of-service.

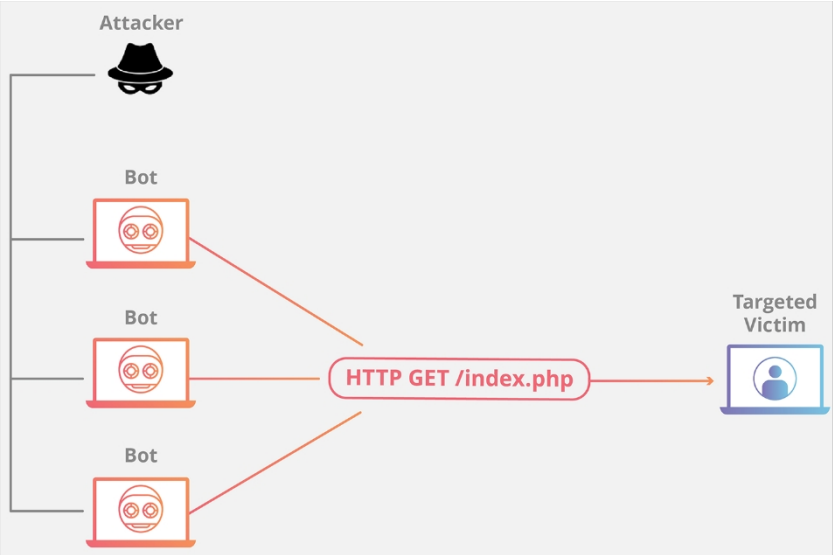
The target of the attack is the server layer that creates the web page and transmits it in response to an HTTP request. While it is computationally relatively inexpensive to execute an HTTP request on the client side, it can be expensive to respond to the destination server, which often has to load multiple files and run database queries to create the web page.

> The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files. computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files A single HTTP request is computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files and runs database queries in order to create a web page.

Layer 7 attacks are difficult to defend against because it is difficult to distinguish between malicious traffic and legitimate traffic.

> These attacks are difficult to defend against, since it can be hard to differentiate malicious traffic from legitimate traffic.

Examples of Attacks Using the Program Layer



HTTP Hungry

An HTTP flood attack is similar to hitting refresh over and over again in a web browser on a large number of different computers at the same time - a massive influx of ***HTTP requests*** to the server, resulting in a denial of service.

> HTTP flood attack is similar to pressing refresh in a web browser over and over on many different computers at once - large numbers of ***HTTP requests flood the server, resulting in denial-of-service. requests*** flood the server, resulting in denial-of-service.

Simpler implementations can use the same range of attacking IP addresses, referrers, and user agents to access a URL, while more complex versions may use a large number of attacking IP addresses and random referrers and user agents to target random web addresses.

> Simpler implementations may access one URL with the same range of attacking IP addresses, referrers and user agents. Complex versions may use a large Complex versions may use a large number of attacking IP addresses, and target random urls using random referrers and user agents.

Two HTTP flooding attacks.

- HTTP GET attack: Using large GET requests to request large resources such as photos from the server.
- HTTP POST attack: A large number of POST requests submit a post form to the server, which consumes a large amount of resources due to persistent operations.

Methods of Protection

- To test whether it is a machine, it is very similar to the CAPTCHA test often used when creating an account online.
- Use Web Application Firewalls (WAF), etc.

Protocol *DDoS* attacks

Attack

Objectiv

es

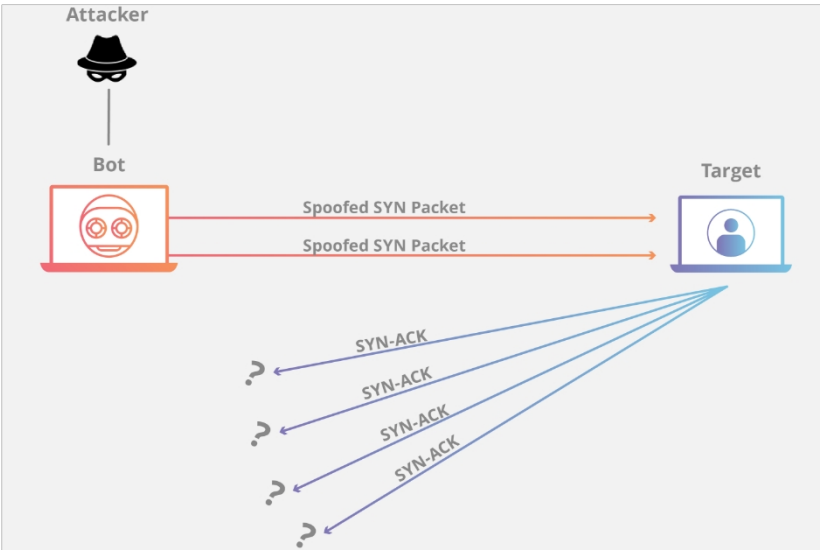
Protocol attacks, also known as stateful exhaustion attacks, can cause service interruptions by over-consuming server resources and/or the resources of network devices such as firewalls and load balancers.

> Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers.

Protocol attacks exploit weaknesses in layers 3 and 4 o f the protocol stack to render objects inaccessible.

> Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

Examples of protocol attacks



SYN Hong-Wui

SYN flooding is achieved using the TCP handshake by sending a large number of TCP "Initial Connection Request" SYN packets to the destination with a forged source IP address.

> A SYN flood attack exploits the TCP handshake by sending a target a large number of TCP "Initial Connection Request" SYN packets with spoofed source IP addresses. packets with spoofed source IP addresses.

The target computer responds to each connection request and then waits for the last step in the handshake, which is never taken, thus exhausting the target computer in the process.
resources.

> The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target 's resources in the process.

1. Attackers usually use spoofed IP addresses to send large numbers of SYN packets to the destination server.
2. The server then responds to each connection request separately and ensures that the open end is ready to receive the response.

3. While the server waits for the last ACK packet, which never arrives, the attacker will continue to send more SYN packets. Each time a new SYN packet arrives, the server temporarily opens a new endpoint and maintains connectivity for a specific period of time; after all available endpoints have been used, the server will be unable to function normally.

[Relief Method

- Increasing Backlog queue
- Recycling the Oldest Half-Open TCP Connection
- SYN Cookie

Capacity Depletion Attack

Attack

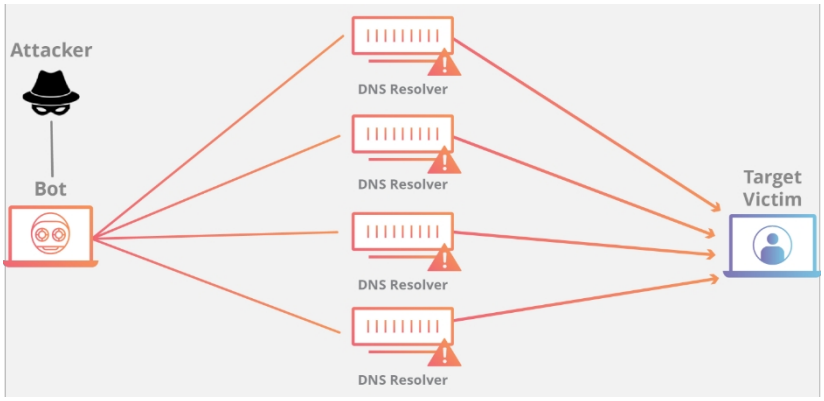
Objectiv

es

This type of attack attempts to cause congestion by consuming all available bandwidth between the destination and the larger Internet network. The attack sends a large amount of data to the destination using some kind of amplification attack or other means of creating a large amount of traffic (e.g., stiffening the web request).

> This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic such as requests from a botnet. data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

DNS Enlargement



When a request is sent to an open DNS server using a fake IP address (the victim's IP address), the destination IP address receives a response back from the server.

> By making a request to an open DNS server with a spoofed IP address (the IP address of the victim), the target IP address then receives a response from the server.

The DNS Enrichment Conference can be divided into four steps:

1. An attacker causes a compromised endpoint to send UDP packets with spoofed IP addresses to a DNS recursive server. The spoofed address on the packet points to
   The real IP address of the victim.
2. Each UDP packet sends a request to the DNS resolver, usually passing a parameter (e.g., "ANY") to receive the largest possible response.
3. The DNS resolver receives the request and sends a larger response to the spoofed IP address.
4. The destination IP address receives the response and its neighboring network infrastructure is flooded with

heavy traffic, leading to a denial of service.

Although a small number of requests are insufficient to bring the web infrastructure offline, the amount of data eventually received by the destination becomes very large after the process is doubled by multiple requests and DNS resolvers.

How to protect against *DDoS* attacks?

The key to mitigating DDoS attacks is to **distinguish between attack traffic and normal traffic**.

> The key concern in mitigating a DDoS attack is differentiating between attack traffic and normal traffic.

speed limit

Limiting the number of requests a server receives at a given time is also a way to protect against denial of service attacks.

> Limiting the number of requests a server will accept over a certain time window is also a way of mitigating denial-of-service attacks.

While rate limiting can be helpful in slowing down web crawlers from stealing content and protecting against forceful cracking attacks, rate limiting alone may not be sufficient to effectively combat sophisticated DDoS attacks.

> While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be insufficient to handle a complex DDoS attack effectively.

Web Application Firewalls

A Web Application Firewall (WAF) is an effective tool to help mitigate Layer 7 DDoS attacks. Deploying a WAF between the Internet and the Source Site
The WAF can then act as a reverse proxy to protect the destination server from specific types of malicious traffic.

> A Web Application Firewall (WAF) is a tool that can assist in mitigating a layer 7 DDoS attack. By putting a WAF between the Internet and an origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic. By putting a WAF between the Internet and an origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic.

Layer 7 attacks can be blocked by filtering requests based on a set of rules used to identify DDoS tools. One of the key values of an effective WAF is the ability to
Rapid implementation of custom rules to respond to attacks.

> By filtering requests based on a series of rules used to identify DDoS tools, layer 7 attacks can be impeded. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack.

Anycast grid diffusion

This mitigation method uses the Anycast network to spread the attack traffic to a distributed server network until the network absorbs the traffic.

> This mitigation approach uses an Anycast network to scatter the attack traffic across a network of distribut ed servers to the point where the traffic is absorbed by the network.

This approach spreads the impact of distributed attack traffic to a manageable level to spread the damage.

> This approach spreads the impact of the distributed attack traffic to the point where it becomes manageable, diffusing any disruptive capability.

The reliability of t h e Anycast grid in mitigating DDoS attacks depends on the scale of the attack and the size and efficiency of the grid.

> The reliability of an Anycast network to mitigate a DDoS attack is dependent on the size of the attack and the size and efficiency of the network.

Web Application Security

Web application security is the practice of **protecting web sites, applications, and *APIs* from attacks**. It is a broad discipline, but its ultimate goal is to keep the Web safe from attacks.
Web applications run smoothly and protect your business from network disruption, data theft, unethical competition, and other negative consequences.

> Web application security is the practice of protecting ***websites***, ***applications***, and ***APIs*** from attacks.

The global nature of the Internet exposes Web applications and APIs to attacks from many locations and at various scales and complexity levels. As a result, Web applications and APIs are exposed to attacks from many locations and at various scales and levels of complexity.
Program security encompasses a variety of strategies that cover many parts of the software supply chain.

Web applications may face many types of attacks, depending on the target of the attacker, the nature of the work of the target organization, and the specific security vulnerabilities of the application.
Holes. Common types of attacks include:

SQL Injection

SQL Insertion By inserting a specialized SQL statement into an input field, an attacker can execute commands that allow data to be retrieved from a database, sensitive data to be corrupted, or other manipulations to be performed.

> By inserting specialized SQL statements into an entry field, a SQL injection attacker is able to execute commands that allow for the retrieval of data from the database, the destruction of sensitive data, or other manipulative behaviors.

By properly executing SQL commands, unauthorized users can assume the identity of a more privileged user, make themselves or others database administrators, tamper with existing data, modify transactions and balances, and retrieve and/or destroy all server data.

How SQL Insertion Attacks Work

An SQL query field that should be reserved for a specific type of data (such as a number) passed unexpected information (such as a command). The command was executed outside of the expected range, allowing potentially harmful behavior. Query fields are typically populated with data that is entered into a form on a web page.

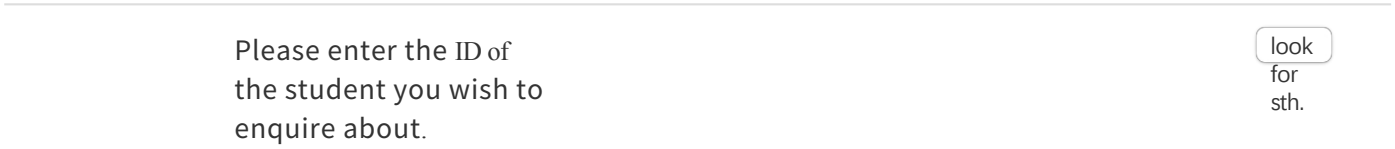
> A SQL query field that is supposed to be reserved for a particular type of data, such as a number is instead passed unexpected information, such as a command. The command, when run, escapes beyond the intended confines, allowing for potentially nefarious behavior. A query field is commonly populated from data A query field is commonly populated from data entered into a form on a webpage.

Let's briefly compare normal and malicious SQL statements:

Normal SQL Query

Let us assume that the front-end page provides a need to inquire about a student's生 ID number and return

all information about the student. The following is an example



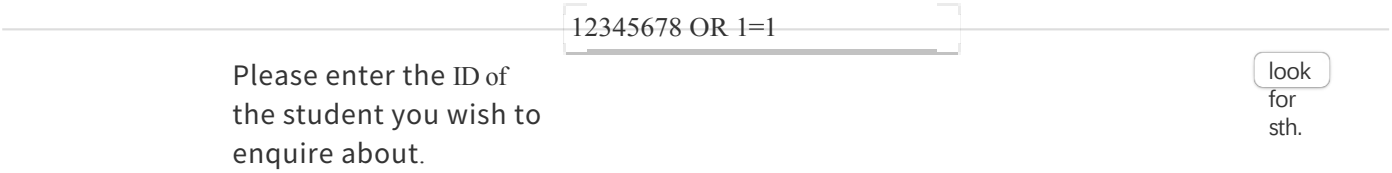
The SQL queries created on the backend will be similar:

```
SELECT * FROM t_stundents WHERE student_id = 12345678.
```

This command will return a record of the student with a specific student_id, as expected by the developers who wrote the API.

SQL Injection Query:

In the example above, the attacker enters a SQL command or conditional logic in the Enter field, and enters the student ID number:



Similarly, the SQL queries created on the backend will be similar:

```
SELECT * FROM t_stundents WHERE student_id = 12345678 OR 1=1;
```

Since 1=1 in the query condition is always TRUE, the query returns all the data in the t_students table to the attacker who executes the query.

How to prevent SQL injection attacks?

Anything consumed by a user program that is external (not directly and exclusively controlled by the user program, such as file systems and databases) **must be verified before consumption**.

Let's explore some of the more common implementations:

- Escape All User Supplied Input [**Escape** All User Supplied Input]:

  When writing SQL, specific characters or words have specific meanings. For example, the "*" character indicates "arbitrary" and "OR" indicates conditional. To prevent users from accidentally or maliciously entering these characters in API requests to the database, the input provided by the user can be escaped. Escaping the characters is a way to tell the database not to parse them as commands or conditions, but rather to treat them as text input.

- Use of Prepared Statements (with Parameterized Queries)]:

  This method of cleaning up the database input requires forcing the developer to define all the SQL code first, and then pass only specific parameters to the SQL query; the input
  The data entered is explicitly given a limited scope and cannot be extended. This allows the database to distinguish between the data being entered and the code to be run, regardless of the type of data provided in the entry field.

Cross Site Scripting *(XSS)*

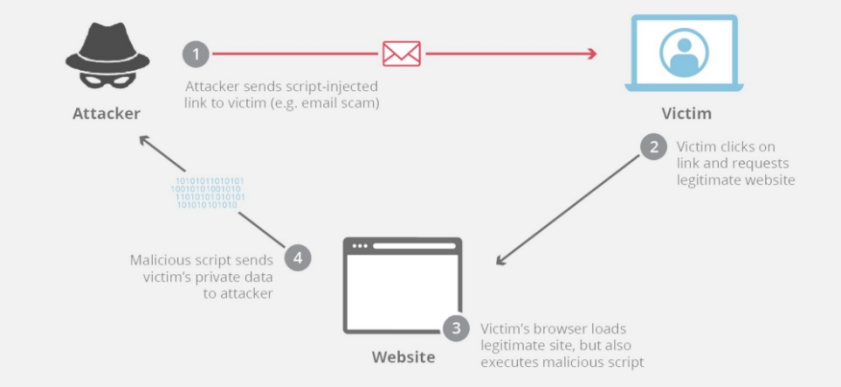
What is cross-site scripting?

Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will

> execute when the victim loads the website. Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the w e b s i t e .

Malicious code can be inserted in several ways. Most commonly, it is added to the end of a URL or posted directly to a page displaying user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.

> That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a URL or posted directly onto a page that displays user- generated content. In more technical terms, cross-site scripting is a client-side code injection attack.



XSS How to Attack

Cross-site scripting attacks are common on **unauthenticated websites with commenting capabilities**. In this case, the attacker posts a message **containing the *<script>* script code Comments on *</script>* tags**. These tags tell the Web browser to interpret everything between the <script> tags as JavaScript code. After the comment appears on the page, any other user who loads the site will have their Web browser execute the malicious code between the script tags, and the user will be the victim of an attack.

> One useful example of cross-site scripting attacks is commonly seen on websites that have unvalidated comment forums. In this case, an attacker will post a comment consisting of executable code wrapped in <These tags tell a web browser to interpret everything between the tags as JavaScript code. Once that comment is on the page, when any Once that comment is on the page, when any other user loads that website, the malicious code between the script tags will be executed by their web browser, and they will become a victim of the attack.

Reflective XSS

This is the most common cross-site scripting attack. In a reflection attack, malicious code is added to the end of a web site URL. When the victim loads this link in a Web browser, the browser executes the code injected into the url.

> This is the most commonly seen cross-site scripting attack. With a reflected attack, malicious code is added onto the end of the url of a website. When the victim loads this link in their web browser, the browser will execute the code injected into the url. The attacker usually uses some form of social engineering to trick the

victim into clicking on the link.

1. The attacker pretends to be a banker and posts a connection with a phishing script (reflexive), as shown below.

> The attacker pretends to be a banker and publishes a connection with a malicious script

```
1 http://example.bank.com/index.html?uesr=<script>This is the malicious code segment here</script>.
```

2. When the victim clicks on the link, the malicious code inside the `<script>` tag is executed.

> When the victim clicks on the link, the malicious code inside the <script> tag is also executed

Persistence XSS

Persistent cross-site scripting occurs on sites that allow users to post content that other users will see, such as comment forums or social media sites. If the site
Failure to properly validate the content created by a user may result in an attacker inserting code that will be executed by other users' browsers when the page is loaded.

> ***Persistent cross-site scripting*** happens on sites that let users post content that other users will see, such as a comments forum or social media site, for If the site doesn't properly validate the inputs for user- generated content, an attacker can insert code that other users' browsers will execute when the page loads. If the site doesn't properly validate the inputs for user- generated content, an attacker can insert code that other users ' browsers will execute when the page loads.

For example, the attacker includes the following in his own profile:

```
1 "Hello, I'm xxx, I'm from xxx, <script>this is a malicious code segment here</script>."
```

Any user attempting to access this personal information will fall victim to the attacker's persistent cross-site scripting attack.

How to prevent XSS

- Validating inputs: Validation forms implement rules to prevent users from posting data to forms that do not meet certain criteria. Example
  For example, an input requesting users to enter "姓氏" should have a validation rule that only allows users to submit data consisting of alphanumeric characters. The validation rule can also be set to reject any tags or characters commonly used in cross-site scripts, such as the <script> tag.

  > Validation means implementing rules that prevent a user from posting data into a form that doesn't meet certain criteria.
  >
  > For example, an input that asks for the user's "Last Name" should have validation rules that only let the user submit data consisting of alphanumeric characters.

- Setting ***WAF* rules**: WAF rules can also be configured to enforce rules to prevent reflective cross-site scripting. These WAF rules
  The policy used will block strange requests to the server, including cross-site scripting attacks.

  > A WAF can also be configured to enforce rules which will prevent reflected cross-site scripting. These WAF rules employ strategies that will block These WAF rules employ strategies that will block strange requests to the server, including cross-site scripting attacks.

Physical strength attack

Power of Attack is a trial-and-error method used to decode sensitive data. It is most often used to crack passwords and encryption keys, and is usually performed by scripts or machines against the web login page.

The difference between forceful attacks and other methods of cracking is that forceful attacks do not use an intellectual strategy; they simply try to use different combinations of characters until they find the right one. to the right combination.

> Brute force attack is a trial and error method used to decode sensitive data. Brute-force attacks are most commonly used to crack passwords and encryption keys. Brute-force password attacks are usually performed by scripts or bots against website login pages.
>
> Brute-force attacks differ from other cracking methods in that brute-force attacks do not employ intellectual strategies; they simply try different Brute-force attacks differ from other cracking methods in that brute-force attacks do not employ intellectual strategies; they simply try different combinations of characters until they find the right one.

Protection against acts of physical force

The following measures can be taken by the developer of the management authorization system:

- For example, locking out IP addresses that have generated too many failed logins
- As well as the inclusion of a time delay mechanism in password checking software. A delay of even

> a few seconds can greatly weaken the effectiveness of a brute force attack. Incorporating a delay
>
> in their password-checking software. A delay of even a few seconds can greatly weaken the effectiveness of a brute force attack.

Web service users can choose longer and more complex passwords to minimize the risk of forceful attacks. In addition, it is recommended to enable two-factor authentication, and non-machine authentication (such as (reCAPTCHA).

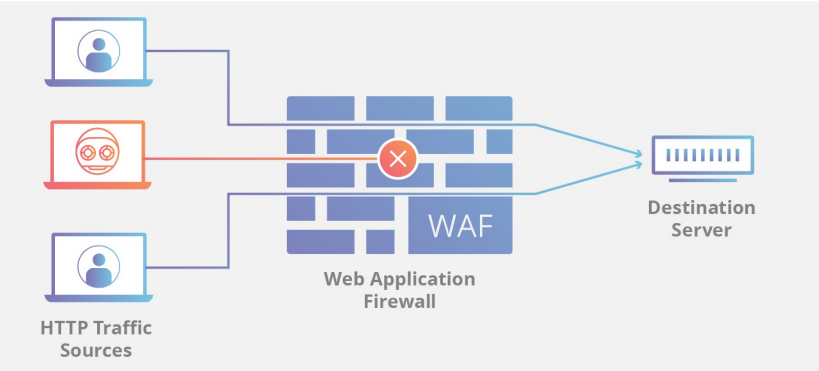
> Web service users can choose longer and complex passwords to reduce the risk of brute force attacks. In addition, it is recommended to enable two-factor authentication, and non-robot authentication (such as reCAPTCHA). authentication, and non-robot authentication (such as reCAPTCHA).

Web Application Firewall *WAF*

WAF (Web Application Firewall) helps protect Web applications by **filtering and monitoring *HTTP* traffic between *them* and the Internet**. It generally protects Web applications against cross-site forgery, cross-site scripting (XSS), file inclusion, SQL injection, and a number of other attacks. a WAF is a protocol Layer 7 defense policy (in the OSI model), and does not protect against all types of attacks. This attack mitigation methodology is usually part of a suite of tools that work together to build a holistic defense against a range of attack tactics.

> A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. A WAF is a protocol layer 7 defense (in the OSI model), and a WAF is a protocol layer 2 defense (in the OSI model). It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of

attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.



Deploying a WAF on the front end of a Web application creates a barrier between the Web application and the Internet, which is a reverse proxy.

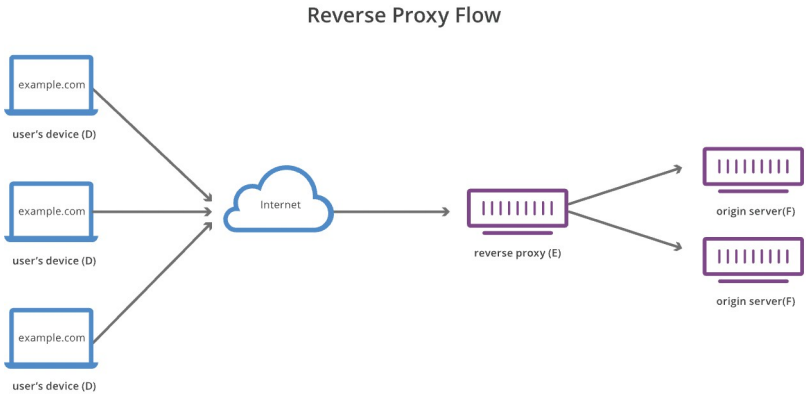
Direct clients to the server via WAF to prevent exposing the server.

> By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. A WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server. A WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

reverse proxy

A reverse proxy is a server that sits in front of one or more Web servers and intercepts requests from clients. With a reverse proxy, when a client sends a request to a source server in the Web site, the reverse proxy server intercepts the request at the edge of the network. The reverse proxy server then sends requests to and receives responses from the source server.

> A reverse proxy is a server that sits in front of one or more web servers, intercepting requests from clients.With a reverse proxy, when clients send With a reverse proxy, when clients send requests to the origin server of a website, those requests are intercepted at the network edge by the reverse proxy server. With a reverse proxy, when clients send requests to the origin server of a website, those requests are intercepted at the network edge by the reverse proxy server.



The following are some of the benefits of reverse proxying:

- **Load Balancing]**: A multi-million dollar user may not be able to use a single source server to handle all incoming site traffic. However, the site can be distributed among a pool of different servers so that all servers handle requests for the same site. In this case, the reverse proxy can provide a load balancing solution that distributes the incoming traffic evenly among the different servers to prevent a single server from becoming overloaded. If a server is completely unavailable, other servers can handle the traffic on its behalf.
- Preventing Attacks: With a reverse proxy, a Web site or service does not need to disclose the IP address of its origin server. This makes it more difficult for attackers to utilize targeted attacks, such as DDoS

attacks.

- Caching: The reverse proxy can also cache content to increase speed. If users are spread around the world, those who are far away from the source server will have a slow connection to the server. Caching can be used to partially speed up access, or a CDN can be used directly.
- SSL Encryption: Encrypting and decrypting each client's SSL (or TLS) communications can be computationally intensive for the origin server. It can be paired with

The reverse proxy decrypts all incoming requests and encrypts all outgoing responses, freeing up valuable resources on the origin server.

VPN

VPN

Typically, most Internet traffic is unencrypted and not very public. When a user creates an Internet connection, the user's device connects to their Internet Service Provider (ISP), which then connects to the Internet to find the appropriate Web server and communicates with it to obtain the requested Web site.

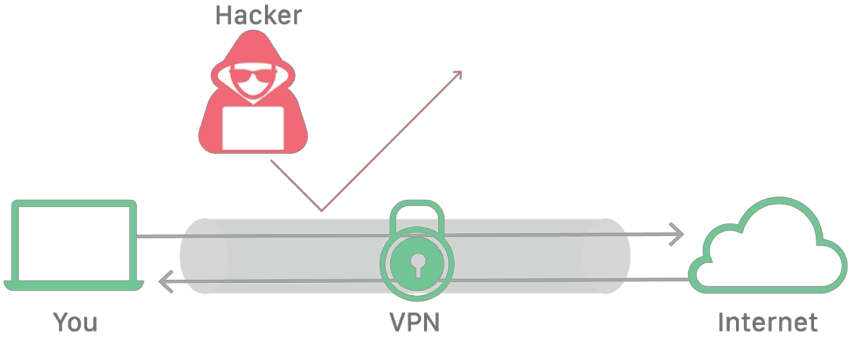
> Ordinarily, most Internet traffic is unencrypted and very public. When a user creates an Internet connection, the user's device will connect to their ISP, and then the ISP will connect to the Internet to find the appropriate web server to communicate with to fetch the requested website. When a user creates an Internet connection, the user's device will connect to their ISP, and then the ISP will connect to the Internet to find the appropriate web server to communicate with to fetch the request website.

The user's IP address is public throughout the process, and the ISP and any other intermediary can keep a record of the user's browsing habits. In addition, the user's device and
The data exchanged between Web servers is not encrypted, and an attacker can listen to it, for example, in an in-transit attack.

> The user's IP address is public throughout, and ISPs and any other intermediaries can keep records of the user's browsing habits. Additionally, the data exchanged between the user device and the web server is not encrypted, allowing an attacker to listen to the data. Additionally, the data exchanged between the user device and the web server is not encrypted, allowing an attacker to listen to the data

A virtual private network (VPN) is an Internet security service that allows users to access the Internet as if it were a private network. This not only encrypts Internet traffic, but also provides a high degree of anonymity. Some of the most common reasons people use VPNs are to prevent eavesdropping on public WiFi, to avoid Internet censorship, or to connect to the company's internal network for remote work.

> A virtual private network (VPN) is an Internet security service that allows users to access the Internet as though they were connected to a private network. This encrypts Internet communications as well as providing a strong degree of anonymity. Some of the most common reasons people use VPNs are to protect against snooping on public WiFi, to circumvent Internet censorship, or to connect to the Internet. Some of the most common reasons people use VPNs are to protect against snooping on public WiFi, to circumvent Internet censorship, or to connect to a business's internal network for the purpose of remote work.



How does a VPN work?

Users connecting to the Internet using a VPN service have a higher level of security and privacy. a VPN connection involves the following four steps:

1. The VPN client connects to the ISP using an encrypted connection.
2. The ISP connects the VPN client to the VPN server and maintains an encrypted connection.
3. The VPN server decrypts data from the user's device and then connects to the Internet with unencrypted communication to access the Web server.

4. The VPN server establishes an encrypted connection with the client called a "VPN tunnel".

The ***VPN*** **tunnel** between the VPN client and the VPN server passes through the ISP, but since all data is encrypted, the ISP cannot view user activity. Communication between the VPN server and the Internet is not encrypted, but the Web server only logs the IP address of the VPN server, so no user information is available.

> The ***VPN tunnel*** between the VPN client and VPN server passes through the ISP, but since all the data is encrypted, the ISP cannot see the user's activity. The VPN server's communications with the Internet are unencrypted, but the web servers will only log the IP address of the VPN server, which gives them no information about the user's activity. The VPN server's communications with the Internet are unencrypted, but the web servers will only log the IP address of the VPN server, which gives them no information about the user.

VPN Benefits

- **Public *WiFi* Grid Protection**: The traffic of users directly using the public WiFi grid is not encrypted, and other users on the same network can monitor their activities using easily available tools. If users connect through a VPN, eavesdropping attackers can only see encrypted data without revealing any sensitive information.

> User traffic directly using public WiFi networks is not encrypted, and other users on the same network can use readily available tools to monitor their activity. If the user is connected through a VPN, the snooping attacker can only see the encrypted data without revealing any sensitive information

- **Telecommuting**]: Many organizations allow their employees to work remotely using a VPN. This not only allows remote employees to access the company's internal network, but it also provides the ability to access the company's internal network.

  Encryption was used to protect the organization from attackers.

> Many businesses allow their employees to work remotely using a VPN. This can allow the remote employee to have access to the company's internal network, as well as provide encryption to protect the business from attackers. This can allow the remote employee to have access to the company's internal network, as well as provide encryption to protect the business from attackers.

- **Access Control**: Control which users are authorized to access which resources. The company sets up several different VPNs, each connecting to a different internal resource. By assigning users to these VPNs, different users can have different levels of data access rights.

  Access control and management are critical to securing company data. Without access control, unauthorized users may be able to view or alter confidential data.

  without leading to a data breach.

> This can control which users have access to which resources. The company sets up several different VPNs, and each VPN connects to different internal resources. By assigning users to these VPNs, different users can have different levels of access to data.
>
> Access control and management is crucial for protecting and securing corporate data. Without access control, unauthorized users could view or alter confidential data, resulting in a data breach. Without access control, unauthorized users could view or alter confidential data, resulting in a data breach.

encrypted

Encryption is a way of scrambling data so that only authorized parties can understand the information.

Technically, it is the process of converting human-readable plaintext files into unintelligible files.

The process of encrypting a file (also known as ciphering). Simply put, encryption takes readable data and modifies it to make it appear random. Encryption requires the use of

Use key: A set of mathematical values agreed upon by the sender and receiver of the encrypted message.

> Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on. message agree on.

Although the encrypted data appears to be random, the encryption is performed in a logical and predictable manner, so receiving the encrypted data and having the correct key is a good idea.
A party can decrypt the data and return it to plain text.

> Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext.

An encryption key is a string of characters used in an encryption algorithm to alter the data so that it appears to be random. Just like a physical key, it locks the
(encrypted) data so that it can only be unlocked (decrypted) by a person with a matching key.

> A ***cryptographic key*** is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it. (encrypts) data so that only someone with the right key can unlock (decrypt) it.

[Two main types of encryption

- Symmetric encryption: There is only one key, and all communicating parties use the same (secret) key for encryption and decryption.

> In symmetric encryption, there is only one key, and all communicating parties use the same (secret) key for both encryption and decryption.

  - Commonly used symmetric encryption algorithms include: AES, 3-DES, SNOW, and AES.
- Asymmetric Encryption: Asymmetric encryption is also known as public key encryption. In asymmetric or public key encryption, there are two keys: one is used for encryption and the other is used for decryption. The decryption key is kept secret (hence the term "private key") and the encryption key is made public and available to anyone (hence the term "public key"). Asymmetric encryption is the technology that underlies TLS (commonly known as SSL).

> In asymmetric, or public key, encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. The decryption key is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name). is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name). Asymmetric encryption is a foundational technology for TLS (often called SSL).

  - Commonly used asymmetric encryption algorithms include: RSA, Elliptic curve cryptography (ECC)

HTTPS Encryption

Encryption is the foundation of a variety of technologies, but it is especially important for securing HTTP requests and responses. The protocol responsible for this function is called HTTPS (Hypertext Transfer Protocol).
(Transport Protocol Security). URLs for sites served over HTTPS instead of HTTP will start with https:// instead of http://.

> Encryption is foundational for a variety of technologies, but it is especially important for keeping HTTP requests and responses secure. The protocol responsible for this is called HTTPS (Hypertext Transfer Protocol Secure). The protocol responsible for this is called HTTPS (Hypertext Transfer Protocol Secure). A website served over HTTPS instead of HTTP will have a URL that begins with https:// instead of http://

How does HTTPS work?

HTTPS encrypts communications using a cryptographic protocol. This protocol is known as **Transport Layer Security *(TLS)***, but was formerly known as Secure Sockets Layer (SSL). The protocol protects communications by using what is known as a non-symmetric public key infrastructure. This type of security system uses two different keys to encrypt communications between two parties:

> HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer Security (TLS), although formerly it was known as Secure Sockets Layer (SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure. This type of security system uses This type of security system uses two different keys to encrypt communications between two parties.

1. Private Key]: This key is controlled by the web site owner and, as the reader may assume, is private. This key is located on the web server and is used to decrypt information encrypted with the public key.

> This key is controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key. This key lives on a web server and is used to decrypt information encrypted by the public key.

2. Public Key] This key can be used by anyone who wants to interact with the server in a secure manner.

> Information that is encrypted with the public key can only be decrypted with the private key. This key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted with the private key. Information that's encrypted by the public key can only be decrypted by the private key.

HTTPS Benefits

Communication over regular HTTP is performed in plain text, making it easily accessible to anyone using the right tools and vulnerable to on-the-go attacks.

> All communications that occur over HTTP occur in plain text, making them highly accessible to anyone with the correct tools, and vulnerable to on-path attacks.

HTTPS p r e v e n t s the web site from broadcasting information in a way that can be easily viewed by anyone snooping on the web.

> With HTTPS, traffic is encrypted such that even if the packets are sniffed or otherwise intercepted, they will come across as nonsensical characters.

Before encryption:

```
1 This is a string of text that is completely readable.
```

Encrypted:

```
1 ITM0IRyiEhVpa6VnKyExMiEgNveroyWBPlgGyfkflYjDaaFf/Kn3bo3OfghBPDWo6AfSHlNtL8N7ITEwIXc1gU5X73x
MsJormzzXlwOyrCs+9XCPk63Y+z0=
```

SSL/TLS

SSL

- To provide a high level of privacy, SSL encrypts data transmitted over the Web. This means that anyone attempting to intercept this data will only see the following

  Just a few garbled characters that can't be decrypted.

> In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt. will only see a garbled mix of characters that is nearly impossible to decrypt.

- SSL initiates an **authentication** process called handshake between two communicating devices to ensure that the two devices are indeed who they claim to be.

> SSL initiates an ***authentication*** process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.

- SSL also digitally signs the data to provide **data integrity**, verifying that the data has not been tampered with before it reaches the destination recipient.

> SSL also digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

- SSL has gone through a number of iterations, with security being enhanced over the generations; SSL was updated to TLS in 1999.

> There have been several iterations of SSL, each more secure than the last. In 1999 SSL was updated to become TLS.

TLS

There are three main components to the functionality implemented by the TLS protocol:

- **Encryption:** hides the data being transferred from third parties.
- **Lifecertification:** Ensure that the parties exchanging information are who they claim to be.

> **Authentication:** ensures that the parties exchanging information are who they claim to be.

- **Integrity:** verifies that the data has not been forged or tampered with.

Workflow

In order for a web site or application to use TLS, it must have a TLS certificate issued by an authoritative organization installed on its origin server. This certificate contains important information about the domain owner and the server's public key, both of which are important for authenticating the server.

> For a website or application to use TLS, it must have a TLS certificate issued by an authority installed on its origin server. This certificate contains important information about the domain owner as well as the server's public key, both of which are important for verifying the server's identity.

- Specify which version of TLS will be used (TLS 1.0, 1.2, 1.3, etc.) Specify which version of TLS will be used
- Decide which encryption algorithm will be used.
- Authenticate the identity of the server using the server's TLS certificate.
  certificate
- After the handshake is complete, create session keys for encrypting messages between the two. generate

session keys for encrypting messages between
They after the handshake is complete

access control

In web security, authentication is the process of verifying the identity of a person or an object. Authentication is usually performed by checking passwords, hardware tokens, or other information that can prove identity.

Authentication is not just for verifying human users. Computer systems also need to be checked for servers, software, APIs, and other computers to ensure that they are the same as the ones used in the computer system. "Claims".

> In cyber security, authentication is the process of verifying someone's or something's identity. Authentication usually takes place by checking a Authentication usually takes place by checking a password, a hardware token, or some other piece of information that proves identity.
>
> Authentication does not just apply to verifying human users. Computer systems also need to check servers, software, APIs, and other computers to be sure they are who they "say" they are. Computer systems also need to check servers, software, APIs, and other computers to be sure *they* are who they "say" they are.

Validation Factors

The characteristics examined in an authentication system are called "factors". Three common types of authentication factors are widely used today:

- **What a person knows**: This authentication factor checks for a secret knowledge that only a person can have. The combination of user name and password is an example of this factor. type
  I'm not sure if I'm going to be able to do that.

> This authentication factor checks a piece of secret knowledge that only the real person should have. A username-and-password combination is the classic example of this factor. example of this factor.

- **What a person owns**: This authentication factor checks whether the person owns the physical object issued to them or known to them. In a digital system, this is accomplished by checking the physical
  A similar principle is used for tokens. There are two types of tokens: soft tokens (authentication codes) and hard tokens (USB keys).

> This authentication factor checks if the person possesses a physical item they were issued or are known to have. In digital systems, a similar principle is used by checking physical tokens. There are two types of tokens: soft token (captcha) and hard token (USB Key).

- **My Body**: This body validation factor assesses the inherent qualities of a person (e.g., their生 characteristics).

> His authentication factor assesses a person's inherent qualities (such like biological characteristics).

Multifactor L身验证

Multi-factor Authentication (MFA) is the process of verifying an individual's identity by checking two or more factors of authentication, not just one.MFA is
A stronger type of authentication than one-factor authentication, as it is much more difficult to falsify two of the

factors than one of them.

> Multi-factor authentication (MFA) is the process of verifying a person's identity by checking two or more authentication factors, rather than just one. MFA is a stronger type of authentication than single-factor authentication, because it is much harder to fake two of these factors than it is to fake one of them. It is much harder to fake two of these factors than it is to fake one of them.

Digital Certificate Authentication

A digital certificate is a small digital file containing information used to verify identity. Digital certificates receive a digital signature from the organization that issued them to prove their authenticity.
Authenticity. An entity that possesses a certificate can use these keys to digitally sign data to prove that it possesses the private key and is therefore authentic.

For the time being, digital certificates are not commonly used to verify personal identity.

> A digital certificate is a small digital file that contains information used to verify identity. Digital certificates receive a digital signature from the authority that issued them to attest to their authenticity. Digital certificates receive a digital signature from the authority that issued them to attest to their authenticity. An entity in possession of a certificate can use these keys to digitally sign data to prove that it possesses the private key and is therefore authentic.

Authorization and Authentication

Authentication means ensuring that a person or device is who (or what) they claim to be. **Authorization** determines what can be viewed and performed by authenticated users.

> ***Authentication*** means ensuring that a person or device is who (or something) they (they) claim to be. ***Authorization*** determines what an authenticated user can see and do.

access control

Access control is a security term that refers to a set of policies used to restrict access to information, tools, and physical locations.

> Access control is a security term used to refer to a set of policies for restricting access to information, tools, and physical locations.

Main types of access control

- **Mandatory Access Control** ***(MAC)***: Mandatory Access Control establishes strict security policies for individual users and the resources, systems, or data they are allowed to access. These policies are controlled by administrators; individual users do not have the power to set, change, or revoke permissions in a way that conflicts with existing policies.

> Mandatory access control establishes strict security policies for individual users and the resources, systems, or data they are allowed to access. These policies are controlled by an administrator; individual users are no t given the authority to set, alter, or revoke permissions in a way that contradicts existing policies.

- ***RBAC***: RBAC establishes rights based on groups (defined sets of users) and colors (defined sets of operations). Limitations. Individuals can perform any of the operations assigned to their colors and can be assigned multiple colors as needed. Users have no right to change the access control level assigned to their tags.

> Role-based access control establishes permissions based on groups (defined sets of users) and roles (defined sets of actions). Individuals can perform any action assigned to their role, and can be assigned as many roles as needed. Users do not have permission to change the access control level assigned to their

role. Users do not have permission to change the access control level assigned to their role.

- **Default Access Control *(DAC)***: Once a user has been granted access to an object (usually by the system administrator or through an existing access control list), the user is not allowed to access the object.

  If the user is authorized to access the site, they can grant access to other users as needed. However, this could lead to a security breach!

> Once a user is given permission to access an object (usually by a system administrator or through an existing access control list), they can grant access to This may introduce security vulnerabilities.

GDPR

The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that establishes a framework for the collection, processing, storage, and transfer of personal data. Its requirements:

- **Record-keeping:** Data processors must keep records of their processing activities.

> **Record keeping:** Data processors must keep records of their processing activities.

- **Security measures: Data controllers and processors must regularly use** and test appropriate

> security measures to protect the data they collect and process. **Security measures:** Data controllers and processors must regularly use and test appropriate security measures to protect the data they collect and process.

- **Data breach notification:** Data controllers who have suffered a personal data breach must notify the relevant authorities within 72 hours, except in exceptional cases. In general.

They must also notify the individuals whose personal data has been affected by the breach.

> **Data breach notification:** Data controllers that suffer a personal data breach have to notify appropriate authorities within 72 hours

- **Data Protection Officer (DPO):** Companies that process data may need to employ a Data Protection Officer (DPO). The DPO leads and oversees all GDPR compliance.

Work.

> Companies that process data may need to hire a Data Protection Officer (DPO)