**OWASP Security Principles for Entry-Level Analysts**

As a **security analyst**, one of your key responsibilities is to protect an organization's **data** and **assets**. In addition to the frameworks and models we've previously discussed (like NIST and the CIA triad), there are **security principles** that will guide you in minimizing threats and risks. One such set of principles comes from the **Open Web Application Security Project (OWASP)**, which offers practical and widely recognized guidelines for securing applications and systems.

Here are some important OWASP principles that you should be familiar with as an entry-level analyst:

**1. Minimize the Attack Surface Area**

The **attack surface** refers to all the potential vulnerabilities that a threat actor can exploit, such as **attack vectors** (paths attackers use to breach security). Common attack vectors include **phishing** emails and **weak passwords**.

To minimize the attack surface, security teams often:

* **Disable unnecessary software features** that may open doors to attackers.
* **Limit access** to certain sensitive assets.
* **Enforce complex password policies** to make it harder for attackers to gain access.

Reducing the attack surface is key to making systems harder to attack.

**2. Principle of Least Privilege**

The **Principle of Least Privilege (PoLP)** ensures that users have the minimum amount of access needed to perform their jobs. Limiting access reduces the impact of a potential breach.

For example:

* As an analyst, you may have access to **log data** but not to change **user permissions**.
* If a threat actor compromises your credentials, they will only be able to access what you have access to, which may not be enough for them to execute a full attack.

The goal is to reduce the amount of damage a breach can cause.

**3. Defense in Depth**

**Defense in Depth** is about using multiple layers of security controls to protect an organization. If one layer is breached, other defenses are still in place to thwart an attack.

Examples of defense mechanisms include:

* **Multi-factor authentication (MFA)**: Users must provide additional proof of identity beyond just a username and password.
* **Firewalls**: These help filter out malicious traffic.
* **Intrusion detection systems (IDS)**: These detect unauthorized access attempts.
* **Permissions settings**: Control who has access to sensitive resources.

A multi-layered approach makes it harder for attackers to breach an organization.

**4. Separation of Duties**

The **Separation of Duties** principle prevents any individual from having too much control or privilege over a process, which could lead to fraudulent or malicious activities.

For example:

* The person who signs **paychecks** should not also be the one who prepares them, as this could allow for unauthorized changes.

By distributing responsibilities, organizations can reduce the risk of internal attacks or errors.

**5. Keep Security Simple**

When implementing security controls, **simplicity** is essential. Overly complex solutions can be difficult to manage, prone to errors, and hinder collaboration across teams.

The principle here is to:

* **Avoid unnecessary complexity** in security measures.
* Ensure that security tools and processes are clear and manageable for everyone.

Simple security controls are easier to maintain and more likely to be followed by all team members.

**6. Fix Security Issues Correctly**

When a security issue is identified, it’s crucial to address it at its **root cause**. Merely applying a temporary fix could lead to the issue recurring. After fixing the issue, **testing** is necessary to ensure that the problem is truly resolved.

For example:

* A **weak password** protecting an organization's **Wi-Fi network** could be a potential entry point for attackers.
* The fix would involve enforcing **stronger password policies** and testing the system to make sure the vulnerability is gone.

Properly addressing and fixing security issues prevents similar problems in the future.

**Summary**

These **OWASP principles** are important for you as an entry-level analyst to understand because they:

* Help minimize potential vulnerabilities.
* Reduce the risk of malicious attacks.
* Ensure security processes are clear and manageable.

By applying these principles alongside the NIST frameworks and CIA triad, you will be better equipped to protect the organization's data and assets, improving your overall security knowledge and standing out as a capable security professional. Keep these principles in mind as you advance in your career!

# More about OWASP security principles

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

## Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event management (SIEM) dashboard, or using a [vulnerability scanner](https://csrc.nist.gov/glossary/term/vulnerability_scanner)

, you will use these principles in some way.

Previously, you were introduced to several OWASP security principles. These included:

* **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
* **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
* **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.
* **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
* **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
* **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

## Additional OWASP security principles

Next, you’ll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

### ****Establish secure defaults****

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

### ****Fail securely****

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

### ****Don’t trust services****

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn’t explicitly trust that their partners’ systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

### ****Avoid security by obscurity****

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016): [OWASP Mobile Top 10](https://owasp.org/www-project-mobile-top-10/2016-risks/)

The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

## Key takeaways

Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.