

# Secure Programming

## — OWASP & WebGoat

*胡天磊, Dr. HU Tianlei*

*Associate Professor*

*College of Computer Science, Zhejiang Univ.*

[htl@zju.edu.cn](mailto:htl@zju.edu.cn)

# Course Outline

- Introduction of OWASP TOP 10
- Introduction of WebGoat

# Introduction of OWASP TOP 10

# OWASP TOP 10

## The Open Web Application Security Project [www.owasp.org](http://www.owasp.org)

- OWASP is dedicated to helping organizations understand and improve the security of their web applications and web services
- It's About Risks, Not Just Vulnerabilities. The title is: "The Top 10 Most Critical Web Application Security Risks."
  - Top 10 Risks – not Top 10 impacts, likelihoods, or vulnerabilities
- First released in 2003, and also in 2004, 2007, 2010, 2013, 2017, 2021
- The newest version, OWASP TOP 10 – 2021, was released at the end of 2021.
  - It is the 7th update of the series.
- Audience
  - Developers, lead developers, architects
  - Framework developers (but they really should be using ASVS)
  - AppSec program management (CISOs, CTOs, and so on)
  - AppSec professionals: consultancies, tools, vendors, trainers

# OWASP TOP 10 – 2021 / Methodology

This installment of the Top 10 is more data-driven than ever but not blindly data-driven. We selected **eight of the ten categories** from contributed data and **two categories** from the Top 10 community survey at a high level.

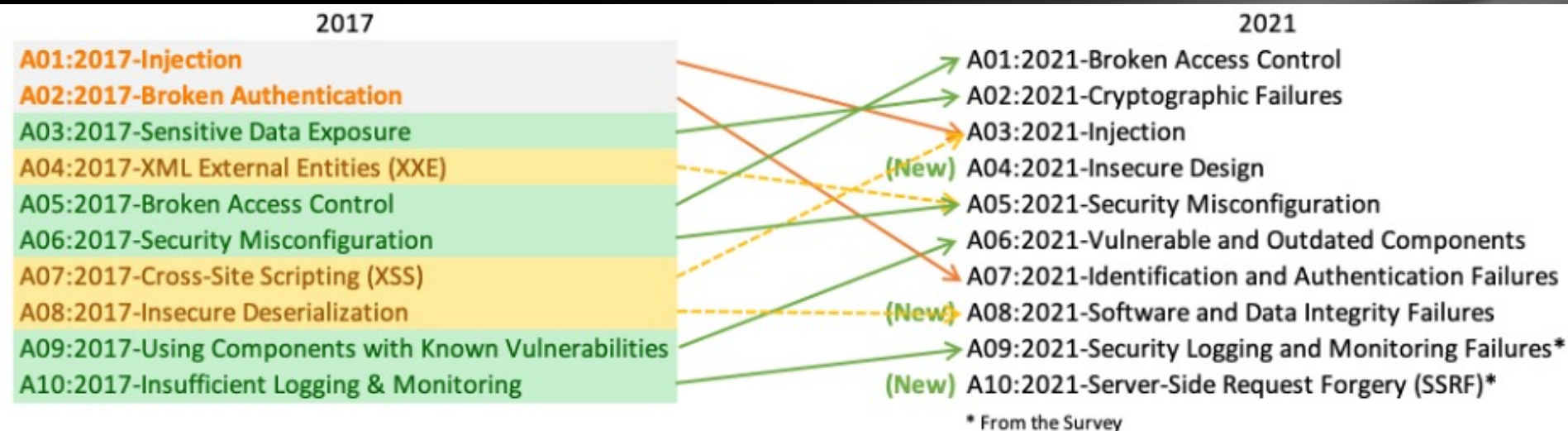
- We do this for a fundamental reason, looking at the contributed data is looking into the past. To balance that view, we use a community survey to ask application security and development experts on the front lines what they see as essential weaknesses that the data may not show yet.

## The Databases:

- **CWE™** is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
  - <https://cwe.mitre.org/index.html>
- The **NVD** is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
  - <https://nvd.nist.gov/>

# OWASP TOP 10 (the transition)

- After nearly 20 years, injection is no longer A1
  - Even with XSS combined into injection
- A1..A10 titles are root causes, not symptoms
  - Four new categories, including Insecure Design and SSRF





# OWASP TOP 10 - 2021

**A01:2021-Broken Access Control** moves up from the fifth position.

94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than in any other category.

**A02:2021-Cryptographic Failures** shifts up one position to #2.

It was previously known as Sensitive Data Exposure, which was a broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.

**A03:2021-Injection** slides down to the third position.

94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

**A04:2021-Insecure Design** is a new category for 2021,

with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

# OWASP TOP 10 - 2021

**A05:2021-Security Misconfiguration** moves up from #6 in the previous edition;

90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.

**A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk.

It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.

**A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position.

It now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.



# OWASP TOP 10 - 2021

**A08:2021-Software and Data Integrity Failures** is a new category for 2021;

It focuses on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.

**A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously.

This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

**A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1).

The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

# OWASP TOP 10 – 2021 / Data Factors

There are data factors that are listed for each of the Top 10 Categories, here is what they mean:

- **CWEs Mapped:** The number of CWEs mapped to a category by the Top 10 team.
- **Incidence Rate:** Incidence rate is the percentage of applications vulnerable to that CWE from the population tested by that org for that year.
- **Weighted Exploit:** The Exploit sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10pt scale.
- **Weighted Impact:** The Impact sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10pt scale.
- **(Testing) Coverage:** The percentage of applications tested by all organizations for a given CWE.
- **Total Occurrences:** Total number of applications found to have the CWEs mapped to a category.
- **Total CVEs:** Total number of CVEs in the NVD DB that were mapped to the CWEs mapped to a category.

# A01:2021 – Broken Access Control

Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*, *CWE-201: Insertion of Sensitive Information Into Sent Data*, and *CWE-352: Cross-Site Request Forgery*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
34	55.97%	3.81%	6.92	5.93	94.55%	47.72%	318487	19013

# Broken Access Control - Examples

**Scenario #1:** The application uses unverified data in aSQL call that is accessing account information:

```
pstmt.setString(1, request.getParameter("acct"));  
ResultSet results = pstmt.executeQuery( );
```

An attacker simply modifies the browser's 'acct' parameter to send whatever account number they want. If not correctly verified, the attacker can access any user's account.

<https://example.com/app/accountInfo?acct=notmyacct>

**Scenario #2:** An attacker simply forces browses to target URLs. Admin rights are required for access to the admin page.

```
https://example.com/app/getappInfo  
https://example.com/app/admin_getappInfo
```

If an unauthenticated user can access either page, it's a flaw. If a non-admin can access the admin page, this is a flaw.

# Broken Access Control - Description

Access control enforces policy that users cannot act outside their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits. Common access control vulnerabilities include:

- **Violation of the principle of least privilege or denial by default**, where access should only be granted for particular capabilities, roles, or users, but is available to anyone.
- **Bypassing access control checks** by modifying the URL (parameter tampering or force browsing), internal application state, or the HTML page, or by using an attack tool to modify API requests.
- **Permitting viewing or editing someone else's account** by providing its unique identifier (insecure direct object references)
- **Accessing API with missing access controls** for POST, PUT and DELETE.
- **Elevation of privilege**. Acting as a user without being logged in or acting as an admin when logged in as a user.
- **Metadata manipulation**, such as replaying or tampering with a JSON Web Token (JWT) access control token or a cookie or hidden field manipulated to elevate privileges or abusing JWT invalidation.
- **CORS (Cross-Origin Resource Sharing) misconfiguration** allows API access from unauthorized/untrusted origins.
- **Force browsing to authenticated pages** as an unauthenticated user or to privileged pages as a standard user.



# Broken Access Control - How to Prevent

Access control is only effective in trusted server-side code or server-less API, where the attacker cannot modify the access control check or metadata.

- **Except for public resources, deny by default.**
- Implement access control mechanisms once and re-use them throughout the application, including minimizing Cross-Origin Resource Sharing (CORS) usage.
- Model access controls should enforce record ownership rather than accepting that the user can create, read, update, or delete any record.
- Unique application business limit requirements should be enforced by domain models.
- Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.
- Log access control failures and alert admins when appropriate (e.g., repeated failures).
- Rate limit API and controller access to minimize the harm from automated attack tooling.
- Stateful session identifiers should be invalidated on the server after logout. Stateless JWT tokens should rather be short-lived so that the window of opportunity for an attacker is minimized. For longer lived JWTs it's highly recommended to follow the OAuth standards to revoke access.

Developers and QA staff should include functional access control unit tests and integration tests.

# A02:2021 – Cryptographic Failures

Shifting up one position to #2, previously known as *Sensitive Data Exposure*, which is more of a broad symptom rather than a root cause, the focus is on failures related to cryptography (or lack thereof). Which often lead to exposure of sensitive data. Notable Common Weakness Enumerations (CWEs) included are *CWE-259: Use of Hard-coded Password*, *CWE-327: Broken or Risky Crypto Algorithm*, and *CWE-331 Insufficient Entropy*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
29	46.44%	4.49%	7.29	6.81	79.33%	34.85%	233788	3075

# Cryptographic Failures - Examples

**Scenario #1:** An application encrypts credit card numbers in a database using automatic database encryption. However, this data is automatically decrypted when retrieved, allowing a SQL injection flaw to retrieve credit card numbers in clear text.

**Scenario #2:** A site doesn't use or enforce TLS for all pages or supports weak encryption. An attacker monitors network traffic (e.g., at an insecure wireless network), downgrades connections from HTTPS to HTTP, intercepts requests, and steals the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data. Instead of the above they could alter all transported data, e.g., the recipient of a money transfer.

**Scenario #3:** The password database uses unsalted or simple hashes to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password database. All the unsalted hashes can be exposed with a rainbow table of pre-calculated hashes. Hashes generated by simple or fast hash functions may be cracked by GPUs, even if they were salted.

# Cryptographic Failures - Description

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

For all such data:

- **Is any data transmitted in clear text?** This concerns protocols such as HTTP, SMTP, FTP also using TLS upgrades like STARTTLS. External internet traffic is hazardous. Verify all internal traffic, e.g., between load balancers, web servers, or back-end systems.
- **Are any old or weak cryptographic algorithms or protocols used** either by default or in older code?
- Are **default crypto keys** in use, **weak crypto keys** generated or re-used, or is **proper key management or rotation** missing? Are **crypto keys checked into** source code repositories?
- **Is encryption not enforced**, e.g., are any HTTP headers (browser) security directives or headers missing?
- **Is the received server certificate and the trust chain properly validated?**

# Cryptographic Failures - Description (cont.)

For all such data (cont.):

- Are initialization vectors ignored, reused, or not generated sufficiently secure for the cryptographic mode of operation? Is an insecure mode of operation such as ECB in use? Is encryption used when authenticated encryption is more appropriate?
- Are passwords being used as cryptographic keys in absence of a password base key derivation function?
- Is **randomness** used for cryptographic purposes that was not designed to meet cryptographic requirements? Even if the correct function is chosen, does it need to be seeded by the developer, and if not, has the developer over-written the strong seeding functionality built into it with a seed that lacks sufficient entropy/unpredictability?
- Are **deprecated** hash functions such as MD5 or SHA1 in use, or are non-cryptographic hash functions used when cryptographic hash functions are needed?
- Are **deprecated** cryptographic padding methods such as PKCS number 1 v1.5 in use?
- Are cryptographic **error messages or side channel information** exploitable, for example in the form of padding oracle attacks?



# Cryptographic Failures - How to Prevent 1/2

Do the following, at a minimum, and consult the references:

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
- Encrypt all data in transit with secure protocols such as TLS with forward secrecy (FS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Disable caching for response that contain sensitive data.
- Apply required security controls as per the data classification.

# Cryptographic Failures - How to Prevent 2/2

Do the following, at a minimum, and consult the references (cont.):

- Do not use legacy protocols such as FTP and SMTP for transporting sensitive data.
- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2.
- Initialization vectors must be chosen appropriate for the mode of operation. For many modes, this means using a CSPRNG (cryptographically secure pseudo random number generator). For modes that require a nonce, then the initialization vector (IV) does not need a CSPRNG. In all cases, the IV should never be used twice for a fixed key.
- Always use authenticated encryption instead of just encryption.
- Keys should be generated cryptographically randomly and stored in memory as byte arrays. If a password is used, then it must be converted to a key via an appropriate password base key derivation function.
- Ensure that cryptographic randomness is used where appropriate, and that it has not been seeded in a predictable way or with low entropy. Most modern APIs do not require the developer to seed the CSPRNG to get security.
- Avoid deprecated cryptographic functions and padding schemes, such as MD5, SHA1, PKCS number 1 v1.5 .
- Verify independently the effectiveness of configuration and settings.

# A03:2021 – Injection

Injection slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3%, and 274k occurrences. Notable Common Weakness Enumerations (CWEs) included are *CWE-79: Cross-site Scripting*, *CWE-89: SQL Injection*, and *CWE-73: External Control of File Name or Path*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
33	19.09%	3.37%	7.25	7.15	94.04%	47.90%	274228	32078

# Injection - Examples

**Scenario #1:** An application uses untrusted data in the construction of the following vulnerable SQL call:

```
String query = "SELECT \* FROM accounts WHERE custID='"  
+ request.getParameter("id") + "'";
```

**Scenario #2:** Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g., Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE custID='"  
+ request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: ' or '1'='1. For example:

```
http://example.com/app/accountView?id=' or '1'='1
```

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data or even invoke stored procedures.

# Injection - Description

An application is vulnerable to attack when:

- **User-supplied data** is not validated, filtered, or sanitized by the application.
- **Dynamic queries or non-parameterized calls** without context-aware escaping are used directly in the interpreter.
- Hostile data is **used within object-relational mapping (ORM) search** parameters to extract additional, sensitive records.
- Hostile data is **directly used or concatenated**. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection.

The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections.

Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged. Organizations can include static (SAST), dynamic (DAST), and interactive (IAST) application security testing tools into the CI/CD pipeline to identify introduced injection flaws before production deployment.



# Injection - How to Prevent

Preventing injection requires keeping data separate from commands and queries:

- **The preferred option is to use a safe API**, which avoids using the interpreter entirely, provides a parameterized interface, or migrates to Object Relational Mapping Tools (ORMs).

***Note:** Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data or executes hostile data with EXECUTE IMMEDIATE or exec().*

- **Use positive server-side input validation.** This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.

- For any residual dynamic queries, **escape special characters** using the specific escape syntax for that interpreter.

***Note:** SQL structures such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.*

- **Use LIMIT and other SQL controls within queries** to prevent mass disclosure of records in case of SQL injection.

# Ao4:2021 – Insecure Design

A new category for 2021 focuses on risks related to design and architectural flaws, with a call for more use of threat modeling, secure design patterns, and reference architectures. As a community we need to move beyond "shift-left" in the coding space to pre-code activities that are critical for the principles of Secure by Design. Notable Common Weakness Enumerations (CWEs) include *CWE-209: Generation of Error Message Containing Sensitive Information*, *CWE-256: Unprotected Storage of Credentials*, *CWE-501: Trust Boundary Violation*, and *CWE-522: Insufficiently Protected Credentials*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
40	24.19%	3.00%	6.46	6.78	77.25%	42.51%	262407	2691

# Insecure Design - Examples

**Scenario #1:** A credential recovery workflow might include “questions and answers,” which is prohibited by NIST 800-63b, the OWASP ASVS, and the OWASP Top 10. Questions and answers cannot be trusted as evidence of identity as more than one person can know the answers, which is why they are prohibited. Such code should be removed and replaced with a more secure design.

**Scenario #2:** A cinema chain allows group booking discounts and has a maximum of fifteen attendees before requiring a deposit. Attackers could threat model this flow and test if they could book six hundred seats and all cinemas at once in a few requests, causing a massive loss of income.

**Scenario #3:** A retail chain’s e-commerce website does not have protection against bots run by scalpers buying high-end video cards to resell auction websites. This creates terrible publicity for the video card makers and retail chain owners and enduring bad blood with enthusiasts who cannot obtain these cards at any price. Careful anti-bot design and domain logic rules, such as purchases made within a few seconds of availability, might identify inauthentic purchases and rejected such transactions.

# Insecure Design – Description 1/3

Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” Insecure design is not the source for all other Top 10 risk categories.

There is a difference between **insecure design** and **insecure implementation**. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation.

- A secure design can still have implementation defects leading to vulnerabilities that may be exploited.
- An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks.

One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

# Insecure Design – Description 2/3

## Secure Development Lifecycle

- Secure software requires a secure development lifecycle, some form of secure design pattern, paved road methodology, secured component library, tooling, and threat modeling.
- Reach out for your security specialists at the beginning of a software project throughout the whole project and maintenance of your software.
- Consider leveraging the [OWASP Software Assurance Maturity Model \(SAMM\)](#) to help structure your secure software development efforts

## Requirements and Resource Management

- Collect and negotiate the business requirements for an application with the business, including the protection requirements concerning confidentiality, integrity, availability, and authenticity of all data assets and the expected business logic.
- Take into account how exposed your application will be and if you need segregation of tenants (additionally to access control).
- Compile the technical requirements, including functional and non-functional security requirements.
- Plan and negotiate the budget covering all design, build, testing, and operation, including security activities.



# Insecure Design – Description 3/3

## Secure Design

Secure design is a culture and methodology that constantly evaluates threats and ensures that code is robustly designed and tested to prevent known attack methods.

- Threat modeling should be integrated into refinement sessions (or similar activities); look for changes in data flows and access control or other security controls.
- In the user story development determine the correct flow and failure states, ensure they are well understood and agreed upon by responsible and impacted parties.
- Analyze assumptions and conditions for expected and failure flows, ensure they are still accurate and desirable.
- Determine how to validate the assumptions and enforce conditions needed for proper behaviors.
- Ensure the results are documented in the user story.
- Learn from mistakes and offer positive incentives to promote improvements.
- Secure design is neither an add-on nor a tool that you can add to software.

# Insecure Design - How to Prevent

Establish and use a secure development lifecycle with AppSec professionals to help evaluate and design security and privacy-related controls

Establish and use a library of secure design patterns or paved road ready to use components.

Use threat modeling for critical authentication, access control, business logic, and key flows.

Integrate security language and controls into user stories.

Integrate plausibility checks at each tier of your application (from frontend to backend).

Write unit and integration tests to validate that all critical flows are resistant to the threat model. Compile use-cases *and* misuse-cases for each tier of your application.

Segregate tier layers on the system and network layers depending on the exposure and protection needs.

Segregate tenants robustly by design throughout all tiers.

Limit resource consumption by user or service.

# A05:2021 – Security Misconfiguration

Moving up from #6 in the previous edition, 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4.%, and over 208k occurrences of a Common Weakness Enumeration (CWE) in this risk category. With more shifts into highly configurable software, it's not surprising to see this category move up. Notable CWEs included are *CWE-16 Configuration* and *CWE-611 Improper Restriction of XML External Entity Reference*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
20	19.84%	4.51%	8.12	6.56	89.58%	44.84%	208387	789

# Security Misconfiguration - Examples

**Scenario #1:** The application server comes with sample applications not removed from the production server. These sample applications have known security flaws attackers use to compromise the server. Suppose one of these applications is the admin console, and default accounts weren't changed. In that case, the attacker logs in with default passwords and takes over.

**Scenario #2:** Directory listing is not disabled on the server. An attacker discovers they can simply list directories. The attacker finds and downloads the compiled Java classes, which they decompile and reverse engineer to view the code. The attacker then finds a severe access control flaw in the application.

**Scenario #3:** The application server's configuration allows detailed error messages, e.g., stack traces, to be returned to users. This potentially exposes sensitive information or underlying flaws such as component versions that are known to be vulnerable.

**Scenario #4:** A cloud service provider (CSP) has default sharing permissions open to the Internet by other CSP users. This allows sensitive data stored within cloud storage to be accessed.

# Security Misconfiguration - Description

The application might be vulnerable if the application is:

- Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services.
- **Unnecessary features** are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
- **Default accounts and their passwords** are still enabled and unchanged.
- **Error handling reveals** stack traces or other overly informative error messages to users.
- For upgraded systems, **the latest security features are disabled** or not configured securely.
- The **security settings** in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values.
- The server does not send security headers or directives, or they are not set to secure values.
- The software is **out of date or vulnerable** (see [Ao6:2021-Vulnerable and Outdated Components](#)).

Without a concerted, repeatable application security configuration process, systems are at a higher risk.



# Security Misconfiguration - How to Prevent

Secure installation processes should be implemented, including:

- A repeatable hardening process makes it fast and easy to deploy another environment that is appropriately locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to set up a new secure environment.
- A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.
- A task to review and update the configurations appropriate to all security notes, updates, and patches as part of the patch management process (see [Ao6:2021-Vulnerable and Outdated Components](#)). Review cloud storage permissions (e.g., S3 bucket permissions).
- A segmented application architecture provides effective and secure separation between components or tenants, with segmentation, containerization, or cloud security groups (ACLs).
- Sending security directives to clients, e.g., Security Headers.
- An automated process to verify the effectiveness of the configurations and settings in all environments.

## Ao6:2021 – Vulnerable and Outdated Components

It was #2 from the Top 10 community survey but also had enough data to make the Top 10 via data. Vulnerable Components are a known issue that we struggle to test and assess risk and is the only category to not have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploits/impact weight of 5.0 is used. Notable CWEs included are *CWE-1104: Use of Unmaintained Third-Party Components* and the two CWEs from Top 10 2013 and 2017.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
3	27.96%	8.77%	5.00	5.00	51.78%	22.47%	30457	0

# Vulnerable and Outdated Components - Examples

**Scenario #1:** Components typically run with the same privileges as the application itself, so flaws in any component can result in serious impact. Such flaws can be accidental (e.g., coding error) or intentional (e.g., a backdoor in a component). Some example exploitable component vulnerabilities discovered are:

- CVE-2017-5638, a Struts 2 remote code execution vulnerability that enables the execution of arbitrary code on the server, has been blamed for significant breaches.
- While the internet of things (IoT) is frequently difficult or impossible to patch, the importance of patching them can be great (e.g., biomedical devices).

There are automated tools to help attackers find unpatched or misconfigured systems. For example, the Shodan IoT search engine can help you find devices that still suffer from Heartbleed vulnerability patched in April 2014.

# Vulnerable and Outdated Components - Description

You are likely vulnerable:

- If you **do not know the versions of all components** you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- If the software is **vulnerable, unsupported, or out of date**. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- If you **do not scan for vulnerabilities regularly** and subscribe to security bulletins related to the components you use.
- If you **do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion**. This commonly happens in environments when patching is a monthly or quarterly task under change control, leaving organizations open to days or months of unnecessary exposure to fixed vulnerabilities.
- If software developers **do not test the compatibility** of updated, upgraded, or patched libraries.
- If you do not secure the components' configurations (see [A05:2021-Security Misconfiguration](#)).

# Vulnerable and Outdated Components - How to Prevent

There should be a patch management process in place to:

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies using tools like versions, OWASP Dependency Check, retire.js, etc.
- Continuously monitor sources like Common Vulnerability and Exposures (CVE) and National Vulnerability Database (NVD) for vulnerabilities in the components.
- Use software composition analysis tools to automate the process. Subscribe to email alerts for security vulnerabilities related to components you use.
- Only obtain components from official sources over secure links. Prefer signed packages to reduce the chance of including a modified, malicious component (See Ao8:2021-Software and Data Integrity Failures).
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a virtual patch to monitor, detect, or protect against the discovered issue.

Every organization must ensure an ongoing plan for monitoring, triaging, and applying updates or configuration changes for the lifetime of the application or portfolio.



# A07:2021 – Identification and Authentication Failures

Previously known as *Broken Authentication*, this category slid down from the second position and now includes Common Weakness Enumerations (CWEs) related to identification failures. Notable CWEs included are *CWE-297: Improper Validation of Certificate with Host Mismatch*, *CWE-287: Improper Authentication*, and *CWE-384: Session Fixation*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
22	14.84%	2.55%	7.40	6.50	79.51%	45.72%	132195	3897

# Identification and Authentication Failures - Examples

**Scenario #1:** Credential stuffing, the use of lists of known passwords, is a common attack. Suppose an application does not implement automated threat or credential stuffing protection. In that case, the application can be used as a password oracle to determine if the credentials are valid.

**Scenario #2:** Most authentication attacks occur due to the continued use of passwords as a sole factor. Once considered best practices, password rotation and complexity requirements encourage users to use and reuse weak passwords. Organizations are recommended to stop these practices per NIST 800-63 and use multi-factor authentication.

**Scenario #3:** Application session timeouts aren't set correctly. A user uses a public computer to access an application. Instead of selecting "logout," the user simply closes the browser tab and walks away. An attacker uses the same browser an hour later, and the user is still authenticated.

# Identification and Authentication Failures - Description

Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application:

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords data stores (see [A02:2021-Cryptographic Failures](#)).
- Has missing or ineffective multi-factor authentication.
- Exposes session identifier in the URL.
- Reuse session identifier after successful login.
- Does not correctly invalidate Session IDs.
- User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity.

# Identification and Authentication Failures - How to Prevent

Where possible, implement multi-factor authentication to prevent automated credential stuffing, brute force, and stolen credential reuse attacks.

Do not ship or deploy with any default credentials, particularly for admin users.

Implement weak password checks, such as testing new or changed passwords against the top 10,000 worst passwords list.

Align password length, complexity, and rotation policies with National Institute of Standards and Technology (NIST) 800-63b's guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence-based password policies.

Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.

Limit or increasingly delay failed login attempts, but be careful not to create a denial of service scenario. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.

Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session identifier should not be in the URL, be securely stored, and invalidated after logout, idle, and absolute timeouts.

# Ao8:2021 – Software and Data Integrity Failures

A new category for 2021 focuses on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data. Notable Common Weakness Enumerations (CWEs) include *CWE-829: Inclusion of Functionality from Untrusted Control Sphere*, *CWE-494: Download of Code Without Integrity Check*, and *CWE-502: Deserialization of Untrusted Data*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
10	16.67%	2.05%	6.94	7.94	75.04%	45.35%	47972	1152



# Software and Data Integrity Failures - Examples

**Scenario #1 Update without signing:** Many home routers, set-top boxes, device firmware, and others do not verify updates via signed firmware. Unsigned firmware is a growing target for attackers and is expected to only get worse. This is a major concern as many times there is no mechanism to remediate other than to fix in a future version and wait for previous versions to age out.

**Scenario #2 SolarWinds malicious update:** Nation-states have been known to attack update mechanisms, with a recent notable attack being the SolarWinds Orion attack. The company that develops the software had secure build and update integrity processes. Still, these were able to be subverted, and for several months, the firm distributed a highly targeted malicious update to more than 18,000 organizations, of which around 100 or so were affected. This is one of the most far-reaching and most significant breaches of this nature in history.

**Scenario #3 Insecure Deserialization:** A React application calls a set of Spring Boot microservices. Being functional programmers, they tried to ensure that their code is immutable. The solution they came up with is serializing the user state and passing it back and forth with each request. An attacker notices the "rOo" Java object signature (in base64) and uses the Java Serial Killer tool to gain remote code execution on the application server.

# Software and Data Integrity Failures - Description

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations.

An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs).

- An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise.
- Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application.
- Attackers could potentially upload their own updates to be distributed and run on all installations.

Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

# Software and Data Integrity Failures - How to Prevent

Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered.

Ensure libraries and dependencies, such as npm or Maven, are consuming trusted repositories. If you have a higher risk profile, consider hosting an internal known-good repository that's vetted.

Ensure that a software supply chain security tool, such as OWASP Dependency Check or OWASP CycloneDX, is used to verify that components do not contain known vulnerabilities

Ensure that there is a review process for code and configuration changes to minimize the chance that malicious code or configuration could be introduced into your software pipeline.

Ensure that your CI/CD pipeline has proper segregation, configuration, and access control to ensure the integrity of the code flowing through the build and deploy processes.

Ensure that unsigned or unencrypted serialized data is not sent to untrusted clients without some form of integrity check or digital signature to detect tampering or replay of the serialized data

# Aog:2021 – Security Logging and Monitoring Failures

Security logging and monitoring came from the Top 10 community survey (#3), up slightly from the tenth position in the OWASP Top 10 2017. Logging and monitoring can be challenging to test, often involving interviews or asking if attacks were detected during a penetration test. There isn't much CVE/CVSS data for this category, but detecting and responding to breaches is critical. Still, it can be very impactful for accountability, visibility, incident alerting, and forensics. This category expands beyond *CWE-778 Insufficient Logging* to include *CWE-117 Improper Output Neutralization for Logs*, *CWE-223 Omission of Security-relevant Information*, and *CWE-532 Insertion of Sensitive Information into Log File*.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
4	19.23%	6.51%	6.87	4.99	53.67%	39.97%	53615	242

# Security Logging and Monitoring Failures - Examples

**Scenario #1:** A children's health plan provider's website operator couldn't detect a breach due to a lack of monitoring and logging. An external party informed the health plan provider that an attacker had accessed and modified thousands of sensitive health records of more than 3.5 million children. A post-incident review found that the website developers had not addressed significant vulnerabilities. As there was no logging or monitoring of the system, the data breach could have been in progress since 2013, a period of more than seven years.

**Scenario #2:** A major Indian airline had a data breach involving more than ten years' worth of personal data of millions of passengers, including passport and credit card data. The data breach occurred at a third-party cloud hosting provider, who notified the airline of the breach after some time.

**Scenario #3:** A major European airline suffered a GDPR reportable breach. The breach was reportedly caused by payment application security vulnerabilities exploited by attackers, who harvested more than 400,000 customer payment records. The airline was fined 20 million pounds as a result by the privacy regulator.



# Security Logging and Monitoring Failures - Description

Returning to the OWASP Top 10 2021, this category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected.

Insufficient logging, detection, monitoring, and active response occurs any time:

- **Auditable events**, such as logins, failed logins, and high-value transactions, are not logged.
- **Warnings and errors** generate no, inadequate, or unclear log messages.
- **Logs of applications and APIs** are not monitored for suspicious activity.
- Logs are **only stored locally**.
- **Appropriate alerting thresholds and response escalation processes** are not in place or effective.
- Penetration testing and scans by dynamic application security testing (DAST) tools (such as OWASP ZAP) do not trigger alerts.
- The application cannot detect, escalate, or alert for active attacks in real-time or near real-time.

You are vulnerable to information leakage by making logging and alerting events visible to a user or an attacker (see [A01:2021-Broken Access Control](#)).

# Security Logging and Monitoring Failures - How to Prevent

Developers should implement some or all the following controls, depending on the risk of the application:

- Ensure all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts and held for enough time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that log management solutions can easily consume.
- Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- DevSecOps teams should establish effective monitoring and alerting such that suspicious activities are detected and responded to quickly.
- Establish or adopt an incident response and recovery plan, such as National Institute of Standards and Technology (NIST) 800-61r2 or later.

There are commercial and open-source application protection frameworks such as the OWASP ModSecurity Core Rule Set, and open-source log correlation software, such as the Elasticsearch, Logstash, Kibana (ELK) stack, that feature custom dashboards and alerting.

# A10:2021 – Server-Side Request Forgery (SSRF)

This category is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage and above-average Exploit and Impact potential ratings. As new entries are likely to be a single or small cluster of Common Weakness Enumerations (CWEs) for attention and awareness, the hope is that they are subject to focus and can be rolled into a larger category in a future edition.

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
1	2.72%	2.72%	8.28	6.72	67.72%	67.72%	9503	385

# SSRF - Examples

Attackers can use SSRF to attack systems protected behind web application firewalls, firewalls, or network ACLs, using scenarios such as:

**Scenario #1:** Port scan internal servers – If the network architecture is unsegmented, attackers can map out internal networks and determine if ports are open or closed on internal servers from connection results or elapsed time to connect or reject SSRF payload connections.

**Scenario #2:** Sensitive data exposure – Attackers can access local files or internal services to gain sensitive information such as `file:///etc/passwd` and `http://localhost:28017/`.

**Scenario #3:** Access metadata storage of cloud services – Most cloud providers have metadata storage such as `http://169.254.169.254/`. An attacker can read the metadata to gain sensitive information.

**Scenario #4:** Compromise internal services – The attacker can abuse internal services to conduct further attacks such as Remote Code Execution (RCE) or Denial of Service (DoS).

# SSRF - Description

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL.

It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

As modern web applications provide end-users with convenient features, fetching a URL becomes a common scenario. As a result, the incidence of SSRF is increasing. Also, the severity of SSRF is becoming higher due to cloud services and the complexity of architectures.



# SSRF - How to Prevent (1/2)

Developers can prevent SSRF by implementing some or all the following defense in depth controls:

## From Network layer

- Segment remote resource access functionality in separate networks to reduce the impact of SSRF
- Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.

### *Hints:*

- ~ Establish an ownership and a lifecycle for firewall rules based on applications.
- ~ Log all accepted *and* blocked network flows on firewalls (see [Aog:2021-Security Logging and Monitoring Failures](#)).

# SSRF - How to Prevent (2/2)

## From Application layer:

- Sanitize and validate all client-supplied input data
- Enforce the URL schema, port, and destination with a positive allow list
- Do not send raw responses to clients
- Disable HTTP redirections
- Be aware of the URL consistency to avoid attacks such as DNS rebinding and “time of check, time of use” (TOCTOU) race conditions
- Do not mitigate SSRF via the use of a deny list or regular expression. Attackers have payload lists, tools, and skills to bypass deny lists.

## Additional Measures to consider:

- Don't deploy other security relevant services on front systems (e.g. OpenID). Control local traffic on these systems (e.g. localhost)
- For frontends with dedicated and manageable user groups use network encryption (e.g. VPNs) on independent systems to consider very high protection needs

# Summary

No.	CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
Ao1	34	55.97%	3.81%	6.92	5.93	94.55%	47.72%	318487	19013
Ao2	29	46.44%	4.49%	7.29	6.81	79.33%	34.85%	233788	3075
Ao3	33	19.09%	3.37%	7.25	7.15	94.04%	47.90%	274228	32078
Ao4	40	24.19%	3.00%	6.46	6.78	77.25%	42.51%	262407	2691
Ao5	20	19.84%	4.51%	8.12	6.56	89.58%	44.84%	208387	789
Ao6	3	27.96%	8.77%	5	5	51.78%	22.47%	30457	0
Ao7	22	14.84%	2.55%	7.4	6.5	79.51%	45.72%	132195	3897
Ao8	10	16.67%	2.05%	6.94	7.94	75.04%	45.35%	47972	1152
Ao9	4	19.23%	6.51%	6.87	4.99	53.67%	39.97%	53615	242
Ao10	1	2.72%	2.72%	8.28	6.72	67.72%	67.72%	9503	385

# Summary: How do you address these problems?

## Develop Secure Code

- Follow the best practices in OWASP's Guide to Building Secure Web Applications
  - [https://www.owasp.org/index.php/OWASP\\_Guide\\_Project](https://www.owasp.org/index.php/OWASP_Guide_Project)
  - And the cheat sheets: [https://www.owasp.org/index.php/OWASP\\_Cheat\\_Sheet\\_Series](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)
- Use OWASP's Application Security Verification Standard as a guide to what an application needs to be secure
  - <https://www.owasp.org/index.php/ASVS>
- Use standard security components that are a fit for your organization
  - Use OWASP's ESAPI as a basis for your standard components
  - <https://www.owasp.org/index.php/ESAPI>

## Review Your Applications

- Have an expert team review your applications
- Review your applications yourselves following OWASP Guidelines
  - OWASP Code Review Guide:  
[https://www.owasp.org/index.php/Code\\_Review\\_Guide](https://www.owasp.org/index.php/Code_Review_Guide)
  - OWASP Testing Guide:  
[https://www.owasp.org/index.php/Testing\\_Guide](https://www.owasp.org/index.php/Testing_Guide)

# Introduction of WebGoat





# WEBGOAT

**WebGoat** is a deliberately insecure web application maintained by [OWASP](#) designed to teach web application security lessons. You can install and practice with WebGoat. There are other 'goats' such as [WebGoat for .Net](#). In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat applications. For example, in one of the lessons the user must use [SQL injection](#) to steal fake credit card numbers. The application aims to provide a realistic teaching environment, providing users with hints and code to further explain the lesson.

Current version: WebGoat 8.0 (released 12 Apr. 2018)

<https://hub.docker.com/r/webgoat/webgoat-8.0/>

Stable version: WebGoat 7.1 (released 19 Nov. 2016)

<https://hub.docker.com/r/webgoat/webgoat-7.1/>

# Review

- Introduction of OWASP TOP 10
- Introduction of WebGoat