[OWASP Top Ten Web Application Security Risks](https://owasp.org/www-project-top-ten/)

1. [**A01:2021-Broken Access Control**](https://owasp.org/Top10/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 any other category.
2. [**A02:2021-Cryptographic Failures**](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/) shifts up one position to #2, previously known as Sensitive Data Exposure, which was 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.
3. [**A03:2021-Injection**](https://owasp.org/Top10/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.
4. [**A04:2021-Insecure Design**](https://owasp.org/Top10/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.
5. [**A05:2021-Security Misconfiguration**](https://owasp.org/Top10/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.
6. [**A06:2021-Vulnerable and Outdated Components**](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/) was previously titled Using Components with Known Vulnerabilities and is #2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.
7. [**A07:2021-Identification and Authentication Failures**](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) was previously Broken Authentication and is sliding down from the second position, and 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.
8. [**A08:2021-Software and Data Integrity Failures**](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/) is a new category for 2021, focusing 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.
9. [**A09:2021-Security Logging and Monitoring Failures**](https://owasp.org/Top10/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.
10. [**A10:2021-Server-Side Request Forgery**](https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_(SSRF)/) 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.
11. A01:2021-Broken Access Control naik dari posisi kelima; 94% aplikasi diuji untuk beberapa bentuk kontrol akses yang rusak. 34 Common Weakness Enumerations (CWE) yang dipetakan ke Broken Access Control memiliki lebih banyak kemunculan dalam aplikasi daripada kategori lainnya.
12. A02:2021-Kegagalan Kriptografis naik satu posisi ke #2, yang sebelumnya dikenal sebagai Paparan Data Sensitif, yang merupakan gejala luas daripada penyebab utama. Fokus baru di sini adalah pada kegagalan yang terkait dengan kriptografi yang sering mengarah pada paparan data sensitif atau kompromi sistem.
13. A03:2021-Injection meluncur turun ke posisi ketiga. 94% aplikasi diuji untuk beberapa bentuk injeksi, dan 33 CWE yang dipetakan ke dalam kategori ini memiliki kejadian terbanyak kedua dalam aplikasi. Skrip Lintas Situs sekarang menjadi bagian dari kategori ini dalam edisi ini.
14. A04:2021-Desain Tidak Aman adalah kategori baru untuk tahun 2021, dengan fokus pada risiko yang terkait dengan kekurangan desain. Jika kita benar-benar ingin "bergerak ke kiri" sebagai sebuah industri, itu membutuhkan lebih banyak penggunaan pemodelan ancaman, pola dan prinsip desain yang aman, dan arsitektur referensi.
15. A05:2021-Security Misconfiguration naik dari #6 di edisi sebelumnya; 90% aplikasi diuji untuk beberapa bentuk kesalahan konfigurasi. Dengan lebih banyak pergeseran ke perangkat lunak yang sangat dapat dikonfigurasi, tidak mengherankan melihat kategori ini naik. Kategori sebelumnya untuk Entitas Eksternal XML (XXE) sekarang menjadi bagian dari kategori ini.
16. A06:2021-Vulnerable and Outdated Components sebelumnya berjudul Using Components with Known Vulnerabilities dan berada di posisi #2 dalam survei komunitas 10 Teratas, tetapi juga memiliki cukup data untuk masuk 10 Besar melalui analisis data. Kategori ini naik dari #9 pada tahun 2017 dan merupakan masalah umum yang kami perjuangkan untuk menguji dan menilai risiko. Ini adalah satu-satunya kategori yang tidak memiliki Common Vulnerability and Exposures (CVEs) yang dipetakan ke CWE yang disertakan, jadi eksploitasi default dan bobot dampak 5.0 diperhitungkan dalam skornya.
17. A07:2021-Kegagalan Identifikasi dan Otentikasi sebelumnya adalah Otentikasi Rusak dan meluncur turun dari posisi kedua, dan sekarang termasuk CWE yang lebih terkait dengan kegagalan identifikasi. Kategori ini masih merupakan bagian integral dari Top 10, tetapi peningkatan ketersediaan kerangka kerja standar tampaknya membantu.
18. A08:2021-Kegagalan Integritas Perangkat Lunak dan Data adalah kategori baru untuk tahun 2021, yang berfokus pada pembuatan asumsi terkait pembaruan perangkat lunak, data penting, dan pipeline CI/CD tanpa memverifikasi integritas. Salah satu dampak berbobot tertinggi dari data Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) yang dipetakan ke 10 CWE dalam kategori ini. Deserialisasi Tidak Aman dari 2017 sekarang menjadi bagian dari kategori yang lebih besar ini.
19. A09:2021-Kegagalan Pencatatan dan Pemantauan Keamanan sebelumnya adalah Pencatatan & Pemantauan yang Tidak Memadai dan ditambahkan dari survei industri (#3), naik dari #10 sebelumnya. Kategori ini diperluas untuk mencakup lebih banyak jenis kegagalan, menantang untuk diuji, dan tidak terwakili dengan baik dalam data CVE/CVSS. Namun, kegagalan dalam kategori ini dapat secara langsung memengaruhi visibilitas, peringatan insiden, dan forensik.
20. A10:2021-Pemalsuan Permintaan Sisi Server ditambahkan dari survei komunitas 10 Teratas (#1). Data menunjukkan tingkat insiden yang relatif rendah dengan cakupan pengujian di atas rata-rata, bersama dengan peringkat di atas rata-rata untuk potensi Eksploitasi dan Dampak. Kategori ini mewakili skenario di mana anggota komunitas keamanan memberi tahu kami bahwa ini penting, meskipun tidak diilustrasikan dalam data saat ini.

commit #1 adalah aplikasi PHP yang sengaja dibuat mengandung banyak *vulnerability* untuk menunjukkan praktek coding mana masuk dalam kategori mana. Dilanjutkan dengan bagaimana cara *fixing*nya.

|  |  |  |
| --- | --- | --- |
| A01:2021 | Contoh source code | Contoh Fix |
| A02:2021 |  |  |
| A03:2021 | [https://github.com/ekorudi/owaspPHP/blob/4bbfad38528128138c06f7ffaa45d1452f28a375/function/actSignin.php#L8](https://github.com/ekorudi/owaspPHP/blob/4bbfad38528128138c06f7ffaa45d1452f28a375/function/actSignin.php" \l "L8) | [https://github.com/ekorudi/owaspPHP/blob/77e386b7fdf87a1949d90a181d5d4c14d76485dc/function/actSignin.php#L8](https://github.com/ekorudi/owaspPHP/blob/77e386b7fdf87a1949d90a181d5d4c14d76485dc/function/actSignin.php" \l "L8) |
| A04:2021 |  |  |