The new OWASP Top 10 for 2021

BY ANNA HAMMOND · SEPTEMBER 10, 2021 · LAST UPDATED ON MARCH 6, 2025

OWASP top 10; Over the last 4 years, the cybersecurity field has continued to see incredible leaps forward at an unimaginable pace. As attacks that used to be prevalent 15 years ago are slowly dying out, new attack vectors are being discovered day in and day out.

Security researchers and bug bounty hunters alike often regard the OWASP top 10 as the official ranking for defining the top 10 most critical web application security risks.

The evolution

Let's take a look at what has changed since 2017:

OWASP Top 10 2021 compared to 2017

A few notable changes here:

- **Cross-Site Scripting (XSS)**, which used to be in the top 3 just 8 years ago has now joined the **Injection** group due to full overlap as XSS is essentially content injection.
- **Server-Side Request Forgery (SSRF)** coming in for the first time. This is an interesting one as it has a fairly low incidence rate, meaning it occurs little, however, the exploit or impact potential is above average. This category did not end up in the list due to its occurrence in the data, but because industry professionals voted it to be of high importance.
- **Broken Authentication** has stood in the 2nd place in the listing since 2010 but is now slowly losing prevalence. This can be attributed to the rise of standardized frameworks. Companies generally aren't writing authentication logic from scratch anymore and that's a great thing.

The top 10

1. Broken Access Control

Time to crown our new number one; Broken Access Control. Moving up the ranking from 5th place, but what does it entail and why is it so important these days?

Access control is exactly what the name suggests; the controlling of access by a user. Users should only be allowed to act within their intended permissions and if that is not the case, then the access controls are broken.

This can include:

- **Unauthorized API access** due to a misconfiguration (CORS, Missing access controls for POST, PUT, and so on)
- **Privilege escalation**

- **Tampering with tokens** such as JWT
- Being able to view another users' records

Popular CWE's mapped to this category are:

- CWE-35: **Path Traversal**
- CWE-352: **Cross-site Request Forgery** (CSRF)
- CWE-601: **Open Redirect**
- And many more

What about these numbers at Intigriti? Well, the numbers down below don't lie. This category is very substantial for our submission counts and that is to be expected. OWASP used real data to compile this list so it's only logical that our data reflects that.

- Open Redirects: 5% of all submissions
- Improper Access Control: 4% of all submissions
- Improper Authentication: 4% of all submissions
- Path Traversal: 2% of all submissions
- CSRF: 1.7% of all submission

2. Cryptographic Failures

Previously known as Sensitive Data Exposure in the OWASP Top 10, Cryptographic Failures shift up one position in the ranking. This renaming occurred because the focus shifted from a symptom to a root cause. Failures related to cryptography often result in data exposure.

Everything in this category relates to the protection of data in transit, in rest, and in use. Data has become a touchy subject with a lot of regulation, however, we're still seeing data being exposed day in and day out.

This can include:

- **Weak cryptographic algorithms** being used
- Improper **key management** causing weak keys, reusage of keys, and so on
- Data being transmitted in **plaintext**, both in external traffic but also in internal traffic.

Popular CWE's mapped to this category are:

- CWE-319: **Cleartext transmission** of sensitive information
- CWE-321: Use of **hard-coded cryptographic key**
- CWE-327: Use of a **broken or risky cryptographic algorithm**

In our data, we see fewer of these issues. This can be because they are difficult to find in black-box testing but also because it's often hard to prove practical impact. These issues are often theoretical or are the result of vulnerabilities in other categories.

- Cleartext Storage of Sensitive Information: 0.8% of all submissions
- Plaintext Storage of a Password: 0.5% of all submissions
- Insecure Storage of Sensitive Information: 0.4% of all submissions
- Cleartext Transmission of Sensitive Information: 0.4% of all submissions

3. Injection

This category is probably the most known of all, including **SQL** injections, **command** injections, **LDAP** injection, and new in this edition; also **XSS**!

In this category, the cause that can be attributed to almost all issues is the lack of validation of user-supplied data.

Popular CWE's mapped to this category are:

- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (**Basic XSS**)
- CWE-77: Improper Neutralization of Special Elements used in a Command ('**Command Injection**')
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('**SQL Injection**')

This category is by far the most popular on Intigriti. This is something that we're seeing everywhere. Most courses mainly cover injection and a lot of researchers focus on it. Let's see the numbers.

- XSS: Over 15% of all submissions
- SQL injection: 2% of all submissions
- Command injection: 0.4% of all submissions

4. Insecure Design

This is a brand new category in the OWASP Top 10 and the idea behind it is that if we want the industry to move forward, then we need to **integrate security in every process**. Security isn't something you can think about after you build an application, it should be incorporated in every aspect and mainly the design.

This category is very broad and hard to define. Things from other categories can often also be due to insecure design.

5. Security Misconfiguration

As explained earlier, the **industry is shifting** more and more towards frameworks and third-party software. One of the things that is very important in these cases is configurability. Hence why we see an increase in this category. More things to configure, results in more possible mistakes to be made.

This can include:

- **Unnecessary features** being enabled
- **Default passwords**
- **Out of date software**

Identifying misconfigurations accounts for at least 5% of all submissions on our platform.

6. Vulnerable and Outdated Components

This overlaps with number 5 in the OWASP Top 10. Again, the usage of more third-party software and frameworks introduces a whole new attack surface. Vulnerabilities can be found in unrelated software and still affect you majorly.

These types of vulnerabilities are easy to automatically find if you maintain proper lists of all components and their versions. Keep everything up to date and keep yourself up to date on the security news!

7. Identification and Authentication Failures

Managing sessions, confirming identity, and properly authenticating users are critical to protecting your data and assets.

This can include:

- **Session fixation**
- Permitting **weak passwords**
- **Brute force attacks** are possible
- No **MFA**

At Intigriti we see a large number of submissions coming in caused by authentication failures.

- Improper authentication: 5% of all submissions
- Session fixation: 0.8% of all submissions

8. Software and Data Integrity Failures

This new category focussed on critical data, the integrity of CI/CD pipelines, and **insecure deserialization**. As the name says, any data or software where the integrity is not verified applies to this category.

If that is all still a bit too theoretical then maybe the SolarWinds malicious update can help you. The integrity was not properly verified and that resulted in one of the most significant breaches of this nature.

Of all the submissions coming in through Intigriti, about 0.3% concerned insecure deserialization.

9. Security Logging and Monitoring Failures

Attacks are happening every single day and the ability to log and monitor your assets is very important. If you don't **properly monitor** then breaches will go undetected. Logs should be readable, monitored, not only stored locally, and should alert.

10. Server-Side Request Forgery

This is a new category that will in the future most likely be enrolled in a bigger one. However, it is very noteworthy that SSRF made it to the list.

This vulnerability occurs when the server makes a request using a user-supplied URL and doesn't validate it properly. This way an attacker can make internal requests, perform a port scan, bypass firewalls, or other ACLs.

Intigriti has also seen an increasing amount of SSRF vulnerabilities coming in. These account for 2% of all submissions Intigriti receives.

What researchers should take away from this new ranking?

Researchers continuously train their current skills and learn new ones. We believe that researchers should take this trend into account. Companies rarely code applications from scratch anymore and modern frameworks are very secure for certain types of attacks. That doesn't mean these attacks aren't feasible anymore but they might decrease in occurrence over the next decade.

If you see that your field of expertise is continuously decreasing in importance in these rankings, then it might be useful to experiment with hunting for an up-and-coming new vulnerability, just to increase your knowledge base. Learning new things runs through the veins of all security researchers, so this will be lots of fun!

However, nobody was surprised by this list. The list has been newly compiled, but researchers have seen these trends in the wild for the past years already. Our advice is to keep on hunting, to keep on making the world safer, whilst getting some well-deserved bounties for it!

What companies should take away from this new ranking?

As a company, there is more to take away from the OWASP Top 10. These are the kinds of attacks that are currently ongoing and will keep on occurring in the near future.

Make sure that you adjust your security training accordingly. Keep your developers up to date on what the new kinds of attacks are and how to prevent them. Awareness is already a big leap towards security. It's hard to protect assets against an unknown enemy. Football teams study every movement of their enemies and change accordingly. We believe security should be treated similarly. It has been proven that security-aware developers develop more secure applications.

However, right now we've only looked at the future, at making sure that going forwards, we don't develop insecure applications. What about our current assets? Are they insecure? Are they vulnerable? It would be

naive to think that these aren't going to be or haven't already been targeted by malicious actors. Therefore, it's important to stay vigilant as a company. Make sure all your assets get tested by individuals with up-to-date skills.

Summary

The new OWASP top 10 ranking shows us the things we've been seeing over the last 4 years in the field. We notice trends of companies opting for frameworks and libraries over custom-coding applications from scratch. This introduces new kinds of vulnerabilities previously unknown to a wider public.

Want to learn more? Have a look at our Hackademy or visit the OWASP site.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com