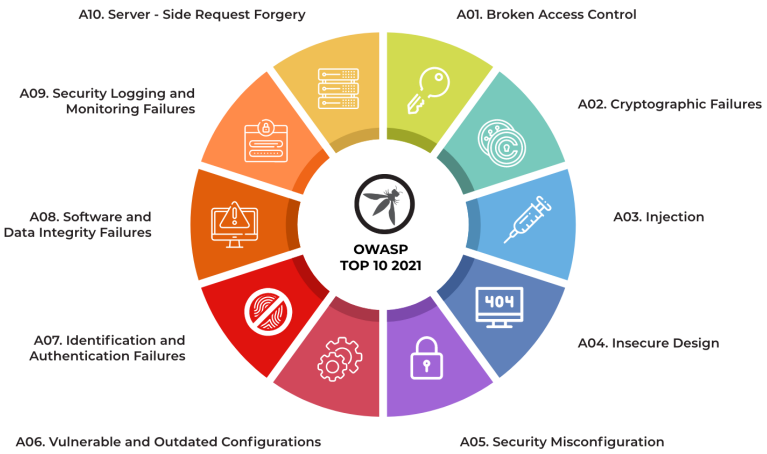
Release of OWASP Top 10 - 2021

OWASP Top 10 (2021) - Security Changes and Real-World Impact

Prepared by Aparna Mishra

INTRODUCTION

The OWASP Top 10 list for 2021 highlights the most critical security risks faced by web applications in the current threat landscape. This documentation aims to provide an in-depth analysis of the updated list, explaining each security risk vector, its real-world implications, and strategies to secure the World Wide Web (WWW) against these vulnerabilities.



SECURITY CHANGES INTRODUCED

1. Broken Access Control

Previously ranked at number 5, broken access control is now considered the most critical security risk according to OWASP. Access control is pivotal in ensuring users operate within their designated permissions. OWASP's tests revealed over 318,000 instances of broken access control, enabling unauthorized user actions. Fixing this vulnerability prevents users from performing unintended actions, securing sensitive data from unauthorized access. Implementing robust access controls in web applications safeguards against unauthorized data modifications or access.

2. Cryptographic Failures

Formerly labeled as Sensitive Data Exposure, cryptographic failures signify inadequate protection of sensitive information like credit card numbers or passwords. GitGuardian's study exposed over 2 million company secrets, indicating a broader issue of secret exposure. Merging the two concepts under cryptographic failures might not accurately address the root cause. Addressing this vulnerability involves securing sensitive data and secrets, preventing unauthorized access and potential data breaches.

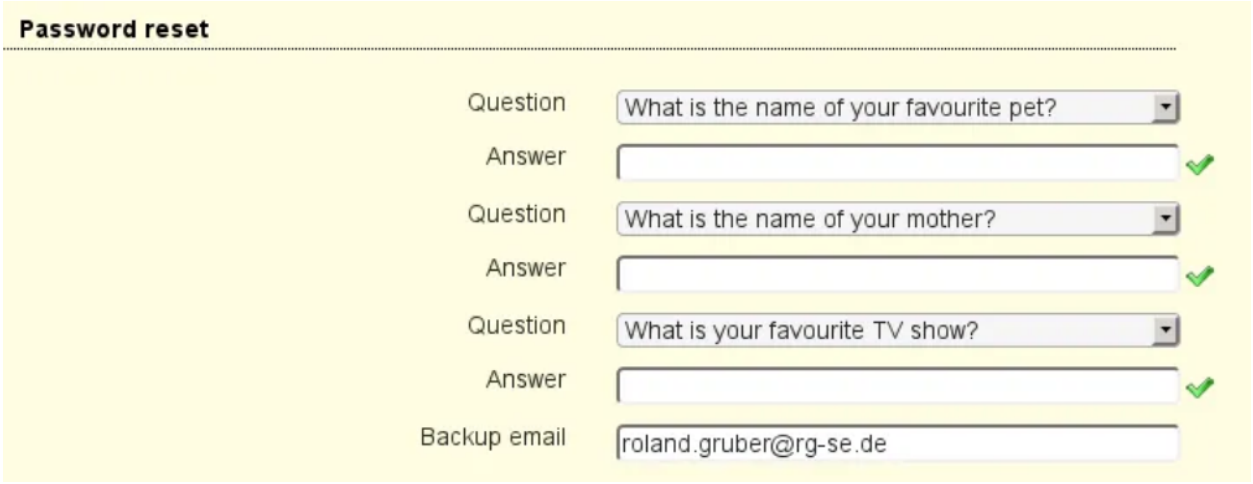
3. Injection

Injection attacks, once at the top spot, now rank third. These attacks exploit applications that accept unfiltered user inputs, leading to vulnerabilities like cross-site scripting and SQL injections. Implementing input validation and proper filtering mechanisms in applications prevents these attacks, securing against data manipulation and unauthorized access.

4. Insecure Design

Insecure application design leads to various security vulnerabilities. Unlike implementation flaws, this stems from a lack of security controls during the application's design phase. A secure-by-design approach ensures the incorporation of robust security

measures from the initial stages, thwarting potential vulnerabilities in the application's architecture.Flaws like using easily guessable security questions for password recovery, or having an architecture that mixes trusted and untrusted data, allowing attackers to take advantage of it.



5. Security Misconfiguration

Security misconfiguration has climbed to number 5 due to increased application configurability, resulting in more room for misconfigurations. Addressing this involves eliminating unnecessary features, setting secure defaults, and ensuring proper access controls to prevent unauthorized access or unnecessary exposure of sensitive data.

6. Vulnerable and Outdated Components

Using outdated or vulnerable components introduces security risks. This includes outdated software versions, vulnerable third-party libraries, or compromised supporting devices like web servers or database management systems. Regular updates, patches, and vetting of components mitigate these vulnerabilities, enhancing overall application security.

7. Identification and Authentication Failures

Previously known as broken authentication, this vulnerability enables attackers to

bypass authentication measures. Weak passwords, inadequate multi-factor authentication, and open-source libraries handling sensitive operations can compromise user accounts or sessions. Strengthening authentication mechanisms and adopting robust password policies thwart unauthorized access attempts.

8. Software and Data Integrity Failures

Failure to ensure software or data integrity poses risks of malicious alterations. Lack of verification in auto-updating functionalities could lead to malware installation. Verifying software and data integrity using file hashes or verification mechanisms prevents tampering and ensures data reliability.

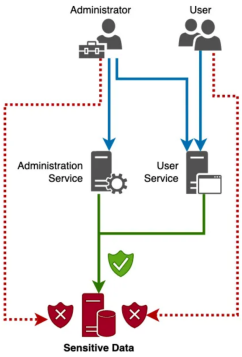
9. Security Logging and Monitoring Failure

Improper logging and monitoring hinder breach detection and response. Implementing robust logging systems helps in identifying, escalating, and responding to active breaches by recording and alerting on security-related events.

10. Server-Side Request Forgery

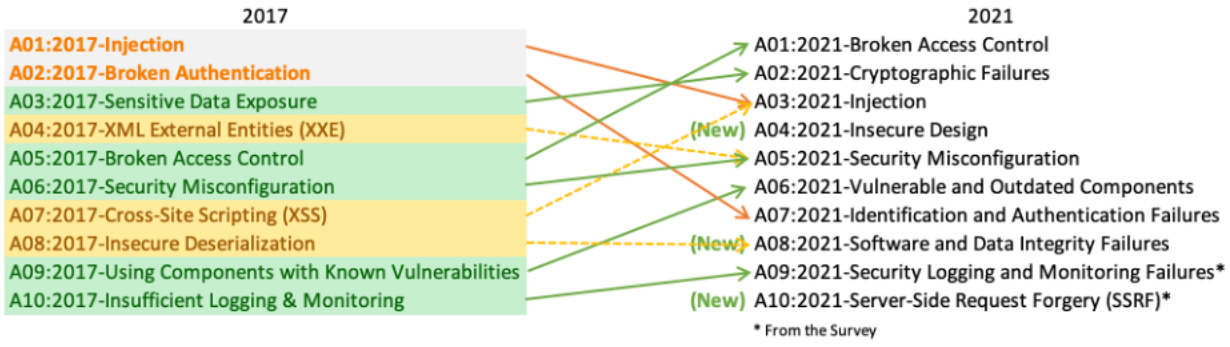
Although not entirely supported by data, SSRF makes the list due to community votes. SSRF vulnerabilities allow attackers to manipulate requests, bypassing network security measures. Addressing SSRF vulnerabilities involves validating user-supplied URLs, preventing attackers from accessing unauthorized resources beyond firewalls or network restrictions, and fortifying web application security.

By addressing these vulnerabilities, organizations can significantly enhance the security posture of their web applications, safeguarding against potential cyber threats and unauthorized access, thereby ensuring a safer and more secure online environment.



These changes in the OWASP Top 10 focus on various ways attackers can exploit weaknesses in website design, configuration, and code integrity to gain unauthorized access or manipulate the system

DIFFERENCE BETWEEN OWASP 2017-2021



The OWASP Top 10 is like a list of the ten most common and risky security problems that can happen to websites and online apps. It's a bit like a "Top 10 Dangers" list for the internet. These risks include things like hackers getting into a website to steal information, weak passwords that make it easy for bad guys to log in, or mistakes in how the website is set up that could let hackers sneak in. By knowing these risks, people who build and manage websites can work to protect against them and keep everyone's information safe.

Lets discuss about the changes:

The future of OWASP (Open Web Application Security Project) is likely to involve ongoing evolution and adaptation to address emerging cybersecurity challenges in web application security. Here are several aspects that could shape the future of OWASP:

Search this file…

	Vulnerability	New	Changed	Unchanged
2	A01:2021-Broken Access Control			✓
3	A02:2021-Cryptographic Failures			✓
4	A03:2021-Injection		✓	
5	A04:2021-Insecure Design	✓		
6	A05:2021-Security Misconfiguration		✓	
7	A06:2021-Vulnerable and Outdated Components			✓
8	A07:2021-Identification and Authentication Failures			✓
9	A08:2021-Software and Data Integrity Failures	✓		
10	A09:2021-Security Logging and Monitoring Failures			✓
11	A10:2021-Server-Side Request Forgery	✓		

FUTURE OF OWASP-10

Advancements in Technology and Threat Landscape:

- OWASP is likely to continue updating its Top 10 and other resources to reflect changes in technology, including the rise of new programming languages, frameworks, and development methodologies.

- With the proliferation of IoT (Internet of Things), cloud computing, AI (Artificial Intelligence), and machine learning, OWASP might expand its focus to cover security concerns specific to these domains.

Emphasis on Secure Development Practices:

- OWASP will likely continue promoting secure coding practices, emphasizing the importance of integrating security into the software development lifecycle (SDLC) from the outset.

- Education and awareness programs aimed at developers and non-security professionals may be expanded to foster a culture of security within organizations.

Continued Community Collaboration:

- OWASP's strength lies in its vibrant community of security professionals, researchers, developers, and volunteers. Continued collaboration within this community will drive the creation of new tools, guidelines, and resources.

- Encouraging contributions and involvement from a diverse range of individuals and organizations worldwide will likely remain a priority.

Focus on Threat Intelligence and Research:

- OWASP may intensify efforts in threat intelligence and ongoing research to identify emerging attack vectors, vulnerabilities, and trends in cyber threats.

- Regular updates to existing resources and the development of new ones based on real-world threats will be crucial to staying relevant.

Expansion of Resources and Frameworks:

- Expectations for OWASP to expand its resources beyond the OWASP Top 10, creating more specialized guidelines and tools for specific vulnerabilities or industries.

- This could include enhanced guidance for securing mobile applications, APIs, microservices, and other specialized domains.

Global Outreach and Impact:

- OWASP will likely continue its global outreach initiatives, aiming to provide accessible security knowledge and resources to regions with varying levels of cybersecurity maturity.

- Collaborations with governments, academia, industry leaders, and international organizations might increase to address broader security challenges.

Overall, OWASP's future lies in its ability to adapt to changing cybersecurity landscapes, meet the evolving needs of developers and security professionals, and remain at the forefront of promoting best practices in web application security. The organization's success will depend on its ability to innovate, collaborate, and engage with a diverse community while staying true to its mission of improving software security worldwide.

FINAL THOUGHTS

The OWASP Top 10 serves as a crucial tool for pinpointing potential security vulnerabilities within applications. Renowned for its comprehensive approach to web application security, the OWASP project stands as a primary resource for safeguarding applications. However, the latest 2021 iteration of the OWASP Top 10 doesn't explicitly address "secret exposure" as a root cause of vulnerabilities. Instead, it has been replaced by "cryptographic failure." Our perspective differs slightly as GitGuardian's research in 2020 revealed over 2 million exposed company secrets, with ongoing discoveries of more than 5,000 company secrets daily. This substantial data illustrates the significant issue of secret exposure in itself. Attackers often exploit publicly accessible secrets, prioritizing them over encrypted ones, even if encryption measures are inadequate. Hence, we believe that merging these two concepts might not adequately encompass the entire breadth of this problem.


OWASP Top 10 vulnerabilities for 2021
01
Broken Access Control
02
Cryptographic Failures
03
Injection
04
Insecure Design
05
Security Misconfiguration
06
Vulnerable and Outdated Components
07
Identification and Authentication Failures
08
Software and Data Integrity Failures
09
Security Logging and Monitoring Failures
10
Server-Side Request Forgery
INFOSECTRAIN
www.infosectrain.com