



Webové aplikace jsou zdrojem informací / zisků / nebezpečí





webová aplikace je když

Webová aplikace v softwarovém inženýrství je aplikace poskytovaná uživateli z webového serveru přes počítačovou síť Internet, nebo její vnitropodnikovou obdobu (intranet).

webové aplikace jsou používány pro implementaci

- podnikových i jiných informačních systémů
- internetových obchodů
- online aukcí
- freemailů
- diskusních fór
- weblogů
- ...



bezpečnostní autority

existuje několik bezpečnostních sad (doporučení na co si dát pozor)

- OWASP (Open Web Application Security Project)
- WASC (Web Application Security Consortium)
- SANS (SysAdmin, Audit, Network, Security) Institute
- ...

A1 Cross Site Scripting (XSS)	The Web Application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
A2 Injection Flaws	Web Applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the Web Application.
A3 Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
A4 Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on user's browser to send a pre-authenticated request to a vulnerable Web Application, which then forces the user's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the Web Application that it attacks.
A6 Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7 Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8 Insecure Cryptographic Storage	Web Applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
A9 Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10 Failure to Restrict URL Access	Applications frequently only protect sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.



realita

❑ *nebezpečí pro webové aplikace*

- číhá skoro všude a hrozí skoro všem
- přichází ze zatím podceňované oblasti
 - hackeři
 - botnety
 - scanery
 - spamy

❑ *nejsou zdroje*

- lidí, kteří vědí co a jak
- strojů / nástrojů pro boj s nebezpečím
- peněz



cloudné řešení

přinášíme vám „cloudné“ řešení

- jednoduché a dostupné
 - stačí změna DNS záznamu
 - žádný HW ani SW
 - dostupná podpora při obsluze
 - ceny od 1250,- Kč
- poskytne potřebný výkon nepřetržitě
 - systém sedí uprostřed českého Internetu
 - oprávněné osoby mohou kdykoliv se systémem pracovat
- usnadní vám život
 - nebudete muset v cyklech točit penetrační testy webu
 - zvýší se výkon vašeho web serveru
 - zvýší se bezpečnost celého systému, do kterého je web zasazen
 - certifikace PCI



Děkuji za pozornost

Otázky Odpovědi

VUMS DataCom, spol. s r.o.

U Ladronky 2331 / 7

169 00 Praha 6 – Břevnov

www.datacom.cz

Ivo Kubíček

ivo.kubicek@datacom.cz

721 129 068