Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	CWE-787	Out-of-bounds Write	11.08
[13]	CWE-287	Improper Authentication	10.78
[14]	CWE-476	NULL Pointer Dereference	9.74
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.33
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type	5.50
[17]	CWE-611	Improper Restriction of XML External Entity Reference	5.48
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')	5.36
[19]	CWE-798	Use of Hard-coded Credentials	5.12
[20]	CWE-400	Uncontrolled Resource Consumption	5.04
[21]	CWE-772	Missing Release of Resource after Effective Lifetime	5.04
[22]	CWE-426	Untrusted Search Path	4.40
[23]	CWE-502	Deserialization of Untrusted Data	4.30
[24]	CWE-269	Improper Privilege Management	4.23
[25]	CWE-295	Improper Certificate Validation	4.06

Figura 7- CWE Top 25 [Fonte: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html]

5.3.4 Common Attack Pattern Enumeration and Classification (CAPEC)

CAPEC è un'iniziativa co-sponsorizzata dal NCSD dell'US DHS e guidata dalla Cigital[15]. Costruttori di software sicuro devono proteggersi da importanti vulnerabilità potenziali. Per identificare e mitigare le vulnerabilità relative al software, la community di sviluppo ha bisogno di capire la prospettiva dell'attaccante e gli approcci utilizzati per sfruttare il software.

Gli schemi di attacco sono le descrizioni di metodi comuni per lo sfruttamento del software, fornendo sia la prospettiva che la guida dell'attaccante sui modi per mitigare il loro effetto. Essi derivano dal concetto di pattern design applicato in un distruttivo, piuttosto che costruttivo, contesto e sono generati da un'analisi approfondita di specifici esempi di casi del mondo reale.

Questa iniziativa mira a fornire un catalogo a disposizione del pubblico di schemi di attacco, insieme ad uno schema di classificazione e tassonomia completo. La filosofia è di evolvere il catalogo con la partecipazione e i contributi pubblici e così consolidare un meccanismo standard per l'identificazione, la raccolta, la raffinazione, e la condivisione di modelli di attacco nella community software.

URL	**https://capec.mitre.org**
Country of HQ location **Geographic Scope**	US National
Type	Government

[15] https://www.synopsys.com/software-integrity.html

Secondo questa iniziativa, le informazioni sugli schemi di attacco, se catturati in modo formale, possono portare un notevole valore per considerazioni di sicurezza del software attraverso tutte le fasi del SDLC e le altre attività relative alla sicurezza, tra cui:

- Raccolta dei requisiti: Identificazione dei requisiti di sicurezza pertinenti, dei misuse e abuse cases.
- Architettura e design: Fornisce il contesto per l'analisi dei rischi architetturali e le linee guida per la sicurezza nelle architetture del software.
- Implementazione e codifica: Prioritizzazione e guida delle attività di revisione sicura del codice.
- Test del software e controllo qualità: Fornisce il contesto per una appropriata analisi del rischio e test di penetrazione.
- Operatività dei sistemi: Sfruttare le esperienze apprese dagli incidenti di sicurezza per fornire una guida preventiva.
- Politiche e generazione di standard: Guida all'identificazione di adeguate politiche e standard organizzativi prescrittivi.

Risultati più rilevanti:

- **List of Attack Patterns** [http://capec.mitre.org/]. L'elenco è disponibile in due diversi formati:
  - View by Mechanisms of Attack [http://capec.mitre.org/data/definitions/1000.html].
  - View by Domains of Attack [http://capec.mitre.org/data/definitions/3000.html].