hackerone

RELATIONSHIP BETWEEN RECOMMENDED WEAKNESS (CAPEC OR CWE) AND HACKERONE LEGACY VULNERABILITY TYPES

The table below provides a mapping between the legacy Vulnerability Types and their corresponding Weaknesses in the upgraded HackerOne taxonomy, along with external references to either Common Weakness Enumeration (CWE) or Common Attack Patter Enumeration and Classification (CAPEC).

Legacy	New	
Vulnerability Type	**Weakness**	**Reference**
Authentication	Improper Authentication - Generic	CWE-287
Command Injection	Command Injection - Generic	CWE-77
Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	CWE-352
Cross-Site Scripting (XSS)	Cross-site Request Forgery (XSS) - Generic	CWE-79
Cryptographic Issue	Cryptographic Issues - Generic	CWE-310
Denial of Service	Denial of Service	CWE-400
Design Issue	Violation of Secure Design Principles	CWE-657
HTTP Response Splitting	HTTP Response Splitting	CWE-113
Information Disclosure	Information Disclosure	CWE-200
Memory Corruption	Memory Corruption - Generic	CWE-119
Missing Best Practice	Violation of Secure Design Principles	CWE-657
None Applicable	-	-
Privilege Escalation	Privilege Escalation	CAPEC-233
Remote Code Execution	Code Injection	CWE-94
SQL Injection	SQL Injection	CWE-89
Server-Side Request Forgery (SSRF)	Server-Side Request Forgery (SSRF)	CWE-918
UI Redressing (Clickjacking)	UI Redressing (Clickjacking)	CAPEC-103
Unvalidated / Open Redirect	Open Redirect	CWE-601
XML External Entities (XXE)	XML External Entities (XXE)	CWE-611