

Insecure.Inc Curriculum

Challenge Name	SANS 25 CWE(s)	OWASP Top 10 2017	PCI-DSS Req. 6
Yellow Belt : Missing Authentication for Critical Function	CWE 306	A2	6.5.10, 6.5.8
Yellow Belt : Reliance on Untrusted Inputs in a Security Decision	CWE 807	A2, A5	6.5.10, 6.5.8
Yellow Belt : Missing Authorization	CWE 862	A5	6.5.10
Orange Belt : Missing Encryption of Sensitive Data	CWE 311	A3	6.5.3, 6.5.4
Orange Belt : Use of a Broken or Risky Cryptographic Algorithm	CWE 327	A3	6.5.3, 6.5.4
Orange Belt : Use of a One-Way Hash without a Salt	CWE 759	A3	6.5.3, 6.5.4
Green Belt : Password Guessing Attack	CWE 307, CWE 798	A2	6.5.10
Green Belt : Integer Overflow or Wraparound	CWE 190	N/A	N/A
Green Belt : Download of Code Without Integrity Check	CWE 494	N/A	N/A
Purple Belt : URL Redirection to Untrusted Site ('Open Redirect')	CWE 601	N/A	N/A
Purple Belt : Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') and related flaws	CWE 79 CWE 829	A7	6.5.7
Purple Belt : Cross-Site Request Forgery (CSRF)	CWE 352	N/A	6.5.9
Blue Belt : Unrestricted Upload of File with Dangerous Type	CWE 434	N/A	6.5.8

Blue Belt : Improper Restriction of XML External Entity Reference ('XXE')	CWE 611	A4	6.5.1
Blue Belt : Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE 22	A5	6.5.8
Brown Belt : Incorrect Authorization	CWE 863	A5	6.5.4
Brown Belt : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') and related flaws	CWE 78 CWE 250 CWE 732	A1	6.5.1
Brown Belt : Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE 89	A1	6.5.1, 6.5.5
Black Belt : Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') and related flaws	CWE 120 CWE 676	N/A	6.5.2
Black Belt : Use of Externally-Controlled Format String	CWE 134	N/A	N/A
Black Belt : Quiz	All of the above	All of the above	All of the above