89 Failure to Preserve SQL Query Structure ('SQL Injection')	CWE/SANS Top 25	R	elease	es
89 Failure to Preserve SQL Query Structure ('SQL Injection')		2009	2010	2011
78	Insecure Interaction between Components			
78				
1	89 Failure to Preserve SQL Query Structure ('SQL Injection")			
434 Unrestricted Upload of File with Dangerous Type				
352 Cross-Site Request Forgery (CSRF)		✓	-	
1901 Program		X	8	
319 Cleartext Transmission of Sensitive Information	352 Cross-Site Request Forgery (CSRF)	✓		
10 Improper Input Validation		X	23	22
116 Improper Encoding or Escaping of Output		✓	Х	X
362 Race Condition		✓	X	X
209 Information Exposure Through an Error Message [1]	116 Improper Encoding or Escaping of Output	✓	Х	Х
Risky Resource Management 120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') x 3 3 3 3 3 22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') x 7 13 494 Download of Code without Integrity Check y 20 14 4 16 98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion') x 14 16 16 16 50 Each of Potentially Dangerous Function x 18 20 Inclusion of Punction of Buffer Size x 18 20 13 4 Uncontrolled Format String x 18 20 19 Integer Overflow or Wraparound x 18 20 Integer Overflow or Wraparound x 19 Integer Overflow or Wraparound x 16 24 External Control of Critical State Data y x 18 20 Integer Overflow or Wraparound x 19 Failure to Constrain Operations within the Bounds of Memory Buffer y x 18 24 26 Unitsued Control of Critical State Data y x 18 24 26 Unitsued Search Path y x 18 24 27 25 External Control of Critical State Data y x 18 26 Integer Overflow or Wraparound x 20 External Control of Critical State Data y x 18 26 Integer Overflow or Wraparound x 20 External Control of Critical State Data y x 18 26 Integer Overflow or Wraparound x 19 External Control of Critical State Data y x 18 26 Integer Overflow or Wraparound x 19 External Control of Critical State Data y x 18 26 Integer Overflow or Wraparound x 19 External Control of Critical State Data y x 18 20 Integer Overflow or Wraparound x 19 External Control of Critical State Data y x 18 20 Integer Overflow or Wraparound x 19 External Control of Critical State Data y x 18 20 Integer Overflow or Wraparound x 19 External Control Critical State Data y x 18 20 Integer Overflow or Wraparound x 19 External Control Critical Function x 19 External Control Critical Functi		✓	25	Х
120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	209 Information Exposure Through an Error Message [1]	✓	17	Х
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Risky Resource Management			
494 Download of Code without Integrity Check 20 14	120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	X		
Big Inclusion of Functionality from Untrusted Control Sphere Statement in PHP Program ('PHP File Inclusion') Inclusion' Inclu				
Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion') X		✓	20	
Inclusion			14	16
131 Incorrect Calculation of Buffer Size 134 Uncontrolled Format String 13 Incorrect Calculation of Buffer Size 134 Uncontrolled Format String 139 Integer Overflow or Wraparound 1419 Failure to Constrain Operations within the Bounds of Memory Buffer 142 External Control of Critical State Data 153 External Control of File Name of Path 1426 Untrusted Search Path 1446 Untrusted Search Path 145 Failure to Control Generation of Code ('Code Injection') 145 Failure to Control Generation of Code ('Code Injection') 146 Failure to Control Generation of Code ('Code Injection') 147 A X X X X X X X X X X X X X X X X X X	Inclusion')	X	14	
134 Uncontrolled Format String 190 Integer Overflow or Wraparound 119 Failure to Constrain Operations within the Bounds of Memory Buffer 4		X	Х	
190 Integer Overflow or Wraparound 119 Failure to Constrain Operations within the Bounds of Memory Buffer 12 External Control of Critical State Data 23 External Control of File Name of Path 24 Cuntrusted Search Path 24 Eallure to Control Generation of Code ('Code Injection') 25 Failure to Control Generation of Code ('Code Injection') 26 Failure to Control Generation of Release 27 Canal Mark State St		X	18	
119 Failure to Constrain Operations within the Bounds of Memory Buffer 642 External Control of Critical State Data 7	134 Uncontrolled Format String	Х	Х	23
642 External Control of Critical State Data 73 External Control of File Name of Path 426 Untrusted Search Path 426 Untrusted Search Path 427 Failure to Control Generation of Code ('Code Injection') 4404 Improper Resource Shutdown or Release 455 Improper Initialization 4582 Incorrect Calculation 4594 Improper Calculation 4595 Buffer Access with Incorrect Length Value 4595 Improper Validation of Array Index 4594 Improper Validation of Array Index 4595 Improper Validation of Array Index 4596 Improper Validation of Array Index 4596 Improper Validation of Resources without Limits or Throttling 4596 Improper Validation of Array Index 4596 Improper Authorization 4596 Improper Authorization 4596 Improper Authorization 4597 Improper Authorization 4507 Improper Restriction of Excessive Authentication Attempts 4507 Improper Restrictio	190 Integer Overflow or Wraparound	Х	16	24
642 External Control of Critical State Data 73 External Control of File Name of Path 426 Untrusted Search Path 426 Untrusted Search Path 427 Failure to Control Generation of Code ('Code Injection') 4404 Improper Resource Shutdown or Release 455 Improper Initialization 4582 Incorrect Calculation 4594 Improper Calculation 4595 Buffer Access with Incorrect Length Value 4595 Improper Validation of Array Index 4594 Improper Validation of Array Index 4595 Improper Validation of Array Index 4596 Improper Validation of Array Index 4596 Improper Validation of Resources without Limits or Throttling 4596 Improper Validation of Array Index 4596 Improper Authorization 4596 Improper Authorization 4596 Improper Authorization 4597 Improper Authorization 4507 Improper Restriction of Excessive Authentication Attempts 4507 Improper Restrictio	119 Failure to Constrain Operations within the Bounds of Memory Buffer	✓	Х	Х
426 Untrusted Search Path 4 Failure to Control Generation of Code ('Code Injection') 4 04 Improper Resource Shutdown or Release 65 Improper Initialization 7		✓	Х	Х
94 Failure to Control Generation of Code ('Code Injection') 404 Improper Resource Shutdown or Release 665 Improper Initialization 682 Incorrect Calculation 805 Buffer Access with Incorrect Length Value 754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling Porous Defences 306 Missing Authentication for Critical Function 862 Missing Authentication for Critical Function 862 Missing Authorization 285 Improper Authorization 285 Improper Authorization 306 Massing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 803 Incorrect Authorization 250 Execution with Unnecessary Privileges 305 Execution with Unnecessary Privileges 306 Incorrect Permission Assignment for Critical Resource 307 Use of Broken or Risky Cryptographic Algorithm 308 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 807 Gold Client-Side Enforcement of Server-Side Security 759 Hard Coded Password	73 External Control of File Name of Path	✓	Х	Х
404 Improper Resource Shutdown or Release 665 Improper Initialization 682 Incorrect Calculation 805 Buffer Access with Incorrect Length Value 754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling 7862 Missing Authentication for Critical Function 862 Missing Authentication 862 Missing Authorization 862 Missing Authorization 863 Improper Authorization 870 Allocation of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 863 Incorrect Authorization 864 Incorrect Permission Assignment for Critical Resource 972 Use of Broken or Risky Cryptographic Algorithm 873 Use of One-Way Hash without Salt 875 Use Enforcement of Server-Side Security 875 Hard Coded Password 875 Authorization 877 Authorization 878 Use of Broken or Risky Cryptographic Algorithm 879 Use of One-Way Hash without Salt 870 Reliance Coded Password 870 Security Security 871 Authorization 872 Use Enforcement of Server-Side Security 873 Use One-Way Hash without Salt 874 Authorization 875 Authorization Auth		✓	Х	Х
404 Improper Resource Shutdown or Release 665 Improper Initialization 682 Incorrect Calculation 805 Buffer Access with Incorrect Length Value 754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling 7862 Missing Authentication for Critical Function 862 Missing Authentication 862 Missing Authorization 862 Missing Authorization 863 Improper Authorization 870 Allocation of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 863 Incorrect Authorization 864 Incorrect Permission Assignment for Critical Resource 972 Use of Broken or Risky Cryptographic Algorithm 873 Use of One-Way Hash without Salt 875 Use Enforcement of Server-Side Security 875 Hard Coded Password 875 Authorization 877 Authorization 878 Use of Broken or Risky Cryptographic Algorithm 879 Use of One-Way Hash without Salt 870 Reliance Coded Password 870 Security Security 871 Authorization 872 Use Enforcement of Server-Side Security 873 Use One-Way Hash without Salt 874 Authorization 875 Authorization Auth	94 Failure to Control Generation of Code ('Code Injection')	✓	Х	Х
665 Improper Initialization		✓	Х	Х
682 Incorrect Calculation 805 Buffer Access with Incorrect Length Value 754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling Porous Defences 306 Missing Authentication for Critical Function 862 Missing Authentication 862 Missing Authorization 862 Missing Authorization 8798 Use of Hard-coded Credentials 811 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 802 Client-Side Enforcement of Server-Side Security 7 X X 259 Hard Coded Password		✓		
805 Buffer Access with Incorrect Length Value 754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling Resources 806 Missing Authentication for Critical Function 862 Missing Authentication for Critical Function 862 Missing Authorization 862 Improper Authorization 8798 Use of Hard-coded Credentials 811 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 863 Incorrect Authorization 863 Incorrect Authorization 863 Incorrect Permission Assignment for Critical Resource 879 Use of Broken or Risky Cryptographic Algorithm 9759 Use of Broken or Risky Cryptographic Algorithm 9759 Use of One-Way Hash without Salt 8602 Client-Side Enforcement of Server-Side Security 9759 Hard Coded Password	682 Incorrect Calculation	✓		
754 Improper Check for Unusual or Exceptional Conditions 129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling x 22 x Porous Defences 306 Missing Authentication for Critical Function 862 Missing Authorization x 5 6 6 285 Improper Authorization x 5 66/15 798 Use of Hard-coded Credentials x 11 7 311 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision x 6 10 250 Execution with Unnecessary Privileges x 11 863 Incorrect Authorization x 5 15 732 Incorrect Permission Assignment for Critical Resource 307 Improper Restriction of Excessive Authentication Attempts x 21 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security x x 259 Hard Coded Password		Х	12	
129 Improper Validation of Array Index 770 Allocation of Resources without Limits or Throttling Porous Defences 306 Missing Authentication for Critical Function 862 Missing Authorization 285 Improper Authorization 285 Improper Authorization 798 Use of Hard-coded Credentials 311 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 807 Reliance ret Authorization 250 Execution with Unnecessary Privileges 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x 15 x 22 x 21 x 22 x 22 x 22 x 24			13	
Porous Defences 306 Missing Authentication for Critical Function 862 Missing Authorization 285 Improper Authorization 798 Use of Hard-coded Credentials 807 Reliance on Untrusted Inputs in a Security Decision 286 Execution with Unnecessary Privileges 863 Incorrect Authorization 732 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 799 Use of One-Way Hash without Salt 709 Execution Sensitive Data 800 Reliance on Untrusted Inputs in a Security Decision 801 Decirion Sensitive Data 802 Execution with Unnecessary Privileges 803 Incorrect Authorization 804 Decirion Sensitive Data 805 Execution With Unnecessary Privileges 806 Incorrect Permission Assignment for Critical Resource 807 Use of Broken or Risky Cryptographic Algorithm 808 Decirion Sensitive Data 809 Use of One-Way Hash without Salt				
306 Missing Authentication for Critical Function 862 Missing Authorization 285 Improper Authorization 798 Use of Hard-coded Credentials 311 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password 2 5 66 2 607 15				
862 Missing Authorization 285 Improper Authorization ^[2] 798 Use of Hard-coded Credentials 311 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x 11 75 60.15 60.	Porous Defences			
285 Improper Authorization ^[2] 798 Use of Hard-coded Credentials 311 Missing Encryption of Sensitive Data 807 Reliance on Untrusted Inputs in a Security Decision 250 Execution with Unnecessary Privileges 4 11 863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password 5 6/16 x 11 x 5 15 x 24 19 x 25 602 Client-Side Enforcement of Server-Side Security		X	19	5
798 Use of Hard-coded Credentialsx117311 Missing Encryption of Sensitive Datax108807 Reliance on Untrusted Inputs in a Security Decisionx610250 Execution with Unnecessary Privileges✓x11863 Incorrect Authorizationx515732 Incorrect Permission Assignment for Critical Resource✓2117327 Use of Broken or Risky Cryptographic Algorithm✓2419307 Improper Restriction of Excessive Authentication Attemptsxx21759 Use of One-Way Hash without Saltxx25602 Client-Side Enforcement of Server-Side Security✓xx259 Hard Coded Password✓xx	862 Missing Authorization	Х		6
798 Use of Hard-coded Credentialsx117311 Missing Encryption of Sensitive Datax108807 Reliance on Untrusted Inputs in a Security Decisionx610250 Execution with Unnecessary Privileges✓x11863 Incorrect Authorizationx515732 Incorrect Permission Assignment for Critical Resource✓2117327 Use of Broken or Risky Cryptographic Algorithm✓2419307 Improper Restriction of Excessive Authentication Attemptsxx21759 Use of One-Way Hash without Saltxx25602 Client-Side Enforcement of Server-Side Security✓xx259 Hard Coded Password✓xx		√	5	6/15
311 Missing Encryption of Sensitive Datax108807 Reliance on Untrusted Inputs in a Security Decisionx610250 Execution with Unnecessary Privileges✓x11863 Incorrect Authorizationx515732 Incorrect Permission Assignment for Critical Resource✓2117327 Use of Broken or Risky Cryptographic Algorithm✓2419307 Improper Restriction of Excessive Authentication Attemptsxx21759 Use of One-Way Hash without Saltxx25602 Client-Side Enforcement of Server-Side Security✓xx259 Hard Coded Password✓xx	798 Use of Hard-coded Credentials	Х	11	
807 Reliance on Untrusted Inputs in a Security Decisionx610250 Execution with Unnecessary Privilegesx11863 Incorrect Authorizationx515732 Incorrect Permission Assignment for Critical Resourcex2117327 Use of Broken or Risky Cryptographic Algorithmx2419307 Improper Restriction of Excessive Authentication Attemptsxx21759 Use of One-Way Hash without Saltxx25602 Client-Side Enforcement of Server-Side Securityxxx259 Hard Coded Passwordxxx		Х	10	8
250 Execution with Unnecessary Privileges 863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password ✓ x x x	807 Reliance on Untrusted Inputs in a Security Decision		6	10
863 Incorrect Authorization 732 Incorrect Permission Assignment for Critical Resource 327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x 5 15 21 17 22 19 23 27 Use of One-Way Hash without Salt x x 25 x x 25 x x x 25	250 Execution with Unnecessary Privileges	✓		
732 Incorrect Permission Assignment for Critical Resource✓2117327 Use of Broken or Risky Cryptographic Algorithm✓2419307 Improper Restriction of Excessive Authentication Attemptsxx21759 Use of One-Way Hash without Saltxx25602 Client-Side Enforcement of Server-Side Security✓xx259 Hard Coded Password✓xx		Х	5	
327 Use of Broken or Risky Cryptographic Algorithm 307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password ✓ x x x	732 Incorrect Permission Assignment for Critical Resource	✓	21	
307 Improper Restriction of Excessive Authentication Attempts 759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x x 21 x x 25 x x x x x x x x x x x x x x x x x x x		✓		
759 Use of One-Way Hash without Salt 602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x x 25 x x x x		Х		
602 Client-Side Enforcement of Server-Side Security 259 Hard Coded Password x x x x				
259 Hard Coded Password ✓ x x				
7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
V V USC OF INSUFFICIENTLY NATIONAL YALACS	330 Use of Insufficiently Random Values	✓	X	X

^[1] Renamed from "Error Message Information Leak" on 1st December 2009

^[2] Renamed from "Improper Access Control (Authorization)" on 29th March 2011