Primeon

DeepSource Application Vulnerability Patterns (Samples)

Input Validation

1 Buffer Overflow
2 By-Passing SiteMinder Input Filter
3 Canonicalization
4 Cross-Site Scripting
5 Cross-Site Scripting by getParameterNames() in JSP
6 Cross-Site Scripting in CGI
7 Cross-Site Scripting through HTTP Request in JSP
8 Cross-Site Scripting through Java Bean in JSP
9 Cross-Site Scripting without Script Tag
10 Data Type Conversion Overflow
11 Flawed Redirection
12 Incomplete Input Validation Filter
13 Incomplete URL Validation
14 JavaScript and HTML Injection
15 JavaScript and HTML Injection in SnoopServlet
16 OS Command Execution through ksh eval
17 OS Command Execution through Open() in Perl
18 OS Command Execution through popen and system in C/C++
19 OS Command Execution through shell invoker in Perl
20 SQL Injection

Authorization

21 “Backdoor”
22 Back-Up Files/Temp Files
23 Business Data File Exposure
24 CGI Source Code Exposure
25 Configuration Files and Template Files
26 Cookie Manipulation
27 Data Files
28 Database Files
29 Debug Functions
30 Elevation of Privilege
31 File Downloading
32 File Listing
33 File Uploading
34 Flawed Access Control
35 Flawed Access Control Policy
36 Flawed in Database Access Validation
37 Flawed in ID Access Privilege Check
38 Flawed Password Change Logic
39 Flawed Person ID Recovery Mechanism
40 Identity Spoofing
41 Including Files
42 Internal Used Servlet Access Control Flaw

43 Missing Entitlement Check
44 Obsolete File Missing Authorization
45 Page Missing Authorization
46 Server Files Exposure
47 Server Memory Pointer Exposure
48 SiteMinder Access Control Interface Exposure
49 Source Content
50 Testing Page Exposure
51 Unauthorized Access to Administration Functions
52 Unauthorized Access to Debug Class (InvokerServlet)
53 Unprotected Transaction Message
54 Weak Authorization
55 Web Services Exposure

Authentication

56 Authentication Missed
57 Brute Force Attacks
58 Issue in Login Page
59 Network Eavesdropping
60 SiteMinder Integration Flaw
61 Weak Session Validation

Configuration Management

62 Debugging Interface
63 Default EPICentric Modules
64 Directory Exposure
65 HTTP Session with Business Critical Info
66 Over-Privileged Process and Services Accounts
67 Profiling
68 Retrieval of Plaintext Configuration Secrets
69 Server Configuration Exposure
70 Unauthorized Access to Administration Interfaces
71 Untrusted Open Source
72 Vendor Component Patch
73 Web Server Configured with TRACE Method

Sensitive Data

74 Access to Sensitive Data in Comment
75 Access to Sensitive Data in Cookies
76 Access to Sensitive Data in History
77 Access to Sensitive Data in Storage
78 Application Critical Info Exposure
79 Debug Page Exposure
80 Sensitive Data Stored in JavaScript

Session Management

81 Session Cookie Management
82 Session Hijacking
83 Session Replay

Parameter Manipulation

84 Request Parameter Manipulation
85 Request Parameter Manipulation in Java
86 Request Parameter Manipulation in JSP

Exception Management

87 Compiler Error Info Exposure
88 Implementation Details Revealed
89 Program Call Stack Exposure
90 SQL Query Statement Exposure

Auditing and Logging

91 Attackers Exploit an Application Without Leaving a Trace
92 Missing Post Parameter Logging

Cryptography

93 Missing Encryption Method
94 Password in Configuration File
95 Unencrypted Password in Source File
96 Weak Encryption Algorithm