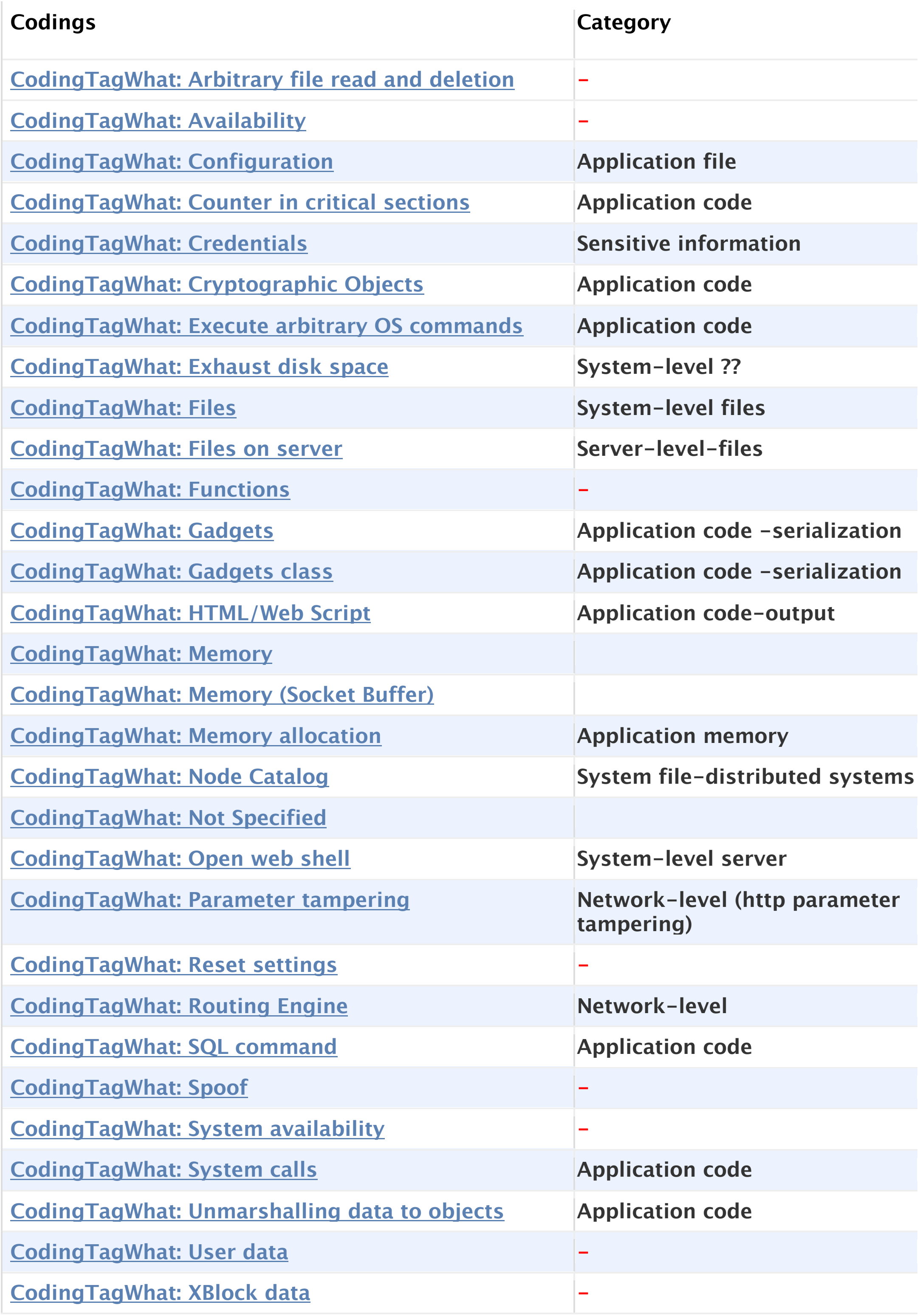
Analysis Notes (2)

A Grounded Theory Based Approach to Characterize Software Attack Surfaces

Memo #1: Open Codes and Initial Concepts for Targets



Codings	Category
CodingTagWhat: Arbitrary file read and deletion	–
CodingTagWhat: Availability	–
CodingTagWhat: Configuration	Application file
CodingTagWhat: Counter in critical sections	Application code
CodingTagWhat: Credentials	Sensitive information
CodingTagWhat: Cryptographic Objects	Application code
CodingTagWhat: Execute arbitrary OS commands	Application code
CodingTagWhat: Exhaust disk space	System-level ??
CodingTagWhat: Files	System-level files
CodingTagWhat: Files on server	Server-level-files
CodingTagWhat: Functions	–
CodingTagWhat: Gadgets	Application code -serialization
CodingTagWhat: Gadgets class	Application code -serialization
CodingTagWhat: HTML/Web Script	Application code-output
CodingTagWhat: Memory	
CodingTagWhat: Memory (Socket Buffer)	
CodingTagWhat: Memory allocation	Application memory
CodingTagWhat: Node Catalog	System file-distributed systems
CodingTagWhat: Not Specified	
CodingTagWhat: Open web shell	System-level server
CodingTagWhat: Parameter tampering	Network-level (http parameter tampering)
CodingTagWhat: Reset settings	–
CodingTagWhat: Routing Engine	Network-level
CodingTagWhat: SQL command	Application code
CodingTagWhat: Spoof	–
CodingTagWhat: System availability	–
CodingTagWhat: System calls	Application code
CodingTagWhat: Unmarshalling data to objects	Application code
CodingTagWhat: User data	–
CodingTagWhat: XBlock data	–

CodingTagWhat: add admin user	Deisgn-level
CodingTagWhat: android activity	Application-code
CodingTagWhat: argument type casting	Application-code
CodingTagWhat: check boundary	Network-level (boundary in network-packet)
CodingTagWhat: configuration file of executable files	Application-data file
CodingTagWhat: critical directory	Server-level directory
CodingTagWhat: deserializing class	Application-code
CodingTagWhat: deserializing polymorphic class	Application-code
CodingTagWhat: device access	Device level
CodingTagWhat: dynamic code inclusion	Application-code
CodingTagWhat: enable escalation of privilege	-
CodingTagWhat: file system	System-level
CodingTagWhat: file upload	Application-code UI
CodingTagWhat: get file content	Application-code
CodingTagWhat: heap-based memory	MEMORY-LEVEL
CodingTagWhat: integer operations	Application-code
CodingTagWhat: kernel memory	MEMORY-LEVEL
CodingTagWhat: kernel stack memory	MEMORY-LEVEL
CodingTagWhat: lock file	Application-data file
CodingTagWhat: loop counting buffer size	Application-code
CodingTagWhat: memory copy	Application-code
CodingTagWhat: memory reallocation	Application-code
CodingTagWhat: metadata	-
CodingTagWhat: object	-
CodingTagWhat: object methods in ORM	-
CodingTagWhat: operating system command	Application-code
CodingTagWhat: port interface management part of the operating system	DESIGN-LEVEL
CodingTagWhat: print output	Application-code
CodingTagWhat: private information	-
CodingTagWhat: remotely execute code	-
CodingTagWhat: run source code	Application-code
CodingTagWhat: sensitive information	-
CodingTagWhat: software related files	-
CodingTagWhat: system reboot	SYSTEM REBOOT

CodingTagWhat: tmp file	Application-DATA FILE
CodingTagWhat: uninitialized memory	Application-code MEMORY
CodingTagWhat: write event log	Application-code

Memo#2: Open Codes and Initial Concepts for Entry Points

CodingTagWhere: APDU command response	Network-related protocol
CodingTagWhere: Account information file	System-level file
CodingTagWhere: Administrative settings	
CodingTagWhere: Administrative user interface	
CodingTagWhere: Application Configuration	Application-level file
CodingTagWhere: Application Configuration (design-level)	
CodingTagWhere: CSS	Application-level code
CodingTagWhere: Chats	
CodingTagWhere: Command line arguments	Input-data
CodingTagWhere: Create Repository	
CodingTagWhere: DLL File(s)	Application-level code
CodingTagWhere: Database	Application-level data resource
CodingTagWhere: Datasource Settings	Application-level code
CodingTagWhere: Decompress collection file	?
CodingTagWhere: Deserialization	Application-level code
CodingTagWhere: Document File Upload (design-level)	Application-level user inteface
CodingTagWhere: EDS File	Input-data file
CodingTagWhere: Editing of system data	Application-level code
CodingTagWhere: Files in post request	Input-data file
CodingTagWhere: Filesystem Handling	Application-level code file manipulation
CodingTagWhere: Firmware update	
CodingTagWhere: HTTP Headers	Application-level code handle requests
CodingTagWhere: HTTP POST	Application-level code handle requests
CodingTagWhere: HTTP POST REQUEST	Application-level code handle requests
CodingTagWhere: HTTP Redirect	Application-level code handle requests
CodingTagWhere: HTTP Request	Application-level code handle requests
CodingTagWhere: IPsec packet	Network-level packets
CodingTagWhere: IPv6 packets	Network-level packets
CodingTagWhere: Image file upload	Application-level code file manipulation
CodingTagWhere: Input/Output	Application-level code handle input data

CodingTagWhere: Insecure direct object reference	?
CodingTagWhere: Install	
CodingTagWhere: Installer component (design-level)	
CodingTagWhere: Login	
CodingTagWhere: Markdown Editor	
CodingTagWhere: Network socket	Network-level sockets
CodingTagWhere: No entry point	
CodingTagWhere: Not Specified	
CodingTagWhere: ORM Query Generator	–
CodingTagWhere: Plugin Administration Page (design-level)	
CodingTagWhere: Port Management Interface System	
CodingTagWhere: Print from file (design-level)	
CodingTagWhere: REST API	Application-level code handle requests
CodingTagWhere: Render document	?
CodingTagWhere: SMB file transfer	Network-related protocol
CodingTagWhere: SQL command	?
CodingTagWhere: System call arguments/driver objects	Input data
CodingTagWhere: Ticket Form	
CodingTagWhere: Token Processing System	
CodingTagWhere: URL	
CodingTagWhere: Update	
CodingTagWhere: User Input	
CodingTagWhere: User console	Application-level User interface console
CodingTagWhere: User console (design-level)	Application-level User interface console
CodingTagWhere: Webconsole admin GUI	Application-level User interface console
CodingTagWhere: access to the system that software installed on	–
CodingTagWhere: application web console	
CodingTagWhere: application web console (design-level)	
CodingTagWhere: device related arguments	
CodingTagWhere: file upload	Application-level code file manipulation
CodingTagWhere: firmware message handlers	Application-level code
CodingTagWhere: http get parameter	Application-level code handle requests

CodingTagWhere: input textbox	Application-level UI
CodingTagWhere: load dll	Application-level code file manipulation
CodingTagWhere: local access	Access-level local access
CodingTagWhere: network request	System-level request ssh
CodingTagWhere: obtain the ability to execute high-privileged code	
CodingTagWhere: request to system service	System-level request network
CodingTagWhere: system call	?

Memo#3: Open Codes and Initial Concepts for Mechanisms

CodingTagHow: Alter application files	-
CodingTagHow: Arguments not being validated.	Application-level Input validation
CodingTagHow: Bad request	-
CodingTagHow: Configuring database using unescaped shell arguments	Application-level Input validation
CodingTagHow: Cross-site Scripting (XSS)	-
CodingTagHow: Decode credentials	
CodingTagHow: File deletion based on user input	Application-level Input validation
CodingTagHow: Filename	-
CodingTagHow: HTTP Request Smuggling	-
CodingTagHow: Hard-coded Credentials	Improper sensitive information protection
CodingTagHow: Improper Configuration	Application-level
CodingTagHow: Improper Screen Resizing	
CodingTagHow: Improper Server Management Configuration	System-level
CodingTagHow: Improper check	Application-level
CodingTagHow: Improper permissions	Application-level
CodingTagHow: Inadequate encryption	Improper sensitive information protection
CodingTagHow: Injecting crafted json	-
CodingTagHow: Intercept HTTP request	-
CodingTagHow: Invoke functions via deserialization	
CodingTagHow: Lack of input validation/sanitization	Application-level Input validation
CodingTagHow: Lack of password validation	Application-level Input validation
CodingTagHow: Low memory	System-level
CodingTagHow: Malformed file	Application-level Input validation
CodingTagHow: Man-in-the-Middle	
CodingTagHow: Manipulating Transfer-Encoding and Content-Length in http headers	
CodingTagHow: Memory allocation with incorrect size	
CodingTagHow: Missing http response security headers	

CodingTagHow: Modification of account information file	
CodingTagHow: Modify file extension	
CodingTagHow: Not Specified	
CodingTagHow: Open file in high privilege mode	
CodingTagHow: Out of bounds memory read	
CodingTagHow: Plaintext password storage	Improper sensitive information protection
CodingTagHow: Race Condition	
CodingTagHow: Repeated requests	Network–level
CodingTagHow: Request service without user ID	System–level
CodingTagHow: Shell Command	–
CodingTagHow: Shell Command via HTTP request	–
CodingTagHow: System functions	–
CodingTagHow: Type confusion	Application–level improper type casting
CodingTagHow: Unauthenticated access	Improper sensitive information protection
CodingTagHow: Uncontrolled recursion	–
CodingTagHow: Unencrypted credentials	Improper sensitive information protection
CodingTagHow: Use file from unsecured directory	Application–level
CodingTagHow: Use of HTTP instead of HTTPS	Application–level unsafe technologies
CodingTagHow: Use third part library	Application–level
CodingTagHow: Using CSRF vulnerability	–
CodingTagHow: Using CSS filter	Application–level unsafe technologies
CodingTagHow: Using symlink	Application–level unsafe technologies
CodingTagHow: accessing buffer in loop without checking the buffer size	Application–level improper check
CodingTagHow: accessing file	–
CodingTagHow: calling system calls with specific parameter	Application–level unsafe technologies
CodingTagHow: continuously sending packet	Network–level
CodingTagHow: do not checking file type	Application–level Input validation
CodingTagHow: does not check input file size	Application–level Input validation
CodingTagHow: gain administrative acess	Sysm–level application–level improper permission
CodingTagHow: have special account	
CodingTagHow: improper input validation	
CodingTagHow: incorrect android activity launch in tasks	Application–level insecure programming practices

CodingTagHow: incorrect checking of boundary	Application-level improper check
CodingTagHow: incorrect type decleration	
CodingTagHow: inject arbitrary code	–
CodingTagHow: injecting malicious command as son parameter	–
CodingTagHow: insert crafted YAML input	Application-level Input validation
CodingTagHow: insert crafted data	–
CodingTagHow: lack of proper locking when performing operations on an object	?
CodingTagHow: managing XBlock resources	–
CodingTagHow: mismatched type casting	Application-level insecure programming practices
CodingTagHow: run executables based on accessible configuration file	
CodingTagHow: running php daemon as root	application-level improper permission
CodingTagHow: sending multiple request together or in a short time	
CodingTagHow: sending repeatedly malformed packets	Network-level
CodingTagHow: serializing android parcel	
CodingTagHow: setting improper permissions for file access	application-level improper permission
CodingTagHow: supply crafted smartcards	–
CodingTagHow: upload crafted file name	–
CodingTagHow: use encryption package	Application-level insecure programming practices
CodingTagHow: web service runs under the root user	System-level improper permission