Attack Surface Categorization

Memo#1: What are the targets?

Coding TagWhat: Crystographic Objects Coding TagWhat: Crystographic Objects Coding TagWhat: Execute arbitrary OS commands Coding TagWhat: Gadgets class Coding TagWhat: Memory Coding TagWhat: Memory Coding TagWhat: Memory Coding TagWhat: Not Specified Coding TagWhat: Not Specified Coding TagWhat: Not Specified Coding TagWhat: Not Specified Coding TagWhat: Parameter tampering Coding TagWhat: Routing Engine Coding TagWhat: Sol. Command Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System calls Coding TagWhat: Charles of the Coding TagWhat: Coding TagWhat: Coding TagWhat: Coding TagWhat: System calls Coding TagWhat: System calls Coding TagWhat: Charles of the Coding TagWhat: Coding TagWhat: System calls Coding TagWhat: Coding TagWhat	CodingTagV	hat: Configuration
Codino TaoWhat: Execute arbitrary OS commands Codino TaoWhat: Execute arbitrary OS commands Codino TaoWhat: Gadoets Codino TaoWhat: Gadoets class Codino TaoWhat: Gadoets class Codino TaoWhat: Memory Codino TaoWhat: Mot Specified Codino TaoWhat: Not Specified Codino TaoWhat: Open web shell Codino TaoWhat: Popen web shell Codino TaoWhat: Reset settinos Codino TaoWhat: Reset settinos Codino TaoWhat: Routino Engine Codino TaoWhat: System availability Codino TaoWhat: System availability Codino TaoWhat: System calls Codino TaoWhat: System calls Codino TaoWhat: System calls Codino TaoWhat: System calls Codino TaoWhat: Alboek data Codino TaoWhat: Alboek data Codino TaoWhat: android activity Codino TaoWhat: argument type casting Codino TaoWhat: check boundary Codino TaoWhat: deserializing class Codino TaoWhat: derect of the codino TaoWhat: configuration file of executable files Codino TaoWhat: deserializing class Codino TaoWhat: deserializing class Codino TaoWhat: deserializing class Codino TaoWhat: derect of the codino TaoWhat: configuration buffer size Codino TaoWhat: loop counting buffer size Codino TaoWhat: loop counting buffer size Codino TaoWhat: object methods in ORM Codino TaoWhat: port interface management part of the operating system Codino TaoWhat: port interface management part of the operating system Codino TaoWhat: port interface management part of the operating system Codino TaoWhat: port interface management part of the operating system Codino TaoWhat: port interface management part of the operating system Codino TaoWhat: port interface management part of the operating system	CodingTagV	/hat: Counter in critical sections
Coding TagWhat: Execute arbitrary OS commands Coding TagWhat: Files Coding TagWhat: Gadgets Coding TagWhat: Gadgets Coding TagWhat: Gadgets class Coding TagWhat: HTML/Web Script Coding TagWhat: Memory (Socket Buffer) Coding TagWhat: Memory (Socket Buffer) Coding TagWhat: Not Specified Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Jagd admin user Coding TagWhat: Jagd admin user Coding TagWhat: Jagd admin user Coding TagWhat: configuration file of executable files Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: better methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	/hat: Credentials
CodinoTagWhat: Gadgets CodinoTagWhat: Gadgets CodinoTagWhat: Gadgets class CodinoTagWhat: Memory CodinoTagWhat: Memory CodinoTagWhat: Memory CodinoTagWhat: Memory CodinoTagWhat: Node Catalog CodinoTagWhat: Node Catalog CodinoTagWhat: Nose Catalog CodinoTagWhat: Open web shell CodinoTagWhat: Open web shell CodinoTagWhat: Specified CodinoTagWhat: Reset settings CodinoTagWhat: Specified CodinoTagWhat: Unmarshalling data to objects CodinoTagWhat: Unmarshalling data to objects CodinoTagWhat: Add admin user CodinoTagWhat: Add admin user CodinoTagWhat: Add admin user CodinoTagWhat: check boundary CodinoTagWhat: check boundary CodinoTagWhat: check boundary CodinoTagWhat: check boundary CodinoTagWhat: deserializing class CodinoTagWhat: deserializing class CodinoTagWhat: deserializing polymorphic class CodinoTagWhat: deserializing polymorphic class CodinoTagWhat: deserializing polymorphic class CodinoTagWhat: kernel stack memory CodinoTagWhat: kernel stack memory CodinoTagWhat: kernel stack memory CodinoTagWhat: hernel stack memory CodinoTagWhat: hernel stack memory CodinoTagWhat: hernel stack memory CodinoTagWhat: botiect CodinoTagWhat: port interface management part of the operating system CodinoTagWhat: port interface management part of the operating system CodinoTagWhat: port interface management part of the operating system CodinoTagWhat: port interface management part of the operating system CodinoTagWhat: port interface management part of the operating system CodinoTagWhat: specified CodinoTagWhat:	CodingTagV	/hat: Cryptographic Objects
CodinaTagWhat: HTML/Web Script CodinaTagWhat: HTML/Web Script CodinaTagWhat: Memory CodinaTagWhat: Memory CodinaTagWhat: Memory CodinaTagWhat: Node Catalog CodinaTagWhat: Not Specified CodinaTagWhat: Dose web shell CodinaTagWhat: Parameter tampering CodinaTagWhat: Parameter tampering CodinaTagWhat: Reset settings CodinaTagWhat: Sol. command CodinaTagWhat: Sol. command CodinaTagWhat: System availability CodinaTagWhat: System availability CodinaTagWhat: System calls CodinaTagWhat: User data CodinaTagWhat: User data CodinaTagWhat: Add admin user CodinaTagWhat: add admin user CodinaTagWhat: add admin user CodinaTagWhat: check boundary CodinaTagWhat: check boundary CodinaTagWhat: check boundary CodinaTagWhat: deserializing class CodinaTagWhat: deserializing polymorphic class CodinaTagWhat: deserializing polymorphic class CodinaTagWhat: kernel stack memory CodinaTagWhat: loop counting buffer size CodinaTagWhat: bothet methods in ORM CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: port interface management part of the operating system CodinaTagWhat: specific polymorphic CodinaTagWhat: specific poly	CodingTagV	/hat: Execute arbitrary OS commands
Coding TagWhat: HTML/Web Script Coding TagWhat: Memory Coding TagWhat: Memory Coding TagWhat: Mode Catalog Coding TagWhat: Not Specified Coding TagWhat: Reset settings Coding TagWhat: Reset settings Coding TagWhat: Reset settings Coding TagWhat: Reset settings Coding TagWhat: Spoof Coding TagWhat: Spoof Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: Juser data Coding TagWhat: and cod activity Coding TagWhat: and cod activity Coding TagWhat: and cod activity Coding TagWhat: configuration file of executable files Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing class Coding TagWhat: deserializing class Coding TagWhat: kernel memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock counting buffer size Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: object methods in OR		
Coding TagWhat: Memory Coding TagWhat: Memory Coding TagWhat: Memory Coding TagWhat: Note Catalog Coding TagWhat: Note Specified Coding TagWhat: Note Specified Coding TagWhat: Note Specified Coding TagWhat: Open web shell Coding TagWhat: Roset settings Coding TagWhat: Roset settings Coding TagWhat: Specified Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: Juser data Coding TagWhat: And admin user Coding TagWhat: configuration file of executable files Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: look file Coding TagWhat: look file Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: object	CodingTagV	/hat: Gadgets
Coding TagWhat: Memory (Socket Buffer) Coding TagWhat: Note Catalog Coding TagWhat: Note Catalog Coding TagWhat: Note Specified Coding TagWhat: Note Specified Coding TagWhat: Open web shell Coding TagWhat: Copen web shell Coding TagWhat: Reset settings Coding TagWhat: Solo command Coding TagWhat: Solo command Coding TagWhat: Solo command Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Jad admin user Coding TagWhat: Jad admin user Coding TagWhat: and catwity Coding TagWhat: and catwity Coding TagWhat: continguration file of executable files Coding TagWhat: critical directory Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	/hat: Gadgets class
Coding TagWhat: Memory (Socket Buffer) Coding TagWhat: Node Catalog Coding TagWhat: Node Catalog Coding TagWhat: Open web shell Coding TagWhat: Parameter tampering Coding TagWhat: Reset settings Coding TagWhat: Socket Buffer Coding TagWhat: Socket Buffer Coding TagWhat: Socket Buffer Coding TagWhat: Socket Buffer Coding TagWhat: System calls Coding TagWhat: System calls Coding TagWhat: System calls Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Add admin user Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: deserializing class Coding TagWhat: deserializing class Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel stack memory Coding TagWhat: kernel stack memory Coding TagWhat: hernel stack memory Coding TagWhat: hernel stack memory Coding TagWhat: netadata Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: sensitive information	CodingTagV	/hat: HTML/Web Script
Coding TagWhat: Node Catalog Coding TagWhat: Not Specified Coding TagWhat: Does web shell Coding TagWhat: Parameter tampering Coding TagWhat: Reset settings Coding TagWhat: Reset settings Coding TagWhat: SoL command Coding TagWhat: SoL command Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: And cod data Coding TagWhat: Check boundary Coding TagWhat: Check boundary Coding TagWhat: Check boundary Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: loop counting buffer size Coding TagWhat: loop counting buffer size Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: sensitive information	CodingTagV	<u> 'hat: Memory</u>
Coding TagWhat: Not Specified Coding TagWhat: Open web shell Coding TagWhat: Reset settings Coding TagWhat: Routing Engine Coding TagWhat: Soo command Coding TagWhat: Soo command Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Unser data Coding TagWhat: User data Coding TagWhat: Albeck data Coding TagWhat: Albeck data Coding TagWhat: and roid activity Coding TagWhat: aroument type casting Coding TagWhat: configuration file of executable files Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing class Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing class Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: look file Coding TagWhat: look file Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Co	CodingTagV	(hat: Memory (Socket Buffer)
Coding TagWhat: Open web shell Coding TagWhat: Parameter tampering Coding TagWhat: Reset settings Coding TagWhat: Routing Engine Coding TagWhat: Spoof Coding TagWhat: Spoof Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System calls Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: Jag Coding TagWhat: User data Coding TagWhat: Jag Coding TagWhat: Allog Coding TagWhat: Allog Coding TagWhat: Allog Coding Coding TagWhat: Allog Coding TagWhat: Allog Coding Coding TagWhat: Allog Coding TagWhat: Coding Co	CodingTagV	hat: Node Catalog
Coding TagWhat: Reset settings Coding TagWhat: Routing Engine Coding TagWhat: Spuce mand Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System calls Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Add admin user Coding TagWhat: Add admin user Coding TagWhat: and rold activity Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: critical directory Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	hat: Not Specified
CodingTagWhat: Routing Engine CodingTagWhat: Spoof CodingTagWhat: System availability CodingTagWhat: System availability CodingTagWhat: System calls CodingTagWhat: Unmarshalling data to objects CodingTagWhat: Jungarshalling data to objects CodingTagWhat: Journal of the CodingTagWhat: Add admin user CodingTagWhat: android activity CodingTagWhat: check boundary CodingTagWhat: check boundary CodingTagWhat: critical directory CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: deserializing polymorphic class CodingTagWhat: kernel stack memory CodingTagWhat: kernel stack memory CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: port interface management part of the operating system CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: sensitive information	CodingTagV	<u>hat: Open web shell</u>
Coding TagWhat: Spot of coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System availability Coding TagWhat: System calls Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: Add admin user Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: file system Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: loop counting buffer size Coding TagWhat: loop counting buffer size Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: private information Coding TagWhat: run source code Coding TagWhat: sensitive information	CodingTagV	<u> hat: Parameter tampering</u>
CodingTagWhat: Spoof CodingTagWhat: System availability CodingTagWhat: System availability CodingTagWhat: System availability CodingTagWhat: Unmarshalling data to objects CodingTagWhat: Unmarshalling data to objects CodingTagWhat: User data CodingTagWhat: User data CodingTagWhat: add admin user CodingTagWhat: add admin user CodingTagWhat: argument type casting CodingTagWhat: check boundary CodingTagWhat: configuration file of executable files CodingTagWhat: configuration file of executable files CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: file system CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: object methods in ORM CodingTagWhat: oper tinterface management part of the operating system CodingTagWhat: private information CodingTagWhat: private information CodingTagWhat: sensitive information	CodingTagV	that: Reset settings
CodingTagWhat: System availability CodingTagWhat: System calls CodingTagWhat: Unmarshalling data to objects CodingTagWhat: Unser data CodingTagWhat: User data CodingTagWhat: Albox data CodingTagWhat: Albox data CodingTagWhat: and roid activity CodingTagWhat: argument type casting CodingTagWhat: configuration file of executable files CodingTagWhat: configuration file of executable files CodingTagWhat: deserializing class CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: file system CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: look file CodingTagWhat: look file CodingTagWhat: not conting buffer size CodingTagWhat: not conting buffer size CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: private information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: software related files	CodingTagV	hat: Routing Engine
Coding TagWhat: System availability Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: User data Coding TagWhat: Add admin user Coding TagWhat: add admin user Coding TagWhat: and roid activity Coding TagWhat: and roid activity Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: critical directory Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: hope counting buffer size Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	/hat: SOL command
Coding TagWhat: Unmarshalling data to objects Coding TagWhat: Unmarshalling data to objects Coding TagWhat: User data Coding TagWhat: Add admin user Coding TagWhat: and roid activity Coding TagWhat: and roid activity Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: critical directory Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: file system Coding TagWhat: here I stack memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: here I stack memory Coding TagWhat: lock file Coding TagWhat: object methods in ORM Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: sensitive information	CodingTagV	hat: Spoof
CodingTagWhat: Unmarshalling data to objects CodingTagWhat: User data CodingTagWhat: User data CodingTagWhat: Add admin user CodingTagWhat: add admin user CodingTagWhat: add admin user CodingTagWhat: add activity CodingTagWhat: check boundary CodingTagWhat: check boundary CodingTagWhat: critical directory CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: deserializing polymorphic class CodingTagWhat: file system CodingTagWhat: kernel stack memory CodingTagWhat: kernel stack memory CodingTagWhat: loop counting buffer size CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: run source code CodingTagWhat: sensitive information	CodingTagV	hat: System availability
Coding TagWhat: User data Coding TagWhat: ABlock data Coding TagWhat: add admin user Coding TagWhat: add admin user Coding TagWhat: argument type casting Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: check boundary Coding TagWhat: deserializing class Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: oper and the command Coding TagWhat: object methods in ORM Coding TagWhat: object methods in ORM Coding TagWhat: oper ting system command Coding TagWhat: private information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	hat: System calls
CodingTagWhat: add admin user CodingTagWhat: add admin user CodingTagWhat: add admin user CodingTagWhat: add admin user CodingTagWhat: argument type casting CodingTagWhat: check boundary CodingTagWhat: configuration file of executable files CodingTagWhat: critical directory CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: file system CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: lock file CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTa	CodingTagV	hat: Unmarshalling data to objects
Coding TagWhat: and admin user, Coding TagWhat: and roid activity Coding TagWhat: argument type casting Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: configuration file of executable files Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: file system Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: kernel stack memory Coding TagWhat: look file Coding TagWhat: look file Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: oper tinterface management part of the operating system Coding TagWhat: private information Coding TagWhat: un source code Coding TagWhat: sensitive information	CodingTagV	That: User data
Coding TagWhat: android activity Coding TagWhat: check boundary Coding TagWhat: deserializing class Coding TagWhat: deserializing polymorphic class Coding TagWhat: deserializing polymorphic class Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: look file Coding TagWhat: loop counting buffer size Coding TagWhat: not pounting buffer size Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: run source code Coding TagWhat: sensitive information	CodingTagV	hat: XBlock data
CodingTagWhat: check boundary CodingTagWhat: deserializing polymorphic class CodingTagWhat: deserializing polymorphic class CodingTagWhat: hersel memory CodingTagWhat: kernel stack memory CodingTagWhat: loop counting buffer size CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: object methods in ORM CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information	CodingTagV	<u>(hat: add admin user</u>
Coding TagWhat: check boundary Coding TagWhat: configuration file of executable files Coding TagWhat: descrializing class Coding TagWhat: descrializing polymorphic class Coding TagWhat: file system Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: kernel stack memory Coding TagWhat: loop counting buffer size Coding TagWhat: hole file Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: object information Coding TagWhat: sensitive information	CodingTagV	<u>/hat: android activity</u>
Coding TagWhat: configuration file of executable files Coding TagWhat: descrializing class Coding TagWhat: descrializing polymorphic class Coding TagWhat: descrializing polymorphic class Coding TagWhat: file system Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: lock file Coding TagWhat: lock file Coding TagWhat: loop counting buffer size Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: sort interface management part of the operating system Coding TagWhat: sprivate information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information Coding TagWhat: sensitive information	CodingTagV	hat: argument type casting
CodingTagWhat: critical directory CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: file system CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: look file CodingTagWhat: loop counting buffer size CodingTagWhat: opercunting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: rivivate information CodingTagWhat: run source code CodingTagWhat: sensitive information	CodingTagV	/hat: check boundary
CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: deserializing polymorphic class CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: private information CodingTagWhat: sensitive information	CodingTagV	hat: configuration file of executable files
CodingTagWhat: deserializing class CodingTagWhat: deserializing polymorphic class CodingTagWhat: deserializing polymorphic class CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: loop counting buffer size CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: private information CodingTagWhat: sensitive information	CodingTagV	/hat: critical directory
Coding TagWhat: deserializing polymorphic class Coding TagWhat: file system Coding TagWhat: kernel memory Coding TagWhat: kernel stack memory Coding TagWhat: look file Coding TagWhat: look file Coding TagWhat: loop counting buffer size Coding TagWhat: object Coding TagWhat: object Coding TagWhat: object methods in ORM Coding TagWhat: port interface management part of the operating system Coding TagWhat: private information Coding TagWhat: sensitive information Coding TagWhat: software related files		
CodingTagWhat: kernel memory CodingTagWhat: kernel stack memory CodingTagWhat: kernel stack memory CodingTagWhat: look file CodingTagWhat: loop counting buffer size CodingTagWhat: netadata CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information		
CodingTagWhat: kernel memory CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: lock file CodingTagWhat: metadata CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: kernel stack memory CodingTagWhat: look file CodingTagWhat: loop counting buffer size CodingTagWhat: metadata CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: operating system command CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information		
CodingTagWhat: look file CodingTagWhat: loop counting buffer size CodingTagWhat: metadata CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: sprivate information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: loop counting buffer size CodingTagWhat: metadata CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: private information CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information		-
CodingTagWhat: metadata CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information		
CodingTagWhat: object CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information		
CodingTagWhat: object methods in ORM CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: sensitive information		
CodingTagWhat: operating system command CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: port interface management part of the operating system CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: sensitive information		
CodingTagWhat: private information CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: run source code CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: sensitive information CodingTagWhat: software related files		
CodingTagWhat: software related files		

Targets are software components or parts of software applications that attackers try to access.

- 1. Operating system commands (system calls)
- 2. Software application files: lock files, tmp files,
- 3. System files: node catalog in distributed systems
- 4. HTML/Webscripts
- Memory allocation/deallocation/tampering/access: socket buffer, kernel memory, kernel stack memory, loops counting buffer size, uninitialized memory, check boundary
- Marshalling/unmarshalling data objects to/from json: deserializing class, deserializing polymorphic class
- 7. Android activity
- 8. Type casting parts
- 9. Executable code
- 10. Database
- 11. Software configuration parts
- 12. Special Objects or Classes: Cryptographic objects, Gadget Classes
- 13. Sensitive/private information: Credentials, userdata, metadata

Memo#2: Input data types:

Tiff file	CVE-2020-6067	Out-of-bounds Write
XML	CVE-2020-6238	CWE-20Improper Input Validation
BLOB A binary large object (blob) is concentrated binary data that's compressed into an individual file inside a database. The large size of the file means they need special storage treatment. Blobs are binary, which means they are usually images, audio or other media.	CVE-2020-7248	Out-of-bounds Write
YAML It's basically a human-readable structured data format. It is less complex and ungainly than XML or JSON, but provides similar capabilities. It essentially allows you to provide powerful configuration settings, without having to learn a more complex code type like CSS, JavaScript, and PHP.	CVE-2020-1947	CWE-502-Deserialization of Untrusted Data
Android Parcel Android Parcel would be that of a message container for lightweight, high-performance Inter- process communication (IPC)	CVE-2020-0017	CWE-200- Exposure of Sensitive Information to an Unauthorized Actor
JSON	CVE-2019-10749 CVE-2019-10748	CWE-89- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
	CVE-2018-7489	CWE-184- Incomplete List of Disallowed Inputs
	CVE-2018-18836	CWE-74- Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
	CVE-2017-18349	CWE20-Improper Input Validation
	CVE-2017-17485	CWE-502- Deserialization of Untrusted Data
	CVE-2014-5017	CWE-89- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
	CVE-2014-3994	CWE-79- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
IPv4 packet	CVE-2020-1638	CWE20-Improper Input Validation

Memo#3: Where are the entry points?

CodingTagWhere: Account information file	
CodingTagWhere: Administrative settings	
CodingTagWhere: Administrative user interface	
CodingTagWhere: Application Configuration	
CodingTagWhere: Application Configuration (design-level)	
CodingTagWhere: CSS	
CodingTagWhere: Chats	
CodingTagWhere: Command line arguments	
CodingTagWhere: DLL File(s)	
CodingTagWhere: Database	
CodingTagWhere: Datasource Settings	
CodingTagWhere: Decompress collection file	
CodingTagWhere: Deserialization	
CodingTagWhere: Document File Upload (design-level)	
CodingTagWhere: EDS File	
CodingTagWhere: Editing of system data	
CodingTagWhere: Files in post request	
CodingTagWhere: Filesystem Handling	
CodingTagWhere: Firmware update	
CodingTagWhere: HTTP Headers	
CodingTagWhere: HTTP POST	
CodingTagWhere: HTTP POST REOUEST	
CodingTagWhere: HTTP Redirect	
CodingTagWhere: HTTP Request	
CodingTagWhere: IPv6 packets	
CodingTagWhere: Image file upload	
CodingTagWhere: Input/Output	
CodingTagWhere: Insecure direct object reference	
CodingTagWhere: Install	
CodingTagWhere: Installer component (design-level)	
CodingTagWhere: Login	
CodingTagWhere: Markdown Editor	
CodingTagWhere: Network socket	
CodingTagWhere: No entry point	
CodingTagWhere: Not Specified	
CodingTagWhere: Plugin Administration Page (design-level)	
CodingTagWhere: Port Management Interface System	
CodingTagWhere: Print from file (design-level)	
CodingTagWhere: REST API	
CodingTagWhere: Render document	
CodingTagWhere: SMB file transfer	
CodingTagWhere: System call arguments	
CodingTagWhere: Ticket Form	
CodingTagWhere: Token Processing System	
CodingTagWhere: URL	
CodingTagWhere: Update	
CodingTagWhere: User Input	
CodingTagWhere: User console	
CodingTagWhere: User console (design-level)	

Entry points are parts of software system that attacker can leverage to access targets.

- System files: account information file (etc/passwd),
- 2. dll files, eds files
- 3. Command line arguments
- 4. Web requests: http post request, http get request, files in post requests
- 5. Packets: IPv6 packets
- 6. Network sockets
- 7. REST APIs
- 8. Device related arguments
- 9. Service requests: such as inter procedural communication

Design-level (system sub-modules):

- 1. Application Configuration
- 2. File system handling
- 3. Installer components
- 4. Update component
- 5. Editor
- 6. Chat
- 7. User Console
- 8. Web console
- 9. Plugin administration
- 10. Port management interface
- 11. File upload
- 12. Access to Local system

Memo#4: How does the attack happen?

CodingTagHow: Use third part library
CodingTagHow: Using CSRF vulnerability
CodingTagHow: Using CSS filter
CodingTagHow: Using symlink
CodingTagHow: accessing buffer in loop without checking the buffer size
CodingTagHow: accessing file
CodingTagHow: calling system calls with specific parameter
CodingTagHow: continuously sending packet
CodingTagHow: do not checking file type
CodingTagHow: does not check input file size
CodingTagHow: dynamic sql query creation with user input
CodingTagHow: gain administrative acess
CodingTagHow: have special account
CodingTagHow: incorrect android activity launch in tasks
CodingTagHow: incorrect checking of boundary
CodingTagHow: inject arbitrary code
CodingTagHow: injecting malicious command as son parameter
CodingTagHow: insert crafted YAML input
CodingTagHow: insert crafted data
CodingTagHow: lack of proper locking when performing operations on an object
CodingTagHow: managing XBlock resources
CodingTagHow: mismatched type casting
Coding TagHow: run executables based on accessible configuration file
CodingTagHow: running php daemon as root
CodingTagHow: sending multiple request together or in a short time
CodingTagHow: setting improper permissions for file access
CodingTagHow: upload crafted file name
CodingTagHow: use encryption package

- 1. Using third party library: encryption package
- 2. Improper permission: for accessing files, running scripts
- 3. Run executables based on accessible configuration files
- 4. Mismatched type casting
- 5. Dynamic SQL query creation
- 6. Do not checking input file: type, size
- 7. Using dangerous technology: CSS filters, symlinks
- 8. Using incorrect (unsafe) technology: http instead of https
- 9. Unauthenticated access to account or services
- 10. Sending multiple requests or packets together in short time