GROUP 2

Given the following CVE descriptions and summaries containing salient information automatically extracted from descriptions, report if each information contained in the summaries is correct or not.

Category	Description
Authentication bypass or Improper Authorization	An exploitation of this issue might allow an attacker to bypass the required authentication. Or the application does not perform properly the authentication check, when an user attempts to access a resource without the necessary permissions.
Cross-Site Scripting or HTML Injection	An exploitation of this issue might allow an attacker to execute arbitrary script code in the web browser of the site visitor and steal his cookie-based authentication credentials.
Denial Of Service (DoS)	An exploitation of this issue might allow an attacker to crash the affected application, denying any further access.
Directory Traversal	An exploitation of this issue might allow an attacker to gain read access to arbitrary file content on the affected system.
Local File Include, Remote File Include and Arbitrary File Upload	An exploitation of this issue might allow an attacker to include arbitrary remote files containing malicious code. The code could then be executed on the affected system with the webserver process privileges.
Information Disclosure and/or Arbitrary File Read	An exploitation of this issue might allow an attacker to get access to arbitrary files on the affected system.
Buffer/Stack/Heap/ Integer Overflow, Format String and Off-by-One	Input data are copied to an insufficiently sized memory buffer. An exploitation of this issue might allow an attacker to execute arbitrary code in the context of the affected application or cause denial of service conditions.
Remote Code Execution	An exploitation of this issue might allow an attacker to execute arbitrary code within the context of the affected application, potentially allowing an unauthorized access or a privilege escalation.
SQL Injection	The vulnerable application does not properly sanitize user supplied input data before using them in a SQL query. An exploitation of this issue might allow an attacker to compromise, access and modify data on the affected system with the database user process privileges.
Unspecified Vulnerability	A successful exploitation of this issue might allow an authenticated attacker to affect confidentiality or integrity or availability or all of them.

CVE DESCRIPTION   #1 (CVE-2015-5174)

Directory traversal vulnerability in path-0 in Apache Tomcat 6_x before 6_0_45, 7_x before 7_0_65, and 8_x before 8_0_27 allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application in a getResource, getResourceAsStream, or getResourcePaths call, as demonstrated by the $CATALINA_BASE/webapps directory.

Name of the software affected by the vulnerability	Apache Tomcat	correct
Versions of the Software affected by the vulnerability	6_x, 7_x, 8_x	correct
Versions before which the software is affected by the vulnerability	6_0_45, 7_0_65, 8_0_27	correct
Vulnerability name	Directory traversal vulnerability	incorrect
Type of Attacker who could exploit the vulnerability	remote authenticated users	correct
Source of the vulnerability		incorrect
Effects of the vulnerability	bypass intended SecurityManager restrictions, list parent directory	correct
Vulnerability Category	Directory Traversal	correct
Time taken to validate the data	2 m	

CVE DESCRIPTION   #2 (CVE-2016-6289)

Integer overflow in the virtual_file_ex function in path-0 in PHP before 5_5_38, 5_6_x before 5_6_24, and 7_x before 7_0_9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

Name of the software affected by the vulnerability	PHP	correct
Versions of the Software affected by the vulnerability	5_6_x, 7_x	correct
Versions before which the software is affected by the vulnerability	5_5_38, 5_6_24, 7_0_9	correct
Vulnerability name	(does not appear in the description)	correct
Type of Attacker who could exploit the vulnerability	Remote attackers	correct
Source of the vulnerability	Crafted extract operation Buffer overflow	incorrect
Effects of the vulnerability	Cause denial of service, have unspecified other impact	correct
Vulnerability Category	Buffer/Stack/Heap/ Integer Overflow, Format String and Off-by-One	correct
Time taken to validate the data	2 m	

CVE DESCRIPTION   #3 (CVE-2016-4072)

The Phar extension in PHP before 5_5_34, 5_6_x before 5_6_20, and 7_x before 7_0_5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in path-0

Name of the software affected by the vulnerability	PHP	correct
Versions of the Software affected by the vulnerability	5_6_x, 7_x	correct
Versions before which the software is affected by the vulnerability	5_5_34, 5_6_20, 7_0_5	correct
Vulnerability name	(does not appear in the description)	correct
Type of Attacker who could exploit the vulnerability	Remote attackers	correct
Source of the vulnerability	Crafted filename	correct
Effects of the vulnerability	execute arbitrary code	correct
Vulnerability Category	Remote Code Execution	correct
Time taken to validate the data	2 m	

CVE DESCRIPTION   #4 (CVE-2016-2108)

The path-0 implementation in OpenSSL before 1_0_1o and 1_0_2 before 1_0_2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

Name of the software affected by the vulnerability	OpenSSL	correct
Versions of the Software affected by the vulnerability	1_0_2	correct
Versions before which the software is affected by the vulnerability	1_0_1o, 1_0_2c	correct
Vulnerability name	(does not appear in the description)	correct
Type of Attacker who could exploit the vulnerability	Remote attackers	correct
Source of the vulnerability	ANY field	incorrect
Effects of the vulnerability	Execute arbitrary code Cause denial of service	correct
Vulnerability Category	Remote Code execution	incorrect
Time taken to validate the data	2 m	

CVE DESCRIPTION   #5 (CVE-2016-7128)

The exif_process_IFD_in_TIFF function in path-0 in PHP before 5_6_25 and 7_x before 7_0_10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

Name of the software affected by the vulnerability	PHP	correct
Versions of the Software affected by the vulnerability	7_x	correct
Versions before which the software is affected by the vulnerability	5_6_25, 7_0_10	correct
Vulnerability name	(does not appear in the description)	correct
Type of Attacker who could exploit the vulnerability	Remote attackers	correct
Source of the vulnerability	Crafted TIFF image	correct
Effects of the vulnerability	Obtain sensitive information	correct
Vulnerability Category	Information Disclosure and/or Arbitrary File Read	correct
Time taken to validate the data	1 m	