

## **GROUP 2**

### **TASK B: VALIDATE INFORMATION CONTAINED IN THE PRE-FILLED FORMS**

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.

<b>Category</b>	<b>Description</b>
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.*

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

## **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.*

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

## **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*

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

## **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.*

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

## **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.*

<b>Name of the software affected by the vulnerability</b>	PHP	correct
<b>Versions of the Software affected by the vulnerability</b>	7_x	correct
<b>Versions before which the software is affected by the vulnerability</b>	5_6_25, 7_0_10	correct
<b>Vulnerability name</b>	(does not appear in the description)	correct
<b>Type of Attacker who could exploit the vulnerability</b>	Remote attackers	correct
<b>Source of the vulnerability</b>	Crafted TIFF image	correct
<b>Effects of the vulnerability</b>	Obtain sensitive information	correct
<b>Vulnerability Category</b>	Information Disclosure and/or Arbitrary File Read	correct
<b>Time taken to validate the data</b>	2m	