GROUP 1

TASK A: EXTRACT USEFUL INFORMATION FROM CVE DESCRIPTIONS

Given the following CVE descriptions, fill the related form with the required information.

EXAMPLE:

CVE DESCRIPTION

The ironic-api service in OpenStack Ironic before 4_2_5 (Liberty) and 5_x before 5_1_2 (Mitaka) allows remote attackers to obtain sensitive information about a registered node by leveraging knowledge of the MAC address of a network card belonging to that node and sending a crafted POST request to the v1/drivers/$DRIVER_NAME/vendor_passthru resource

Name of the software affected by the vulnerability	OpenStack Ironic
Versions of the Software affected by the vulnerability	5_x
Versions before which the software is affected by the vulnerability	5_1_2
Vulnerability name	(in this case the name of the vulnerability does not appear in the description)
Type of Attacker who could exploit the vulnerability	Remote Attackers
Source of the vulnerability	Leveraging knowledge of the address and sending POST request
Effects of the vulnerability	Obtain sensitive information
Vulnerability Category	Information Disclosure and/or Arbitrary File Read
Time taken to extract the required information	1m 42s

Categories of Vulnerabilities

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
Versions of the Software affected by the vulnerability	6_x, 7_x, 8_x
Versions before which the software is affected by the vulnerability	6_0_45, 7_0_65, 8_0_27
Vulnerability name	Directory Trasversal
Type of Attacker who could exploit the vulnerability	Remote authenticated users
Source of the vulnerability	To execute a getResource, getResourceAsSream or getResourcePaths call
Effects of the vulnerability	To bypass intented SecurityManager restrictions and list a parent directory via a/.. in a pathname used by a web application
Vulnerability Category	Directory Trasversal
Time taken to extract the required information	3min 52sec

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
Versions of the Software affected by the vulnerability	5_5_x, 5_6_x, 7_x
Versions before which the software is affected by the vulnerability	5_5_38, 5_6_24, 7_0_9
Vulnerability name	In this case the name of the vulnerability does not appear in the description
Type of Attacker who could exploit the vulnerability	Remote attackers
Source of the vulnerability	Integer overflow in the virtual_file_ex function in path-0
Effects of the vulnerability	To cause a denial of service or possibly unspecified other impact via a crafted extract operation on a zip archive
Vulnerability Category	Integer overflow
Time taken to extract the required information	2min 37sec

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
Versions of the Software affected by the vulnerability	5_5_x, 5_6_x, 7_x
Versions before which the software is affected by the vulnerability	5_5_34, 5_6_20, 7_0_5
Vulnerability name	None
Type of Attacker who could exploit the vulnerability	Remote attackers
Source of the vulnerability	Mishandling of \0 characters by the phar_analyze_path funcition in path-0
Effects of the vulnerability	To execute arbitrary code via a crafted filename
Vulnerability Category	Remote code execution
Time taken to extract the required information	3min 43sec

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
Versions of the Software affected by the vulnerability	1_0_1, 1_0_2
Versions before which the software is affected by the vulnerability	1_0_1o, 1_0_2c
Vulnerability name	None
Type of Attacker who could exploit the vulnerability	Remote attackers
Source of the vulnerability	ANY field in crafted serialized data
Effects of the vulnerability	To execute arbitrary code or cause a denial of service (buffer overflow and memory corruption)
Vulnerability Category	Cross site Scripting or HTML injection
Time taken to extract the required information	3min 57sec

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
Versions of the Software affected by the vulnerability	5_6_x, 7_x
Versions before which the software is affected by the vulnerability	5_6_25, 7_0_10
Vulnerability name	None
Type of Attacker who could exploit the vulnerability	Remote attackers
Source of the vulnerability	Process memory via a crafted TIFF image in the exif_process_IFD_in_TIFF function in path-0
Effects of the vulnerability	To obtain sensitive information
Vulnerability Category	Remote file include and arbitrary file upload
Time taken to extract the required information	5min 38sec