

## **GROUP 2**

### **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*

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

## **Categories of Vulnerabilities**

<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-2016-0777)**

*The resend\_bytes function in path-0 in the client in OpenSSH 5\_x, 6\_x, and 7\_x before 7\_1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.*

<b>Name of the software affected by the vulnerability</b>	OpenSSH
<b>Versions of the Software affected by the vulnerability</b>	5_x, 6_x and 7_x
<b>Versions before which the software is affected by the vulnerability</b>	7_1p2
<b>Vulnerability name</b>	(in this case the name of the vulnerability does not appear in the description)
<b>Type of Attacker who could exploit the vulnerability</b>	Remote server
<b>Source of the vulnerability</b>	Exploiting process memory by requesting transmission of an entire buffer
<b>Effects of the vulnerability</b>	Obtain sensitive information
<b>Vulnerability Category</b>	Information disclosure and/or Arbitrary File Read
<b>Time taken to extract the required information</b>	3 m

## **CVE DESCRIPTION #2 (CVE-2015-6658)**

***Cross-site scripting (XSS) vulnerability in the Autocomplete system in Drupal 6\_x before 6\_37 and 7\_x before 7\_39 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, related to uploading files.***

<b>Name of the software affected by the vulnerability</b>	Drupal
<b>Versions of the Software affected by the vulnerability</b>	6_x, 7_x
<b>Versions before which the software is affected by the vulnerability</b>	Before 6_37, before 7_39
<b>Vulnerability name</b>	Cross-site scripting (XSS)
<b>Type of Attacker who could exploit the vulnerability</b>	Remote attackers
<b>Source of the vulnerability</b>	Leveraging crafted URL, related to uploading files
<b>Effects of the vulnerability</b>	Inject arbitrary web script or HTML
<b>Vulnerability Category</b>	Cross Site Scripting or HTML Injection
<b>Time taken to extract the required information</b>	2 m 30 s

## **CVE DESCRIPTION #3 (CVE-2016-2560)**

***Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4\_0\_x before 4\_0\_10\_15, 4\_4\_x before 4\_4\_15\_5, and 4\_5\_x before 4\_5\_5\_1 allow remote attackers to inject arbitrary web script or HTML via (1) a crafted Host HTTP header, related to path-0 (2) crafted JSON data, related to path-1 (3) a crafted SQL query, related to path-2 (4) the initial parameter to path-3 in the user accounts page; or (5) the it parameter to path-4 in the zoom search page.***

<b>Name of the software affected by the vulnerability</b>	phpMyAdmin
<b>Versions of the Software affected by the vulnerability</b>	4_0, 4_4_x, 4_5_x
<b>Versions before which the software is affected by the vulnerability</b>	Before 4_0_10_15, 4_4_15_5, 4_5_5_1
<b>Vulnerability name</b>	Multiple cross-site scripting (XSS)
<b>Type of Attacker who could exploit the vulnerability</b>	Remote attackers
<b>Source of the vulnerability</b>	Leveraging crafted Host http Header, related to path-0 crafted JSON data, related to path-1 a crafted SQL query, related to path-2 the initial parameter to path-3 in the user accounts page; or the it parameter to path-4 in the zoom search page
<b>Effects of the vulnerability</b>	Inject arbitrary web script or HTML
<b>Vulnerability Category</b>	Cross Site Scripting or HTML Injection
<b>Time taken to extract the required information</b>	3 m

## **CVE DESCRIPTION #4 (CVE-2015-1927)**

*The default configuration of IBM WebSphere Application Server (WAS) 7\_0\_0 before 7\_0\_0\_39, 8\_0\_0 before 8\_0\_0\_11, and 8\_5 before 8\_5\_5\_6 has a false value for the path-0 WebContainer property, which allows remote attackers to obtain privileged access via unspecified vectors.*

<b>Name of the software affected by the vulnerability</b>	IBM WebSpher Application Server (WAS)
<b>Versions of the Software affected by the vulnerability</b>	7_0_0, 8_0_0, 8_5
<b>Versions before which the software is affected by the vulnerability</b>	Before 7_0_0_39, 8_0_0_11, 8_5_5_6
<b>Vulnerability name</b>	(in this case the name of the vulnerability does not appear in the description)
<b>Type of Attacker who could exploit the vulnerability</b>	Remote attackers
<b>Source of the vulnerability</b>	Leveraging a false value for the path-0 WebContainer property, via unspecified vectors
<b>Effects of the vulnerability</b>	Obtain privileged access
<b>Vulnerability Category</b>	Authentication bypass or Improper Authorization
<b>Time taken to extract the required information</b>	2 m

## **CVE DESCRIPTION #5 (CVE-2015-5352)**

*The x11\_open\_helper function in path-0 in ssh in OpenSSH before 6\_9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.*

<b>Name of the software affected by the vulnerability</b>	OpenSSH
<b>Versions of the Software affected by the vulnerability</b>	All versions
<b>Versions before which the software is affected by the vulnerability</b>	Before 6_9
<b>Vulnerability name</b>	(in this case the name of the vulnerability does not appear in the description)
<b>Type of Attacker who could exploit the vulnerability</b>	Remote attackers
<b>Source of the vulnerability</b>	Lacks a check of the refusal deadline for X connections, via a connection outside of the permitted time window
<b>Effects of the vulnerability</b>	To bypass intended access restrictions
<b>Vulnerability Category</b>	Authentication bypass or Improper Authorization
<b>Time taken to extract the required information</b>	3 m