# GROUP 1

## 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.

| 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-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.***

| | | |
|---|---|---|
| **Name of the software affected by the vulnerability** | OpenSSH | correct |
| **Versions of the Software affected by the vulnerability** | 5_x, 6_x, 7_x | correct |
| **Versions before which the software is affected by the vulnerability** | 7_1p2 | correct |
| **Vulnerability name** | (does not appear in the description) | correct |
| **Type of Attacker who could exploit the vulnerability** | Remote servers | incorrect |
| **Source of the vulnerability** | Requesting transmission buffer<br>Reading key | incorrect |
| **Effects of the vulnerability** | Obtain sensitive information | correct |
| **Vulnerability Category** | Information Disclosure and/or Arbitrary File Read | incorrect |
| **Time taken to validate the data** | 3m 20s | |

# 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.***

| | | |
|---|---|---|
| **Name of the software affected by the vulnerability** | Autocomplete Drupal | incorrect |
| **Versions of the Software affected by the vulnerability** | 6_x, 7_x | correct |
| **Versions before which the software is affected by the vulnerability** | 6_37, 7_39 | correct |
| **Vulnerability name** | Cross-site scripting vulnerability | correct |
| **Type of Attacker who could exploit the vulnerability** | Remote attackers | correct |
| **Source of the vulnerability** | Crafted URL | correct |
| **Effects of the vulnerability** | Inject arbitrary web script HTML | correct |
| **Vulnerability Category** | Cross-Site Scripting or HTML Injection | correct |
| **Time taken to validate the data** | 3m | |

# 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.***

| | | |
|---|---|---|
| **Name of the software affected by the vulnerability** | phpMyAdmin | correct |
| **Versions of the Software affected by the vulnerability** | 4_0_x, 4_4_x, 4_5_x | correct |
| **Versions before which the software is affected by the vulnerability** | 4_0_10_15, 4_4_15_5, 4_5_5_1 | correct |
| **Vulnerability name** | Multiple cross-site scripting vulnerabilities | correct |
| **Type of Attacker who could exploit the vulnerability** | Remote attackers | correct |
| **Source of the vulnerability** | Crafted Host HTTP header<br>JSON daa | incorrect |
| **Effects of the vulnerability** | Inject arbitrary web script<br>Crafted SQL-query | incorrect |
| **Vulnerability Category** | Cross-Site Scripting or HTML Injection | incorrect |
| **Time taken to validate the data** | 3m | |

# 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.***

| | | |
|---|---|---|
| **Name of the software affected by the vulnerability** | IBM WebSphere Application Server | correct |
| **Versions of the Software affected by the vulnerability** | 7_0_0, 8_0_0, 8_5 | correct |
| **Versions before which the software is affected by the vulnerability** | 7_0_0_39, 8_0_0_11, 8_5_5_6 | 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** | unspecified vectors | correct |
| **Effects of the vulnerability** | obtain privileged access | correct |
| **Vulnerability Category** | Authentication bypass or Improper Authorization | incorrect |
| **Time taken to validate the data** | 3m | |

# 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.***

| | | |
|---|---|---|
| **Name of the software affected by the vulnerability** | OpenSSH | correct |
| **Versions of the Software affected by the vulnerability** | | correct |
| **Versions before which the software is affected by the vulnerability** | 6_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** | Connection outside | correct |
| **Effects of the vulnerability** | Bypass intended access restrictions | correct |
| **Vulnerability Category** | Authentication bypass or Improper Authorization | correct |
| **Time taken to validate the data** | 2m | |