3.4 Assignment - CVEs

Case 1: MySQL Stored SQL Injection (CVE-2013-0375)

- **Attack Vector (AV): Network (AV:N)**
- This one's a network-based vulnerability, meaning the attacker doesn't need to be anywhere near the MySQL server physically. If they've got network access to the system, they're already halfway there.
- **Attack Complexity (AC): Low (AC:L)**
- This attack is low complexity no configuration or system quirks to figure out. Anyone with basic SQL knowledge and some understanding of how databases work can get this done.
- **Privileges Required (PR): Low (PR:L)**
- The attacker just needs basic user-level permissions—nothing fancy. With even limited access, they can inject malicious queries, mess with data, or pull out information they shouldn't have access to.
- **User Interaction (UI): None (UI:N)**
- This is a no-hands-needed attack. Users don't need to click anything or trigger any actions. The attacker talks directly to the database and makes it happen.
- **Scope (S): Unchanged (S:U)**
- The damage stays isolated to the database server. It's bad, but it doesn't spill over into other systems or services.
- **Confidentiality Impact (C): Low (C:L)**
- The attacker might get their hands on some extra data, but nothing too sensitive or mission-critical.
- **Integrity Impact (I): Low (I:L)**
- Some data can be altered, but nothing that will break the overall system. The database still works, just with a few unwanted edits.
- **Availability Impact (A): None (A:N)**
- The system doesn't crash or go down—everything stays online and operational.

Base Score: 5.4 (Medium)

Case 2: Remote Code Execution in Oracle Outside In Technology (CVE-2016-5558)

- **Attack Vector (AV): Network (AV:N)**
- This attack happens remotely over a network connection. The attacker doesn't need to touch the system—they just need to reach it.
- **Attack Complexity (AC): Low (AC:L)**
- It's a straightforward attack. No special conditions, no complex configurations—just a vulnerable version running and the attacker can take over.
- **Privileges Required (PR): None (PR:N)**
- This is the scary part: the attacker doesn't need any permissions or credentials. They don't even need to be logged in. It's a completely unauthenticated attack.
- **User Interaction (UI): None (UI:N)**
- Users don't need to do anything for this to work. The attacker can trigger it entirely on their own.
- **Scope (S): Unchanged (S:U)**
- The attack is contained to the Oracle component, so it doesn't spread beyond that.
- **Confidentiality Impact (C): High (C:H)**
- A successful exploit gives the attacker access to sensitive data—internal files, confidential reports, or whatever the system processes.
- **Integrity Impact (I): Low (I:L)**
- The attacker can tamper with some data, but the system doesn't lose its overall integrity.
- **Availability Impact (A): Low (A:L)**
- There might be some minor crashes or disruptions, but the system will mostly keep running.

Base Score: 8.6 (High)

Case 3: Web Server Exposing Internal Commands (Hypothetical Scenario)

- **Attack Vector (AV): Network (AV:N)**

- This attack is entirely remote. The attacker just needs to send some crafty HTTP requests to the webserver to get the ball rolling.
- **Attack Complexity (AC): Low (AC:L)**
- It's as easy as it sounds. No special system conditions are required. The attacker just sends well-crafted commands to exploit the vulnerability.
- **Privileges Required (PR): None (PR:N)**
- No login, no permissions, no credentials—nothing. The attacker exploits the vulnerability completely unauthenticated.
- **User Interaction (UI): None (UI:N)**
- The user doesn't need to be involved at all. The attacker operates independently and directly targets the system.
- **Scope (S): Changed (S:C)**
- Here's where it gets dangerous. The attack starts with the web server but doesn't stop there. Once the attacker is in, they can escalate privileges and take control of the entire system and its connected components.
- **Confidentiality Impact (C): High (C:H)**
- The attacker gets access to internal files, credentials, and sensitive system data. If there's critical information stored on the server, it's fair game.
- **Integrity Impact (I): High (I:H)**
- The attacker can completely corrupt, modify, or delete important data, compromising the integrity of the entire system.
- **Availability Impact (A): High (A:H)**
- The attacker can take down the system entirely, causing total disruption or denial of service. Think complete shutdown.

Base Score: 10.0 (Critical)

Summary of CVE Scores

- **CVE-2013-0375:** 5.4 (Medium)
- **CVE-2016-5558:** 8.6 (High)
- **Web Server RCE:** 10.0 (Critical)

Resources

- **CVE-2013-0375:** MySQL Stored SQL Injection
- https://nvd.nist.gov/vuln/detail/CVE-2013-0375
- **CVE-2016-5558:** Oracle Outside In Technology
- https://nvd.nist.gov/vuln/detail/CVE-2016-5558
- **CVE Scoring Calculator:**
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator