SQL CVE Queries and Results

Query 1

SELECT CVE.CVE_ID, IMPACT.IMPACT_LEVEL, CVE.CVSS_SCORE FROM CVE JOIN IMPACT ON CVE.CVSS_SCORE BETWEEN IMPACT.CVSS_MIN AND IMPACT.CVSS_MAX;

Result

CVE_ID	IMPACT_LEVEL	CVSS_SCORE
CVE-2020-2021	Critical	10.0
CVE-2021-38647	Critical	9.8
CVE-2020-3161	Critical	9.8
CVE-2020-17530	Critical	9.8
CVE-2020-10148	Critical	9.8
CVE-2020-3952	Critical	9.8
CVE-2020-4427	Critical	9.8
CVE-2021-1498	Critical	9.8
CVE-2021-21985	Critical	9.8
CVE-2019-2725	Critical	9.8
CVE-2022-27518	Critical	9.8
CVE-2022-40684	Critical	9.8
CVE-2022-42475	Critical	9.8
CVE-2023-23397	Critical	9.8
CVE-2023-28206	Critical	9.8
CVE-2022-4135	Critical	9.6

Query 2

SELECT CVE.VULN_TYPE, COUNT(*) AS TOTAL_COUNT FROM CVE JOIN VULNERABILITY ON CVE.VULN_TYPE = VULNERABILITY.VULN_TYPE GROUP BY CVE.VULN_TYPE ORDER BY TOTAL_COUNT DESC;

Result

VULN_TYPE	TOTAL_COUNT
Remote Code Execution	10
Privilege Escalation	10
Buffer Overflow	8
Authentication Bypass	8
DoS	3
Information Disclosure	3
Injection	3
XSS	3
Misconfiguration	2
Cryptographic	1
CSRF/SSRF	1

Query 3

SELECT CVE.CVE_ID, IMPACT.IMPACT_LEVEL, COUNT(INCIDENT_ID) AS INCIDENT_COUNT FROM CVE JOIN INCIDENT ON CVE.CVE_ID = INCIDENT.CVE_ID JOIN IMPACT ON CVE.CVSS_SCORE BETWEEN IMPACT.CVSS_MIN AND IMPACT.CVSS_MAX WHERE CVE.PATCH_AVAILABLE = TRUE GROUP BY CVE.CVE_ID, IMPACT.IMPACT_LEVEL ORDER BY INCIDENT_COUNT DESC;

Result

CVE_ID	IMPACT_LEVEL	INCIDENT_COUNT
CVE-2020-4006	Critical	3
CVE-2023-28206	Critical	2
CVE-2016-3351	Low	2
CVE-2013-1690	Critical	2
CVE-2021-21017	High	2
CVE-2022-32917	High	2
CVE-2022-27518	Critical	2
CVE-2021-30563	High	1
CVE-2021-21224	High	1
CVE-2021-30665	High	1
CVE-2021-30983	High	1
CVE-2021-34484	High	1
CVE-2021-37976	Medium	1
CVE-2021-38003	High	1
CVE-2021-38647	Critical	1
CVE-2021-38649	High	1

Query 4

SELECT PRODCT.PRODUCT_NAME, COUNT(INCIDENT_ID) AS INCIDENT_COUNT FROM PRODUCT JOIN INCIDENT ON PRODUCT.PRODUCT_NAME = INCIDENT.PRODUCT_NAME GROUP BY PRODUCT.PRODUCT_NAME ORDER BY INCIDENT_COUNT DESC;

Result

PRODUCT_NAME	INCIDENT_COUNT
Windows	7
Chromium V8 Engine	5
FortiOS	4
Apple iOS	4
vCenterServer	3
macOS	2
ADC	2
Azure OMI	2
Chrome	2
PANOS	2
Identity Manager	1
Office	1
Data Risk Manager	1
iOS Mail	1
HyperFlex HX	1
Acrobat	1

Query 5

SELECT PRODUCT.PRODUCT_NAME, PRODUCT.VENDOR_NAME FROM PRODUCT JOIN VENDOR ON PRODUCT.VENDOR_NAME = VENDOR.VENDOR_NAME WHERE PRODUCT.PRODUCT_EOL_YEAR = 'TBD' ORDER BY VENDOR.VENDOR_NAME;

Result

PRODUCT_NAME	VENDOR_NAME
Android OS	Android
Apple iOS	Apple
Safari	Apple
macOS	Apple
iOS Mail	Apple
HyperFlex HX	Cisco
Workspace	Citrix
Gateway	Citrix
ADC	Citrix
Desktop CE	Docker
FortiOS	Fortinet
Chrome	Google
Chromium V8 E...	Google
Data Risk Manager	IBM
Kernel	Linux
Edge	Microsoft
Office	Microsoft

Query 6

SELECT CVE.CVE_ID, VULNERABILITY.VULNERABILITY_TYPE FROM CVE JOIN VULNERABILITY ON CVE.VULN_TYPE = VULNERABILITY.VULN_TYPE WHERE VULNERABILITY.OWASP_10 = TRUE ORDER BY VULN_TYPE;

Result

CVE_ID	VULN_TYPE
CVE-2020-10148	Authentication Bypass
CVE-2020-2021	Authentication Bypass
CVE-2020-4427	Authentication Bypass
CVE-2020-8196	Authentication Bypass
CVE-2022-27518	Authentication Bypass
CVE-2022-40684	Authentication Bypass
CVE-2022-44698	Authentication Bypass
CVE-2023-24880	Authentication Bypass
CVE-2020-0601	Cryptographic
CVE-2021-21973	CSRF/SSRF
CVE-2019-2725	Injection
CVE-2020-4006	Injection
CVE-2021-1498	Injection
CVE-2019-5591	Misconfiguration
CVE-2021-38003	Misconfiguration

Query 7

SELECT CVE.CVE_ID, CVE.CVSS_SCORE, COUNT(INCIDENT.INCIDENT_ID) AS INCIDENT_COUNT FROM CVE JOIN INCIDENT ON CVE.CVE_ID = INCIDENT.CVE_ID GROUP BY CVE.CVE_ID, CVE.CVSS_SCORE HAVING COUNT(INCIDENT.INCIDENT_ID) >= 2 ORDER BY INCIDENT_COUNT DESC;

Result

CVE_ID	CVSS_SCORE	INCIDENT_COUNT
CVE-2020-4006	9.1	3
CVE-2013-1690	9.3	2
CVE-2016-3351	3.1	2
CVE-2020-3580	6.1	2
CVE-2021-21017	8.8	2
CVE-2022-27518	9.8	2
CVE-2022-32917	7.8	2
CVE-2023-28206	9.8	2

Query 8

SELECT CVE.VULN_TYPE, AVG(CVE.CVSS_SCORE) AS AVG_CVSS_SCORE, COUNT(CVE.CVE_ID) AS CVE_COUNT FROM CVE GROUP BY CVE.VULN_TYPE ORDER BY AVG_CVSS_SCORE DESC;

Result

VULN_TYPE	AVG_CVSS_SCORE	CVE_COUNT
Injection	9.56667	3
Remote Code Execution	9.25000	10
Buffer Overflow	8.33750	8
Cryptographic	8.10000	1
Privilege Escalation	7.95000	10
DoS	7.93333	3
Authentication Bypass	7.91250	8
Misconfiguration	7.65000	2
Information Disclosure	6.46667	3
XSS	6.10000	3
CSRF/SSRF	5.30000	1

Query 9

SELECT CVE.VULN_TYPE, VULNERABILITY.VULN_DESCRIPTION, MAX(CVE.CVSS_SCORE) AS MAX_CVSS_SCORE FROM CVE
JOIN VULNERABILITY ON CVE.VULN_TYPE = VULNERABILITY.VULN_TYPE
GROUP BY CVE.VULN_TYPE ORDER BY MAX_CVSS_SCORE DESC;

Result

VULN_TYPE	VULN_DESCRIPTION	MAX_CVSS_SCORE
Authentication Bypass	Allows an attacker to bypass authentication mechanisms, gain unauthorized access, and potentially perform malicious actions.	10.0
Remote Code Execution	Allows an attacker to execute arbitrary code on a target system from a remote location to take control of the system, steal data, or carry out other malicious activities.	9.8
Information Disclosure	Allows an attacker to access sensitive information on a target system from a remote location to steal data, gain access to other systems, or carry out further attacks.	9.8
Buffer Overflow	Occurs when a program tries to store more data in a buffer than it was designed to handle, potentially allowing an attacker to execute arbitrary code.	9.8
Privilege Escalation	Allows an attacker to escalate their privileges within a system or gain access to resources they should not have access to.	9.8
Injection	Allows an attacker to inject malicious code into a system, potentially causing it to execute unintended commands or reveal sensitive information.	9.8
DoS	Occurs when an attacker floods a system with requests, causing it to crash or become unresponsive.	9.3
Misconfiguration	Occurs when a system is configured improperly, potentially allowing an attacker to gain access to sensitive information or perform malicious actions.	8.8
Cryptographic	Occurs when a system's cryptographic algorithms or implementations are flawed, potentially allowing an attacker to bypass encryption or access sensitive data.	8.1
XSS	Allows an attacker to inject malicious code into a website or web application, potentially allowing them to steal sensitive information or take control of the site.	6.1
CSRF/SSRF	Allows an attacker to perform actions on behalf of an authenticated user, potentially leading to unauthorized actions being taken or sensitive information being exposed.	5.3

Query 10

```
SELECT PRODUCT.PRODUCT_NAME, VENDOR.VENDOR_NAME,
COUNT(INCIDENT.INCIDENT_ID) AS INCIDENT_COUNT FROM PRODUCT
JOIN VENDOR ON PRODUCT.VENDOR_NAME = VENDOR.VENDOR_NAME
JOIN INCIDENT ON PRODUCT.PRODUCT_NAME =
INCIDENT.PRODUCT_NAME GROUP BY PRODUCT.PRODUCT_NAME,
VENDOR.VENDOR_NAME HAVING INCIDENT_COUNT >= 3;
```

Result

PRODUCT_NAME	VENDOR_NAME	INCIDENT_COUNT
Windows	Microsoft	7
Chromium V8 Engine	Google	5
FortiOS	Fortinet	4
vCenterServer	VMware	3
Apple iOS	Apple	4