RCE VULNERABILITY CHECKLIST

1- RCE via Dependency Confusion

```
Writeup:-
https://systemweakness.com/rce-via-dependency-confusion-e0ed2a127013
https://chevonphillip.medium.com/rce-due-to-dependency-confusion-5000-bounty-fd1b294d645f
https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
https://hackerone.com/reports/1104693
```

2- rce via file upload

```
Writeup:-
https://book.hacktricks.xyz/pentesting-web/file-upload
https://sidblog.medium.com/file-upload-to-rce-7c04b3b252de
https://hackerone.com/reports/678727
```

3- rce via sql injection

```
https://www.oxeye.io/resources/rce-through-sql-injection-vulnerability-in-hashicorps-vault
https://systemweakness.com/sql-injection-to-remote-command-execution-rce-dd9a75292d1d
```

4- rce via lfi

```
https://github.com/RoqueNight/LFI---RCE-Cheat-Sheet
https://himanshugurjar-10413.medium.com/rce-via-lfi-log-poisoning-3a33632caf4a
https://aditya-chauhan17.medium.com/local-file-inclusion-lfi-to-rce-7594e15870e1
```

5- rce via ssrf

```
https://www.youtube.com/watch?v=Vj6oY6IaJdU
https://infosecwriteups.com/exploiting-server-side-request-forgery-ssrf-vulnerability-faeb7ddf
https://aditya-chauhan17.medium.com/server-side-request-forgery-ssrf-to-rce-c0cb5fc88a94
```

6- rce via xxe

```
https://airman604.medium.com/from-xxe-to-rce-with-php-expect-the-missing-link-a18c265ea4c7
https://www.youtube.com/watch?v=Gz4iPauycKs
https://hackerone.com/reports/227880
```

7- rce via command injection

```
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX%20Injection#command-exec
```

8- rce via Insecure deserialization

```
https://secure-cookie.io/attacks/insecuredeserialization/
https://www.bugbountyhunter.com/hackevents/report?id=867
https://www.bugbountyhunter.com/hackevents/report?id=776
https://portswigger.net/web-security/deserialization/exploiting
```

9- rce via SSTI

```
https://medium.com/r3d-buck3t/rce-with-server-side-template-injection-b9c5959ad31e
https://github.com/epinna/tplmap
https://secure-cookie.io/attacks/ssti/
```