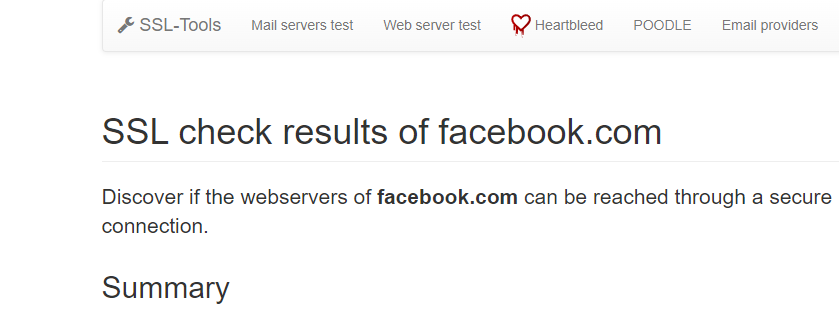
**SSL Tools**



**Introduction**

SSL (Secure Sockets Layer) tools are essential for analyzing and ensuring the security of SSL/TLS certificates on web servers. These tools help identify potential vulnerabilities, misconfigurations, and compliance issues in SSL/TLS implementations, ensuring that web communications are secure and encrypted.





**Scenario**

Imagine you are a security analyst tasked with assessing the SSL/TLS configuration of a company's web servers. Your goal is to identify any weaknesses in their SSL implementation and ensure they are using best practices to protect their users' data.

**Process to Perform**

**Step 1:** Click on this link to access SSL tool <https://ssl-tools.net/> or open any web browser on your PC and type **SSLtools** in the address bar.

**Step 2:** Click on the second link and click on web server test

**Step 3:** Enter **facebook.com** in the search bar

**Step 4:** Capture the Flag

**Question**

Flag 1: What is the encryption key of SHA256?

Answer:84:CF:0D:D6:38:64:A8:2B:4E:6E:F3:3A:B8:9A:3B:41:4C:54:78:CD:66:FB:B9:2F:DB:F5:97:6D:4E:E3:41:9D

Flag Captured

Flag 2: What is the login id of timestamp **Apr 8 00:27:16.416 2024 GMT?**

Answer: DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:

91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB

Flag Captured

Flag 3: What is the certificatePolicy number?

Answer: 2.23.140.1.2.2

Flag Captured

Hints

