CPP Snippets(OWASP Top 10)

1. **Plaintext Password in Source (A02: Cryptographic Failures)**

```cpp
#include <iostream>
using namespace std;

int main() {
    string password = "supersecret123";
    cout << "Password stored: " << password << endl;
    return 0;
}
```

🔴 **Vulnerability:** Sensitive data hardcoded and exposed in plaintext.
✅ **Fix:** Use secure credential storage (environment variables, vaults).

---

2. **System Call without Sanitization (A05: Security Misconfiguration / A03: Injection)**

```cpp
system("ls");
```

🔴 **Vulnerability:** Dangerous use of `system()` – could lead to command injection if input concatenated.
✅ **Fix:** Avoid `system()`; use standard library APIs.

---

3. **Command Injection via User Input (A03: Injection)**

```cpp
string ip;
cin >> ip;
string cmd = "ping " + ip;
system(cmd.c_str());
```

🔴 **Vulnerability:** User-controlled input passed directly to system → Command Injection (`; rm -rf /`).
✅ **Fix:** Validate input (regex for IP), or use safe APIs.

4. Broken Access Control (A01: Broken Access Control)

```
if(user == "guest") {
    cout << "Welcome Guest, but here’s the Admin Panel!" << endl;
}
```

🔴 **Vulnerability:** Incorrect access logic → Guest gets admin access.
✅ **Fix:** Enforce role-based checks properly.

5. Sensitive Data Exposure in Logs (A02: Cryptographic Failures)

```
cout << "Credit Card: " << cardNumber << endl;
```

🔴 **Vulnerability:** Logs full sensitive data (credit card).
✅ **Fix:** Mask or avoid logging sensitive information.

6. Over-Permissive File Permissions (A05: Security Misconfiguration)

```
chmod("file.txt", 0777);
```

🔴 **Vulnerability:** File permissions set to world-readable, writable, executable.
✅ **Fix:** Use least privilege (e.g., `0640`).

📌 Summary Table – C++ Specific Vulnerabilities

#	Vulnerability	OWASP Top 10 (2021)
1	Hardcoded plaintext password	A02: Cryptographic Failures
2	Unsafe system call (`system("ls")`)	A05: Security Misconfiguration / A03: Injection
3	Command Injection via `system(cmd)`	A03: Injection

#	Vulnerability	OWASP Top 10 (2021)
4	Broken access logic → Guest as Admin	A01: Broken Access Control
5	Sensitive data exposure in logs	A02: Cryptographic Failures
6	Over-permissive file permissions (0777)	A05: Security Misconfiguration