# Testing SSL/TLS Configuration with testssl.sh

## Introduction

`testssl.sh` is a command-line tool used to test SSL/TLS configurations of servers and detect vulnerabilities. It supports various ciphers, protocols, and security checks to ensure your SSL setup is secure.

## Installation

To use `testssl.sh`, you need to install it first.

### Download and Extract

wget https://github.com/drwetter/testssl.sh/archive/refs/heads/master.zip

## Running SSL Tests

You can check the SSL/TLS configuration of a server by running:

./testssl.sh https://your\_domain\_name.com

### Check HTTP Headers for Security

./testssl.sh --headers https://your\_domain\_name.com

## Generating Reports

You can generate different formats of reports for analysis.

### Generate JSON Report

./testssl.sh --jsonfile output.json https://your\_domain\_name.com

### Generate CSV Report

./testssl.sh --csvfile output.csv https://your\_domain\_name.com

### Generate HTML Report

./testssl.sh --htmlfile output.html https://your\_domain\_name.com

## Interpreting Results

- \*\*Vulnerabilities\*\*: Check for warnings about weak ciphers, outdated TLS versions, or missing security headers.  
- \*\*Cipher Strength\*\*: Ensure strong ciphers (AES256, TLS 1.2, and TLS 1.3) are used.  
- \*\*Certificate Expiry\*\*: Verify the certificate expiration date.

## Conclusion

Using `testssl.sh` ensures that your SSL/TLS configurations are secure and follow best practices. Regularly running these tests helps to prevent security breaches and maintain compliance with industry standards.