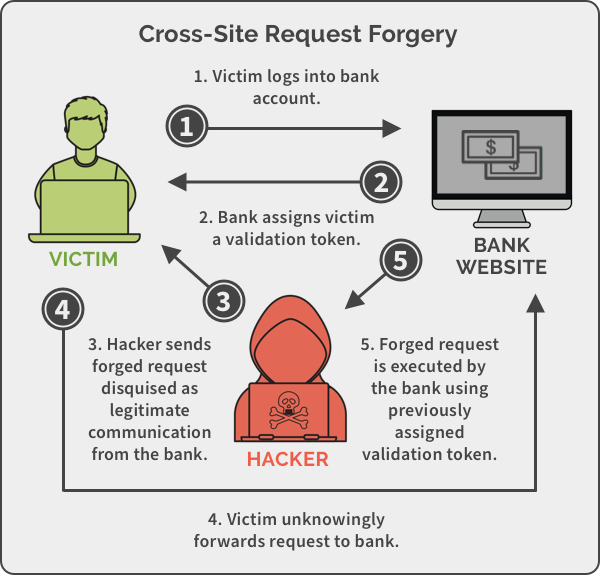
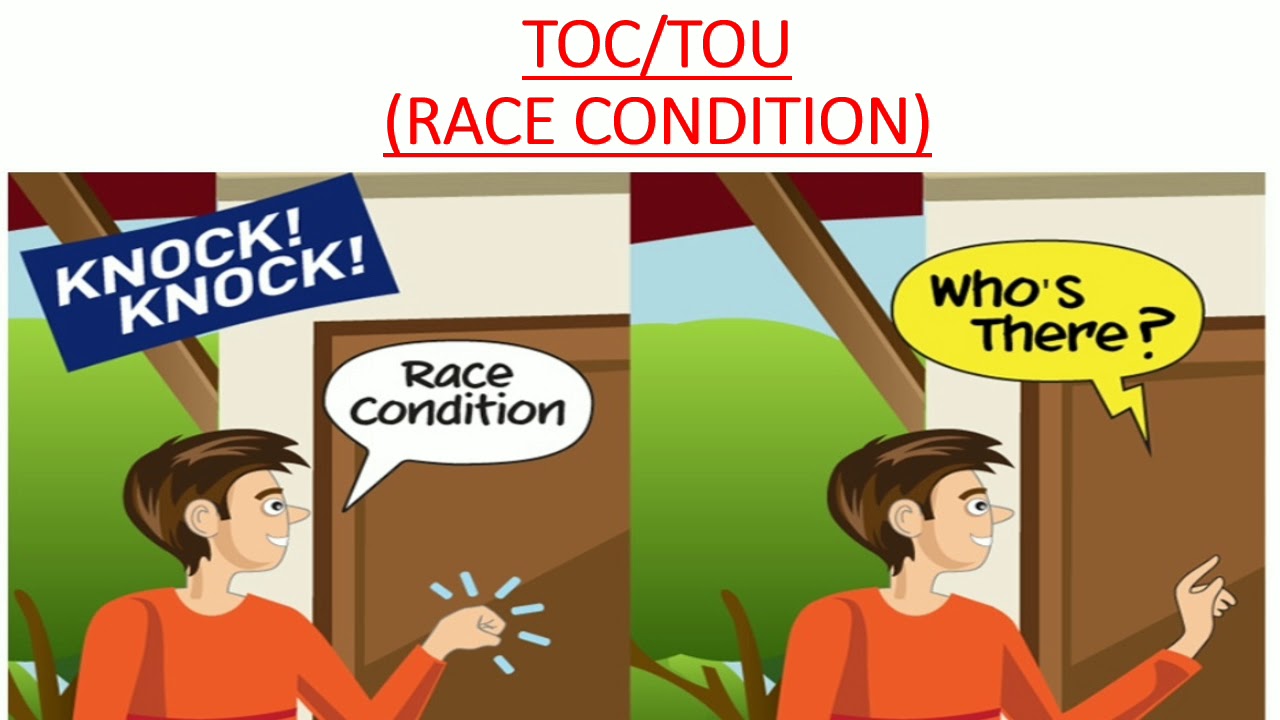
Cross-site Request Forgery (CSRF / XSRF) is a type of attack that occurs when a victim’s web browser is forced to perform an unwanted action, on a trusted site, while the user is authenticated by a malicious site, blog, email, program, or instant message.

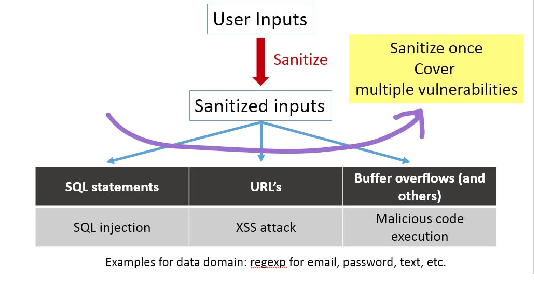


A race condition attack happens when a computing system that’s designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously. This technique takes advantage of a time gap between the moment a service is initiated and the moment a security control takes effect. Other names used to refer to this include Time of Check/Time of Use or TOC/TOU attacks.

* A system splits up its identification, authentication, and authorization steps.
* Attacker uses a race condition and makes the authorization step take place before the authentication step.
* Now the attacker does not need to be authenticated to carry out a specific task.



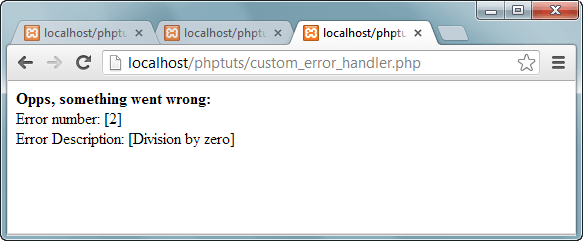
Improper Input Handling is the term used to describe functions such as validation, sanitization, filtering, or encoding and/or decoding of input data. Improper Input Handling is a leading cause of critical vulnerabilities that exist in today’s systems and applications. The root cause of Improper Input Handling is the application trusting rather than validating data inputs. One of the critical aspects of input handling is validating that the information satisfies specific criteria.



Error handling attacks occur when an error message that’s displayed to an end user provides clues about how an application or website operates

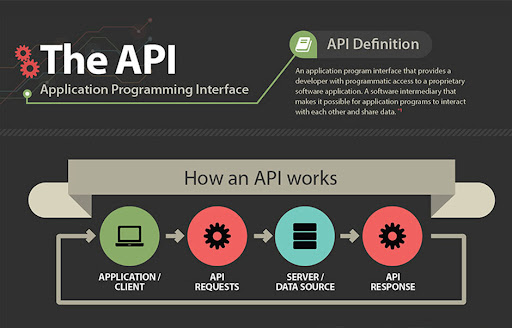
The following are examples of error handling flaws:

* A message that includes server software version details
* A message that reveals where a configuration file holding credential information is located
* An "access denied" message that suggests the existence of hidden files
* A message that includes a stack trace or other “traceback” details
* An authentication error message that behaves differently when the user identifier exists than when it does not

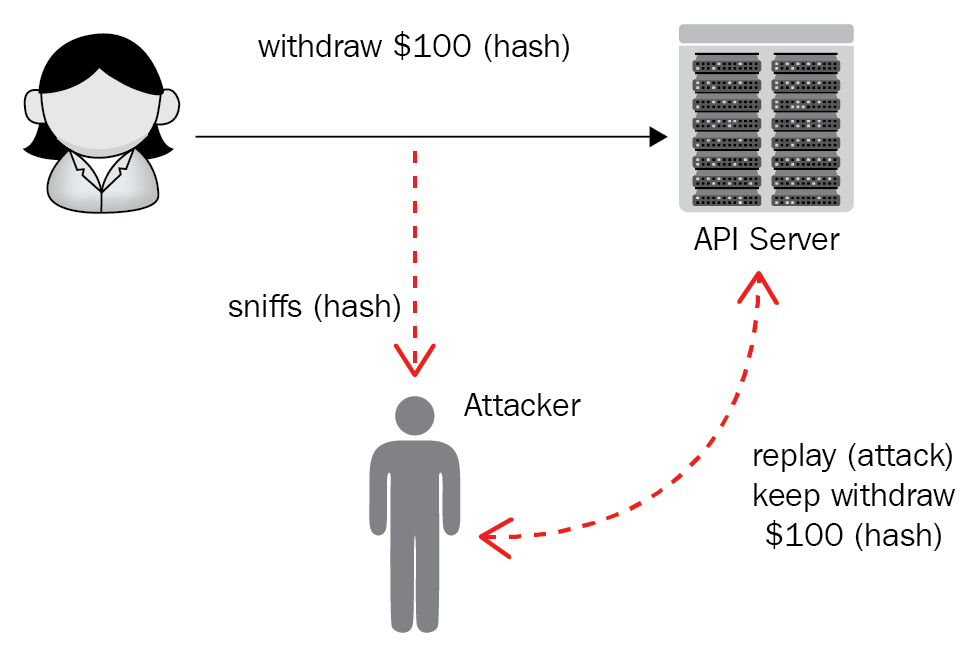


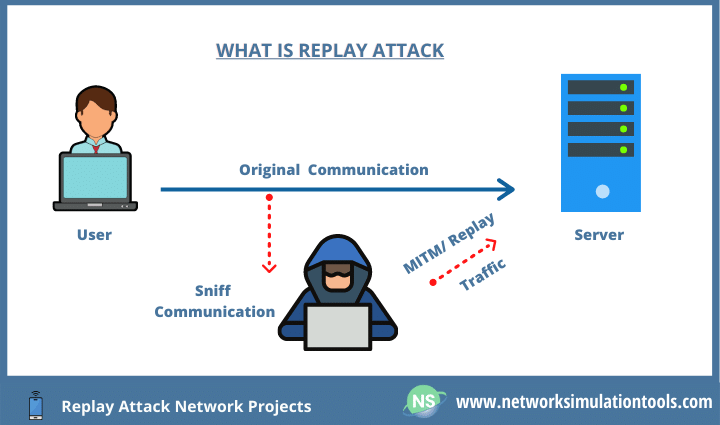
Application Programming Interfaces (APIs), software that allows two different applications to talk to each other and work together. Think of when someone goes to a travel website to see which airline has the lowest price and best schedule for their vacation. It’s an API that connects the travel site to the airline’s system to get them the information they need. One may never see or interact with an API, but it’s there working in the background.



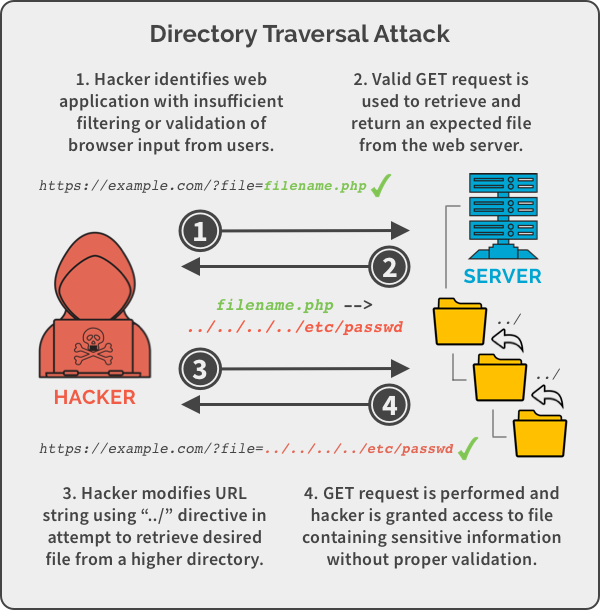


A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.





Directory traversal or [Path Traversal](https://www.acunetix.com/blog/articles/path-traversal/) is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.



Resource exhaustion attacks are computer security exploits that crash, hang, or otherwise interfere with the targeted program or system. They are a form of denial-of-service attack, which involve overwhelming a network host such as a web server with requests from many locations. It can also result in damaging the victims’ hardware in the host server or computer.

