Injection Flaws

2 min

Injection flaws are a type of

Preview: Docs Loading link description

vulnerability

that involves data being misinterpreted as instructions. Injection attacks often occur on web servers since they receive constant untrusted data in requests.

One of the most well-known types of Injection is

Preview: Docs Loading link description

SQL Injection

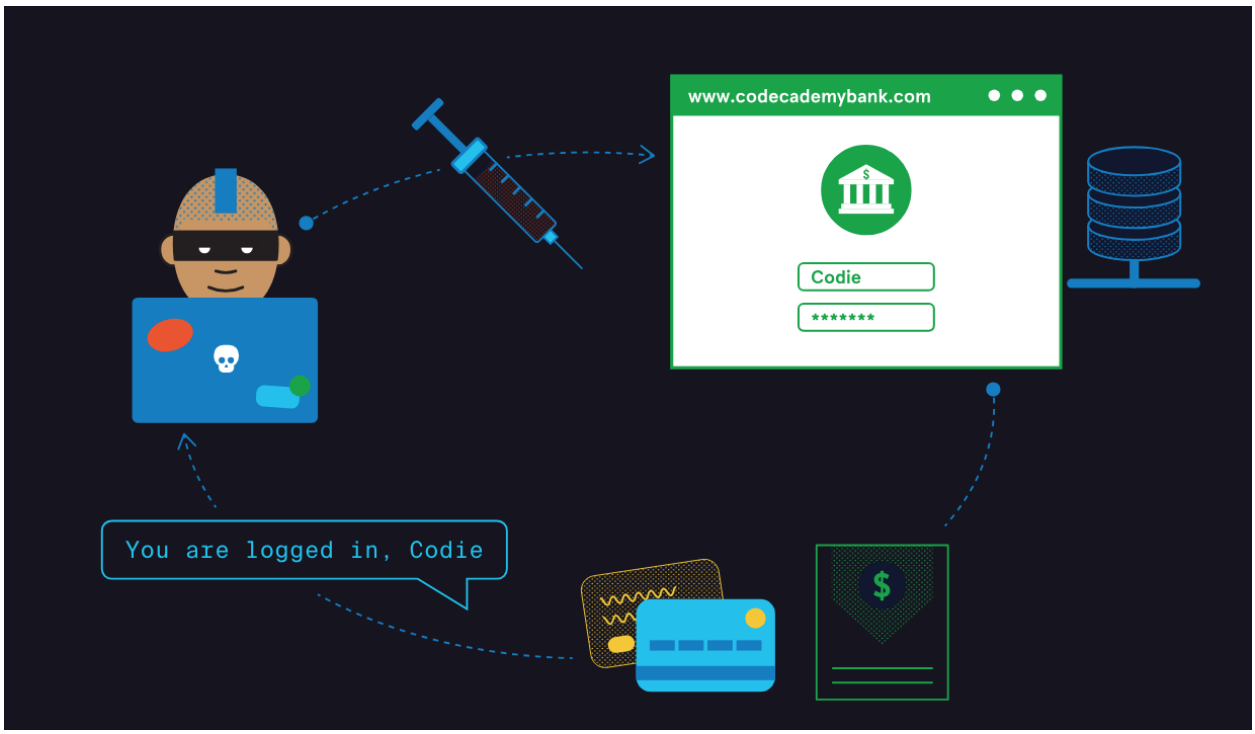
, where a maliciously crafted input causes a SQL interpreter to begin executing instructions contained within the input. SQL injection is so well-known because SQL is used to query databases, and databases are often used to store sensitive information like password hashes, personally identifiable information, etc…

A much simpler type of injection is Command Injection. Command Injection can occur when a program executes a shell command and passes it to the user. Maliciously crafted user input can cause the intended command to exit early, causing the shell to execute a command contained within the input.

For example, if we have a vulnerable script that takes a filename and prints the contents of that file using cat, with a format of cat “<user_provided_filename>” an attacker could give program an input of somefile” || whoami”. This would be passed to the shell as cat “somefile” || whoami””, which would execute cat and then whoami. Of course, an attacker could substitute whoami for a more devious set of commands.

The basic way to prevent injection attacks is through Input Sanitization, which removes or neutralizes dangerous characters from an input. It’s usually better to deny all characters that are not explicitly allowed rather than vice versa. For SQL Injection specifically, it’s a best practice to use Parameterized Queries.

Besides SQL and Command Injection, there are many other injection attacks, such as LDAP Injection, Cross-Site Scripting, and more. In general, take care any time you have an interpreter processing data, especially if that data comes from the outside world – it could be a vector for an injection attack.


www.codecademybank.com
Codie
****
You are logged in, Codie