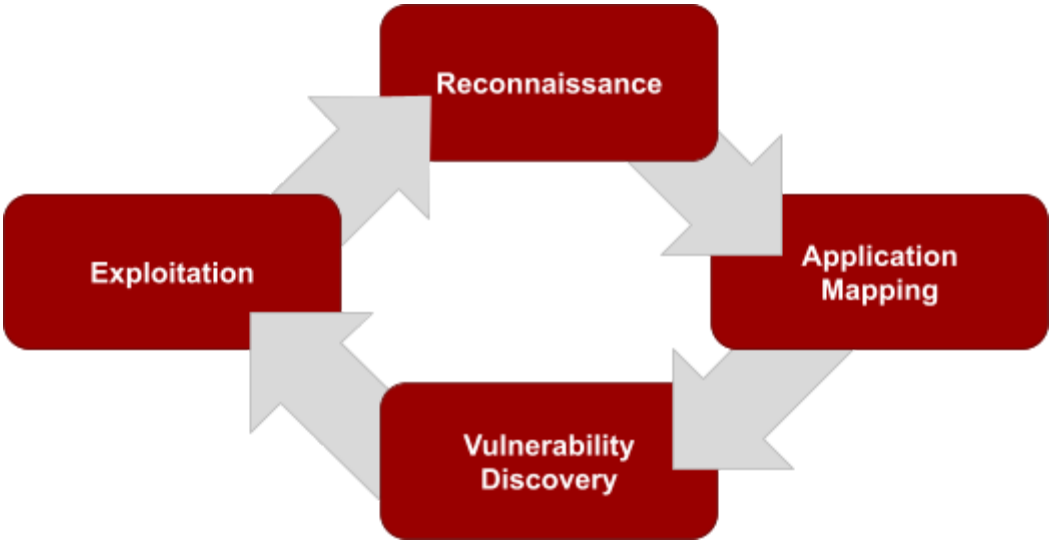
Secure Ideas follows an industry standard methodology for testing the security of web applications. As no current industry standard exists for API penetration testing, Secure Ideas has adapted the standard web application methodology, which begins with the following four-step process:



Note that the methodology is cyclical in nature. Successful exploitation may lead to additional iterations through the methodology.

Reconnaissance:
During reconnaissance, Secure Ideas staff will search public sources for information regarding the target API. Examples of information that is gathered during reconnaissance include:

- Code, keys, and notes found on public repositories such as github
- Information regarding the API that has been otherwise indexed in Google
- Host configuration information, if applicable
- Vulnerabilities that have been publicly disclosed in the past, if applicable

Secure Ideas will include information discovered as part of the final report if it is relevant to any of the exploitable findings found during the penetration testing.

Mapping:
The next step in the methodology is mapping, which is where Secure Ideas will study the behavior and data in the target API. This activity involves the study of provided API documentation including:

- Open API or Swagger definitions
- Postman collections
- Other API documents and example requests (e.g. using curl)

The primary goal of this phase is to understand the inputs into the API endpoints and how they impact data returned in subsequent calls. In addition, Secure Ideas will gain a clear understanding of how any authentication mechanism works, such as the provisioning of API keys.

Discovery:
During the discovery stage of the API penetration test, Secure Ideas will use the information gathered in the previous two steps to assist our staff in finding the vulnerabilities within the target APIs. Using this information combined with custom scripts, automated tools and manual testing, Secure Ideas will provide thorough coverage for all API vulnerabilities and will also seek out less common vulnerabilities depending on the specific architecture and features of the API.

Exploitation:
Exploitation is the final step of the web application penetration test. By exploiting the vulnerability, Secure Ideas is able to provide a realistic understanding of the business exposure from the target. Depending on the flaws discovered, exploitation exercises are often limited to the minimum required to build a proof of concept so that developers and security staff may reproduce the issue. If discovered vulnerabilities allow access to the underlying system, Secure Ideas will begin to reiterate through the methodology by performing reconnaissance on the server and/or network. Further mapping and discovery of the local network will wait until Secure Ideas confirms the scope with [***CLIENT]'s point of contact. Secure Ideas will not conduct exploitation of Denial of Service flaws or other vulnerabilities where a reasonable risk of disruption of business or data loss is perceived without written prior permission.