bounti XP

Application Authentication

Summary

While there are as many proprietary authentication methods as there are systems that utilise it, it is most often variations of a few major approaches. These approaches were developed to address the limitations in early communications and internet systems, and as such, typically use bad existing architectural approaches with novel implementations to allow authentication to occur.

bountiXP regards data protection as one of it's platform's highest priorities. As a result, we have decided to utilise two of these well-known methods to add security to our APIs; namely HTTP Basic Auth and oAuth.

Authentication models

HTTP Basic Authentication

In this method, an HTTP user agent enters a username and password to authenticate. This method does not require cookies, sessions or any other speciality solutions. And, because it uses the HTTP header itself there is no need for complex response systems. We use SSL for security so that the data transmitted is over secure lines.

oAuth

In this method, the user logs into the system. The system then requests authentication, usually in the form of a token. The user will then forward this request to an authentication server, which will either reject or allow this authentication. From this point, the token is provided in each request the user makes to validate the token. This can be used over time with strictly limited scope and age of validity.

This is a very secure and powerful method because it allows for the soft establishment of scope. That is: what systems the key allows the user to authenticate to and validity (meaning the key doesn't have to be purposely revoked by the system, it will automatically become deprecated in time).