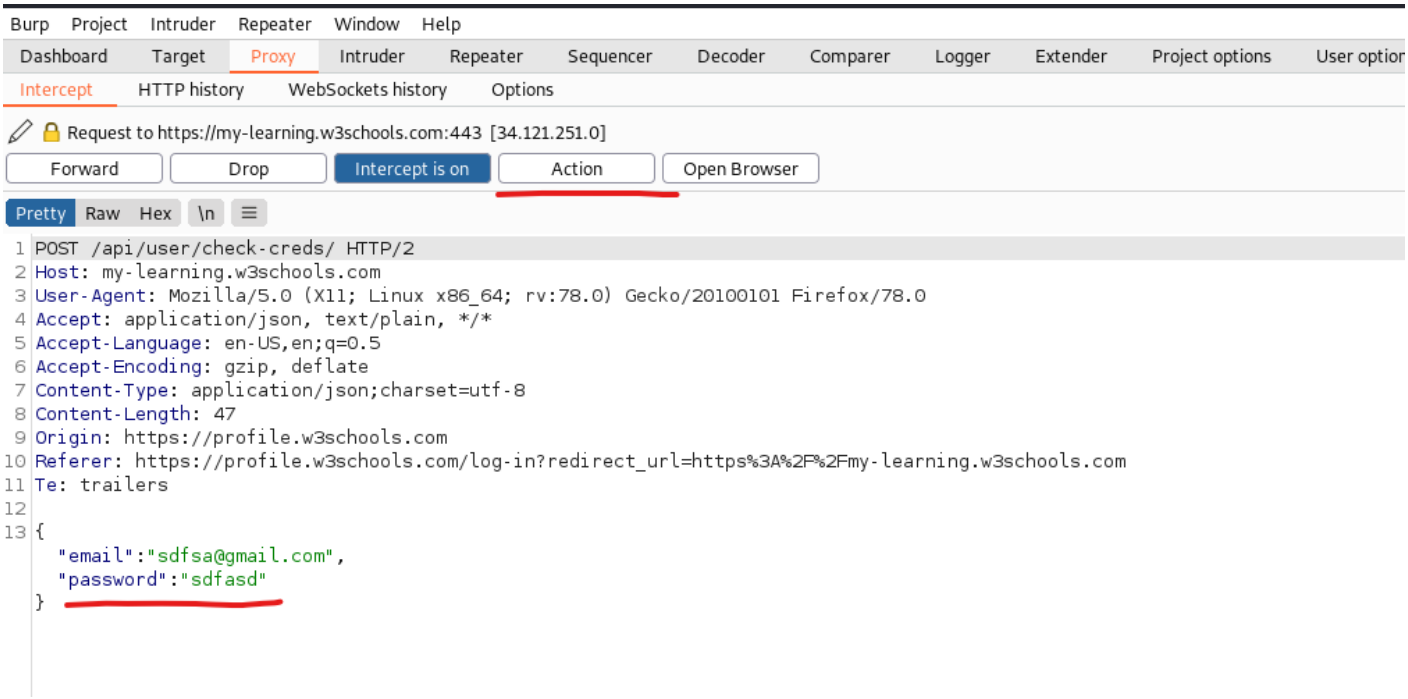
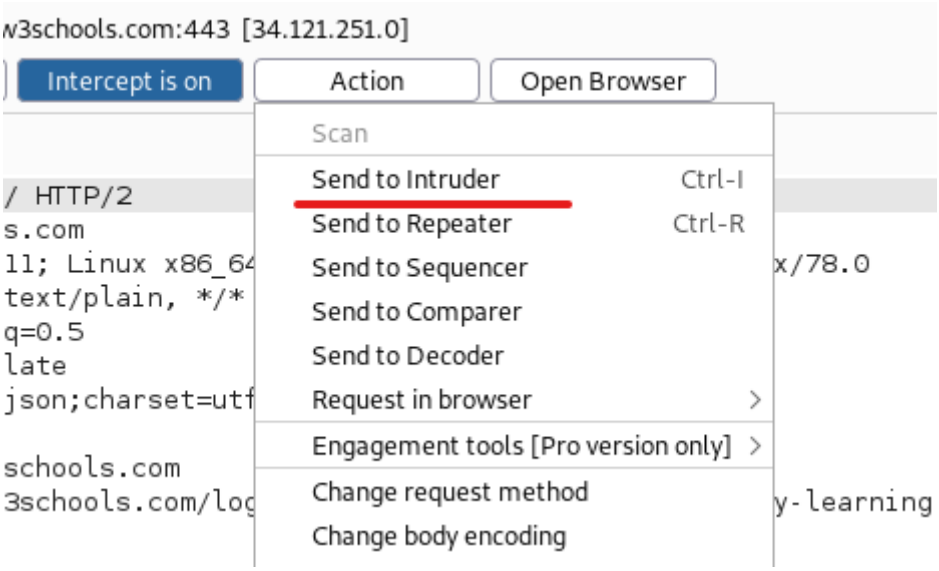
BurpSuite

BurpSuite is a tool which normally is used for Web Application Analysis. But it has some tools which allows to do brute force.
To do this we intercept traffic where we try to log in ourselves. Once we have the request we forward it to the **intruder**.
From there we define which field should get brute forced like for example the password field.
Below you see an example of an intercepted login.
ia Actions you can send the fetched login to the intruder. Shortcut would be **Ctrl + I**.





Now change to the intruder tab. And click **Positions**. There you can define which field should get brute forced in this case we choose the password field. To define a field enter **§** or click **Add §**. Important choose **Sniper** as attack type. There are various attack typed but sniper is the most common.

1. *Sniper* - The most popular attack type, this cycles through our selected positions, putting the next available payload (item from our wordlist) in each position in turn. This uses only one set of payloads (one wordlist).

2. *Battering Ram* - Similar to Sniper, Battering Ram uses only one set of payloads. Unlike Sniper, Battering Ram puts every payload into every selected position. Think about how a battering ram makes contact across a large surface with a single surface, hence the name battering ram for this attack type.

3. *Pitchfork* - The Pitchfork attack type allows us to use multiple payload sets (one per position selected) and iterate through both payload sets *simultaneously*. For example, if we selected two positions (say a username field and a password field), we can provide a username and password payload list. Intruder will then cycle through the combinations of usernames and passwords, resulting in a total number of combinations equalling the smallest payload set provided.

4. *Cluster Bomb* - The Cluster Bomb attack type allows us to use multiple payload sets (one per position selected) and iterate through all combinations of the payload lists we provide. For example, if we selected two positions (say a username field and a password field), we can provide a username and password payload list. Intruder will then cycle through the combinations of usernames and passwords, resulting in a total number of combinations equalling usernames x passwords. *Do note, this can get pretty lengthy if you are using the community edition of Burp.*

https://portswigger.net/burp/documentation/desktop/tools

https://portswigger.net/burp/documentation/desktop/tools/intruder

---

Revision #2
Created 9 July 2022 13:09:12 by Togoboi
Updated 9 July 2022 13:16:53 by Togoboi