#### **Purpose**

In this discussion, I would like you to share your experience using web applications. Please share a typical web-based data input scenario in which you can enter arbitrary data.

#### **Tasks**

To make the discussion concise, please focus one specific example. Please submit one original post using the following guideline:

* Describe your example.
* Describe the specific end user input under your defined circumstance.
* Discuss the potential consequence when the web application receives this arbitrary user input.

A common web-based data input scenario that everyone has encountered is logging into any website. Think of any website you would like as an example (Facebook, Youtube, Amazon, etc…). Almost all of the time, the username field is a free-text input. I personally try to avoid using free-text input as much as possible, but it cannot be avoided in this case since there is no way to provide the username to all of the time. Using predictive text entry would also leak usernames, which obviously isn’t good. A malicious actor could use this field to pass unwanted code into the system if it is not protected correctly. This may include a direct SQL injection, some possible method of changing the HTML structure, remote code execution, or other means of attacking. The consequences of this can be relatively tame, like modifying a few displayed values, to extremely dangerous, such as giving remote access to another system or internal data destruction and manipulation. It is important that developers take the appropriate steps to securing user input fields. This can include input sanitation or passing requests through a proxy server that limits exposed data.