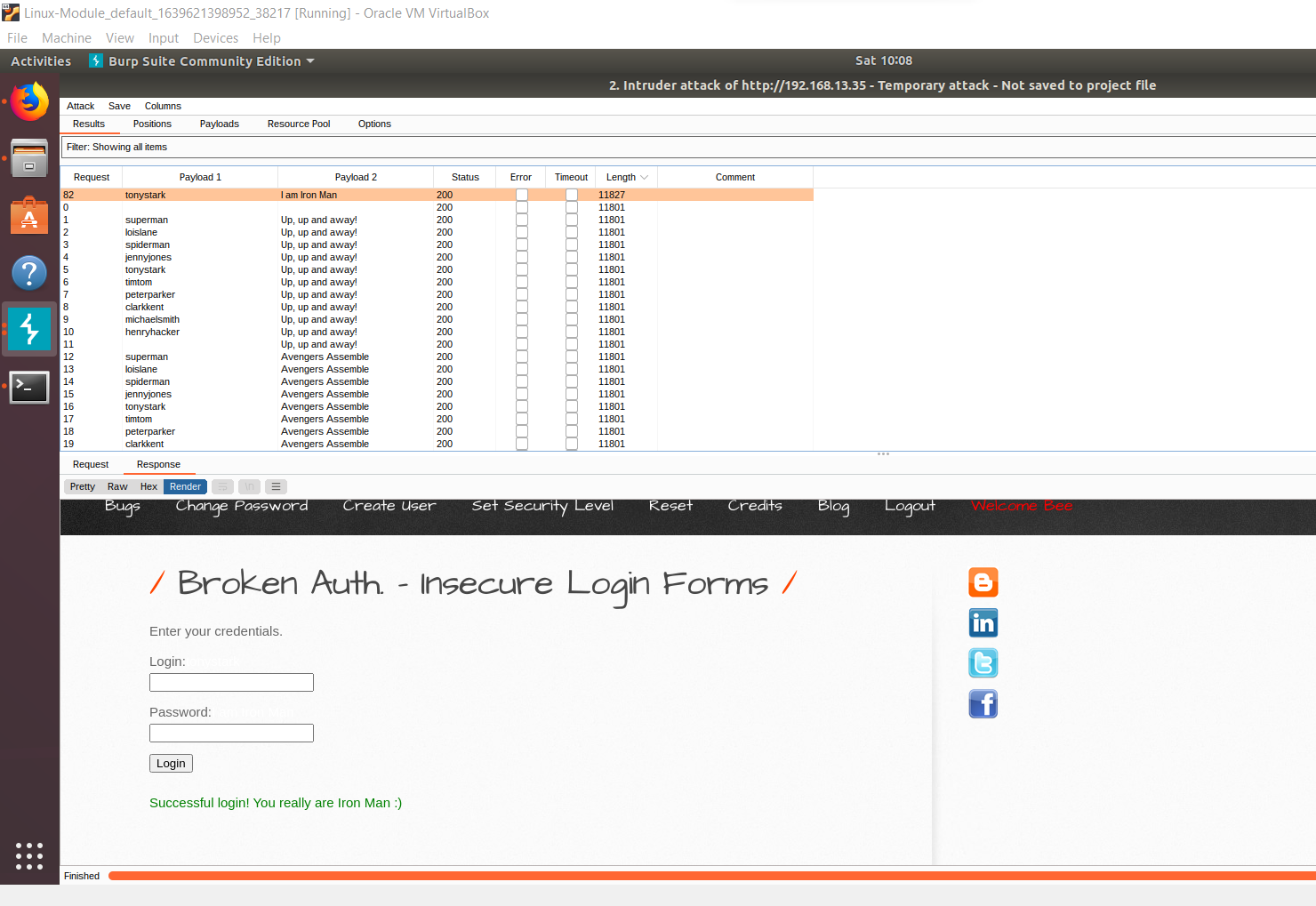
Text

Description automatically generated

**Mitigation Strategies:**

* Use of Prepared Statements: this restricts the user input by forcing developers to write command and user inputted data separately in SQL queries
* Allow-list Input Validation: this can be used to restrict user inputted data to numeric values and symbols with structures similar to IP addresses.

<https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>



Mitigation Strategies:

* Locking accounts: To prevent brute force attacks, the number of login attempts can be limited, and the account is locked after the number of allowed attempts has been reached.
* CAPTCHAs: this program could be used along with username and password to identify whether a computer or a user is trying to access the account.

A screenshot of a computer

Description automatically generated

Graphical user interface, application

Description automatically generated

A screenshot of a computer

Description automatically generated

Mitigation Strategies:

* Consistently sanitize data so that unwanted/unsafe characters are removed from the data
* Have an allow list of known safe data for user input. This will treat all data from an external sources as untrusted and will need to be validated