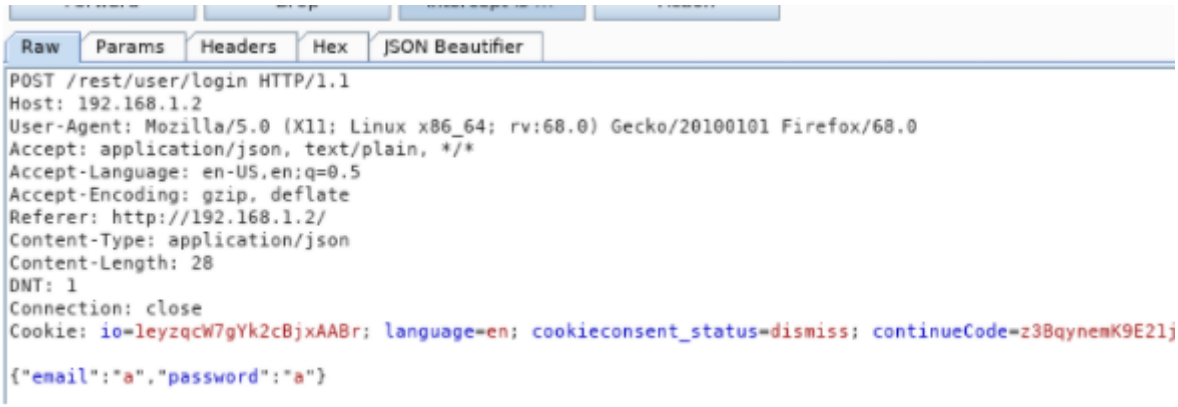
SQLi

SQL injection in general

SQL Injection is when an attacker enters a malicious or malformed query to either retrieve or tamper data from a database. And in some cases, log into accounts.

Method 1: true statement

In an example navigate yourself to a log in. Intercept the request and edit the login fields like this:



{“email”:”’ or 1=1--“,”password”:”a”}

Why does this work?

- The character ' will close the brackets in the SQL query
- **'OR'** in a SQL statement will return true if either side of it is true. As **1=1 is always true**, the whole statement is true. Thus it will tell the server that the email is valid, and log us into **user id 0**, which happens to be the administrator account.
- The **--** character is used in SQL to comment out data, any restrictions on the login will no longer work as they are interpreted as a comment. This is like the **#** and **//** comment in python and javascript respectively.

Method 2: do not force to be true

Similar to what we did in Example 1, we will now log into Bender's account! Capture the login request again, but this time we will put:

`bender@juice-sh.op'--`

as the email.

```
{"email":"bender@juice-sh.op'--","password":"a"}
```

Well, as the email address is valid (which will return **true**), we do not need to force it to be **true**. Thus we are able to use **'--** to bypass the login system. Note the **1=1** can be used when the email or username is not known or invalid.

Revision #3
Created 9 July 2022 14:52:53 by Togoboi
Updated 10 July 2022 08:30:40 by Togoboi