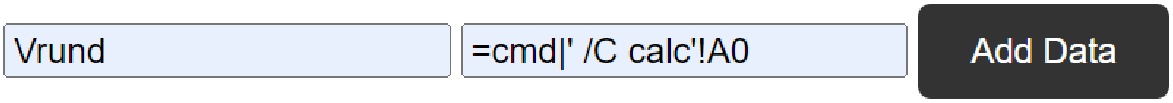
# Project Write Up

CSCI 3450U

Vrund Patel - 100780642

### Easy Bug - CSV Injection

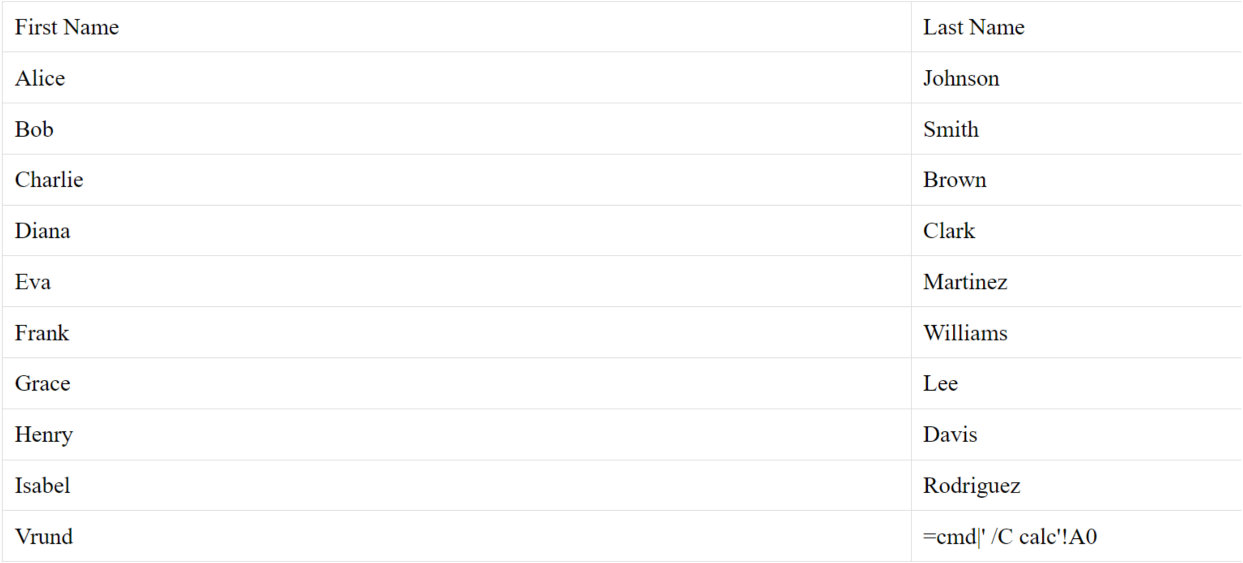
Let’s try to input a first name in the first name input field and “=cmd|' /C calc'!A0” into the last name field.



Vrund

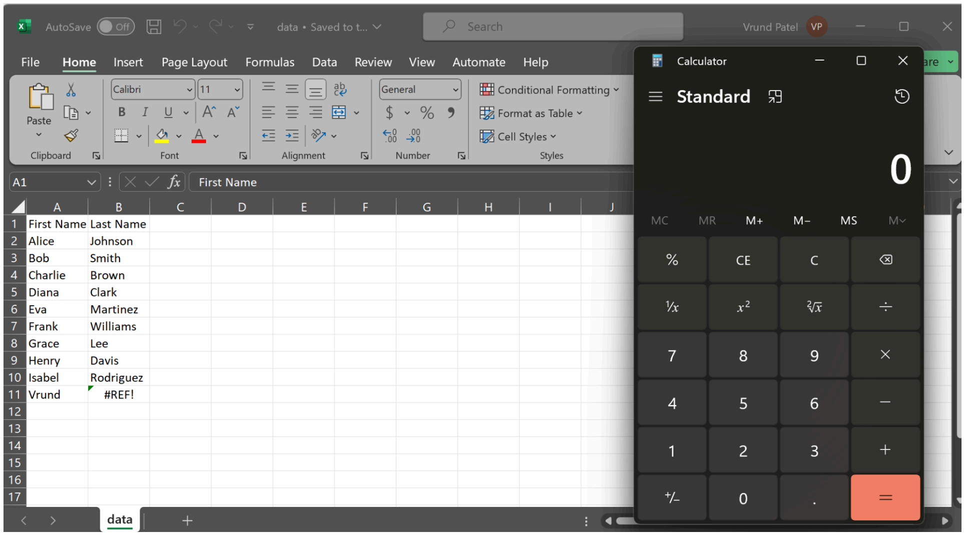
=cmd|' /C calc'!A0

After Clicking add data, you should get prompted and the dynamic table should be able to display the new values.



| First Name | Last Name |
|---|---|
| Alice | Johnson |
| Bob | Smith |
| Charlie | Brown |
| Diana | Clark |
| Eva | Martinez |
| Frank | Williams |
| Grace | Lee |
| Henry | Davis |
| Isabel | Rodriguez |
| Vrund | =cmd|' /C calc'!A0 |

Now let’s press the Open Excel button to open Excel, and open the data.csv file. You will be prompted by a potential csv injection, and it will ask if you want to run cmd. Click “enable for the first prompt, yes for the second, and don’t update for the third prompt. This should open the calculator app on your computer.



A1 | First Name

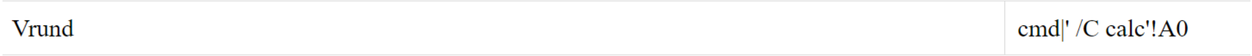
| | A | B |
|---|---|---|
| 1 | First Name | Last Name |
| 2 | Alice | Johnson |
| 3 | Bob | Smith |
| 4 | Charlie | Brown |
| 5 | Diana | Clark |
| 6 | Eva | Martinez |
| 7 | Frank | Williams |
| 8 | Grace | Lee |
| 9 | Henry | Davis |
| 10 | Isabel | Rodriguez |
| 11 | Vrund | #REF! |

0

Finally, on the website click on the entry with the “=cmd|' /C calc'!A0” value to delete the last row, the website should highlight the cell as you hover over it.

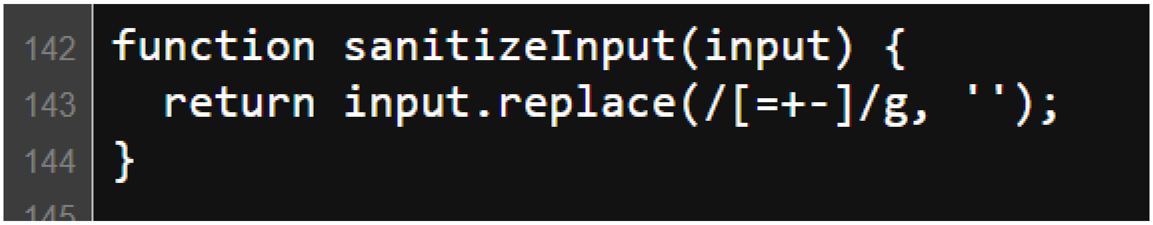
**Medium Bug - CSV Injection**

Try inputting the same values that you inputted for the Easy Bug, you will notice that the “=” operator is missing.



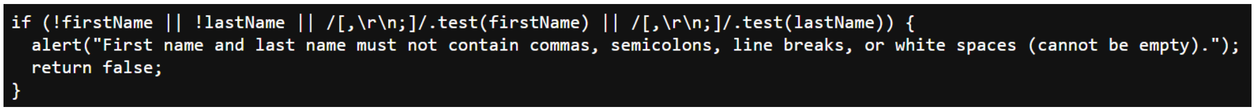
| | |
|---|---|
| Vrund | cmd\|' /C calc'!A0 |

This is because the website sanitized the following input characters: =,+,-, this can also be seen when you right click on the webpage and inspect the page source.



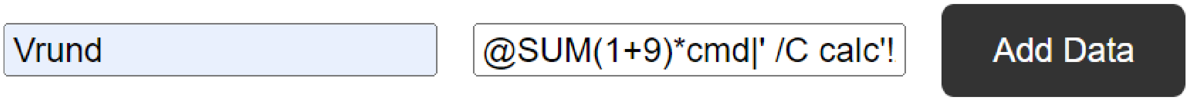
```
function sanitizeInput(input) {
  return input.replace(/[=+-]/g, '');
}
```

You also learn that the text fields do not allow for commas, semicolons line breaks or white spaces which can be used by attackers to start a new cell.



```
if (!firstName || !lastName || /[,\r\n;]/.test(firstName) || /[,\r\n;]/.test(lastName)) {
  alert("First name and last name must not contain commas, semicolons, line breaks, or white spaces (cannot be empty).");
  return false;
}
```

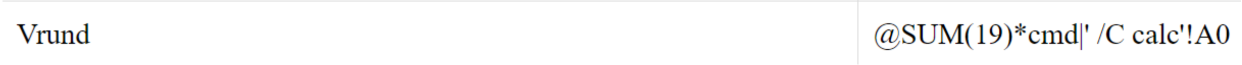
There is a way around this, we can use the “@” operator to open the calculator app on excel, try inputting a first name and “@SUM(1+9)*cmd|' /C calc'!A0” into the last name field.



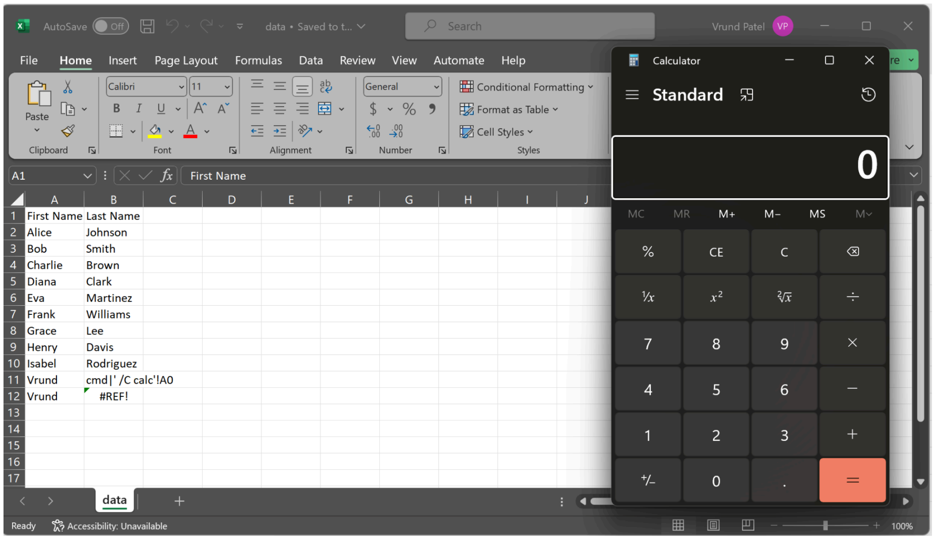
Vrund

@SUM(1+9)*cmd|' /C calc'!

We can see that the “@” operator was not sanitized and once we open the data file on excel we can see that it runs the calculator. Finally, make sure to remove any added entries.



| | |
|---|---|
| Vrund | @SUM(19)*cmd\|' /C calc'!A0 |



AutoSave Off
data • Saved to t...
Search
Vrund Patel
File Home Insert Page Layout Formulas Data Review View Automate Help
Calculator
Standard
0
A1
First Name
data
Ready
Accessibility: Unavailable
100%

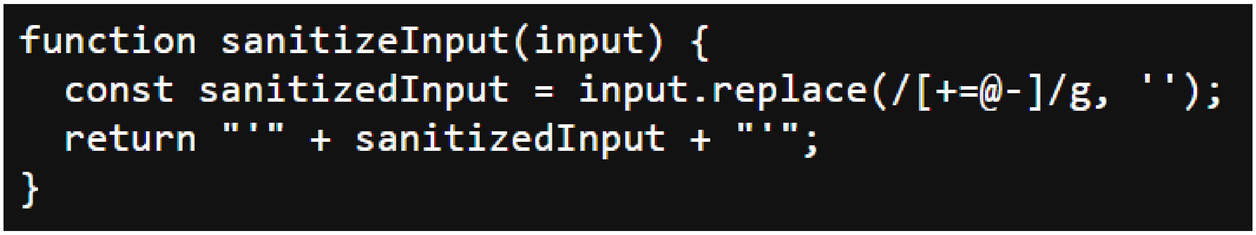
| | A | B |
|---|---|---|
| 1 | First Name | Last Name |
| 2 | Alice | Johnson |
| 3 | Bob | Smith |
| 4 | Charlie | Brown |
| 5 | Diana | Clark |
| 6 | Eva | Martinez |
| 7 | Frank | Williams |
| 8 | Grace | Lee |
| 9 | Henry | Davis |
| 10 | Isabel | Rodriguez |
| 11 | Vrund | cmd\|' /C calc'!A0 |
| 12 | Vrund | #REF! |

## Hard Bug - CSV Injection

Let’s try to add the same two injection lines as the medium bug.

| | |
|---|---|
| 'Vrund' | 'cmd\|' /C calc'!A0' |
| 'Vrund' | 'SUM(19)*cmd\|' /C calc'!A0' |

We can see that both the “=” and “@” operators have been removed. This can also be seen by inspecting the source code where the operators are removed with a white space.



```
function sanitizeInput(input) {
  const sanitizedInput = input.replace(/[+=@-]/g, '');
  return "'" + sanitizedInput + "'";
}
```

In addition to this, the sanitize input function wraps the inputs in single quotes. In Excel, single quotes are escape characters, and any operator (such as @ or =) will not work inside those single quotes because anything wrapped in single quotes gets treated as text, the same concept applies to double quotes.