

Curtis Pettit

## Assumptions

It is acceptable to have multiple employees with the same name.

The rounding done on benefits cost and net pay complies with relevant laws and policies.

The dashboard should be easy to use.

- People using this dashboard are not expected to use browser debugging tools to see errors.
- Preventing errors is important.

Dashboard is only used to calculate the effect on pay of benefits, other withholdings like taxes are out of scope.

## Issues

### Issue #1

**Area:** Api Docs

**Title:** Stray <b> tag in Postman Add employee sample.

#### Repro Steps

Navigate to <https://documenter.getpostman.com/view/2314100/SWTEbbi6#8326ed3a-9c55-43ef-a9d9-c63cd2c73ac1>

Scroll to POST Add Employee

View Body sample

**Expected:** Json text only

**Observed:** "firstName": "<b>New"

Apparently, a stray HTML tag

```
{  
  "firstName": "<b>New",  
  "lastName": "Employee",  
  "dependants": 3  
}
```

**Notes:** I don't see any other examples with tags like this and can't think of a reason for it to be there (other than giving me a hint to try HTML injection).

## Issue #2

**Area:** Front End Usability

**Title:** No user feedback when session expires

### Repro Steps

Navigate to <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Log in with valid username and password

Wait for login to expire (1 hour appears to work)

Refresh page

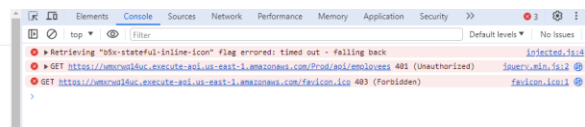
**Expected:** Error message saying that the authentication has timed out and redirected to login page

**Observed:** User is given no feedback as to what is wrong. Only error message is in developer console.

**Notes:** Any other calls, Add, update, or Delete will also fail silently.

Paylocity Benefits Dashboard

Id	Last Name	First Name	Dependents	Salary	Gross Pay	Benefits Cost	Net Pay	Actions
Add Employee								



**Callstack:**

GET https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees  
401 (Unauthorized)

send @ jquery.min.js:2

ajax @ jquery.min.js:2

get @ employeeClient.js:18

loadTable @ Benefits:210

(anonymous) @ Benefits:149

l @ jquery.min.js:2

c @ jquery.min.js:2

setTimeout (async)

(anonymous) @ jquery.min.js:2

u @ jquery.min.js:2

fireWith @ jquery.min.js:2

fire @ jquery.min.js:2

u @ jquery.min.js:2

fireWith @ jquery.min.js:2

ready @ jquery.min.js:2

\_ @ jquery.min.js:2

favicon.ico:1

## Issue #3

**Area:** Frontend

**Title:** Fav Icon is missing

### Repro Steps

Open Browser Debug tools

Navigate to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

**Expected:** No errors

**Observed:**

Call to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/favicon.ico> return 403{"message":"Forbidden"}

**Notes:** Reproduces in Chrom, Edge and Firefox on Windows 10

## Issue #4

**Area:** Backend Security

**Title:** Api accepts html

### Repro Steps

Post to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees>  
Api with the following body

```
{
  "firstName": "HTML <a href=https://www.w3schools.com>click</a>",
  "lastName": " Attack",
  "dependants": 7
}
```

**Expected:** Server returns 400 with something like

```
[
  {
    "memberNames": [
      "FirstName"
    ],
    "errorMessage": "The field FirstName cannot contain special characters /<>; ."
  }
]
```

**Observed:**

Sever accepts and stores the HTML. Front end renders it.

**Notes:**

This is high severity. A bad actor could exploit this to get users to click on a nefarious link, obfuscate the data that is displayed on the UI, or make it look like a person has been added

when they have not. Also, it is possible that this vulnerability would allow other types of code (SQL) to be run on the server, potentially allowing a bad actor to view or edit data they would not otherwise be able to.

Reproduces with last name as well. Can also be entered with the UI. It would be nice if the UI also did input validation to present the user with good error messages but it's crucial on the backend.

## Issue #5

**Area:** Front End Usability

**Title:** Error messages are not surfaced to users

### Repro Steps

Navigate to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Log in with valid username and password

Click Add Employee button

Enter a name over 50 characters Ex. "Bob realllllllllllllllllllly Long name mannnnn" in First name or Last name fields.

Click Add

**Expected:** Error message visible to the user saying "The field FirstName must be a string with a maximum length of 50."

**Observed:** User gets no error message. The only feedback that indicates something is wrong is that the dialog box does not close.

**Notes:** Reproduces across browsers. Name too long is just one example the behavior is the same for all the fields and error messages I was able to discover.

## Issue #6

**Area:** Front End Usability

**Title:** Dependents field accepts invalid inputs

### Repro Steps

Navigate to <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Log in with valid username and password

Click Add Employee button

Enter a valid first and last name

Enter a string that starts with a number Examples: 1.5, 1p, 9+

**Expected:** Input is rejected with error message like “Dependents can only be a whole number between 0 and 32.”

**Observed:** Input is accepted with only the number in front being used. I.E 1 is used if 1.5 is entered.

**Notes:** I feel that this will increase the number of input errors that make it into the database. It's usually safe to trim whitespace, but other characters is risky. The user may be expecting it to accept decimals or it may be trying to type a 2 digit number '10' and their finger slips to type '1p'. It is better to force the user to resolve the discrepancy immediately.

## Issue #7

**Area:** Backend Get Employee

**Title:** Internal server error (500) when sending null for Employee Id

Repro Steps

GET <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees/null>

**Expected:** 400 Bad Request with an error message like “Must specify a valid employee id”

**Observed:** 500 Internal Server Error and an error webpage

**Notes:** Response had no call stack or error details. It probably would if the environment were in “Development” mode.

## Issue #8

**Area:** Backend Usability

**Title:** Get Employee returns 200 OK when id is not found

**Repro Steps**

Send a GET to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees/00000000-0000-0000-0000-000000000001> (or another id that does not exist).

**Expected:** 400 Bad Request or 404 Not Found

**Observed:** 200OK with no body

## Issue #9

**Area:** Front End Mobile

**Title:** Paylocity Logo overflows login box on mobile

**Repro Steps**

Navigate to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login> on a small screen


**Expected:** Logos scale to fit available space

**Observed:** See screenshot

1:50 [notification icons] [alarm icon] [Wi-Fi icon] [cellular signal icon] 67% [battery icon]

[home icon] [address icon] amazonaws.com [plus icon] [90] [three dots icon]

## Paylocity Benefits Dashboard



Username

Password

Log In



**Notes:** taken with older android phone on chrome. Also reproducible by resizing browsers on windows.

## Issue #10

**Area:** Front End Mobile

**Title:** Box around the dashboard does not scale properly on smaller screens

### Repro Steps

Navigate to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login> on a small screen

Login

View Dashboard

**Expected:** All the elements scale together

**Observed:** Box around the outside of the dashboard overlaps the content. see screenshot

Paylocity Benefits Dashboard [Log Out](#)

Id	Last Name	First Name	Dependents	Salary	Gross Pay
19da2073-6d36-4bf6-bd04-b2a51fe1efd3	first	last	1	52000.00	2000.00
90f4d94e-43de-4c16-97ee-11c657d6576a	first	last	4	52000.00	2000.00
a72951a2-c609-4767-af5f-c06be1f74680	first	last	4	52000.00	2000.00
ba4cb3bb-97a9-42db-acb6-57015ddfc044	first	last	2	52000.00	2000.00
bcb99e76-1ee0-4145-99bd-01bc105ed4bc	first	last	3	52000.00	2000.00
f638a7b0-add2-49d2-8a18-29ed82e794e5	first	last	4	52000.00	2000.00

AMF

**Notes:** Discovered on android phone but reproduces by resizing on windows browsers.

## Issue #11

**Area:** Front End Mobile

**Title:** New/Update dialog box does not scale properly on smaller screens

### **Repro Steps**

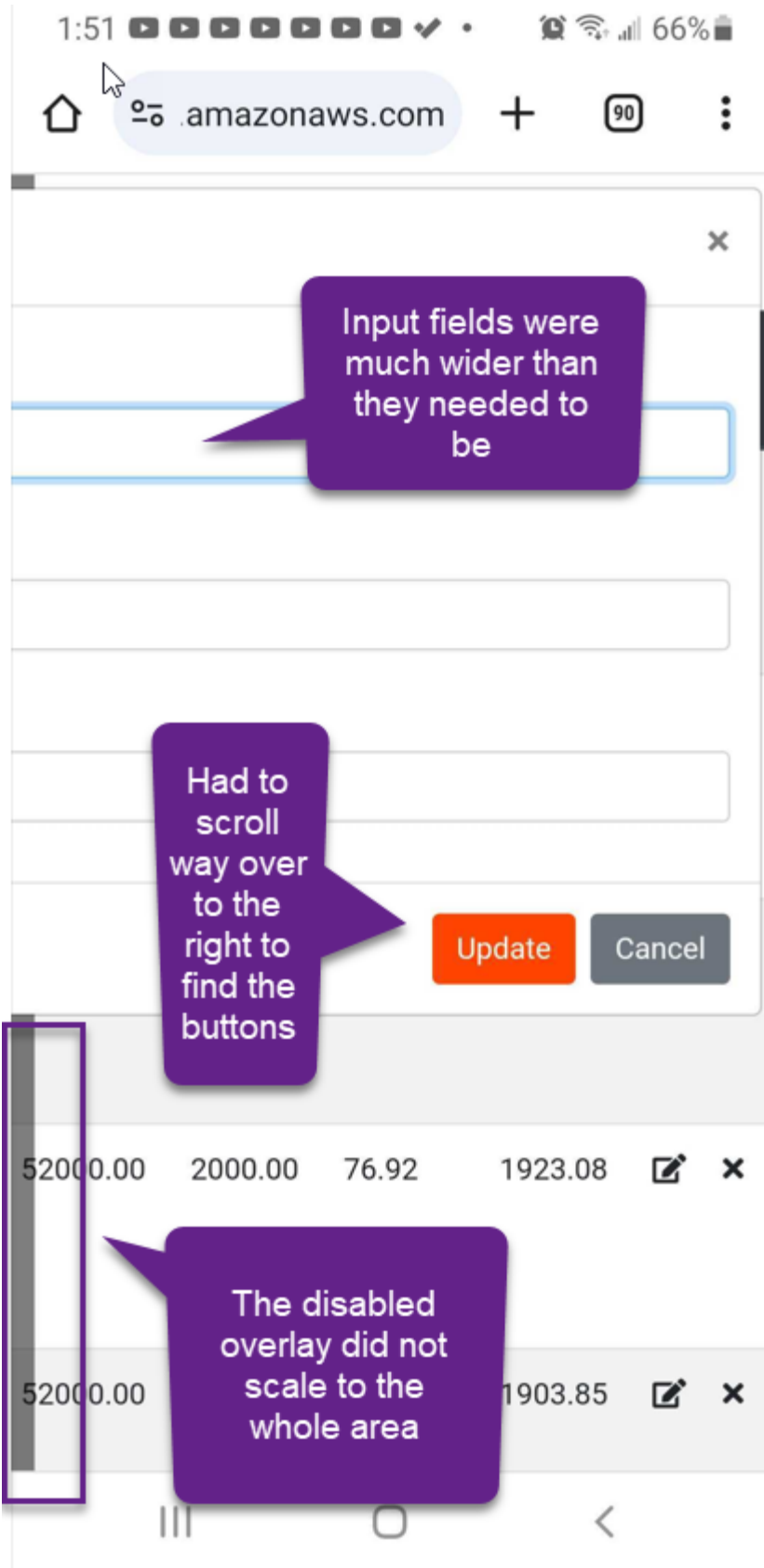
Navigate to <https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login> on a small screen

Login

Click Add Employee

**Expected:** Elements scale to fit withing the screen width

**Observed:** see screenshot



**Notes:** Discovered on android phone but reproduces by resizing on windows browsers.

## Issue #12

**Area:** Front End Accessibility

**Title:** Update and Delete buttons are missing screen reader accessible labels

### Repro Steps

With a screen reader turned on

Navigate to <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Login

Navigate the screen reader to the Actions Column

**Expected:** The pencil-box icon reads as “Update Employee” and the x icon reads as “Delete Employee”

**Observed:** These icons are invisible to screen reader

**Notes:** This was tested with the built in voice assistant on android.

## Issue #13

**Area:** Backend Update

**Title:** Update acts as Add for entries which don't exist

### Repro Steps:

Send a put to

PUT <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees>

"Request Body": "{\r\n \"id\": \"1945d706-39f3-49eb-bea8-98abcf766e5e\", \r\n \"firstName\": \"Wanda\", \r\n \"lastName\": \"Maximoff\", \r\n \"dependants\": 2\r\n}",

**Expected:** 404 Not Found

**Observed:** Item with that Id is added to database, missing data fields (salary, gross pay) are defaulted to 0.

**Notes:** Doesn't seem to use the provided id for the new entry

## Issue #14

**Area:** Backend Update

**Title:** Update takes values that should be read-only

### Repro Steps

Send a put to

PUT <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees>

Include the following in the body (along with a correct id)

```
"salary": 60,  
"gross": 9000
```

**Expected:** Only first name, last name, and dependents are updated.

**Observed:** Salary and gross are updated

**Notes:** Its reasonable for an app like this to have variable Salary and Gross, however the assumptions that came with the exercise specified them as immutable.

## Issue #15

**Area:** Fit and finish

**Title:** Api and UI use different spelling for “Dependents”

### Repro Steps

Compare api documentation and UI dashboard column name

**Expected:** Use the same spelling

**Observed:** Api uses “dependants” UI uses “Dependents”

### Notes:

It seems like both are acceptable with A being more common in UK and E being more common in the US; conceivable that it it’s been localized to EN-US but doesn’t seem likely for a test app.

It would be nice if they matched, however if the api is already implemented by 3<sup>rd</sup> parties it may be unproductive to change it.

## Issue #16

**Area:** Front End Accessibility

**Title:** Update and Delete Buttons are not accessible by keyboard

### Repro Steps

Navigate to <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Login

Set Focus on Log Out Button

Press Tab on the keyboard

**Expected:** Focus shifts to the Update Employee button for the first in the row

**Observed:** Focus shifts to 'Add Employee' at the bottom

Notes: keyboard accessibility is important for several kinds of legally protected disabilities as well as convenient for able bodied people.

## Issue #17

**Area:** Frontend Security

**Title:** Dashboard visible after logout

### Repro Steps

Navigate to <https://wmxrwwq14uc.execute-api.us-east-1.amazonaws.com/Prod/Account/Login>

Login

Click Log Out

Click Back button

**Expected:** Not able to see dashboard

**Observed:** Can see everything that was on the page when it was logged out

**Notes:** This can be a severe security issue if it's used on computers which are shared or otherwise accessible by unauthorized persons.

## Issue #18

**Area:** Backend Security

**Title:** Internal Server Error on invalid credentials

### Repro Steps

Send a request to the Api with invalid credentials

EX: Authorization: Basic foo

**Expected:** 401 Unauthorized

**Observed:** 500 Internal Server Error

**Notes:** Depending on the nature of the error happening on the serve this may be exploitable

## Further Testing Ideas

The full version of this site likely includes the ability to change passwords. Explore password updates including whether existing sessions are properly ended.

Likely this website should work on browsers from iOS and macOS, but I don't have such devices handy.

I found a concerning security issue. The application should have a threat model created and reviewed with appropriate security professionals.

Find out what happens when an entry 'expires'. Requires waiting 1month or DB access.

### Environment:

Windows 10 Pro 19045.4291

Chrome 124.0.6367.61

Firefox 124.0.2

Edge 123.0.2420.97

Samsung Galaxy S9

Android 10

Chrome 124.0.6367.54