API Bug Report

ID: BUG-0003
Title: API allows modifying fixed paycheck amount via PUT violating business rules.
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

Employees must receive a fixed paycheck amount of **$2000 times 26**, and this value **should not be editable** via API

Steps to Reproduce:

- Open POSTMAN
- Set method PUT
- URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees
- Headers:
  Content-Type: application/json
  Authorization: Basic {{token}}
- Body (raw, JSON)
  {
  "id": "71b019c8-6a42-4641-87c3-e94aaab279c6",
  "firstName": "New",
  "lastName": "Employee",
  "dependants": 5,
  "salary": 10000
  }
- Click send

Actual result:

- Using the API, a different paycheck amount (e.g., $2500) can be set or updated via PUT

Expected Result:

- This area should not be editable via API nor UI

ID: BUG-0004
Title: API incorrectly accepts benefits field in PUT and POST requests across multiple modules, despite being a calculated value
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

The API allows clients to include the benefits field in PUT requests across four different functional areas (e.g., HR, Payroll, Finance, Self-service), and returns a **200 OK** status — even though this field is **backend-calculated** and **should not be editable**.

This behavior is **misleading**, as the field is not actually updated, yet the API provides no warning or error.

Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT or POST
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees

- Headers:
  Content-Type: application/json
  Authorization: Basic {{token}}

- Body (raw, JSON)
  {
  "id": "71b019c8-6a42-4641-87c3-e94aaab279c6",
  "firstName": "New",
  "lastName": "Employee",
  "dependants": 5,
  "salary": 10000,
  “gross”:52,
  “benefitCost”:10000
  “net”:25
  }

- Click send

- Observe that

1. The response is `200 OK`.
2. No error or warning is returned.
3. The UI still reflects the correct backend-calculated benefits.
4. The input value `9999` is silently ignored.

Actual result:

API accepts the benefits field in PUT requests across 4 modules.

Returns 200 OK.

The benefits value is **not updated**, as it's **calculated based on fixed business rules**:

- $1000/year per employee
- $500/year per dependent

Expected Result:

The benefits field should **not be accepted** in client PUT requests.

If present, the API should:

- Return a **400 Bad Request**, or
- Clearly **ignore** the field with proper documentation or a warning response.

ID: BUG-0005
Title: API is giving and 200 OK status after trying to delete an unexisting ID of a recently deleted ID
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

API is giving and 200 OK status after trying to delete an unexisting ID of a recently deleted ID
Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT or POST
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees/{{id}}

4. Id should be and unexisting ID with the correct format or a recently deleted ID
5. Headers:
   Content-Type: application/json
   Authorization: Basic {{token}}
6. Click send
7. Observe that status 200 Ok comes as response

Actual result:

API accepts unexsting of recently deleted ID's.

Returns 200 OK.

Expected Result:

Status 404 Not Found or 204 No Content should be returned as response

ID: BUG-0006
Title: API is giving and 200 OK status after trying to delete an ID with random body content
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

API is giving and 200 OK status after trying to delete an ID with random body content

Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT or POST
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees/{{id}}
4. Id should be an existing ID
5. Put random body in JSON format
6. Headers:
   Content-Type: application/json
   Authorization: Basic {{token}}
7. Click send

8. Observe that status 200 Ok comes as response

Actual result:

API accepts random body in DELETE method

Returns 200 OK.

Expected Result:

Status 400 Bad Request

ID: BUG-0007
Title: API is giving a 200 OK status after trying to get an unexisting ID
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

API is giving and 200 OK status after trying to GET an unexisting o recently deleted ID

Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT or POST
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees/{{id}}
4. Id should be an existing ID
5. Headers:
   Authorization: Basic {{token}}
6. Click send
7. Observe that status 200 Ok comes as response

Actual result:

API accepts unexisting ID

Returns 200 OK.

Expected Result:

Status 404 Not found is expected

ID: BUG-0008
Title: Validation data bug in POST method
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Description:

API is giving 200 OK status after trying to POST data in firstName and lastName with entirely numeric String

Steps to Reproduce:

1. Open POSTMAN
2. Set method POST
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees
4. Headers:
   Authorization: Basic {{token}}
   Content-Type: application/json
5. Body:
   {
   “firstName”: “132”,
   “lastName”:”123”,
   “dependants:”1”
6. Click send
7. Observe that status 200 Ok comes as response

Actual result:

200 Ok status is being received having a data validation issue

Expected Result:

Status 400 Bad request

ID: BUG-0009
Title: PUT request to non-existent employee ID creates a new employee instead of returning 404
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees
4. Headers:
   Authorization: Basic {{token}}
   Content-Type: application/json
5. **Put in body an unexsting ID with valid format**
6. Body:
   {
   “id”:”${unexisting if}”
   “firstName”: “132”,
   “lastName”:”123”,
   “dependants:”1”
7. Click send
8. Observe that status 200 Ok comes as response

Actual result:

200 Ok status and new user is being created

Expected Result:

Status 404 not found

ID: BUG-0010
Title: PUT request resets omitted field dependants to 0 instead of preserving or rejecting the request
Priority: High
Severity: High
Reported by: César Rosales

Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Steps to Reproduce:

1. Open POSTMAN
2. Set method PUT
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees
4. Headers:
   Authorization: Basic {{token}}
   Content-Type: application/json
5. **Put in body an unexsting ID with valid format**
6. Body:
   {
   “id”:”${ID}”
   “firstName”: “132”,
   “lastName”:”123
7. Click send
8. Observe that status 200 Ok comes as response

Actual result:

200 Ok status and sets dependents value to 0

Expected Result:

Info should be kept or bad request should be displayed

ID: BUG-0011
Title: API accepts script injection in all fields without validation or sanitization
Priority: High
Severity: High
Reported by: César Rosales
Date: May 18, 2025
Status: Open
Assigned to: Development Team – Backend
System Version: -
Environment: QA – Windows 10 / Chrome 123.0

Steps to Reproduce:

1. Open POSTMAN

2. Set method PUT
3. URL: https://wmxrwq14uc.execute-api.us-east-1.amazonaws.com/Prod/api/employees
4. Headers:
   Authorization: Basic {{token}}
   Content-Type: application/json
5. **Put in body an unexsting ID with valid format**
6. Body:
   {
   “id”:”${ID}”
   “firstName”: “<script>alert('Hacked!');</script>”,
   “lastName”:”123
7. Click send
8. Observe that status 200 Ok comes as response

Actual result:

200 Ok status comes

Expected Result:

API should **reject** or **sanitize** input containing malicious scripts.

Response should be **HTTP 400 Bad Request** with an appropriate validation error message.

Stored values should never include executable HTML/JavaScript code.