

Infor > Vulnerability

 Copy

! Insecure direct object references (IDOR)

Infor Global HR 11.24.10.01.33 and prior are affected by an Insecure Direct Object Reference (IDOR) vulnerability.

Insecure Direct Object Reference (IDOR):

Infor Global HR 11.24.10.01.33 and prior versions are affected by an Insecure Direct Object Reference (IDOR) vulnerability that exposes sensitive pay information. The issue occurs through modification of the `EmployeeID` parameter in a GET request. Exploitation requires authentication.

Description:

The Insecure Direct Object Reference (IDOR) vulnerability has been identified in Infor Global HR v11.24.10.01.33 and prior. This issue resides in the Employee Compensation View functionality of the application. It occurs due to improper authorization checks and insecure handling of user-supplied input in the `EmployeeID` parameter of the following URL:



```
/lmhcm_in4prd1/EmployeeSelfService/form/Employee(<EmployeeID>).LRCEmployeeViewCompensation?menu=LRCEmployeeMenu.ViewCompensation
```

By modifying the `EmployeeID` value in the request, authenticated users are able to access compensation information for other employees. While the compensation web page itself does not display full details by default, it includes a search function that accepts a "Pay Rate" value.

When the correct pay rate is entered for a given employee ID:

- The application reveals the employee's position number in the UI.
- The HTTP response length/size differs compared to an incorrect guess.

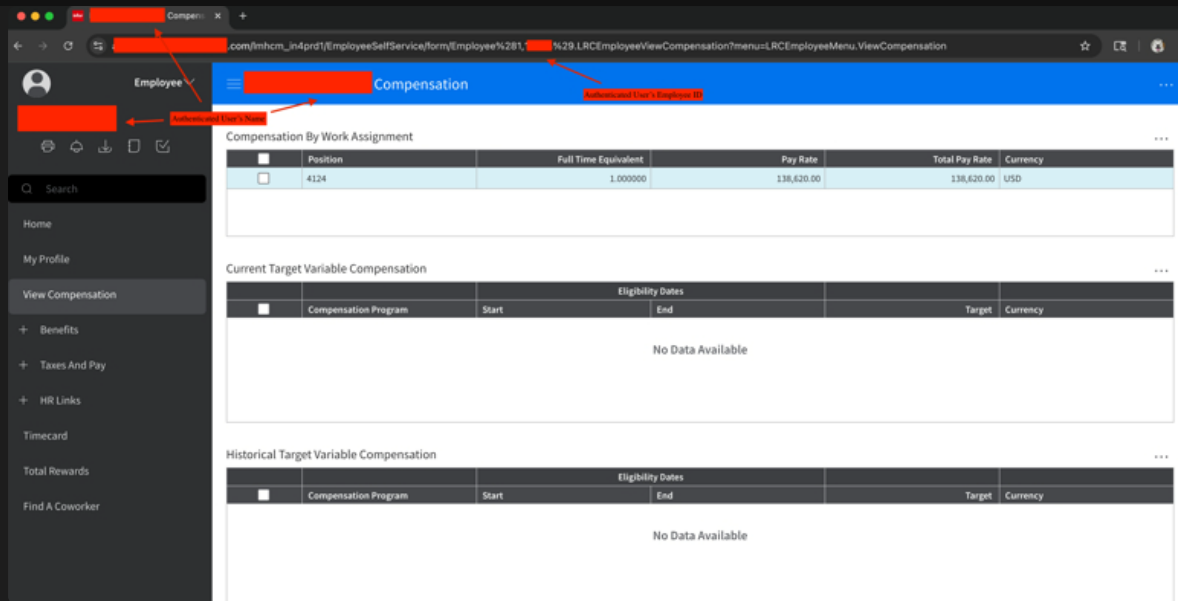
Because incorrect pay rates produce no change in the UI while correct values reveal employee details and modify the response, an attacker can brute-force or systematically guess pay rates. This allows enumeration of sensitive compensation data for arbitrary employees.

Exploitation:

- Within the UI:
 - Modify the `EmployeeID` within the GET request to the target's ID
 - Search Compensation by Work Assignment
 - Enter new Pay Rate until the UI displays a position number, indicating the correct Pay Rate has been entered
- Using a Proxy:
 - Modify the `EmployeeID` within the GET request to the target's ID
 - Search Compensation by Work Assignment
 - Target the PayRate and iterate through a list of numbers
 - Once the correct Pay Rate has been entered notice the increase in response byte size

Example 1:

View the authenticated users compensation:



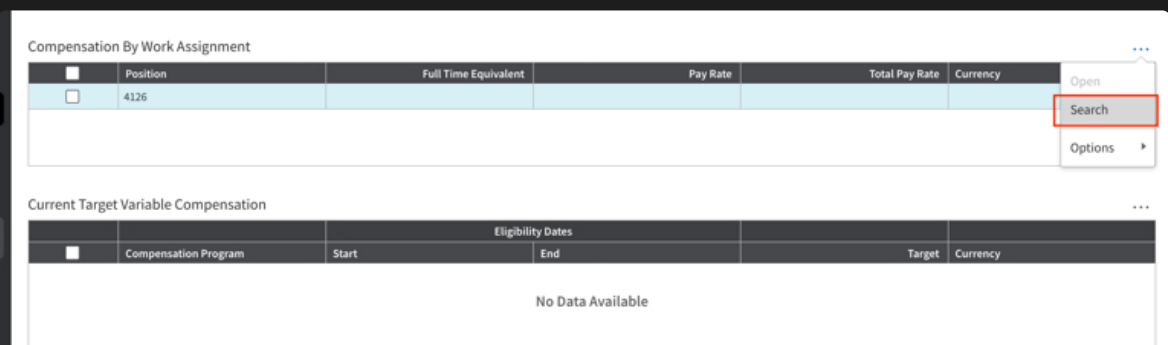
The screenshot shows a web application interface for viewing compensation. The browser address bar contains a URL with an Employee ID. The page title is "Compensation". The left sidebar has a search bar and a menu with "View Compensation" selected. The main content area has three sections: "Compensation By Work Assignment", "Current Target Variable Compensation", and "Historical Target Variable Compensation". The first section contains a table with one row for Position 4124.

	Position	Full Time Equivalent	Pay Rate	Total Pay Rate	Currency
☐	4124	1.000000	138,620.00	138,620.00	USD

Modify the Employee ID value:

1/EmployeeSelfService/form/Employee%281,1234%29.LRCEmployeeViewCompensati
4prd1/EmployeeSelfService/form/Employee%281,1234%29.LRCEmployeeViewC

Search Compensation By Work Assignment:



The screenshot shows the "Compensation By Work Assignment" table with a search dropdown menu open. The table has one row for Position 4126. The dropdown menu has three options: "Open", "Search", and "Options". The "Search" option is highlighted.

	Position	Full Time Equivalent	Pay Rate	Total Pay Rate	Currency
☐	4126				

Search for possible Pay Rates:

Compensation By Work Assignment

Position	Full Time Equivalent	Pay Rate	Total Pay Rate	Currency
[A] ▾	▾	123,456,789.000000		[A] ▾

No Search Results Found

Current Target Variable Compensation

Compensation Program	Start	End	Target	Currency
No Data Available				

Correct Pay Rate being entered:

Compensation By Work Assignment

Position	Full Time Equivalent	Pay Rate	Total Pay Rate	Currency
[A] ▾	▾	125,700.000000		[A] ▾
4126				

Current Target Variable Compensation

Compensation Program	Start	End	Target	Currency

Example 2:

Compare the response sizes to determine the correct Pay Rate:

1	100	200	4869
2	200	200	4869
3	300	200	4869
4	400	200	4869
5	500	200	4869
6	600	200	4869
7	700	200	8221
8	800	200	4869
9	900	200	4869

Last updated 11 months ago

