

miguelgrinberg / Flask-HTTPAuth Public

<> Code Issues 9 Pull requests 1 Actions Projects Wiki Security

# Commit b15ffe9



miguelgrinberg committed last week · ✓ 47 / 47 · Verified

Do not accept empty tokens

main · v4.8.1

1 parent [bc68912](#) commit b15ffe9

2 files changed +19 -2 lines changed

[↑ Top](#)

- ▼ src
  - flask\_httpauth.py
- ▼ tests
  - test\_token.py

2 files changed +19 -2 lines changed

```

src/flask_httpauth.py
@@ -620,8 +620,8 @@ def verify_token(token):
620 620         return f
621 621
622 622     def authenticate(self, auth, stored_password):
623 -         token = getattr(auth, 'token', '')
624 -         if self.verify_token_callback:
623 +         token = getattr(auth, 'token', None)
624 +         if token and self.verify_token_callback:
625 625         return self.ensure_sync(self.verify_token_callback)(token)
626 626
627 627

```

```

    ↓
  tests/test_token.py
  ↑
  @@ -15,11 +15,13 @@ def setUp(self):
15 15
16 16     @token_auth.verify_token
17 17     def verify_token(token):
18 18 +         assert token
18 19         if token == 'this-is-the-token!':
19 20             return 'user'
20 21
21 22     @token_auth3.verify_token
22 23     def verify_token3(token):
24 24 +         assert token
23 25         if token == 'this-is-the-token!':
24 26             return 'user'
25 27
  ↓
  ↑
  @@ -92,6 +94,15 @@ def test_token_auth_login_invalid_token(self):
92 94     self.assertEqual(response.headers['WWW-Authenticate'],
93 95                          'MyToken realm="Foo"')
94 96
97 97 +     def test_token_auth_login_empty_token(self):
98 98 +         response = self.client.get(
99 99 +             '/protected', headers={'Authorization':
100 100 +                 'MyToken '})
101 101 +         self.assertEqual(response.status_code, 401)
102 102 +         self.assertTrue('WWW-Authenticate' in response.headers)
103 103 +         self.assertEqual(response.headers['WWW-Authenticate'],
104 104 +             'MyToken realm="Foo"')
105 105 +
95 106     def test_token_auth_login_invalid_scheme(self):
96 107         response = self.client.get(
97 108             '/protected', headers={'Authorization': 'Foo this-is-the-token!'})
  ↓
  ↑
  @@ -129,6 +140,12 @@ def test_token_auth_custom_header_invalid_token(self):
129 140     self.assertEqual(response.status_code, 401)
130 141     self.assertTrue('WWW-Authenticate' in response.headers)
131 142
143 143 +     def test_token_auth_custom_header_empty_token(self):

```

```
144 + response = self.client.get(  
145 +     '/protected3', headers={'X-API-Key': ''})  
146 + self.assertEqual(response.status_code, 401)  
147 + self.assertTrue('WWW-Authenticate' in response.headers)  
148 +  
132 149 def test_token_auth_custom_header_invalid_header(self):  
133 150     response = self.client.get(  
134 151         '/protected3', headers={'API-Key': 'this-is-the-token!'})
```



## Comments 0



Please [sign in](#) to comment.