- Sign In
- Create Account
-
- Guided tour
- FAQ
- Feedback

The easiest way to test APIs

Make HTTP requests, extract values from the responses, assert the values are correct, reuse variables across steps, or inject custom logic using JavaScript. Build a single test to quickly validate an endpoint or build a whole suite of tests to run at the click of a button.

View example Visit FAQ
Don't show this again.

Build your test

View example
Click to add or remove steps
Collapse / Expand

- Insert Step Before
- Insert Step After
- Move Step Up
- Move Step Down
- Duplicate Step
- Remove Step

1
Request Step Name
POST https://creditpolicy.herokuapp
Post Data

```
{"customer_income":
1000,"customer_debt
":
500,"payment_remark
s_12m":
```

Headers
+ Add Request Header
Add Step
TestSave to Account Share Test Config
PASSN. Virginia
Seconds elapsed:4
Results55 ms

Message

```
[Step 1] POST https://creditpolicy.herokuapp.com/CheckCreditPolicy/ passed
```

Viewing a Request Step
1

- 1
Request

Connection Information

```
  Trying 34.195.54.37...
Name '0.0.0.0' family 2 resolved to '0.0.0.0' family 2
Local port: 0
```

```
Connected to creditpolicy.herokuapp.com (34.195.54.37) port 443 (#0)
ALPN, offering http/1.1
Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
successfully set certificate verify locations:
  CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
TLSv1.2 (OUT), TLS header, Certificate Status (22):
TLSv1.2 (OUT), TLS handshake, Client hello (1):
TLSv1.2 (IN), TLS handshake, Server hello (2):
TLSv1.2 (IN), TLS handshake, Certificate (11):
TLSv1.2 (IN), TLS handshake, Server key exchange (12):
TLSv1.2 (IN), TLS handshake, Server finished (14):
TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
TLSv1.2 (OUT), TLS change cipher, Client hello (1):
TLSv1.2 (OUT), TLS handshake, Finished (20):
TLSv1.2 (IN), TLS change cipher, Client hello (1):
TLSv1.2 (IN), TLS handshake, Finished (20):
SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
ALPN, server did not agree to a protocol
Server certificate:
         subject: C=US; ST=California; L=San Francisco; O=Heroku, Inc.; CN=*.herokuapp.com
         start date: Jun 15 00:00:00 2020 GMT
         expire date: Jul  7 12:00:00 2021 GMT
         issuer: C=US; O=DigiCert Inc; OU=www.digicert.com; CN=DigiCert SHA2 High Assurance Ser
         SSL certificate verify ok.
upload completely sent off: 111 out of 111 bytes
Connection #0 to host creditpolicy.herokuapp.com left intact
```

Request

Request Headers

```
POST /CheckCreditPolicy/ HTTP/1.1
Host: creditpolicy.herokuapp.com
Accept: */*
User-Agent: Mozilla/5.0 (compatible; Rigor/1.0.0; http://rigor.com)
Content-Length: 111
Content-Type: application/x-www-form-urlencoded
```

Request Body

```
{"customer_income": 1000,"customer_debt": 500,"payment_remarks_12m": 0,"payment_remarks": 1,"cu
```

Response

Response Headers

```
HTTP/1.1 200 OK
Connection: keep-alive
Server: gunicorn
Date: Sun, 11 Apr 2021 17:24:14 GMT
Content-Type: application/json
X-Frame-Options: DENY
Content-Length: 36
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Via: 1.1 vegur
```

Response Body

```
{"message": "ACCEPT", "reason": " "}
```

Variables