Acunetix by Invicti

# Comprehensive Report


## Acunetix Threat Level 3

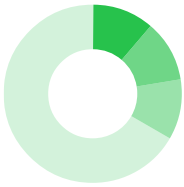
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

## Scan Detail

| | |
|---|---|
| Target | globaltaxnyc.ssbmultiservices.com |
| Scan Type | Full Scan |
| Start Time | Jan 1, 2024, 12:11:10 AM GMT+8 |
| Scan Duration | 1 hour, 15 minutes |
| Requests | 116991 |
| Average Response Time | 33ms |
| Maximum Response Time | 11104ms |
| Application Build | v23.7.230728157 |

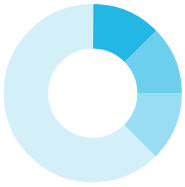

| Severity | Vulnerabilities | Instances |
|---|---|---|
| High | 1 | 1 |
| Medium | 2 | 2 |
| Low | 8 | 8 |
| Informational | 8 | 9 |
| Total | 19 | 20 |

## Informational



| | Instances |
|---|---|
| Content Security Policy (CSP) not implement… | 1 |
| Content type is not specified | 1 |
| Email addresses | 1 |
| Others | 6 |

## Low Severity



| | Instances |
|---|---|
| Clickjacking: X-Frame-Options header | 1 |
| Composer installed.json publicly accessible | 1 |
| Cookies with missing, inconsistent or contra… | 1 |
| Others | 5 |

## Medium Severity

| | Instances |
|---|---|
| Development configuration files | 1 |
| Laravel debug mode enabled | 1 |

## High Severity

| | Instances |
|---|---|
| Dotenv .env file | 1 |

# Impacts

| SEVERITY | IMPACT | |
|---|---|---|
| High | 1 | Dotenv .env file |
| Medium | 1 | Development configuration files |
| Medium | 1 | Laravel debug mode enabled |
| Low | 1 | Clickjacking: X-Frame-Options header |
| Low | 1 | Composer installed.json publicly accessible |
| Low | 1 | Cookies with missing, inconsistent or contradictory properties |
| Low | 1 | Cookies without HttpOnly flag set |
| Low | 1 | Cookies without Secure flag set |
| Low | 1 | HTTP Strict Transport Security (HSTS) not implemented |
| Low | 1 | Insecure Inline Frame (iframe) |
| Low | 1 | Possible sensitive files |
| Informational | 1 | Content Security Policy (CSP) not implemented |
| Informational | 1 | Content type is not specified |
| Informational | 1 | Email addresses |
| Informational | 2 | Outdated JavaScript libraries |
| Informational | 1 | Permissions-Policy header not implemented |
| Informational | 1 | Possible server path disclosure (Unix) |
| Informational | 1 | Reverse proxy detected |
| Informational | 1 | Subresource Integrity (SRI) not implemented |

# Dotenv .env file

A dotenv file (**.env**) was found in this directory. Dotenv files are used to load environment variables from a .env file into the running process.

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

## Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

### https://globaltaxnyc.ssbmultiservices.com/project/ Verified

File: **.env**
Pattern found:

```
APP_ENV=
```

#### Request

```
GET /project/.env HTTP/1.1
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6InE0Wm1nZFYvYWhYVHdUOG0zSHNTOWc9PSIsInZhbHVlIjoiYVFlUEo3bXdPa3E0RkhCY0NZTW9uc3BFM05aen
lUVjhETnpveWg3Y1ZXN3lTSzZQRkhmTStER01iaDV4SDN3dFVQbElhMlBwWldwa2llRk9yN1lJQ1loYkF0U3EyMXgxVWEwbE81Tm
Y1OFpIeit4VTVQYmtiZUpBbkxVcjRvUmYiLCJtYWMiOiI1MzAxMDc4OGJiOGZlNmQwZDMzZmFjYjY5ZjhjNmM3ZmJhMzk2YTNjZW
M1NjBhMzU0M2E3MTUxOWNlZWMyZTA0IiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImpPVVkyWnR1d0N0NjZFbE52L0RLSGc9PSIsInZhbHVlIjoicG16bktGVFJEQjc2VWg5QjRNT
FEyY1BuVEZySksxOFFtd1pRRzMyUXdNMWcyWFhWcTVuSTEzYjU2Y2c2VGM5RHRIaVB3NjFYRWxUTC9UM3BGY1V2NUMya0NDK0hyV
HFPK2JuSVRzWGF5bm9ubVN1REN6QXdzRjJFLzdWbWJnRW8iLCJtYWMiOiI5NWMyNDJkZjI4OTg0YTVlZWMwYWQxZjVlNDBhM2Q1N
2FiYzZhNDAyYzFlYWM3OGViM2NjYTRkMDgxMGI1YTBiIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Remove or restrict access to all configuration files acessible from internet.

# Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

## Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

## https://globaltaxnyc.ssbmultiservices.com/

Development configuration files:

- https://globaltaxnyc.ssbmultiservices.com/project/**package.json**

  ```
  package.json => Grunt configuration file. Grunt is a JavaScript task runner.
  ```

- https://globaltaxnyc.ssbmultiservices.com/project/**composer.json**

  ```
  composer.json => Composer configuration file. Composer is a dependency manager
  for PHP.
  ```

- https://globaltaxnyc.ssbmultiservices.com/project/**composer.lock**

  ```
  composer.lock => Composer lock file. Composer is a dependency manager for PHP.
  ```

- https://globaltaxnyc.ssbmultiservices.com/project/**docker-compose.yml**

  ```
  docker-compose.yml => Docker Compose configuration file. Docker Compose is a tool
  for defining and running multi-container Docker applications.
  ```

### Request

```
GET /project/package.json HTTP/1.1
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6InE0Wm1nZFYvYWhYVHdUOG0zSHNTOWc9PSIsInZhbHVlIjoiYVFlUEo3bXdPa3E0RkhCY0NZTW9uc3BFM05aen
lUVjhETnpveWg3Y1ZXN3lTSzZQRkhmTStER01iaDV4SDN3dFVQbElhMlBwWldwa2llRk9yN1lJQ1loYkF0U3EyMXgxVWEwbE81Tm
Y1OFpIeit4VTVQYmtiZUpBbkxVcjRvUmYiLCJtYWMiOiI1MzAxMDc4OGJiOGZlNmQwZDMzZmFjYjY5ZjhjNmM3ZmJhMzk2YTNjZW
M1NjBhMzU0M2E3MTUxOWNlZWMyZTA0IiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImpPVVkyWnR1d0N0NjZFbE52L0RLSGc9PSIsInZhbHVlIjoicG16bktGVFJEQjc2VWg5QjRNT
FEyY1BuVEZySksxOFFtd1pRRzMyUXdNMWcyWFhWcTVuSTEzYjU2Y2c2VGM5RHRIaVB3NjFYRWxUTC9UM3BGY1V2NUMya0NDK0hyV
HFPK2JuSVRzWGF5bm9ubVN1REN6QXdzRjJFLzdWbWJnRW8iLCJtYWMiOiI5NWMyNDJkZjI4OTg0YTVlZWMwYWQxZjVlNDBhM2Q1N
2FiYzZhNDAyYzFlYWM3OGViM2NjYTRkMDgxMGI1YTBiIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Remove or restrict access to all configuration files acessible from internet.

# Laravel debug mode enabled

The web application uses Laravel framework. Laravel Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

## Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

## https://globaltaxnyc.ssbmultiservices.com/

### Request

```
PUT /index.php HTTP/1.1
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6IlJ1VU9kTTN1b3VzQlVsb1hCREcva2c9PSIsInZhbHVlIjoiM2ZTOS9HcmZYZW1xTFoySmV4UTVBRk80eXExN1
dkSXcyUnRRSkxJMlRtazJnSmJCVFQ0bkxxTjRPeVE3NVBmcjlvcTZpd1FlYXpqRjdaL1FkUno4VmJmclY1RlB4dXJMcTcvVC8wdj
NuNHNqaElUVGoySzZLeVJaRG8yZm5kNjciLCJtYWMiOiI2M2Y2MGRhYmI5MDE1YTg4YmU5MWMxNjQ0YWFiNDBiNzI2NTU5MmVmYz
VhMWRhZWVlMzMwZWE3N2YxMzY5ZDJhIiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6IjM3N3ZBOE9jQXZlWUtvZXlLblJXQ2c9PSIsInZhbHVlIjoicG16U25iVHNJWWhRZ1BRN0E5R
WZiQ0lWc2wyYUlleUw4TFBJQlJQQldNcUhWd0ZBanZQcE0rcEZWdWc1d2VRa2RySkNhbzVkWEN0ZlBmejhnYS9iWlNSeVM3MlpmY
nFEa2tYNmw5NEJoaG54SEdzdGd5OEJvanptaFR6QS9EelIiLCJtYWMiOiJjZDlkNDE5OTM2ODAwYmYyN2NlYzFhNDdlNDBlM2I3M
zQxOTE1NTFlNDA3MjU3YmRjMTIzNjY4NzRmMmQ2ZDA4IiwidGFnIjoiIn0%3D
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Disable the debug mode by setting APP_DEBUG to false

### References

Error Handling
https://laravel.com/docs/7.x/errors#configuration

# Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

## Impact

The impact depends on the affected web application.

### https://globaltaxnyc.ssbmultiservices.com/

Paths without secure XFO header:

- https://globaltaxnyc.ssbmultiservices.com/
- https://globaltaxnyc.ssbmultiservices.com/upload/header-footer/
- https://globaltaxnyc.ssbmultiservices.com/about-us
- https://globaltaxnyc.ssbmultiservices.com/archives
- https://globaltaxnyc.ssbmultiservices.com/consultation
- https://globaltaxnyc.ssbmultiservices.com/contact-us
- https://globaltaxnyc.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020

- https://globaltaxnyc.ssbmultiservices.com/immigration
- https://globaltaxnyc.ssbmultiservices.com/index.php
- https://globaltaxnyc.ssbmultiservices.com/irs-publications
- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us
- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator
- https://globaltaxnyc.ssbmultiservices.com/latest-issues
- https://globaltaxnyc.ssbmultiservices.com/make-payment
- https://globaltaxnyc.ssbmultiservices.com/subscribe
- https://globaltaxnyc.ssbmultiservices.com/tax-accounting
- https://globaltaxnyc.ssbmultiservices.com/where-refund
- https://globaltaxnyc.ssbmultiservices.com/tax-form
- https://globaltaxnyc.ssbmultiservices.com/tax-rates
- https://globaltaxnyc.ssbmultiservices.com/project/vendor/autoload.php

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

## References

The X-Frame-Options response header

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking

https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster

https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

# Composer installed.json publicly accessible

A **installed.json** file was discovered. Composer is a tool for dependency management in PHP. It allows you to declare the libraries your project depends on and it will manage (install/update) them for you. After installing the dependencies, Composer stores the list of them in a special file for internal purposes.

As the file is publicly accessible, it leads to disclosure of information about components used by the web application.

## Impact

installed.json discloses sensitive information. This information can be used to launch further attacks.

## https://globaltaxnyc.ssbmultiservices.com/project/vendor/

### Request

```
GET /project/vendor/composer/installed.json HTTP/1.1
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6InE0Wm1nZFYvYWhYVHdUOG0zSHNTOWc9PSIsInZhbHVlIjoiYVFlUEo3bXdPa3E0RkhCY0NZTW9uc3BFM05aen
lUVjhETnpveWg3Y1ZXN3lTSzZQRkhmTStER01iaDV4SDN3dFVQbElhMlBwWldwa2llRk9yN1lJQ1loYkF0U3EyMXgxVWEwbE81Tm
Y1OFpIeit4VTVQYmtiZUpBbkxVcjRvUmYiLCJtYWMiOiI1MzAxMDc4OGJiOGZlNmQwZDMzZmFjYjY5ZjhjNmM3ZmJhMzk2YTNjZW
M1NjBhMzU0M2E3MTUxOWNlZWMyZTA0IiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImpPVVkyWnR1d0N0NjZFbE52L0RLSGc9PSIsInZhbHVlIjoicG16bktGVFJEQjc2VWg5QjRNT
FEyY1BuVEZySksxOFFtd1pRRzMyUXdNMWcyWFhWcTVuSTEzYjU2Y2c2VGM5RHRIaVB3NjFYRWxUTC9UM3BGY1V2NUMya0NDK0hyV
HFPK2JuSVRzWGF5bm9ubVN1REN6QXdzRjJFLzdWbWJnRW8iLCJtYWMiOiI5NWMyNDJkZjI4OTg0YTVlZWMwYWQxZjVlNDBhM2Q1N
2FiYzZhNDAyYzFlYWM3OGViM2NjYTRkMDgxMGI1YTBiIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Restrict access to vendors directory

### References

Composer Basic usage
https://getcomposer.org/doc/01-basic-usage.md

# Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

## Impact

Cookies will not be stored, or submitted, by web browsers.

### https://globaltaxnyc.ssbmultiservices.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://globaltaxnyc.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=70c7d991c42bb0b11a5cb26af73ad3d9; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/_ignition

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=5d0e017965b7c14b3f7e401f0f12bcb7; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/about-us

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=5b220b6b6e448c3fd0c81e4cc5dfcf05; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/archives

  Cookie was set with:

```
Set-Cookie: PHPSESSID=e8749be181699829eb035e01148101f7; path=/
```

This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=fb948baaaa5c054e33909651097a7551; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/subscribe-action

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=61ed2b2d366b63fcae59fd342da1b136; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/cgi-sys/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=8efa3752a8ac9afbc1588bd9f6732400; path=/
  ```

  This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://globaltaxnyc.ssbmultiservices.com/consultation

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=a3e6e1778bd26cd45a225d73ad757004; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/database/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=dd190f0104175463fad51ab0eb71f95c; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/immigration

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=afc4449460fab031846fd4246b5b97e4; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://globaltaxnyc.ssbmultiservices.com/index.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=b5e8c19232140f095524e8589178081d; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/irs-publications

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=92aea0b5acffc4302bf14fc8b5683e0b; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/tax-form

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=ac21c79a374bca135f26b4c62d002ec9; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/latest-issues

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=721ea0ef54d0ba9d86c1d4af5518241b; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/where-refund

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=aa7008bb3c64b6e3478b463917be84dd; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/mailman/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=11edbc0fff55fd4a637e1ab7eb9b590a; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/make-payment

  Cookie was set with:

```
Set-Cookie: PHPSESSID=688f93db088fccd5e2a6834a21101301; path=/
```

This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://globaltaxnyc.ssbmultiservices.com/subscribe

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=37944c2f180fc8bca2a771a5803523b8; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/tax-accounting

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=11e8e0dd0562c14891cda51c3a2f72bc; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://globaltaxnyc.ssbmultiservices.com/tax-rates

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d2a431d42f5de88c2a8fea1223194c84; path=/
  ```

  This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Ensure that the cookies configuration complies with the applicable standards.

### References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

## Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

## Impact

Cookies can be accessed by client-side scripts.

## https://globaltaxnyc.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://globaltaxnyc.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; path=/
```

- https://globaltaxnyc.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJ1VU9kTTN1b3VzQlVsb1hCREcva2c9PSIsInZhbHVlIjoiM2ZTOS9HcmZYZW1xTFo
ySmV4UTVBRk80eXExN1dkSXcyUnRRSkxJMlRtazJnSmJCVFQ0bkxxTjRPeVE3NVBmcjlvcTZpd1FlYXpq
RjdaL1FkUno4VmJmclY1RlB4dXJMcTcvVC8wdjNuNHNqaElUVGoySzZLeVJaRG8yZm5kNjciLCJtYWMiO
iI2M2Y2MGRhYmI5MDE1YTg4YmU5MWMxNjQ0YWFiNDBiNzI2NTU5MmVmYzVhMWRhZWVlMzMwZWE3N2YxMz
Y5ZDJhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:11:11 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/about-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkprYWNjZHp5TFZmVHdwb0s5UDNUZnc9PSIsInZhbHVlIjoiYytDNzJrbDRVa2dSMll
rMG9xQ2Z0Q0xJVER2YXJRUlVmZFEybFhPeTJqRnBhTFVmb3VTZW1maU9kWFdwMk55d3l0MkRieFQwNzZI
UkFOZm5NVWROcDYxM1FVNUR5MEhLN3dLc045SVhQNDl1MmhKQUJOc3drcmFOZmUvV1gxWCsiLCJtYWMiO
iJlM2YyOGUwM2RkMDJhOWY1NWExMzI0NmRhNWZlN2ZjNDBjNTAxYjU1MjJlZjE1MDlhOTE4MjhhNGM1ND
Q2ZjFjIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:18:33 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJTT0xIc2RVaFRVVFh0V01maEJGb0E9PSIsInZhbHVlIjoibnNJMnByaXhtaHZIRWV
DT09lKzQ4SjFFcm5pNXJ2b2pIWW1WMjVUZFhpaWtDQlRMNjJWMFlBSXQzUDY4VlBMUG1LWldwUVZkQjdH
dC9pQWlZOTQrdGhUSVE2RTlpdnZFR3N6TmpuWjdrQjJhRU5jdTdZRDYwTHprdlNiSEl4dk4iLCJtYWMiO
iI5N2I0YTc0MjMzYmZhNGRlMjljYjYwZGFmZmZhOTBiZjc0M2Y0OGY3MjIxN2I1NDAxZTA0YzMzNzI0MT
```

```
EwNTNmIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:05 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/consultation

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImhjK2VqQUlPUDFJMy9FUVd1VW1mUFE9PSIsInZhbHVlIjoiRzY3QnVpM1lMR2dNM3o
ySklYa2FEMWhrN0I2K0NXNDVUdGliUTNzU3h1VlhIYUVuQUpsbVg3dE9CRGQzaWZEUWhlV1Y3dzVseVZx
aENxVjBhU0hEVlZCNmFZUzMrNStSY0hBQU9YaHlDdUdaYWZxRWVpRHoxcjRBdk9WMGxwY3AiLCJtYWMiO
iIwY2UwMTU4YjNlNTk4YmFlNjk2YjdjZGQwNTVkZjM4MDczNTUzMzc2ZWIxZGQ4OGM2NTUwNzRhMGJmNj
c1ZTRiIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik9BSlZRSmdsNkxMNGFXdUE2TG4xWEE9PSIsInZhbHVlIjoiN0E1Q3ZCSEZ1Q0FrUXI
yekFWZGRYeElndDRldW5LYXhPSHl1WHpOdzJWZ243YjUwWG5pdHBQLzBxakU3bnM4ekRWYmo2N0dMOGxY
SE0wZ3E0MlE2NjJRVlp4eTcrazZiUWFjMyt1Z2R6S3h3d25SSlp5M1FLc3dtbzJzdFpvR2IiLCJtYWMiO
iI2YTNhMzBlNzYzYjRhZDc2OGE4MTlmM2QwMzRlYjhlMzU3NWQ5MzY5YmVmYWExZDdiYTRmMzAxODc2MG
FmMDNhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IldjR2lRMEJZQjJLVWlpODB6eGo5NWc9PSIsInZhbHVlIjoiMFpOKytPcWhCT2xqSS9
sQUlwS0pJSGxra3g1UjgvZy9EM0V4U0tpOVZNbnJTN01VbDQvOHBRVVJ3SHg4UUs5VzhYcktnREExNWG5T
WHliK0IwQUwzQ1pycmdqd0lxOTUwWmNScW11YXZvblFreTl2YllzTFowbzZWWE1GaTYrajciLCJtYWMiO
iJhZGVkZmNiMTA5Y2Q1ZjY2YjllODg1ZDdkM2ZjM2RiYmIwYzQ4MjM1YmQ3NTBiNzYxNzQyN2VjZjMzMj
dmNmEyIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:27 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlFpR0UrWHZndmV4eG45eStVU1JSOVE9PSIsInZhbHVlIjoiZ0NvME9OeFNFMjRydGF
uYjZRWFNSZlRDREEvY256OWpvMEQwam0ySFQvM2JEK0hUSkZaTGMzQnpwUUE0QkcvVmkzNmJhRmdRYXNZ
S1gySmJLT3FhUWhVbWswcHNpemVub2NTQnFaN0JvbjNKQWg3S05xSXl3SXYwZjN3Z296bUwiLCJtYWMiO
iIxOTk3ZWI5YjUyYzU4OTFjOTE1MGRkM2I3MTUyMmIwYTAxMTJjN2NhZjljZTExMjNhMjQ4YzA4NmZmNG
```

```
NjOGYzIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/immigration

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkNYMHl6N1dsdUQxc2RnUFEzVklJY0E9PSIsInZhbHVlIjoiU2JmQ0Zqck9QS3VwOHA
rV3hyUjBCV24zcHBlTHh2d1Y0a3E2a3k3eXozc1k1SUNFOHAwMWg3MElhZ25ZOWFoaFB6K1VSek0rVG5m
T3VoRmYySWVEWkhpYXNzVC9DbzUreFZiSVN5cWJia2s5bXJXMDdBalJoSlVsOTh4bGVKb20iLCJtYWMiO
iJlNDQ0M2JkNGQxN2RhMWMyMDI1ZDYxNmRlNjlhZDQxODRkZDdhZjUzMmVhOTFmNDE0YWFjMDU5NGMzYm
VmNzM1IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjFvMFdLN21Lb0xTaXMxTjhYZVE0OFE9PSIsInZhbHVlIjoiUzRRZ1cvbkhwS2xCcm9
0WllrWVBDL0hrVTM1VjJEVzUzMGc3aVc3a0JERGdBbXgxSDRZSTcxeVVFMHB1RlFmbkYrTlQvdHlzMzE2
by9oZVAzUUFNMmpubnRyVmdQeWEyS1B4SzZGUm1sZ2lYTk05ajdZOW4zdzlvWUljNG96Q0UiLCJtYWMiO
iJkNmQ5NWI5N2M4ZGM1YWM3NThlZjcwYzk5ZTNmOGM0NjEyMzM2MTZmNTc0YjYwM2QzZjUxNDBkZGRhYT
EzZTNmIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/irs-publications

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlYzQVRSNVpRQnZ5Njc2V2tCN29RdUE9PSIsInZhbHVlIjoiOGxHTUN0STNKZm15emJ
BaHRNVnFGR0dhYzJ3dzc0QSt4ZTJtajFNaEw5MXhZc1VGOEJITnpvMERremcrekI5ZDcwcEtDSTNFcysv
MUJiU3lIdUM0Zlltckx5RmRyQ1VRS0tUdDlKTzJuK254d1M2TWk4K3RsL0xjM1I2cTFRR1kiLCJtYWMiO
iJhMmM4ZjU3ZGJhMmRlYWYwMTc5MTliNGE2Mzc1MjdhYzQ2M2MzYzEyZDYxMzE1YzA2YmQ5ZWNkNGVkMj
c5YWVlIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImhnU1kydXdSZG8xazRxT2UwMzhQOUE9PSIsInZhbHVlIjoiL01HK2JoWkRVeGU4S0Q
rb2Y5cDVIMFh5TDFuNjZuQ2dYSmllRlZ1S0RlL2VBbVhSNjYvRjFrZHpDZ1R5LzdmQzZ1YTQyLzJmZ3ph
blo4YnJxTWlwdHpyR0RINURzdlBJR0tjQ05OM3ZOeDFHKzJDR0cvWWwzY0dKOXVHRTNEYnYiLCJtYWMiO
iJhYmEwYmI1NTNiZDc5ODEyNzgyODQ4NGZkN2Y5ZDAyZWFjMzlhNzBkMmY0NTQyYmUyMmRjMWRhMDk0ZG
```

```
Q5NDdhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:03 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Im9XQXoyOFV0MlFTT3I2cXdoTzN5R1E9PSIsInZhbHVlIjoicUtVMVZ6S1dNdmRLamh
iNkh4Y3lqSW1BMitpTkNkN3k3RDZJb1A4Qmtqd1NlMHlXYlFKbGNwNmxKTVNkcjd0djlwNEQrUWtCM2dm
ZHM3OGM0VzFORXJZbFR6V0RoL29JcTFCZnF3NlptR1lHSHpXYlR3YkxqT0pUdnFNcjMvaGEiLCJtYWMiO
iJmOWU2OWM3MzkzOWRmZGRjOWYyOTQ4ZWIwNDk4NmY1YzdiNGZhZmE4N2Y4NjFhYWVjNTdlMzc5MTk5Yj
dhODdhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:03 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/latest-issues

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlorN1UwRWlBR3lGaWljT1lXVkpIZGc9PSIsInZhbHVlIjoiTUZTSUR2NnozL29nS2V
saXIrY3JGNndOV3VRV2tPNjZ5M2gvYXd0b0pBTFRxOXdIM3lZb1lWdnR3R0lCTEIvMnAxTS92Q08rMzZV
d3JGU0FNMndPS25XT3pVUk5ldVpzMGJNZzhLSjdSVG8vYjBqcm0xc0lNTFVad0pna2tiVmQiLCJtYWMiO
iIyNDFiYjNjOWYwMDlkOGM5MmRkMWNkZmNjOTEyM2NjYzRkMWMxNWQ5MWE3NTIyZTI0YmUwNDBlYjMzNG
QxZmY4IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:04 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/make-payment

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjFIeXhQdSt3R0ltbEswa2FlVWVVQnc9PSIsInZhbHVlIjoiTktaWXAxOGJqYU9tYkp
IS1pwYWk0MWxXQjVFN0l0N1ZMNGswNU9MTWZVem9DNG9VaXdlSzkrbHRmbDBwKzkxa0UxaDdhTE5UdWoz
RTUwUGJuVjRtdzJUUGdGZEZMTDNsQ2NHZHVmM2dNK0JZMUNGTVBwSDRzY3RjMHQxVjREM2giLCJtYWMiO
iIwZDkyZmU2ZjE2YzI0NmY4OTc0YzlmNzFjODA3MzFiMTBkYjlkYzJlYmZjMTFiZDM4ZmI2OGQzNjZiMT
YwM2I4IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:04 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/subscribe

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImJyRGx3MUU1MUdJcjZ1cE01R1NjbFE9PSIsInZhbHVlIjoieGRzWWxERWdBaEtvUHp
uZ2tybHlZREFLNzNNOGNDdXdyYnFKbzR4Z3hnVzdVOUt0VFNJZ3BNWWtaWW01dTBIdlVPUk9YeWFCN1pN
dHFNcENYWjlSakh6RDhvV1liMnVNUGJCbnFkaHc4QitKTFJCR1oweEZBeVA4emtLV1diZXAiLCJtYWMiO
iI0NmJkMjUzMjJiMjM1MTAzZGI1MTRiNGFhN2NmNDc1Mzg5YTc5ZTAzMTlhYzdjZjFlZGYwY2MxODNmZT
```

```
lkZjQwIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:05 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/subscribe-action

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ilp6YXlqemVhSWFoenp2dWwzdStYc3c9PSIsInZhbHVlIjoiM3MwOEdOTnFuT0NSb1V
jaW1tQkt1ZjFHRWlVcFRWVlVhM2RkMURMRUZSZGFZRlZOV2xMLzBocG1GNVV6ZnpxTzNrcHRHSEpTcGRY
cXhhRHNQOFJDc2c1TFJjd0VFbXZUSnA5eG9oVitIb2lZQ0RjeWM0ZzBuemk2a1BxSXYwZWgiLCJtYWMiO
iI3ZTZiZjBkMmI3NzU2YmM3Y2I4MmY0YmFkNTYwMTk0MWJmOWZlZGY2NjI5NjEyYWFhMWU2MzY3MWZiND
RjMjhiIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:22 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/tax-accounting

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IitSSFpLY0pQLzNJcDJaOU0xTkZQQ2c9PSIsInZhbHVlIjoiQk0zZ3hRSEpOMFJMbHJ
UQ0IyL1NteWxvY3ZYVEpUdWdSbTRsSWtuemZPSmJMLzIySktrRXBIa3BKK0FPN3NEbjh5U3N3bnNVdmNy
WkVEYWxTQ0tBK1NlN0tUSmRQSUpWU3ltY0JvcE1qMHhYZTBtY0lNdWxmajgydXhha0t1bDAiLCJtYWMiO
iIzOGUxOWZiZWNjNjAzZDViYzBlYTJhZDZhNTVlYmIzNjQzM2VjZTA2YTI3NmRlNzVkYTQ1MmQ1Yjk1OD
M1YjAyIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:23 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/where-refund

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InE0Wm1nZFYvYWhYVHdUOG0zSHNTOWc9PSIsInZhbHVlIjoiYVFlUEo3bXdPa3E0Rkh
CY0NZTW9uc3BFM05aenlUVjhETnpveWg3Y1ZXN3lTSzZQRkhmTStER01iaDV4SDN3dFVQbElhMlBwWldw
a2llRk9yN1lJQ1loYkF0U3EyMXgxVWEwbE81TmY1OFpIeit4VTVQYmtiZUpBbkxVcjRvUmYiLCJtYWMiO
iI1MzAxMDc4OGJiOGZlNmQwZDMzZmFjYjY5ZjhjNmM3ZmJhMzk2YTNjZWM1NjBhMzU0M2E3MTUxOWNlZW
MyZTA0IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:22:43 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/tax-form

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklCWlZoUmNpRUx2eUNhcHR5aTFNdFE9PSIsInZhbHVlIjoiMFlmZ2w5bXBudkkrNjd
JUnlIc2JLQ3pzUUdYaEx3bmZoc3MyR1pONktzNGlpc3RnZCtwODRqTTBLTkk1Nk4wUnhidmFLb0ptSno2
RzF2eWJSM0xQc3pMNVNGbUd5b0FhWTMxL2pUOCtNZUkyQWZCbzNpelVQZFpGZmt4Y0Y4Uy8iLCJtYWMiO
iJlZWUwNmZhYTgxOGZiNjExNDk4ZWYyZThhYmNmMzgyODNiNDkyNTUzNjhiMDljMDNhMTBhYTVlZmU3NT
```

```
AwMWFiIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:23 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/tax-rates

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImlFeHNjeVdsRzR3eTFqcE5xNW5WWUE9PSIsInZhbHVlIjoieWlXbHBlaEFGRFlhVkR
2bmMvVklJSjdaVk5rbXB5RHpsM0pvZytMN0I3andFVjRUdmtnQnQ3amtpZmtOYzFtdU95emtUYkNGalp2
d2tCcWdnckgwbDk1TEdka2VmQlhuNXBLSFhQRSszS0EyTGwwYStYdnBBMDFpRU9RT1VrSnMiLCJtYWMiO
iI3OWFjMDRhY2QwNWI0MzhjZDZlNDUyYzVjNzE4YjFmNWMyOWYxYTY0ODgzOTUxZDc0ODllZWRiNWFjMD
E5NDNkIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:21:24 GMT; Max-Age=7200;
path=/; samesite=lax
```

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

If possible, you should set the HttpOnly flag for these cookies.

# Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

### Impact

Cookies could be sent over unencrypted channels.

**https://globaltaxnyc.ssbmultiservices.com/** Verified

Cookies without Secure flag set:

- https://globaltaxnyc.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; path=/
```

- https://globaltaxnyc.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJ1VU9kTTN1b3VzQlVsb1hCREcva2c9PSIsInZhbHVlIjoiM2ZTOS9HcmZYZW1xTFo
ySmV4UTVBRk80eXExN1dkSXcyUnRRSkxJMlRtazJnSmJCVFQ0bkxxTjRPeVE3NVBmcjlvcTZpd1FlYXpq
RjdaL1FkUno4VmJmclY1RlB4dXJMcTcvVC8wdjNuNHNqaElUVGoySzZLeVJaRG8yZm5kNjciLCJtYWMiO
iI2M2Y2MGRhYmI5MDE1YTg4YmU5MWMxNjQ0YWFiNDBiNzI2NTU5MmVmYzVhMWRhZWVlMzMwZWE3N2YxMz
Y5ZDJhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:11:11 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/

```
Set-Cookie:
global_tax_session=eyJpdiI6IjM3N3ZBOE9jQXZlWUtvZXlLblJXQ2c9PSIsInZhbHVlIjoicG16U2
5iVHNJWWhRZ1BRN0E5RWZiQ0lWc2wyYUlleUw4TFBJQlJQQldNcUhWd0ZBanZQcE0rcEZWdWc1d2VRa2R
ySkNhbzVkWEN0ZlBmejhnYS9iWlNSeVM3MlpmYnFEa2tYNmw5NEJoaG54SEdzdGd5OEJvanptaFR6QS9E
elIiLCJtYWMiOiJjZDlkNDE5OTM2ODAwYmYyN2NlYzFhNDdlNDBlM2I3MzQxOTE1NTFlNDA3MjU3YmRjM
TIzNjY4NzRmMmQ2ZDA4IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:11:11 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/about-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkprYWNjZHp5TFZmVHdwb0s5UDNUZnc9PSIsInZhbHVlIjoiYytDNzJrbDRVa2dSMll
rMG9xQ2Z0Q0xJVER2YXJRUlVmZFEybFhPeTJqRnBhTFVmb3VTZW1maU9kWFdwMk55d3l0MkRieFQwNzZI
UkFOZm5NVWROcDYxM1FVNUR5MEhLN3dLc045SVhQNDl1MmhKQUJOc3drcmFOZmUvV1gxWCsiLCJtYWMiO
iJlM2YyOGUwM2RkMDJhOWY1NWExMzI0NmRhNWZlN2ZjNDBjNTAxYjU1MjJlZjE1MDlhOTE4MjhhNGM1ND
Q2ZjFjIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:18:33 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/about-us

```
Set-Cookie:
global_tax_session=eyJpdiI6ImNiVjF0eHpHRkNmSUc4bTlnUkhFV2c9PSIsInZhbHVlIjoiK2NTdn
BQaTZKUzBXVzZlZW5aTlVwZWZzVXBmOGVKK3kwSXhHZ3RncEJ2MUhSSG9leTd2MDBBbWVJclNEa3VPN2F
kbDhTOTlQR2VSdUhUUWV5bzBodWpjYVQ2RlBTS3VhZklDNThmN25YUUdGVlorSVliRm1kUzlmSTdCRGxn
a2EiLCJtYWMiOiI1ODM2ZmZlNWNmNjBlM2ZlMTQ2MWU4YmE2MzA3OTAzMTgxMzIyY2U0ZDNhOTRkYWQ0Z
GFiYzNjOGYwN2ZiMjJiIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:18:33 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJTT0xIc2RVaFRVVFh0V01maEJGb0E9PSIsInZhbHVlIjoibnNJMnByaXhtaHZIRWV
DT09lKzQ4SjFFcm5pNXJ2b2pIWW1WMjVUZFhpaWtDQlRMNjJWMFlBSXQzUDY4VlBMUG1LWldwUVZkQjdH
dC9pQWlZOTQrdGhUSVE2RTlpdnZFR3N6TmpuWjdrQjJhRU5jdTdZRDYwTHprdlNiSEl4dk4iLCJtYWMiO
iI5N2I0YTc0MjMzYmZhNGRlMjljYjYwZGFmZmZhOTBiZjc0M2Y0OGY3MjIxN2I1NDAxZTA0YzMzNzI0MT
EwNTNmIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:05 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives

```
Set-Cookie:
global_tax_session=eyJpdiI6IngzMnFscWt4ZEJCczBwdmtaV0FDWFE9PSIsInZhbHVlIjoiT1J0RT
lraVFSWjFKL3NqSGthdFFpUXhGNzlKbDZJMi95RE01c3ExNFJ2NTA4bi9ZT2ZxN1RqRmJVM2hWRmdKTk9
2U2xZODdnTU9xWitnM1YwTXBYRU1vRGVVbVA5SHV3L2ludXBBZDU0SVVrWkVSUW9jYjNhNTdqWDRMUVVI
U24iLCJtYWMiOiJlNjM3NTI4OTZlYTgwZjlkZDg0NTEzZmE5MDBhYzQ2Y2VlZDAwOGY3YmFlY2NiYTQxM
TdjNjk1ZGUwYjc1YzA2IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:05 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/consultation

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImhjK2VqQUlPUDFJMy9FUVd1VW1mUFE9PSIsInZhbHVlIjoiRzY3QnVpM1lMR2dNM3o
ySklYa2FEMWhrN0I2K0NXNDVUdGliUTNzU3h1VlhIYUVuQUpsbVg3dE9CRGQzaWZEUWhlV1Y3dzVseVZx
aENxVjBhU0hEVlZCNmFZUzMrNStSY0hBQU9YaHlDdUdaYWZxRWVpRHoxcjRBdk9WMGxwY3AiLCJtYWMiO
iIwY2UwMTU4YjNlNTk4YmFlNjk2YjdjZGQwNTVkZjM4MDczNTUzMzc2ZWIxZGQ4OGM2NTUwNzRhMGJmNj
c1ZTRiIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/consultation

```
Set-Cookie:
global_tax_session=eyJpdiI6IjlibVdHclBiczVhV2h2NHJxcWF2Mmc9PSIsInZhbHVlIjoieEVQZn
Q0aElScXpEU3F0ZmM2QTZrd0kvZHUxQk5sdkUwNHZYWjR3MTNqRUo0bE9XYWNLQmROZXJ6b2FCb0I2TWd
YeEVVLzc0amJSM3dlODVsdGY0V0JXMjVyaUFiSTZldlBvNThGdmlmOXg5V2U2UURQcW9yMCtNOHFzV05B
UHkiLCJtYWMiOiI5MDNkN2ViYjkwMjA3MGEwYjBjMTczY2Q0ZGMyMzc3Yzk1OTMyNzE4NTNkNjk4NjBlY
mQwMGY5NzkxNWQwOTc3IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik9BSlZRSmdsNkxMNGFXdUE2TG4xWEE9PSIsInZhbHVlIjoiN0E1Q3ZCSEZ1Q0FrUXI
yekFWZGRYeElndDRldW5LYXhPSHl1WHpOdzJWZ243YjUwWG5pdHBQLzBxakU3bnM4ekRWYmo2N0dMOGxY
SE0wZ3E0MlE2NjJRVlp4eTcrazZiUWFjMyt1Z2R6S3h3d25SSlp5M1FLc3dtbzJzdFpvR2IiLCJtYWMiO
iI2YTNhMzBlNzYzYjRhZDc2OGE4MTlmM2QwMzRlYjhlMzU3NWQ5MzY5YmVmYWExZDdiYTRmMzAxODc2MG
FmMDNhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie:
global_tax_session=eyJpdiI6ImFHWWxNSW1zWHVxUUNlbkhna0lZc2c9PSIsInZhbHVlIjoiRzlFdU
dubVA0VERLelN1NTF3OTU5ZXN3VlVLNktaT2Nsa3F6UDE2VCtvSVBadmwvbGFYTm5oalVWbFRBOFZ3d21
uczNhU0Y2eVV3TytEUG44eDhnY1NhenNqK1V3SnpSTmMzTzVtNXBDcDcyanRZRTVTODZ5SnNWaHA0RU9V
c0oiLCJtYWMiOiIyNDUxNWFkNjhkNjdhY2EwZTA0MTI4MWVlYjI1ZDllZDk2NzZmZjE2OTI5ODYxY2FkM
2Q5MzQxMTc1Mzk1NGViIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:06 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IldjR2lRMEJZQjJLVWlpODB6eGo5NWc9PSIsInZhbHVlIjoiMFpOKytPcWhCT2xqSS9
sQUlwS0pJSGxra3g1UjgvZy9EM0V4U0tpOVZNbnJTN01VbDQvOHBRVVJ3SHg4UUs5VzhYcktnRExNWG5T
WHliK0IwQUwzQ1pycmdqd0lxOTUwWmNScW11YXZvblFreTl2YllzTFowbzZWWE1GaTYrajciLCJtYWMiO
iJhZGVkZmNiMTA5Y2Q1ZjY2YjllODg1ZDdkM2ZjM2RiYmIwYzQ4MjM1YmQ3NTBiNzYxNzQyN2VjZjMzMj
dmNmEyIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:27 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/contact-us

```
Set-Cookie:
global_tax_session=eyJpdiI6ImI4ZnlPcXZNdWExQVZUQ0orSzRsYkE9PSIsInZhbHVlIjoiYW5KdG
hHaFFGOU96d291RVh5WG1hZ1loZ2xSSU5vRnJGYk0wWXhhZDA5UVc2OURmYnVHODlObGRvMFBEV2s4cGt
GejJUZnBmb3hEZkRiTzJJS2pjU1V0WVM3Z2lvRmI2Mm01VjY1Ukl6RGx2OS9TbUwzb1d4NFRSNmxraDJt
OFYiLCJtYWMiOiIxMzlhZGI5YjUzMTA3ZTQ4ZTJhNWMyMTI5NDJkNDA2OWQ5MGQ3OTY0YjExYzYyY2UyZ
GYyZjYyNTc4YmI5NTExIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:19:27 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlFpR0UrWHZndmV4eG45eStVU1JSOVE9PSIsInZhbHVlIjoiZ0NvME9OeFNFMjRydGF
uYjZRWFNSZlRDREEvY256OWpvMEQwam0ySFQvM2JEK0hUSkZaTGMzQnpwUUE0QkcvVmkzNmJhRmdRYXNZ
S1gySmJLT3FhUWhVbWswcHNpemVub2NTQnFaN0JvbjNKQWg3S05xSXl3SXYwZjN3Z296bUwiLCJtYWMiO
iIxOTk3ZWI5YjUyYzU4OTFjOTE1MGRkM2I3MTUyMmIwYTAxMTJjN2NhZjljZTExMjNhMjQ4YzA4NmZmNG
NjOGYzIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020

```
Set-Cookie:
global_tax_session=eyJpdiI6IitLWU9qZHpCSnFKMkRDUUJrNThabnc9PSIsInZhbHVlIjoiYzhwTW
xDbG0yOGJuTGY0Q3VWakduenFaaVplb3lORWEyN3ZLbVpPVVU0YTRQWVAzZnBxTjFXUUdUTkJVUndVUEl
4S3habWovOVJOK2FLUkxlQlg1R3VoRzhITTcyVERRRjRUMFhBMzN4N1JuL0VySzEyTkh5OVNrMit4N291
NG0iLCJtYWMiOiIyZTk2YmQ1N2I4NDdkN2Y5MzFmYTQzYjc4ZWEwMjVjMTRhOGIwZmQyMmQ5MmMzMzQ4M
TJlN2YzNTE1MmY2NTkyIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/immigration

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkNYMHl6N1dsdUQxc2RnUFEzVklJY0E9PSIsInZhbHVlIjoiU2JmQ0Zqck9QS3VwOHA
rV3hyUjBCV24zcHBlTHh2d1Y0a3E2a3k3eXozc1k1SUNFOHAwMWg3MElhZ25ZOWFoaFB6K1VSek0rVG5m
T3VoRmYySWVEWkhpYXNzVC9DbzUreFZiSVN5cWJia2s5bXJXMDdBalJoSlVsOTh4bGVKb20iLCJtYWMiO
iJlNDQ0M2JkNGQxN2RhMWMyMDI1ZDYxNmRlNjlhZDQxODRkZDdhZjUzMmVhOTFmNDE0YWFjMDU5NGMzYm
VmNzM1IiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/immigration

```
Set-Cookie:
global_tax_session=eyJpdiI6IkRLQzlFMWY2Nkd3c2lpbWRwdm1GaGc9PSIsInZhbHVlIjoicTQxRW
93TXNJcW9WM1hXdlA0NjhQL1RkaVF1WTJPODhEYlRJQ1hWVVdmOUxJSGt4TWJvUjg5SkFRYzhrUGxGMmR
QQlB0eFBpS0NIdHNvd08vRWpjRlhJWUduTk8wZDNNMnFwb25KM1YvdHVBNk9iMTVSOUtXMTNzd1NERkJq
SlQiLCJtYWMiOiJlOThjMzc2NDI5ZGYzM2NlNDQ2ZDU1MTQ0ZGRjOWY3MTA4OTlhMzU4MTZiODEzN2ZkM
2RiNjhmY2RjZTBmNTdhIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:46 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/index.php

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjFvMFdLN21Lb0xTaXMxTjhYZVE0OFE9PSIsInZhbHVlIjoiUzRRZ1cvbkhwS2xCcm9
0WllrWVBDL0hrVTM1VjJEVzUzMGc3aVc3a0JERGdBbXgxSDRZSTcxeVVFMHB1RlFmbkYrTlQvdHlzMzE2
by9oZVAzUUFNMmpubnRyVmdQeWEyS1B4SzZGUm1sZ2lYTk05ajdZOW4zdzlvWUljNG96Q0UiLCJtYWMiO
iJkNmQ5NWI5N2M4ZGM1YWM3NThlZjcwYzk5ZTNmOGM0NjEyMzM2MTZmNTc0YjYwM2QzZjUxNDBkZGRhYT
EzZTNmIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/index.php

```
Set-Cookie:
global_tax_session=eyJpdiI6IlNiVCtZOUIwRFZvOVRGbC9UbysySVE9PSIsInZhbHVlIjoiRXdONC
8zdGxmc3R5aEl4NnVua1ExcHRSYTZKbHlMWFZ6N2N5YzM1SFdoTGNXUVFnZm1WY2V1aG14b0JQb3hELzR
vS2IxajlFVVNxaytHb2locEdRd1h2dUZqaHUrSGROMC9NcExJNFFORHhReTVDU0ZsaHlaVXRQZWlXUjZJ
UUoiLCJtYWMiOiI3ZTU5MWI2YjI2OTIxNTE0MjY0YTQ3ZTJhMjY2MTI2M2EwMzZhN2ZlYWY0NmE4NjMxN
GMwOTUwNjQxZGEzMDliIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/irs-publications

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlYzQVRSNVpRQnZ5Njc2V2tCN29RdUE9PSIsInZhbHVlIjoiOGxHTUN0STNKZm15emJ
BaHRNVnFGR0dhYzJ3dzc0QSt4ZTJtajFNaEw5MXhZc1VGOEJITnpvMERremcrekI5ZDcwcEtDSTNFcysv
MUJiU3lIdUM0Zlltckx5RmRyQ1VRS0tUdDlKTzJuK254d1M2TWk4K3RsL0xjM1I2cTFRR1kiLCJtYWMiO
iJhMmM4ZjU3ZGJhMmRlYWYwMTc5MTliNGE2Mzc1MjdhYzQ2M2MzYzEyZDYxMzE1YzA2YmQ5ZWNkNGVkMj
c5YWVlIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globaltaxnyc.ssbmultiservices.com/irs-publications

```
Set-Cookie:
global_tax_session=eyJpdiI6Ild3VE5IOVQyTHZ1ZElSaUR1VXhRSkE9PSIsInZhbHVlIjoiQVVKYz
YzaDJpM3FyaVJ0NFhTaUV0TEpLbFJ6RDJkbTkvb0x2MzdiTnVHZ2VhT05nM3FXQ3FiTGYxRGk4M2Y5cTV
JSVhPbXdwWklrNit0ejExV1JtOTdQekpwOFhiTHBUWGRuMHZPS2owVXlFK3hFSy9EMTRIb3NpYVlMYXhQ
anIiLCJtYWMiOiIzNGFkMjg3OGYzZDg2ODE1NjBiYmZkNGVhMjNmMWY4OGU2YjI1MTBmYTIyZTZlMGJmY
zc3ZDFiNTAyMzZhMTVkIiwidGFnIjoiIn0%3D; expires=Sun, 31-Dec-2023 18:20:47 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

**Request**

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

If possible, you should set the Secure flag for these cookies.

# HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

### Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

### https://globaltaxnyc.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://globaltaxnyc.ssbmultiservices.com/
- https://globaltaxnyc.ssbmultiservices.com/upload/header-footer/
- https://globaltaxnyc.ssbmultiservices.com/about-us

- https://globaltaxnyc.ssbmultiservices.com/archives
- https://globaltaxnyc.ssbmultiservices.com/consultation
- https://globaltaxnyc.ssbmultiservices.com/contact-us
- https://globaltaxnyc.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020
- https://globaltaxnyc.ssbmultiservices.com/immigration
- https://globaltaxnyc.ssbmultiservices.com/index.php
- https://globaltaxnyc.ssbmultiservices.com/irs-publications
- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us
- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator
- https://globaltaxnyc.ssbmultiservices.com/latest-issues
- https://globaltaxnyc.ssbmultiservices.com/make-payment
- https://globaltaxnyc.ssbmultiservices.com/subscribe
- https://globaltaxnyc.ssbmultiservices.com/tax-accounting
- https://globaltaxnyc.ssbmultiservices.com/where-refund
- https://globaltaxnyc.ssbmultiservices.com/tax-form
- https://globaltaxnyc.ssbmultiservices.com/tax-rates
- https://globaltaxnyc.ssbmultiservices.com/project/vendor/autoload.php

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

## References

hstspreload.org
https://hstspreload.org/

Strict-Transport-Security
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

# Insecure Inline Frame (iframe)

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

## Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

### https://globaltaxnyc.ssbmultiservices.com/contact-us Verified

An iframe tag references an external resource, and no sandbox attribute is set.

#### Request

```
GET /contact-us HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6IkprYWNjZHp5TFZmVHdwb0s5UDNUZnc9PSIsInZhbHVlIjoiYytDNzJrbDRVa2dSMllrMG9xQ2Z0Q0xJVER2YX
JRUlVmZFEybFhPeTJqRnBhTFVmb3VTZW1maU9kWFdwMk55d3l0MkRieFQwNzZIUkFOZm5NVWROcDYxM1FVNUR5MEhLN3dLc045SV
hQNDl1MmhKQUJOc3drcmFOZmUvV1gxWCsiLCJtYWMiOiJlM2YyOGUwM2RkMDJhOWY1NWExMzI0NmRhNWZlN2ZjNDBjNTAxYjU1Mj
JlZjE1MDlhOTE4MjhhNGM1NDQ2ZjFjIiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImNiVjF0eHpHRkNmSUc4bTlnUkhFV2c9PSIsInZhbHVlIjoiK2NTdnBQaTZKUzBXVzZlZW5aT
lVwZWZzVXBmOGVKK3kwSXhHZ3RncEJ2MUhSSG9leTd2MDBBbWVJclNEa3VPN2FkbDhTOTlQR2VSdUhUUWV5bzBodWpjYVQ2RlBTS
3VhZklDNThmN25YUUdGVlorSVliRm1kUzlmSTdCRGxna2EiLCJtYWMiOiI1ODM2ZmZlNWNmNjBlM2ZlMTQ2MWU4YmE2MzA3OTAzM
TgxMzIyY2U0ZDNhOTRkYWQ0ZGFiYzNjOGYwN2ZiMjJiIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

## References

MDN | iframe: The Inline Frame Element
https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe

HTML Standard: iframe
https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element

HTML 5.2: 4.7. Embedded content
https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox

# Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

## Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

## https://globaltaxnyc.ssbmultiservices.com/

Possible sensitive files:

- https://globaltaxnyc.ssbmultiservices.com/**web.config**

### Request

```
GET /web.config HTTP/1.1
Accept: whaslene/fjye
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6IlJ1VU9kTTN1b3VzQlVsb1hCREcva2c9PSIsInZhbHVlIjoiM2ZTOS9HcmZYZW1xTFoySmV4UTVBRk80eXExN1
dkSXcyUnRRSkxJMlRtazJnSmJCVFQ0bkxxTjRPeVE3NVBmcjlvcTZpd1FlYXpqRjdaL1FkUno4VmJmclY1RlB4dXJMcTcvVC8wdj
NuNHNqaElUVGoySzZLeVJaRG8yZm5kNjciLCJtYWMiOiI2M2Y2MGRhYmI5MDE1YTg4YmU5MWMxNjQ0YWFiNDBiNzI2NTU5MmVmYz
VhMWRhZWVlMzMwZWE3N2YxMzY5ZDJhIiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6IjM3N3ZBOE9jQXZlWUtvZXlLblJXQ2c9PSIsInZhbHVlIjoicG16U25iVHNJWWhRZ1BRN0E5R
WZiQ0lWc2wyYUlleUw4TFBJQlJQQldNcUhWd0ZBanZQcE0rcEZWdWc1d2VRa2RySkNhbzVkWEN0ZlBmejhnYS9iWlNSeVM3MlpmY
nFEa2tYNmw5NEJoaG54SEdzdGd5OEJvanptaFR6QS9EelIiLCJtYWMiOiJjZDlkNDE5OTM2ODAwYmYyN2NlYzFhNDdlNDBlM2I3M
zQxOTE1NTFlNDA3MjU3YmRjMTIzNjY4NzRmMmQ2ZDA4IiwidGFnIjoiIn0%3D
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Restrict access to this file or remove it from the website.

### References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

# Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

## Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

### https://globaltaxnyc.ssbmultiservices.com/

Paths without CSP header:

- https://globaltaxnyc.ssbmultiservices.com/
- https://globaltaxnyc.ssbmultiservices.com/upload/header-footer/
- https://globaltaxnyc.ssbmultiservices.com/about-us

- https://globaltaxnyc.ssbmultiservices.com/archives
- https://globaltaxnyc.ssbmultiservices.com/consultation
- https://globaltaxnyc.ssbmultiservices.com/contact-us
- https://globaltaxnyc.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020
- https://globaltaxnyc.ssbmultiservices.com/immigration
- https://globaltaxnyc.ssbmultiservices.com/index.php
- https://globaltaxnyc.ssbmultiservices.com/irs-publications
- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us
- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator
- https://globaltaxnyc.ssbmultiservices.com/latest-issues
- https://globaltaxnyc.ssbmultiservices.com/make-payment
- https://globaltaxnyc.ssbmultiservices.com/subscribe
- https://globaltaxnyc.ssbmultiservices.com/tax-accounting
- https://globaltaxnyc.ssbmultiservices.com/where-refund
- https://globaltaxnyc.ssbmultiservices.com/tax-form
- https://globaltaxnyc.ssbmultiservices.com/tax-rates
- https://globaltaxnyc.ssbmultiservices.com/project/vendor/autoload.php

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
```

```
Connection: Keep-alive
```

### Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

### References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

# Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

### Impact

None

### https://globaltaxnyc.ssbmultiservices.com/ Verified

Pages where the content-type header is not specified:

- https://globaltaxnyc.ssbmultiservices.com/web.config
- https://globaltaxnyc.ssbmultiservices.com/project/.env
- https://globaltaxnyc.ssbmultiservices.com/project/composer.lock
- https://globaltaxnyc.ssbmultiservices.com/project/docker-compose.yml

#### Request

```
GET /web.config HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6InE0Wm1nZFYvYWhYVHdUOG0zSHNTOWc9PSIsInZhbHVlIjoiYVFlUEo3bXdPa3E0RkhCY0NZTW9uc3BFM05aen
lUVjhETnpveWg3Y1ZXN3lTSzZQRkhmTStER01iaDV4SDN3dFVQbElhMlBwWldwa2llRk9yN1lJQ1loYkF0U3EyMXgxVWEwbE81Tm
```

```
Y1OFpIeit4VTVQYmtiZUpBbkxVcjRvUmYiLCJtYWMiOiI1MzAxMDc4OGJiOGZlNmQwZDMzZmFjYjY5ZjhjNmM3ZmJhMzk2YTNjZW
M1NjBhMzU0M2E3MTUxOWNlZWMyZTA0IiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImpPVVkyWnR1d0N0NjZFbE52L0RLSGc9PSIsInZhbHVlIjoicG16bktGVFJEQjc2VWg5QjRNT
FEyY1BuVEZySksxOFFtd1pRRzMyUXdNMWcyWFhWcTVuSTEzYjU2Y2c2VGM5RHRIaVB3NjFYRWxUTC9UM3BGY1V2NUMya0NDK0hyV
HFPK2JuSVRzWGF5bm9ubVN1REN6QXdzRjJFLzdWbWJnRW8iLCJtYWMiOiI5NWMyNDJkZjI4OTg0YTVlZWMwYWQxZjVlNDBhM2Q1N
2FiYzZhNDAyYzFlYWM3OGViM2NjYTRkMDgxMGI1YTBiIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Set a Content-Type header value for these page(s).

# Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

### Impact

Email addresses posted on Web sites may attract spam.

### https://globaltaxnyc.ssbmultiservices.com/

Emails found:

- https://globaltaxnyc.ssbmultiservices.com/
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/about-us
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/archives
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/consultation
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/contact-us
  **globaloffice2006@gmail.com**

- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/immigration
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/index.php
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/irs-publications
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/latest-issues
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/make-payment
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/make-payment
  **abc@yahoo.com**
- https://globaltaxnyc.ssbmultiservices.com/subscribe
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/tax-accounting
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/where-refund
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/tax-form
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/tax-rates
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/archives/index.php
  **globaloffice2006@gmail.com**
- https://globaltaxnyc.ssbmultiservices.com/index.php/archives
  **globaloffice2006@gmail.com**

### Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Check references for details on how to solve this problem.

### References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

# Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

## Impact

Consult References for more information.

### https://globaltaxnyc.ssbmultiservices.com/ Confidence: 95%

- **jQuery 3.5.1**
  - URL: https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js
  - Detection method: The library's name and version were determined based on the file's CDN URI.
  - References:
    - https://code.jquery.com/

#### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### https://globaltaxnyc.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 4.5.2**
  - URL: https://globaltaxnyc.ssbmultiservices.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.

- References:
  - https://github.com/twbs/bootstrap/releases

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

Upgrade to the latest version.

# Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

## Impact

### https://globaltaxnyc.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://globaltaxnyc.ssbmultiservices.com/
- https://globaltaxnyc.ssbmultiservices.com/upload/header-footer/
- https://globaltaxnyc.ssbmultiservices.com/about-us
- https://globaltaxnyc.ssbmultiservices.com/archives
- https://globaltaxnyc.ssbmultiservices.com/consultation
- https://globaltaxnyc.ssbmultiservices.com/contact-us
- https://globaltaxnyc.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globaltaxnyc.ssbmultiservices.com/archives/May%202020
- https://globaltaxnyc.ssbmultiservices.com/immigration
- https://globaltaxnyc.ssbmultiservices.com/index.php
- https://globaltaxnyc.ssbmultiservices.com/irs-publications
- https://globaltaxnyc.ssbmultiservices.com/index.php/about-us
- https://globaltaxnyc.ssbmultiservices.com/irs-withholding-calculator
- https://globaltaxnyc.ssbmultiservices.com/latest-issues

- https://globaltaxnyc.ssbmultiservices.com/make-payment
- https://globaltaxnyc.ssbmultiservices.com/subscribe
- https://globaltaxnyc.ssbmultiservices.com/tax-accounting
- https://globaltaxnyc.ssbmultiservices.com/where-refund
- https://globaltaxnyc.ssbmultiservices.com/tax-form
- https://globaltaxnyc.ssbmultiservices.com/tax-rates
- https://globaltaxnyc.ssbmultiservices.com/project/vendor/autoload.php

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

# Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

### Impact

Possible sensitive information disclosure.

### https://globaltaxnyc.ssbmultiservices.com/

Pages with paths being disclosed:

- https://globaltaxnyc.ssbmultiservices.com/subscribe-action **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/swiftmailer/swiftmailer/lib/classes/Swift/Transport/Esmtp/AuthHandler.php**
- https://globaltaxnyc.ssbmultiservices.com/where-refund **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globaltaxnyc.ssbmultiservices.com/tax-form **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globaltaxnyc.ssbmultiservices.com/subscribe-action **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globaltaxnyc.ssbmultiservices.com/index.php/subscribe-action **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globaltaxnyc.ssbmultiservices.com/index.php/tax-form **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globaltaxnyc.ssbmultiservices.com/index.php/where-refund **/home/ssbmul5/globaltaxnyc.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**

### Request

```
POST /subscribe-action HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/subscribe
Cookie: PHPSESSID=1163fd80abb18e7769abf6a9579703dd; XSRF-
TOKEN=eyJpdiI6ImJyRGx3MUU1MUdJcjZ1cE01R1NjbFE9PSIsInZhbHVlIjoieGRzWWxERWdBaEtvUHpuZ2tybHlZREFLNzNNOG
NDdXdyYnFKbzR4Z3hnVzdVOUt0VFNJZ3BNWWtaWW01dTBIdlVPUk9YeWFCN1pNdHFNcENYWjlSakh6RDhvV1liMnVNUGJCbnFkaH
c4QitKTFJCR1oweEZBeVA4emtLV1diZXAiLCJtYWMiOiI0NmJkMjUzMjJiMjM1MTAzZGI1MTRiNGFhN2NmNDc1Mzg5YTc5ZTAzMT
lhYzdjZjFlZGYwY2MxODNmZTlkZjQwIiwidGFnIjoiIn0%3D;
global_tax_session=eyJpdiI6ImJwUEdmb0lGdTNJdmRQZGtXYUk0cVE9PSIsInZhbHVlIjoiVDJ4ZytMMFp5VlBIZTY0SnJBS
nNKbzhzMnRMVU9oSjlrbW83WUxKY2k5YXJURi9oWFlpUVFQbS8xMHBPdTFqWUNtYTZ4MG9kdXZxWGJRK3VJYW1HUnJ4QURRYklJe
FFSbnRJa2tzWmlpWnplTkQxaGdUYmRPOEhvMTQvbFA2dlgiLCJtYWMiOiI2NmI4YTM5Y2ZkMzJjNDcyMTZiZjczOTBmY2M2NWQxM
GQ3NWI5Nzg1MzYyODYzYTVjOTdmMjU4NWE5ODE2YjA5IiwidGFnIjoiIn0%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 114
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive

_token=vUCRxTKPMsDnaxxc9p2QiHr6YfGMC5rUaDFDtdl9&email=testing%40example.com&first_name=BzenyKyK&last
_name=BzenyKyK
```

## Recommendation

Prevent this information from being displayed to the user.

### References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

# Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

## Impact

No impact is associated with this vulnerability.

### https://globaltaxnyc.ssbmultiservices.com/

Detected reverse proxy: Apache httpd

#### Request

```
GET / HTTP/1.1
Max-Forwards: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

None

# Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing

developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

## Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

## https://globaltaxnyc.ssbmultiservices.com/

Pages where SRI is not implemented:

- https://globaltaxnyc.ssbmultiservices.com/
  Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js**

- https://globaltaxnyc.ssbmultiservices.com/
  Script SRC: **https://cdnjs.cloudflare.com/ajax/libs/lightgallery/1.9.0/js/lightgallery-all.min.js**

- https://globaltaxnyc.ssbmultiservices.com/
  Script SRC: **https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js**

### Request

```
GET / HTTP/1.1
Referer: https://globaltaxnyc.ssbmultiservices.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: globaltaxnyc.ssbmultiservices.com
Connection: Keep-alive
```

## Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

## References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

## Coverage

- https://globaltaxnyc.ssbmultiservices.com
  - Inputs
    - GET iv, value, mac, tag
  - _ignition
    - Inputs
      - GET iv, value, mac, tag
    - health-check
      - Inputs
        - GET iv, value, mac, tag
  - archives
    - Inputs
      - GET iv, value, mac, tag
    - index.php
      - Inputs
        - GET iv, value, mac, tag
    - May%202020
      - Inputs
        - GET iv, value, mac, tag
    - May%202021
      - Inputs
        - GET iv, value, mac, tag
  - assets
    - Inputs
      - GET iv, value, mac, tag
    - admin
      - Inputs
        - GET iv, value, mac, tag
    - front
      - Inputs
        - GET iv, value, mac, tag
      - css

- style.css
- fonts
  - fontawesome
    - css
      - all.css
    - webfonts
      - Inputs
        - GET iv, value, mac, tag
- image
  - client
    - Inputs
      - GET iv, value, mac, tag
  - recognized-by
    - Inputs
      - GET iv, value, mac, tag
- js
  - google.translate.js
  - main.js
  - sweet-alert.min.js
- logo
  - Inputs
    - GET iv, value, mac, tag
- owl-carousel
  - owl.carousel.min.css
  - owl.carousel.min.js

- cgi-sys
  - Inputs
    - GET iv, value, mac, tag
- database
  - Inputs
    - GET iv, value, mac, tag
- index.php
  - Inputs

- GET iv, value, mac, tag
- archives
  - Inputs
    - GET iv, value, mac, tag
  - May%202020
    - Inputs
      - GET iv, value, mac, tag
  - May%202021
    - Inputs
      - GET iv, value, mac, tag
- about-us
  - Inputs
    - GET iv, value, mac, tag
- archives
  - Inputs
    - GET iv, value, mac, tag
- consultation
  - Inputs
    - GET iv, value, mac, tag
- contact-us
  - Inputs
    - GET iv, value, mac, tag
    - POST iv, value, mac, tag
    - POST _token, email, message, name, phone, submit
- immigration
  - Inputs
    - GET iv, value, mac, tag
- index.php
  - Inputs
    - GET iv, value, mac, tag
- irs-publications
  - Inputs
    - GET iv, value, mac, tag

- irs-withholding-calculator
  - Inputs
    - GET iv, value, mac, tag
- latest-issues
  - Inputs
    - GET iv, value, mac, tag
- make-payment
  - Inputs
    - GET iv, value, mac, tag
- record-retention-guide
  - Inputs
    - GET iv, value, mac, tag
- subscribe
  - Inputs
    - GET iv, value, mac, tag
- subscribe-action
  - Inputs
    - POST iv, value, mac, tag
    - POST _token, email, first_name, last_name
    - GET iv, value, mac, tag
- tax-accounting
  - Inputs
    - GET iv, value, mac, tag
- tax-appointment-checklist
  - Inputs
    - GET iv, value, mac, tag
- tax-form
  - Inputs
    - POST iv, value, mac, tag
    - POST states
    - GET iv, value, mac, tag
- tax-rates
  - Inputs
    - GET iv, value, mac, tag

- where-refund
  - Inputs
    - POST iv, value, mac, tag
    - POST states
    - GET iv, value, mac, tag
- mailman
  - Inputs
    - GET iv, value, mac, tag
- project
  - Inputs
    - GET iv, value, mac, tag
  - config
    - Inputs
      - GET iv, value, mac, tag
  - database
    - Inputs
      - GET iv, value, mac, tag
  - resources
    - Inputs
      - GET iv, value, mac, tag
  - storage
    - Inputs
      - GET iv, value, mac, tag
  - tests
    - Inputs
      - GET iv, value, mac, tag
  - vendor
    - Inputs
      - GET iv, value, mac, tag
    - bin
      - Inputs
        - GET iv, value, mac, tag
    - autoload.php

Inputs

GET iv, value, mac, tag

.env

Inputs

GET iv, value, mac, tag

composer.json

Inputs

GET iv, value, mac, tag

composer.lock

Inputs

GET iv, value, mac, tag

docker-compose.yml

Inputs

GET iv, value, mac, tag

package.json

Inputs

GET iv, value, mac, tag

upload

Inputs

GET iv, value, mac, tag

header-footer

Inputs

GET iv, value, mac, tag

service-photo

Inputs

GET iv, value, mac, tag

slider-image

Inputs

GET iv, value, mac, tag

team-member-image

Inputs

GET iv, value, mac, tag

_ignition

- Inputs
  - GET iv, value, mac, tag

- about-us
  - Inputs
    - GET iv, value, mac, tag

- archives
  - Inputs
    - GET iv, value, mac, tag

- consultation
  - Inputs
    - GET iv, value, mac, tag

- contact-us
  - Inputs
    - GET iv, value, mac, tag
    - POST iv, value, mac, tag
    - POST _token, email, message, name, phone, submit

- immigration
  - Inputs
    - GET iv, value, mac, tag

- index.php
  - Inputs
    - GET iv, value, mac, tag

- irs-publications
  - Inputs
    - GET iv, value, mac, tag

- irs-withholding-calculator
  - Inputs
    - GET iv, value, mac, tag

- latest-issues
  - Inputs
    - GET iv, value, mac, tag

- make-payment
  - Inputs
    - GET iv, value, mac, tag

- record-retention-guide
  - Inputs
    - GET iv, value, mac, tag
- robots.txt
  - Inputs
    - GET iv, value, mac, tag
- subscribe
  - Inputs
    - GET iv, value, mac, tag
- subscribe-action
  - Inputs
    - POST iv, value, mac, tag
    - POST _token, email, first_name, last_name
    - GET iv, value, mac, tag
- tax-accounting
  - Inputs
    - GET iv, value, mac, tag
- tax-appointment-checklist
  - Inputs
    - GET iv, value, mac, tag
- tax-form
  - Inputs
    - POST iv, value, mac, tag
    - POST states
    - GET iv, value, mac, tag
- tax-rates
  - Inputs
    - GET iv, value, mac, tag
- web.config
  - Inputs
    - GET iv, value, mac, tag
- where-refund
  - Inputs