Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 3

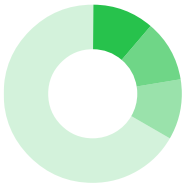
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	globalgroupny.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 2, 2024, 12:26:06 PM GMT+8
Scan Duration	1 hour, 3 minutes
Requests	194840
Average Response Time	33ms
Maximum Response Time	7380ms
Application Build	v23.7.230728157

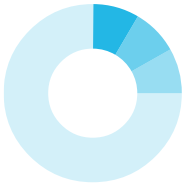
Severity	Vulnerabilities	Instances
High	1	1
Medium	4	4
Low	11	12
Informational	8	9
Total	24	26

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	9

Medium Severity

	Instances
Development configuration files	1
Directory listings	1
Laravel debug mode enabled	1
Others	1

High Severity

	Instances
Vulnerable package dependencies [high]	1

Impacts

SEVERITY	IMPACT	
High	1	Vulnerable package dependencies [high]
Medium	1	Development configuration files
Medium	1	Directory listings
Medium	1	Laravel debug mode enabled
Medium	1	Vulnerable package dependencies [medium]
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	Documentation files
Low	1	HTTP Strict Transport Security (HSTS) not implemented
Low	2	Insecure Inline Frame (iframe)
Low	1	Passive Mixed Content over HTTPS
Low	1	Possible sensitive directories
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

SEVERITY	IMPACT	
Informational	1	Possible server path disclosure (Unix)
Informational	1	Reverse proxy detected

Vulnerable package dependencies [high]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

https://globalgroupny.ssbmultiservices.com/project/

List of vulnerable **composer** packages:

Package: guzzlehttp/guzzle
Version: 7.4.0
CVE: CVE-2022-29248
Title: Reliance on Cookies without Validation and Integrity Checking
Description: Guzzle is a PHP HTTP client. Guzzle prior to versions 6.5.6 and 7.4.3 contains a vulnerability with the cookie middleware. The vulnerability is that it is not checked if the cookie domain equals the domain of the server which sets the cookie via the Set-Cookie header, allowing a malicious server to set cookies for unrelated domains. The cookie middleware is disabled by default, so most library consumers will not be affected by this issue. Only those who manually add the cookie middleware to the handler stack or construct the client with ['cookies' => true] are affected. Moreover, those who do not use the same Guzzle client to call multiple domains and have disabled redirect forwarding are not affected by this vulnerability. Guzzle versions 6.5.6 and 7.4.3 contain a patch for this issue. As a workaround, turn off the cookie middleware.
CVSS V2: AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
CWE: CWE-565
References:

- https://github.com/guzzle/guzzle/commit/74a8602c6faec9ef74b7a9391ac82c5e65b1cdab
- https://github.com/guzzle/guzzle/pull/3018
- https://github.com/guzzle/guzzle/security/advisories/GHSA-cwmx-hcrq-mhc3
- https://www.drupal.org/sa-core-2022-010
- https://www.debian.org/security/2022/dsa-5246

Package: guzzlehttp/guzzle
Version: 7.4.0
CVE: CVE-2022-31043
Title: Improper Removal of Sensitive Information Before Storage or Transfer
Description: Guzzle is an open source PHP HTTP client. In affected versions `Authorization` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a

URI with the `http` scheme, we should not forward the `Authorization` header on. This is much the same as to how we don't forward on the header if the host changes. Prior to this fix, `https` to `http` downgrades did not result in the `Authorization` header being removed, only changes to the host. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach which would be to use their own redirect middleware. Alternately users may simply disable redirects all together if redirects are not expected or required.
CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: CWE-212
References:

- https://github.com/guzzle/guzzle/security/advisories/GHSA-w248-ffj2-4v5q
- https://github.com/guzzle/guzzle/commit/e3ff079b22820c2029d4c2a87796b6a0b8716ad8
- https://www.rfc-editor.org/rfc/rfc9110.html#name-redirection-3xx
- https://www.drupal.org/sa-core-2022-011
- https://www.debian.org/security/2022/dsa-5246

Package: guzzlehttp/guzzle
Version: 7.4.0
CVE: CVE-2022-31091
Title: Exposure of Sensitive Information to an Unauthorized Actor
Description: Guzzle, an extensible PHP HTTP client. `Authorization` and `Cookie` headers on requests are sensitive information. In affected versions on making a request which responds with a redirect to a URI with a different port, if we choose to follow it, we should remove the `Authorization` and `Cookie` headers from the request, before containing. Previously, we would only consider a change in host or scheme. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. An alternative approach would be to use your own redirect middleware, rather than ours, if you are unable to upgrade. If you do not require or expect redirects to be followed, one should simply disable redirects all together.
CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
CWE: CWE-200
References:

- https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fbd82
- https://github.com/guzzle/guzzle/security/advisories/GHSA-q559-8m2m-g699
- https://www.debian.org/security/2022/dsa-5246
- https://security.gentoo.org/glsa/202305-24

Package: guzzlehttp/guzzle
Version: 7.4.0
CVE: CVE-2022-31090
Title: Improper Removal of Sensitive Information Before Storage or Transfer
Description: Guzzle, an extensible PHP HTTP client. `Authorization` headers on requests are sensitive information. In affected versions when using our Curl handler, it is possible to use the `CURLOPT_HTTPAUTH` option to specify an

`Authorization` header. On making a request which responds with a redirect to a URI with a different origin (change in host, scheme or port), if we choose to follow it, we should remove the `CURLOPT_HTTPAUTH` option before continuing, stopping curl from appending the `Authorization` header to the new request. Affected Guzzle 7 users should upgrade to Guzzle 7.4.5 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.8 or 7.4.5. Note that a partial fix was implemented in Guzzle 7.4.2, where a change in host would trigger removal of the curl-added Authorization header, however this earlier fix did not cover change in scheme or change in port. If you do not require or expect redirects to be followed, one should simply disable redirects all together. Alternatively, one can specify to use the Guzzle steam handler backend, rather than curl.
CVSS V2: AV:N/AC:L/Au:S/C:P/I:N/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
CWE: CWE-212
References:

- https://github.com/guzzle/guzzle/commit/1dd98b0564cb3f6bd16ce683cb755f94c10fbd82
- https://github.com/guzzle/guzzle/security/advisories/GHSA-25mq-v84q-4j7r
- https://www.debian.org/security/2022/dsa-5246
- https://security.gentoo.org/glsa/202305-24

Package: guzzlehttp/guzzle
Version: 7.4.0
CVE: CVE-2022-31042
Title: Improper Removal of Sensitive Information Before Storage or Transfer
Description: Guzzle is an open source PHP HTTP client. In affected versions the `Cookie` headers on requests are sensitive information. On making a request using the `https` scheme to a server which responds with a redirect to a URI with the `http` scheme, or on making a request to a server which responds with a redirect to a a URI to a different host, we should not forward the `Cookie` header on. Prior to this fix, only cookies that were managed by our cookie middleware would be safely removed, and any `Cookie` header manually added to the initial request would not be stripped. We now always strip it, and allow the cookie middleware to re-add any cookies that it deems should be there. Affected Guzzle 7 users should upgrade to Guzzle 7.4.4 as soon as possible. Affected users using any earlier series of Guzzle should upgrade to Guzzle 6.5.7 or 7.4.4. Users unable to upgrade may consider an alternative approach to use your own redirect middleware, rather than ours. If you do not require or expect redirects to be followed, one should simply disable redirects all together.
CVSS V2: AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE: CWE-212
References:

- https://github.com/guzzle/guzzle/security/advisories/GHSA-f2wf-25xc-69c9
- https://github.com/guzzle/guzzle/commit/e3ff079b22820c2029d4c2a87796b6a0b8716ad8
- https://www.rfc-editor.org/rfc/rfc9110.html#name-redirection-3xx
- https://www.drupal.org/sa-core-2022-011
- https://www.debian.org/security/2022/dsa-5246

Package: guzzlehttp/psr7
Version: 2.1.0
CVE: CVE-2022-24775

Title: Improper Input Validation
Description: guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds.
CVSS V2: AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE: CWE-20
References:

- https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96
- https://github.com/guzzle/psr7/pull/485/commits/e55afaa3fc138c89adf3b55a8ba20dc60d17f1f1
- https://github.com/guzzle/psr7/pull/486/commits/9a96d9db668b485361ed9de7b5bf1e54895df1dc
- https://www.drupal.org/sa-core-2022-006

Package: guzzlehttp/psr7
Version: 2.1.0
CVE: CVE-2023-29197
Title: Interpretation Conflict
Description: guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Affected versions are subject to improper header parsing. An attacker could sneak in a newline (\n) into both the header names and values. While the specification states that \r\n\r\n is used to terminate the header list, many servers in the wild will also accept \n\n. This is a follow-up to CVE-2022-24775 where the fix was incomplete. The issue has been patched in versions 1.9.1 and 2.4.5. There are no known workarounds for this vulnerability. Users are advised to upgrade.
CVSS V2:
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE: CWE-436
References:

- https://github.com/guzzle/psr7/security/advisories/GHSA-q7rv-6hp3-vh96
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-24775
- https://github.com/guzzle/psr7/security/advisories/GHSA-wxmh-65f7-jcvw
- https://www.rfc-editor.org/rfc/rfc7230#section-3.2.4
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/O35UN4IK6VS2LXSRWUDFWY7NI73RKY2U/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/FJANWDXJZE5BGLN4MQ4FEHV5LJ6CMKQF/

Package: symfony/http-kernel
Version: 5.3.10
CVE: CVE-2022-24894
Title: Improper Authorization
Description: Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The Symfony HTTP cache system, acts as a reverse proxy: It caches entire responses (including headers) and returns them to the clients. In a recent change in the `AbstractSessionListener`, the response might contain a `Set-Cookie` header. If the Symfony HTTP cache system is enabled, this response might bill stored and return to the next clients. An attacker can use this vulnerability to retrieve the victim's session. This issue has been patched and is available for

branch 4.4.

CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE: CWE-285

References:

- https://github.com/symfony/symfony/commit/d2f6322af9444ac5cd1ef3ac6f280dbef7f9d1fb
- https://github.com/symfony/symfony/security/advisories/GHSA-h7vf-5wrv-9fhv
- https://lists.debian.org/debian-lts-announce/2023/07/msg00014.html

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

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://globalgroupny.ssbmultiservices.com/

Development configuration files:

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

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

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

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

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

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

- https://globalgroupny.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=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6InNrMVJyTkpodmtvTnpmeG04U1R6OFE9PSIsInZhbHVlIjoiRFJKbjNmbm5JZXI5dU40UWVXYU5uYmgzY1dLTm
tPUWZCbkhtOEU2aE1oMTdXQmZnYUhldVhrUndGZ3Zib0FpQzZkUWNIZDBQMG9xbUJqdC9HZU9zd0loVlZyVTlpN3VBZ1E3Q2lCcn
Y1Ly9maU9LVlVKcGZTTFh4N3ljeTRYRlQiLCJtYWMiOiIzYjc3ZDIwODEzOGYwZTg5ZGZlOTJmZWVhNGFhZDIxNzAwMTI1MTFkYT
Q0OThhZGViZDUzYTk1NGVmZmVkZDk2IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6IktMN2hldjE4ZXo5d3ZFOGQyTFdTSVE9PSIsInZhbHVlIjoiRUdQVVZxR0owbFZGdDJjT
3VRVFBHaTJlUFZCeGI2UDV0ZExrVW5GNDZid2FFRjlmRjR0TDV0NjZNdWdPR1VFZHpIanJSQ2JkZXY5ekdGTUl6eEM4S3h4TzhJT
y9QTkxYSjI2ZmtVT29QbWNDVHlVc3ZYUlR2QVNqTThwN2o3T3QiLCJtYWMiOiJlOTNlN2VjNTY4NDY5NGY5NDRmMjk4MmFmYzAwM
2Y3NzhiZTA3NWZkYzlmMTA0MzI4ZjIwYzliZjU2M2Q2ODM2IiwidGFnIjoiIn0%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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

https://globalgroupny.ssbmultiservices.com/ Verified

Folders with directory listing enabled:

- https://globalgroupny.ssbmultiservices.com/assets/
- https://globalgroupny.ssbmultiservices.com/assets/front/
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/

- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://globalgroupny.ssbmultiservices.com/assets/front/css/
- https://globalgroupny.ssbmultiservices.com/upload/
- https://globalgroupny.ssbmultiservices.com/upload/client-review/
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globalgroupny.ssbmultiservices.com/project/
- https://globalgroupny.ssbmultiservices.com/project/vendor/
- https://globalgroupny.ssbmultiservices.com/upload/header-footer/
- https://globalgroupny.ssbmultiservices.com/project/vendor/asm89/
- https://globalgroupny.ssbmultiservices.com/upload/real-state/
- https://globalgroupny.ssbmultiservices.com/project/vendor/asm89/stack-cors/
- https://globalgroupny.ssbmultiservices.com/upload/service-photo/
- https://globalgroupny.ssbmultiservices.com/assets/front/image/
- https://globalgroupny.ssbmultiservices.com/assets/front/image/recognized-by/
- https://globalgroupny.ssbmultiservices.com/upload/slider-image/
- https://globalgroupny.ssbmultiservices.com/upload/post-image/
- https://globalgroupny.ssbmultiservices.com/assets/front/js/

Request

```
GET /assets/ HTTP/1.1
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6IkEwTk43enVXeDJFdlN5TGVJeFIwOGc9PSIsInZhbHVlIjoiNTQyYWY0RnNVOXVsUjFIcENFdTNGYTBLTXhWVE
t6eW16STg3YlN1V3A1VUlGUWo3Z24wdEtqYnJUait6VlpPZ3hoQ1V4UmY5NTBtemxQbkdublphVXFGcWdObElTaTNqeTFUQ1pZRE
xVVVRENm9ZODlXKy81NDB4NUowOG5EN3UiLCJtYWMiOiI0ZmUzNjExNTcxMjQ4ZjgwNzFmZjY3ZjVkMjU4ODRhODkyOTBjNDg2Nj
g1OWI5YzM0Njk0NDE0ZTYyMmRlNmRiIiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6ImQzTHNWUW94Nm10SnAvUE9KVjhDTnc9PSIsInZhbHVlIjoiL0pmUmlGeFUxYVk5N0dmZ
U1VN2g5bThPTGFScEpWU0EwMkd2eitqYkszQllPNzRzci9ORHpDS01oWUtwbkxNeWxCRUZBenJPb0k4dDdiUmV1bzJ1YVZOSTllZ
3YzZmlUSnNIcFc4K1lCOGtnNWlaM3Z4ek1VenhYMTloRlU4VlIiLCJtYWMiOiI0NjRhOTg5NGYwYjFiMWVkNGIwY2YxNmVhYWMzN
TkyNzkyY2NiZmI1ODRmN2MxNjRjMGViN2E4YzM3ZDY3OWE1IiwidGFnIjoiIn0%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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

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://globalgroupny.ssbmultiservices.com/

Request

```
PUT /index.php HTTP/1.1
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6IkEwTk43enVXeDJFdlN5TGVJeFIwOGc9PSIsInZhbHVlIjoiNTQyYWY0RnNVOXVsUjFIcENFdTNGYTBLTXhWVE
t6eW16STg3YlN1V3A1VUlGUWo3Z24wdEtqYnJUait6VlpPZ3hoQ1V4UmY5NTBtemxQbkdublphVXFGcWdObElTaTNqeTFUQ1pZRE
xVVVRENm9ZODlXKy81NDB4NUowOG5EN3UiLCJtYWMiOiI0ZmUzNjExNTcxMjQ4ZjgwNzFmZjY3ZjVkMjU4ODRhODkyOTBjNDg2Nj
g1OWI5YzM0Njk0NDE0ZTYyMmRlNmRiIiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6ImQzTHNWUW94Nm10SnAvUE9KVjhDTnc9PSIsInZhbHVlIjoiL0pmUmlGeFUxYVk5N0dmZ
U1VN2g5bThPTGFScEpWU0EwMkd2eitqYkszQllPNzRzci9ORHpDS01oWUtwbkxNeWxCRUZBenJPb0k4dDdiUmV1bzJ1YVZOSTllZ
3YzZmlUSnNIcFc4K1lCOGtnNWlaM3Z4ek1VenhYMTloRlU4VlIiLCJtYWMiOiI0NjRhOTg5NGYwYjFiMWVkNGIwY2YxNmVhYWMzN
TkyNzkyY2NiZmI1ODRmN2MxNjRjMGViN2E4YzM3ZDY3OWE1IiwidGFnIjoiIn0%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: globalgroupny.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

Vulnerable package dependencies [medium]

One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.

Impact

The impact of this vulnerability is different for each vulnerable package. It's recommended to investigate each vulnerable package individually.

https://globalgroupny.ssbmultiservices.com/project/

List of vulnerable **composer** packages:

Package: laravel/framework
Version: 8.69.0
CVE: CVE-2021-43808
Title: Use of a Broken or Risky Cryptographic Algorithm
Description: Laravel is a web application framework. Laravel prior to versions 8.75.0, 7.30.6, and 6.20.42 contain a possible cross-site scripting (XSS) vulnerability in the Blade templating engine. A broken HTML element may be clicked and the user taken to another location in their browser due to XSS. This is due to the user being able to guess the parent placeholder SHA-1 hash by trying common names of sections. If the parent template contains an exploitable HTML structure an XSS vulnerability can be exposed. This vulnerability has been patched in versions 8.75.0, 7.30.6, and 6.20.42 by determining the parent placeholder at runtime and using a random hash that is unique to each request.
CVSS V2: AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-327
References:

- https://github.com/laravel/framework/releases/tag/v6.20.42
- https://github.com/laravel/framework/commit/b8174169b1807f36de1837751599e2828ceddb9b
- https://github.com/laravel/framework/pull/39909
- https://github.com/laravel/framework/pull/39908
- https://github.com/laravel/framework/security/advisories/GHSA-66hf-2p6w-jqfw
- https://github.com/laravel/framework/pull/39906
- https://github.com/laravel/framework/releases/tag/v7.30.6
- https://github.com/laravel/framework/releases/tag/v8.75.0

Package: symfony/http-kernel
Version: 5.3.10
CVE: CVE-2021-41267
Title: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
Description: Symfony/Http-Kernel is the HTTP kernel component for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Headers that are not part of the "trusted_headers" allowed list

are ignored and protect users from "Cache poisoning" attacks. In Symfony 5.2, maintainers added support for the `X-Forwarded-Prefix` headers, but this header was accessible in SubRequest, even if it was not part of the "trusted_headers" allowed list. An attacker could leverage this opportunity to forge requests containing a `X-Forwarded-Prefix` header, leading to a web cache poisoning issue. Versions 5.3.12 and later have a patch to ensure that the `X-Forwarded-Prefix` header is not forwarded to subrequests when it is not trusted.

CVSS V2: AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

CWE: CWE-444

References:

- https://github.com/symfony/symfony/security/advisories/GHSA-q3j3-w37x-hq2q
- https://github.com/symfony/symfony/releases/tag/v5.3.12
- https://github.com/symfony/symfony/commit/95dcf51682029e89450aee86267e3d553aa7c487
- https://github.com/symfony/symfony/pull/44243

Recommendation

It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.

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://globalgroupny.ssbmultiservices.com/

Paths without secure XFO header:

- https://globalgroupny.ssbmultiservices.com/
- https://globalgroupny.ssbmultiservices.com/upload/client-review/
- https://globalgroupny.ssbmultiservices.com/archives
- https://globalgroupny.ssbmultiservices.com/blogs
- https://globalgroupny.ssbmultiservices.com/archives/May%202020
- https://globalgroupny.ssbmultiservices.com/consultation
- https://globalgroupny.ssbmultiservices.com/contact-us
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globalgroupny.ssbmultiservices.com/driving-school
- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
- https://globalgroupny.ssbmultiservices.com/immigration
- https://globalgroupny.ssbmultiservices.com/irs-withholding-calculator
- https://globalgroupny.ssbmultiservices.com/make-payment
- https://globalgroupny.ssbmultiservices.com/privacy-policy
- https://globalgroupny.ssbmultiservices.com/profile
- https://globalgroupny.ssbmultiservices.com/real-estate
- https://globalgroupny.ssbmultiservices.com/real-state-home
- https://globalgroupny.ssbmultiservices.com/tax-form
- https://globalgroupny.ssbmultiservices.com/subscribe
- https://globalgroupny.ssbmultiservices.com/tax-accounting
- https://globalgroupny.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/project/vendor/

Request

```
GET /project/vendor/composer/installed.json HTTP/1.1
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6InNrMVJyTkpodmtvTnpmeG04U1R6OFE9PSIsInZhbHVlIjoiRFJKbjNmbm5JZXI5dU40UWVXYU5uYmgzY1dLTm
tPUWZCbkhtOEU2aE1oMTdXQmZnYUhldVhrUndGZ3Zib0FpQzZkUWNIZDBQMG9xbUJqdC9HZU9zd0loVlZyVTlpN3VBZ1E3Q2lCcn
Y1Ly9maU9LVlVKcGZTTFh4N3ljeTRYRlQiLCJtYWMiOiIzYjc3ZDIwODEzOGYwZTg5ZGZlOTJmZWVhNGFhZDIxNzAwMTI1MTFkYT
Q0OThhZGViZDUzYTk1NGVmZmVkZDk2IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6IktMN2hldjE4ZXo5d3ZFOGQyTFdTSVE9PSIsInZhbHVlIjoiRUdQVVZxR0owbFZGdDJjT
3VRVFBHaTJlUFZCeGI2UDV0ZExrVW5GNDZid2FFRjlmRjR0TDV0NjZNdWdPR1VFZHpIanJSQ2JkZXY5ekdGTUl6eEM4S3h4TzhJT
y9QTkxYSjI2ZmtVT29QbWNDVHlVc3ZYUlR2QVNqTThwN2o3T3QiLCJtYWMiOiJlOTNlN2VjNTY4NDY5NGY5NDRmMjk4MmFmYzAwM
2Y3NzhiZTA3NWZkYzlmMTA0MzI4ZjIwYzliZjU2M2Q2ODM2IiwidGFnIjoiIn0%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: globalgroupny.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://globalgroupny.ssbmultiservices.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://globalgroupny.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; 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://globalgroupny.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=760adfa10beee4274a0990d30f8dd4c5; 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://globalgroupny.ssbmultiservices.com/archives

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=924d387f169f090d268516b461759d98; 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://globalgroupny.ssbmultiservices.com/blogs

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=974ae08f4c6f1d3a9e9535ed01904e8c; 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://globalgroupny.ssbmultiservices.com/cgi-sys/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=4ebf78686da651a05282664ba10a98c2; 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://globalgroupny.ssbmultiservices.com/contact-us

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=87ccca07e082685c3084e16edf4acbac; 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://globalgroupny.ssbmultiservices.com/consultation

  Cookie was set with:

```
Set-Cookie: PHPSESSID=a1ac5810e021861cca66e26d70288ffc; 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://globalgroupny.ssbmultiservices.com/subscribe-action

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=a9399812c82ad9f11b3fbf0096821b67; 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://globalgroupny.ssbmultiservices.com/driving-school

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d252cb3c78b62dd62e035e682f89ccf1; 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://globalgroupny.ssbmultiservices.com/immigration

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=4cd074b6821268ad2f4a7b749b403e82; 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://globalgroupny.ssbmultiservices.com/index.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=4540606fe0680a2eccdd2fe7207309c8; 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://globalgroupny.ssbmultiservices.com/irs-publications

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=cc42f0bef852314e7250e932a61795aa; 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://globalgroupny.ssbmultiservices.com/mailman/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=dda3c0d81f72d0c6ec00c1c7593fd2f2; 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://globalgroupny.ssbmultiservices.com/tax-form

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=fd957d54b927c0f69f0321a28e5e9efc; 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://globalgroupny.ssbmultiservices.com/make-payment

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=c1bf6170d9802ae968923153f671f318; 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://globalgroupny.ssbmultiservices.com/where-refund

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=343bcb111ff07479219ca7c3e0d21a82; 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://globalgroupny.ssbmultiservices.com/privacy-policy

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=a654651a45f8080247b80556b444d8a6; 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://globalgroupny.ssbmultiservices.com/profile

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=b5b4d0fd4f32e5c27afd92476416a53e; 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://globalgroupny.ssbmultiservices.com/real-estate

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=8727339810d3a168fcf241dc91e58300; 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://globalgroupny.ssbmultiservices.com/real-state-home

  Cookie was set with:

```
Set-Cookie: PHPSESSID=c0d10143e1a08937c39c17e95a68846b; 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://globalgroupny.ssbmultiservices.com/subscribe

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=81b87d6362e3ae7e16495218f205dc14; 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://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://globalgroupny.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; path=/
```

- https://globalgroupny.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkEwTk43enVXeDJFdlN5TGVJeFIwOGc9PSIsInZhbHVlIjoiNTQyYWY0RnNVOXVsUjF
IcENFdTNGYTBLTXhWVEt6eW16STg3YlN1V3A1VUlGUWo3Z24wdEtqYnJUait6VlpPZ3hoQ1V4UmY5NTBt
emxQbkdublphVXFGcWdObElTaTNqeTFUQ1pZRExVVVRENm9ZODlXKy81NDB4NUowOG5EN3UiLCJtYWMiO
iI0ZmUzNjExNTcxMjQ4ZjgwNzFmZjY3ZjVkMjU4ODRhODkyOTBjNDg2Njg1OWI5YzM0Njk0NDE0ZTYyMm
RlNmRiIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:26:08 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImVGWVdHR3JwcWdmYUR4dUhUa01MZ2c9PSIsInZhbHVlIjoiRU1EYysyaGUwSjVCT1U
xeGdoeXJPN0hsLzllNERtWXlUNy9hUFB0aGRSNkZUbTBlZ0R6QjhlMXlraWN1N0hySkh1c0xXVk1lZTBn
bmhSSnlrY3pGUVNUV0FzazBKelNqbXpTd1JHMWFROFhHV3BnQnpDZDR5WXNqTUcyaTV6QXoiLCJtYWMiO
iIwZTZkNTgyYjE0Yzg4MGM3YWU4ZGQ0YmQ1ODA5MDU0ODA2NjQzYjI2MmQ4MGEzMGYxZjQ1NzIzN2UxNz
VlNWExIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:58 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blogs

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjlrdkVQNXFCWHZQK2ZSMnVtN3R1TUE9PSIsInZhbHVlIjoicTNuUFJGQ0prVktXRzh
4SGtyV1V5Zm1NZkRzZDRSNWVLZ3Z6clRFOURraVdRZWhmU2gxdStMcE04ZHQ2aEQ0Tm5GSkhZcVZrUlBR
cFlCV0MxdSt3ck1vZkcvRHlHWTduL0xoTHFUYk5zenVDRFkraHJtT09uQ25GTWlNWkpJcFYiLCJtYWMiO
iJmNzU4MTJmMmU5MDkwM2E0ZWM2ODIxZWUxOTYyZmZiZDZmNjJhMGE5NmIxNjIwNmQ4ZDgwNmU2MjQzMG
QwZGQ1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:02 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImFMUHVBM3pMTk95UHNKeFdJTk1xSUE9PSIsInZhbHVlIjoiTmtUVVhwMEt2VldWT1F
ka0htaStMeUVSUVpjSFZFekxZdXFOdmFSM25KT2xINXJNR0FzOHVYRktwc1FwYllNU0tqY1pNdnlUckNM
YWR6M1piczF4RlB2RGZGQjVxWFJvZTZLc3NHMGhYV3VCRC9UYXlOK3Z6allmR2kyYUJwZVEiLCJtYWMiO
iI0ZTIyNDEwNjFjM2JiNjJkOWQxY2ExOWY5ZTRmOGIxZTRiOWI3NDVkOTA4Yjk0YzMyY2EyODhhYTQ1ZW
QyMTUyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:05 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImtrOHdHT3krV1lsQktldHZYNk5CZFE9PSIsInZhbHVlIjoicnpvMXJGY2FrQ3VpOGl
0cFZqOHByMk9wT3VuSVVGQTdrUTVRMTZaQjFTSkFOM1ZkMnZhbjhNbmpDYVYza2dTYmNBbGdiL0JsQ29P
L2RtNkl5NzF0UkZEUlR6L3liUG1OYkNlRmh5Rzl1dXQ5ZVhkZEU5SXhOSjRlZ0NZWEtESEciLCJtYWMiO
iJjZDNjMTQxZmFjNzU0YjMyNzkzOTc4ZmU2OTJlNTVlNjNmY2E5YjUxZDg1MWEzNjg0YzJmYWI2M2RmMT
Y4NDI0IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ii9GV2tJUldGcUQrNlJ2T1RxUGs4V2c9PSIsInZhbHVlIjoiWVFsN1Y2MzI1NmVYRlR
aMmpRWnh2MmRhMndFSExFUjdndTZ2b0RPakZUZmtlekp5bmg5dFltanE4K1dmeEx0QlIzU2V3UUw2M3F1
ZDluamdtUjRxREhEb0poblgyd3N2RW1uMWJpbEVmb25NVmdBWFZXblNkWmRNY29iVVdQTmciLCJtYWMiO
iI2NTg4NTZhNWM4MmE0YWViNGY4MjcxMmUwMWRkNDExMjg5NzA3YzYyOGI5ODg0YWRmODExNWNjMzlkZW
E5Zjg3IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/driving-school

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkJGckphQytjN1VXZktUM0RmNVUwelE9PSIsInZhbHVlIjoiZVBNK3lvc2N3WmoySmo
vbjJLMXhTbnhzaFZKKzZJZ2poR2tRc2d4bWhqRFZNNjdsZnc5ZG10dUVuakxKOENjK0ZCWEhKUkVxVE9p
R2NHMm5KUG1aRWhIZWdKbE5IcDA5L01NT3NkMzA2cUlwSnBEZnp0TUM1a2R6dzgyaGtDdSsiLCJtYWMiO
iIxOTJhMjhhOTAzMjY5ZGE5ZGQyNTE4ODRjZTRkYTM0ZWYzOTFhYTMxNTQ0MTM5ZmJiZWJkNGZkYjAzOT
czYmM5IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:15 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjR0Wi9heW96RXU0Zm5VRW51clVLTnc9PSIsInZhbHVlIjoiY2RSOWkwMHVjNk5uMGc
vbDNMRnA1Q0JUTVpCWnVKMVR5RUwzMDEyRFZWSHIxV2tnMk5OS25EU3BOYWhyZ3kyUEV0VGVPT1dvUVFh
Z3hMVm9UV04xOG9LTmxBdHBQTXVONVZRbG9vamcrMUk1OXhGZzNrdVFveDczR0U5RGhHd1YiLCJtYWMiO
iI2ZTU5MWYwNGY1ZTRkOWE2ZWY3OGQ0YTFkZDVjM2EwNmJlMDRlZjE5N2FjNWFmNGJlZTczNjcyOGEzNj
Q3ZDUwIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:22 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlBLVzZER3dLUHpoazZFeEU3d29mQmc9PSIsInZhbHVlIjoiRjJWQ1RvTkQwY1laUmh
xcHlkN0VZNUEwQmt6Tk42bi9HSzJlTGtRckJrLy9Eblc5MUI0RVNMMU1NbHcrRWFBZlcxR1hydnFQWGQ4
T0taWHpsWldoRDJWNjNNY08zNHVVR3ZoTWNnUWV6UjR3SjRmYUpQSjlUUHpWMUtFb3E5K0siLCJtYWMiO
iJiZTU2M2U5MDY2YjIyZjVhMTc2NTYzOWQ3YTg0ZTJjM2M2NDExZDEwZWI0NDRhZTM2ZTQ5NGEyM2I2OT
dhNWIwIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:21 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InpVT0NFSEFEWXZ0aGIrQnFGZ0tPNHc9PSIsInZhbHVlIjoidCtWa25ZM2dFY0xZMHZ
4QVpxMk1OUUl4VU4vZWZpT1JmbFNpNWJtOGYzR3V1SmN0VUlUY0tKR1hwMGRhM3NYTXFyVUgzd3dLQ2Nl
WC83dEduN2FWYVNFU0JwMEErQTd5QWVXNkd5QUNtTDdWdUM2eDBVY215YWhkNDB5Rk9EMGgiLCJtYWMiO
iJmYjM5ODQ2YmI4MDIxMjU2M2JhZmMzZTM2YWJlNGM0ODhkODE3NjA0ZDUyOGMwNDFmMDkwMjUyOGI0ZT
NkMzNmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJ5aVZ5OHo3aWQ3L08rSXJYMkdDUEE9PSIsInZhbHVlIjoiam91OUx1NWhvbmpwMkV
lN2twMXBtZW9wZGdSSEpkdXF6U2d1bFZjWlNUTVNqZlAzSWJlUE5QUC9sQkFXdkxXUGxKZHZXRjB1NlpO
WUhMZ2dGM3N3TXREbUxHbHRNOWtQbXZNTlBQa3FSbnlzNm02L1cybzYzeWFiZHBUVitrVDMiLCJtYWMiO
iIxNzBkMmE4NGFhY2NlZDNkOTQ3MDlkM2QzZmI1NDU3NWFkZDM4MmNjYjk1NmRiYTQxMGQzOWQxNmI0YW
QzMWZlIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImRyam1UY0c0eGVTb2k2aXZVR2hjeEE9PSIsInZhbHVlIjoiTlRqSXdHZU1xS2cyTVU
vUTcvUklRZk9QSHFadnM3QWcyTTN2dkMxNVNvYjhZQVkwZUVqYitOeUR6cXJ1VUxlV0dkNmZ1aS81Zi9U
V0I2YlZ1UFphVWdvbGJiMEpRRDRvNDEzc3JheWRNZGhSZzVpZEtpNmU1UTZKVTVmZkZ3NG4iLCJtYWMiO
iJhMDhjNjQ2MzA3NTNhOTkxNDkyZmRkODhiZjc4YzBhZDhmYmE0MDQ4Yjk4ODE2MTVkOWM5YjNkYjQzYj
c5NDk1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/privacy-policy

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVSa0VwY0I1U3YydnNzWm9ZSk1hNGc9PSIsInZhbHVlIjoiTkVWYWhNZHJMTzYxNFp
NVVVMR3gwWVJ0U1ZzbE0wNzdsNk0yQzhXWkY4MjJ1cHBmSlhkUWNpVkhSQ1hwWmlhZmJRajF6QkZGSjFt
amZzK1p0WVhybm1scmxPVnRCc0lxeDFFcFRjQzhKT3A5Zkc3WHlCMU1wck5iOURVdWNYVXoiLCJtYWMiO
iIxY2ExY2JjNjNiOGZmMjZiM2E2NTZhZjA0N2M3Njk1NGRmOTVkM2MzOTRjYzBhNTk0ODI4Yjk3ODFlYz
NlNjk2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/profile

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlBSLzlzY05PV0hGOXNiejNNZnR0bVE9PSIsInZhbHVlIjoiampOUXQwSkJ4UEhYKzR
MTnRBYnZqRXhvOEZrVmZqaXhibkFmK0h4Z2cxSmJld0dKbU15ek1EdHBwaU5CQjR4aXBpZlhBbFo2VDN1
WUFwMGI1dktoQStJd1R2ZjRvSjJtcU55TGpvNGxYM2laSUNuZ0hzSEZtbG9PcWx5QWxtbGgiLCJtYWMiO
iIzNjkxMzZkNGYyZTg1NWU4OTg2N2RjZDNlZTY5NTUyYmUxOTQ3N2QzNWM4ZTM0ZDdhMmJlMWRkZmI5ZG
U2YTRmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:53 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/real-estate

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImlmeW85YXRaTHpiZkVyL2F2aDdtbVE9PSIsInZhbHVlIjoiOHAwUWVPeS8xTDVmWGd
GUWhES3A5WGpoU1RROXNoNGx1cWszLzRhTENKOTg1LzJvdEZMSUpSQW9QczdhSVkxZVdoMFp0cG1RWjEw
ckZUU3FUZU1acjN0YUpqeVllcGtPbkhReGpYSXpTYVFvYStTS2p5bEVMbzhicXRUOHlkcHMiLCJtYWMiO
iJjMDRmMWM3ZDc4YTUyNTAwZWRhZDc4OTRkMWUzMjIzNDAwNWIwZjFkYWUyZjM3OWE5NTBmMTM2ODZlYj
g5NjI5IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:57 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/real-state-home

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlNROEhrVTY2cWtUOFpSZWx1amlMQlE9PSIsInZhbHVlIjoidm53ZllmazhDNVNhL0p
FNkZHRVUybEo0bXdiWEIwTXk0b2cwWGZmMDhDUDMxY2Y0N3FtbEpWaHYrUStwaHdQdTY2VzNwb0xLeTZG
U0FSazZDdnBFczNRbERXL09qckVzVWVXZVgxRVMrS2hhRnF5MXZaeEN5dkh6VmZyWXR0T0wiLCJtYWMiO
iJjZDkyOTNiMTZmNDMwODk3YTBlNzI1ZmE1NGI5N2UxNzhmMDVkYmNlY2YyYjUxY2RhN2Q3OWI1NmI1ZW
Q4MmE1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:57 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InF0VkYzSjVwMVFDNXJnNUI2TjdTZHc9PSIsInZhbHVlIjoic3RFa2YwU2JVOTcwTVN
TbXYvRW1rT1hUUE5QTGd4SmJmeFI5b2tRaThEOE5SZUU3N2N0WVg4MGRYTEdDWmxSQ2tBdTRlV3VTelEw
dVllNmp0S0RIK0R4eEdjTFlKWDNMdndPUzB5YUdxMURGZmRCTmF6MFhsN1MwZGFlM01ncFIiLCJtYWMiO
iI2YjE1YTk4OTdjNWZlYmFkMDg0MzU4NzQ4M2JkMjVhM2YxZWRjNGY5ZDI5NjU2MDE5ZjM0YTY2ZDgxNj
FhZTMzIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:58 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZMbGQrR3RhaTdGclF1RGFRVVkwRUE9PSIsInZhbHVlIjoiOExpSi9XcC9uV3JMZmd
QUDMrTUNDUTZPYXN2WS9LR21GVVNTWmg3Vy83cXB5Sm1kaUpaaXZOSGlpTjVYSzlmRlRVTVhNM2I4NXVv
TjN6WFFrc2hnQnZJVXZ3OXAyNkxXVU5pazc4M3ZwRkhjUkQzREEorbHB5VE8ySGVhN0ZVVngiLCJtYWMiO
iI0MDYyYTZlOGMzMGVhYzc1NjIwMjdlMzAzZmE3OTZiMWRhODZiNzUzZDNlMjEyOTRkNGM3YWIzMzJiOG
FiMjNiIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:57 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkIzdEdpc3hwa0N2QVRaZk85WjZiUWc9PSIsInZhbHVlIjoiZGMydWtnZnovYWJFREh
mNFNRTWl4QThCYkNKWmYxS3Fxc1hrejU2MjJ2RVJ0K3dKVkhEZVc4a0FkeGZraTZDaHlTcGJYMDZsNlI5
a0V3SFQyZmpVSzJJL1JpU01KVEpvTXpZS0ZJaUJXTEM1UTBWTER0bUNqQ1pCZEtyL3ZKdkgiLCJtYWMiO
iIwYzU5OTAxYTU1MjQ4ZmJlYzk3MGQ3Yzk0YTU3ZjE2MTRlZWMwZjJiYjEwMzk5M2QyYWFkNzBiNzM2NT
M5ZTg2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:57 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlRyd3BvWXk0NEVCUTVBOTRkVDVWd3c9PSIsInZhbHVlIjoiOFFIc3hLRm44eG1HTDE
1U2dTRnhBS0F5bUYzbllloQnZzSUdRS2RPVUhIVFhvWmNRVnBSRjBGcURCQ0xuTUFPWDBUSXpSU013M3Fy
eWl5cVpaRU4xN295Y21OVGN6VGhGZGJEMXlaUlg5bVZIdHVLeWovN25mYXByZWd0eThuazEiLCJtYWMiO
iJmMjdkMDI5MTViNWM0ZGViMjI4MjA1YzA3NTJmNWJlZmE2MjhmMzU2YmNkMWFmYTJlMWE0MmZlMDAzM2
Y5Zjk4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:29:04 GMT; Max-Age=7200;
path=/; samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/ Verified

Cookies without Secure flag set:

- https://globalgroupny.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; path=/
```

- https://globalgroupny.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkEwTk43enVXeDJFdlN5TGVJeFIwOGc9PSIsInZhbHVlIjoiNTQyYWY0RnNVOXVsUjF
IcENFdTNGYTBLTXhWVEt6eW16STg3YlN1V3A1VUlGUWo3Z24wdEtqYnJUait6VlpPZ3hoQ1V4UmY5NTBt
emxQbkdublphVXFGcWdObElTaTNqeTFUQ1pZRExVVVRENm9ZODlXKy81NDB4NUowOG5EN3UiLCJtYWMiO
iI0ZmUzNjExNTcxMjQ4ZjgwNzFmZjY3ZjVkMjU4ODRhODkyOTBjNDg2Njg1OWI5YzM0Njk0NDE0ZTYyMm
RlNmRiIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:26:08 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/

```
Set-Cookie:
global_gropuny_session=eyJpdiI6ImQzTHNWUW94Nm10SnAvUE9KVjhDTnc9PSIsInZhbHVlIjoiL0
pmUmlGeFUxYVk5N0dmZU1VN2g5bThPTGFScEpWU0EwMkd2eitqYkszQllPNzRzci9ORHpDS01oWUtwbkx
NeWxCRUZBenJPb0k4dDdiUmV1bzJ1YVZOSTllZ3YzZmlUSnNIcFc4K1lCOGtnNWlaM3Z4ek1VenhYMTlo
```

```
RlU4VlIiLCJtYWMiOiI0NjRhOTg5NGYwYjFiMWVkNGIwY2YxNmVhYWMzNTkyNzkyY2NiZmI1ODRmN2MxN
jRjMGViN2E4YzM3ZDY3OWE1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:26:08 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImVGWVdHR3JwcWdmYUR4dUhUa01MZ2c9PSIsInZhbHVlIjoiRU1EYysyaGUwSjVCT1U
xeGdoeXJPN0hsLzllNERtWXlUNy9hUFB0aGRSNkZUbTBlZ0R6QjhlMXlraWN1N0hySkh1c0xXVk1lZTBn
bmhSSnlrY3pGUVNUV0FzazBKelNqbXpTd1JHMWFROFhHV3BnQnpDZDR5WXNqTUcyaTV6QXoiLCJtYWMiO
iIwZTZkNTgyYjE0Yzg4MGM3YWU4ZGQ0YmQ1ODA5MDU0ODA2NjQzYjI2MmQ4MGEzMGYxZjQ1NzIzN2UxNz
VlNWExIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:58 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6InRyV3Mva2FRR2F2bW14WnU1dzFLeUE9PSIsInZhbHVlIjoiRV
dvQm9odmVURktLN2EzYjQxNFVSTnpabFlLRGt3NHI3cmVBYko4d2ZSOTVFYlR5ZGpDcFBwdGMzb2l5d2N
BaWhQT3M5RVRzanFGcDJFR2g1NVZxZyt2YjZYNVZUTGhUWVFCNEFOUFhicSsza2VaaEpPUXZlL1RoOWY5
SGI4d1MiLCJtYWMiOiJlMjI1NTZkODg2ZWRmMjU5OWUwYmUwM2U3YWMwNzMyOWQ3ZmQyZmM4NWY2ZjgxO
GMyODNmYzMyZjA2YTI0YzczIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:27:58 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blogs

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjlrdkVQNXFCWHZQK2ZSMnVtN3R1TUE9PSIsInZhbHVlIjoicTNuUFJGQ0prVktXRzh
4SGtyV1V5Zm1NZkRzZDRSNWVLZ3Z6clRFOURraVdRZWhmU2gxdStMcE04ZHQ2aEQ0Tm5GSkhZcVZrUlBR
cFlCV0MxdSt3ck1vZkcvRHlHWTduL0xoTHFUYk5zenVDRFkraHJtT09uQ25GTWlNWkpJcFYiLCJtYWMiO
iJmNzU4MTJmMmU5MDkwM2E0ZWM2ODIxZWUxOTYyZmZiZDZmNjJhMGE5NmIxNjIwNmQ4ZDgwNmU2MjQzMG
QwZGQ1IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:02 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blogs

```
Set-Cookie:
global_gropuny_session=eyJpdiI6IjFyelllV3RVWlI1MGt5WmhXbEluSXc9PSIsInZhbHVlIjoia1
JVanNrcjlGOWVLaW10eWI2QjJiQ3FuYkpoK3lHejR1QWd3MUMxZ28yazNHSmFPUkw2bEdYUk9BVmFOS08
3ejg3YUxKWCszbFdBUkplZ0dlNlZua01pR3J3Qm5aWVVZM0tjNGoxb1pXNVV1S0xtQUxuOVRmcGt5bnE4
```

```
OHREWlMiLCJtYWMiOiIyNGNlYmFlZDE4NDc4MmViNmQ1M2M5ZjA2OTg2NzAxMTA4MThlMzNmNjhkNGM1M
zRlZDg0MDNmNzBmNDNjMjk2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:02 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImFMUHVBM3pMTk95UHNKeFdJTk1xSUE9PSIsInZhbHVlIjoiTmtUVVhwMEt2VldWT1F
ka0htaStMeUVSUVpjSFZFekxZdXFOdmFSM25KT2xINXJNR0FzOHVYRktwc1FwYllNU0tqY1pNdnlUckNM
YWR6M1piczF4RlB2RGZGQjVxWFJvZTZLc3NHMGhYV3VCRC9UYXlOK3Z6allmR2kyYUJwZVEiLCJtYWMiO
iI0ZTIyNDEwNjFjM2JiNjJkOWQxY2ExOWY5ZTRmOGIxZTRiOWI3NDVkOTA4Yjk0YzMyY2EyODhhYTQ1ZW
QyMTUyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:05 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6Ikk3dG9hZzFxVFRxUnY0bzd1c29ldlE9PSIsInZhbHVlIjoiZG
12ZEZwOXNvNkZkMVpYUGdBandyTHFJQ0tRa3FnZGxQbndDTVhtaWNURXBPUkRjSklBZFR6Zk44elZBR0F
ZV01EcFVrZ2tyZ3p0TUxuaTVzeGx2czc3WW1PaGVpVHlJSi8rZWZINTczYS9keGR1c3dJZ3NHakdLM3dW
NThWY2EiLCJtYWMiOiJiOWVjMjIzY2RhN2NiMTQ1MWRiZjMxN2U0ZGQzNmNkMjY0OTA2NjljM2EwNzM3N
TUzNjdiZDYwMDNhN2I3ODAzIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:05 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImtrOHdHT3krV1lsQktldHZYNk5CZFE9PSIsInZhbHVlIjoicnpvMXJGY2FrQ3VpOGl
0cFZqOHByMk9wT3VuSVVGQTdrUTVRMTZaQjFTSkFOM1ZkMnZhbjhNbmpDYVYza2dTYmNBbGdiL0JsQ29P
L2RtNkl5NzF0UkZEUlR6L3liUG1OYkNlRmh5Rzl1dXQ5ZVhkZEU5SXhOSjRlZ0NZWEtESEciLCJtYWMiO
iJjZDNjMTQxZmFjNzU0YjMyNzkzOTc4ZmU2OTJlNTVlNjNmY2E5YjUxZDg1MWEzNjg0YzJmYWI2M2RmMT
Y4NDI0IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6Ik5HT2RXeHhQcnpWS2pQMTZaUmcrT3c9PSIsInZhbHVlIjoiZm
dNOU9oVGNWTnJMVFJ1THYxMU9LNW00MFRYNW5SWlV0aDdMazBaTkt3S2p4UGNSSlhpeThNL3dyWlEya2J
xR1FBN05JZGd3Qmxic21lZlBkQ09TZFJFN2VTdDF5MWNjOTcxRDJBNzlKOTljZG1kRzNsTDh3VXk1RzA0
```

```
MFpEM2UiLCJtYWMiOiI4NmMyNDBiOWFlMGI1ZDQzZWQ3MTkxNzU3NmFjMDljOGVmOTYxZDE5ZTEwMTRkO
TQ4MjhiY2QxYTQzNzg5ZTcyIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ii9GV2tJUldGcUQrNlJ2T1RxUGs4V2c9PSIsInZhbHVlIjoiWVFsN1Y2MzI1NmVYRlR
aMmpRWnh2MmRhMndFSExFUjdndTZ2b0RPakZUZmtlekp5bmg5dFltanE4K1dmeEx0QlIzU2V3UUw2M3F1
ZDluamdtUjRxREhEb0poblgyd3N2RW1uMWJpbEVmb25NVmdBWFZXblNkWmRNY29iVVdQTmciLCJtYWMiO
iI2NTg4NTZhNWM4MmE0YWViNGY4MjcxMmUwMWRkNDExMjg5NzA3YzYyOGI5ODg0YWRmODExNWNjMzlkZW
E5Zjg3IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6IlBqb2NHVHpOVkFVOEFkVkdOWCt5bWc9PSIsInZhbHVlIjoiU0
JGMGVGU3JxRnl5RUVwQVFBSVRzdXAzOGNyRGxVWlhXN2VpSzNaU05uelRUOVpkSE1wdnE1VWdzd1FDaWt
PTTNnVDhndVJpMDBRdWdnRFI1cGxaekJhbGx4VFRsOEx5VUwrY2t3dTdpc3N6K1lQemN3ckxUVm9oRW1R
TUU2WUYiLCJtYWMiOiJkYjEzYzI4Mzg1M2JlMDU2ZjdkNDY2OTY1MzZiZTU3NDg2ZjlmYWU4MDUzOWI2Z
DQ1Y2YyMGNjYzYyN2MyMDJkIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:07 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/driving-school

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkJGckphQytjN1VXZktUM0RmNVUwelE9PSIsInZhbHVlIjoiZVBNK3lvc2N3WmoySmo
vbjJLMXhTbnhzaFZKKzZJZ2poR2tRc2d4bWhqRFZNNjdsZnc5ZG10dUVuakxKOENjK0ZCWEhKUkVxVE9p
R2NHMm5KUG1aRWhIZWdKbE5IcDA5L01NT3NkMzA2cUlwSnBEZnp0TUM1a2R6dzgyaGtDdSsiLCJtYWMiO
iIxOTJhMjhhOTAzMjY5ZGE5ZGQyNTE4ODRjZTRkYTM0ZWYzOTFhYTMxNTQ0MTM5ZmJiZWJkNGZkYjAzOT
czYmM5IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:15 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/driving-school

```
Set-Cookie:
global_gropuny_session=eyJpdiI6Im8wVWdSeWhONU9jaHR2UGtFVTY2Q2c9PSIsInZhbHVlIjoiZT
ZGUDdsdll3QitoRkxubk9kMEdMME9HM0NuckhzMkFTd3lmcmZDcjlxMmQybE1XMTRqN3dQUTY5NnRzQkh
leTNDV0dFc2x5aTlFSDV6UFNtaFlva3hRZjVLeitsdmRtZFBua3U3T3NHWmZkVmpsbjgrQ3FjTWVudEtG
```

```
YmFndFUiLCJtYWMiOiI4ZmY4MDI0N2ExYWY0Y2Q3ZmEyMmU1MDM0NmYzZWJlNjgwZGFjMDEwYWZhZDBhN
jhhMjI3NzY2MGJiYTdkMmY2IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:15 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjR0Wi9heW96RXU0Zm5VRW51clVLTnc9PSIsInZhbHVlIjoiY2RSOWkwMHVjNk5uMGc
vbDNMRnA1Q0JUTVpCWnVKMVR5RUwzMDEyRFZWSHIxV2tnMk5OS25EU3BOYWhyZ3kyUEV0VGVPT1dvUVFh
Z3hMVm9UV04xOG9LTmxBdHBQTXVONVZRbG9vamcrMUk1OXhGZzNrdVFveDczR0U5RGhHd1YiLCJtYWMiO
iI2ZTU5MWYwNGY1ZTRkOWE2ZWY3OGQ0YTFkZDVjM2EwNmJlMDRlZjE5N2FjNWFmNGJlZTczNjcyOGEzNj
Q3ZDUwIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:22 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6ImtqK1g1L1J1NDFQOFcwbzI5SlZteHc9PSIsInZhbHVlIjoiME
trbFNOTTR0R0JCMytGZ0p4VHJiYUNRWFAzV1hMUnlXd0toZVRaUWlsdHFPMCtKTGdtc1VQMDZodnMyU25
ydXl3MFdBRWNRb3gyRUZRTmJBQkQvY01yQTVhRTRFTzRGeDFWakplbGFlbVBZbWdZREtmekN5L2w4T2tC
UXRKdDEiLCJtYWMiOiIzMTkwNDZjNWMwYjA4NDVjOGQxZWZlZjk5YmIzMjU3ZTNmNWM2NzFiMGIzNmNmM
DQ1MmFjMDg4MDM5Nzk4MTA4IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:22 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlBLVzZER3dLUHpoazZFeEU3d29mQmc9PSIsInZhbHVlIjoiRjJWQ1RvTkQwY1laUmh
xcHlkN0VZNUEwQmt6Tk42bi9HSzJlTGtRckJrLy9Eblc5MUI0RVNMMU1NbHcrRWFBZlcxR1hydnFQWGQ4
T0taWHpsWldoRDJWNjNNY08zNHVVR3ZoTWNnUWV6UjR3SjRmYUpQSjlUUHpWMUtFb3E5K0siLCJtYWMiO
iJiZTU2M2U5MDY2YjIyZjVhMTc2NTYzOWQ3YTg0ZTJjM2M2NDExZDEwZWI0NDRhZTM2ZTQ5NGEyM2I2OT
dhNWIwIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:21 GMT; Max-Age=7200;
path=/; samesite=lax
```

- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea

```
Set-Cookie:
global_gropuny_session=eyJpdiI6InhCMTFjWU03Wi9RZkkwR2U2cWYyWWc9PSIsInZhbHVlIjoiOU
```

```
hxQnB1R2RhWlpJL0xKQTNsakhES0ExVGpUc0piNjFFd0JRVURGNDRYZVJEbl1adVNKelRaa1VEMDQ5S0R
zNWpwZEFmSlAxdEdkbU9hVFlDNFd5QlFuaE9mcEcyWTcrUU91dXBRVmNiTjg1VVhHaVgvUTR5S0hsKzcw
d0lDY1EiLCJtYWMiOiI4NmU5YjNiZmEwNzFmOTUyYWQ0MGQ4Yjc3NmJjODhlNmVjOTExZTRmNTJkZTkwO
DZhZGI0M2JjNzI1YzdhMjY0IiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:21 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InpVT0NFSEFEWXZ0aGIrQnFGZ0tPNHc9PSIsInZhbHVlIjoidCtWa25ZM2dFY0xZMHZ
4QVpxMk1OUUl4VU4vZWZpT1JmbFNpNWJtOGYzR3V1SmN0VUlUY0tKR1hwMGRhM3NYTXFyVUgzd3dLQ2Nl
WC83dEduN2FWYVNFU0JwMEErQTd5QWVXNkd5QUNtTDdWdUM2eDBVY215YWhkNDB5Rk9EMGgiLCJtYWMiO
iJmYjM5ODQ2YmI4MDIxMjU2M2JhZmMzZTM2YWJlNGM0ODhkODE3NjA0ZDUyOGMwNDFmMDkwMjUyOGI0ZT
NkMzNmIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT; Max-Age=7200;
path=/; samesite=lax
```

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

```
Set-Cookie:
global_gropuny_session=eyJpdiI6IkV2dlQrUWNTbyt5aHBVNVNOb2Vvdmc9PSIsInZhbHVlIjoiQV
I2cDRESHlycHl6QmsrTXJDajA4VkgzV2RWYXRWWHZpNnpsamhQRzRzWVBORXZmaldna2FsYXBTZFo0eTh
6N0d6QjBpQU5mTFhzQThUQnErMU1hcmtIRU54ZXNTMCtna1Z1bWdmNmY2YjVNcnNGRFhCQ0RGN2RJZkdT
U2FjZVYiLCJtYWMiOiIxZDc4N2Y1NDYwMWY5OTFkNmQ2M2ZkNDcwNzYwZDBmMDc1MjliM2JhY2ViYzlhN
2QyZTI3MTlmYWMwNmI4YjBkIiwidGFnIjoiIn0%3D; expires=Tue, 02-Jan-2024 06:28:52 GMT;
Max-Age=7200; path=/; httponly; samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

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

https://globalgroupny.ssbmultiservices.com/

Documentation files:

- https://globalgroupny.ssbmultiservices.com/project/**README.md**
  File contents (first 100 characters):

```
<p align="center"><a href="https://laravel.com" target="_blank"><img
src="https://raw.githubusercont ...
```

Request

```
GET /project/README.md HTTP/1.1
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6InNrMVJyTkpodmtvTnpmeG04U1R6OFE9PSIsInZhbHVlIjoiRFJKbjNmbm5JZXI5dU40UWVXYU5uYmgzY1dLTm
tPUWZCbkhtOEU2aE1oMTdXQmZnYUhldVhrUndGZ3Zib0FpQzZkUWNIZDBQMG9xbUJqdC9HZU9zd0loVlZyVTlpN3VBZ1E3Q2lCcn
Y1Ly9maU9LVlVKcGZTTFh4N3ljeTRYRlQiLCJtYWMiOiIzYjc3ZDIwODEzOGYwZTg5ZGZlOTJmZWVhNGFhZDIxNzAwMTI1MTFkYT
Q0OThhZGViZDUzYTk1NGVmZmVkZDk2IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6IktMN2hldjE4ZXo5d3ZFOGQyTFdTSVE9PSIsInZhbHVlIjoiRUdQVVZxR0owbFZGdDJjT
3VRVFBHaTJlUFZCeGI2UDV0ZExrVW5GNDZid2FFRjlmRjR0TDV0NjZNdWdPR1VFZHpIanJSQ2JkZXY5ekdGTUl6eEM4S3h4TzhJT
y9QTkxYSjI2ZmtVT29QbWNDVHlVc3ZYUlR2QVNqTThwN2o3T3QiLCJtYWMiOiJlOTNlN2VjNTY4NDY5NGY5NDRmMjk4MmFmYzAwM
2Y3NzhiZTA3NWZkYzlmMTA0MzI4ZjIwYzliZjU2M2Q2ODM2IiwidGFnIjoiIn0%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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file acessible from internet.

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://globalgroupny.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://globalgroupny.ssbmultiservices.com/
- https://globalgroupny.ssbmultiservices.com/upload/client-review/
- https://globalgroupny.ssbmultiservices.com/archives
- https://globalgroupny.ssbmultiservices.com/blogs
- https://globalgroupny.ssbmultiservices.com/archives/May%202020
- https://globalgroupny.ssbmultiservices.com/consultation
- https://globalgroupny.ssbmultiservices.com/contact-us
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globalgroupny.ssbmultiservices.com/driving-school
- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
- https://globalgroupny.ssbmultiservices.com/immigration
- https://globalgroupny.ssbmultiservices.com/irs-withholding-calculator
- https://globalgroupny.ssbmultiservices.com/make-payment
- https://globalgroupny.ssbmultiservices.com/privacy-policy
- https://globalgroupny.ssbmultiservices.com/profile
- https://globalgroupny.ssbmultiservices.com/real-estate
- https://globalgroupny.ssbmultiservices.com/real-state-home
- https://globalgroupny.ssbmultiservices.com/tax-form
- https://globalgroupny.ssbmultiservices.com/subscribe
- https://globalgroupny.ssbmultiservices.com/tax-accounting
- https://globalgroupny.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/ Verified

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

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.ssbmultiservices.com
```

```
Connection: Keep-alive
```

https://globalgroupny.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://globalgroupny.ssbmultiservices.com/
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6ImFMUHVBM3pMTk95UHNKeFdJTk1xSUE9PSIsInZhbHVlIjoiTmtUVVhwMEt2VldWT1Fka0htaStMeUVSUVpjSF
ZFekxZdXFOdmFSM25KT2xINXJNR0FzOHVYRktwc1FwYllNU0tqY1pNdnlUckNMYWR6M1piczF4RlB2RGZGQjVxWFJvZTZLc3NHMG
hYV3VCRC9UYXlOK3Z6allmR2kyYUJwZVEiLCJtYWMiOiI0ZTIyNDEwNjFjM2JiNjJkOWQxY2ExOWY5ZTRmOGIxZTRiOWI3NDVkOT
A4Yjk0YzMyY2EyODhhYTQ1ZWQyMTUyIiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6Ikk3dG9hZzFxVFRxUnY0bzd1c29ldlE9PSIsInZhbHVlIjoiZG12ZEZwOXNvNkZkMVpYU
GdBandyTHFJQ0tRa3FnZGxQbndDTVhtaWNURXBPUkRjSklBZFR6Zk44elZBR0FZV01EcFVrZ2tyZ3p0TUxuaTVzeGx2czc3WW1Pa
GVpVHlJSi8rZWZINTczYS9keGR1c3dJZ3NHakdLM3dWNThWY2EiLCJtYWMiOiJiOWVjMjIzY2RhN2NiMTQ1MWRiZjMxN2U0ZGQzN
mNkMjY0OTA2NjljM2EwNzM3NTUzNjdiZDYwMDNhN2I3ODAzIiwidGFnIjoiIn0%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: globalgroupny.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

Passive Mixed Content over HTTPS

Acunetix detected a mixed content loaded over HTTP within an HTTPS page. If the HTTPS page includes content retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

Impact

A man-in-the-middle attacker can intercept the request and also rewrite the response to include malicious or deceptive content. This content can be used to steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

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

The following issues were detected:

- The tag **img** references the resource **http://shariftaxservice.com/upload/gallery-image/img_1621849573_60ab75e52c98b.jpg**

Request

```
GET /tax-accounting HTTP/1.1
Referer: https://globalgroupny.ssbmultiservices.com/
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6ImlmeW85YXRaTHpiZkVyL2F2aDdtbVE9PSIsInZhbHVlIjoiOHAwUWVPeS8xTDVmWGdGUWhES3A5WGpoU1RROX
NoNGx1cWszLzRhTENKOTg1LzJvdEZMSUpSQW9QczdhSVkxZVdoMFp0cG1RWjEwckZUU3FUZU1acjN0YUpqeVllcGtPbkhReGpYSX
pTYVFvYStTS2p5bEVMbzhicXRUOHlkcHMiLCJtYWMiOiJjMDRmMWM3ZDc4YTUyNTAwZWRhZDc4OTRkMWUzMjIzNDAwNWIwZjFkYW
UyZjM3OWE5NTBmMTM2ODZlYjg5NjI5IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6Ik1kcXpjczJnZkhvSHJXVWV4dU0rNmc9PSIsInZhbHVlIjoieXdZRExzVnhwdXp1dENJb
EZ0Z0trZVlGUk9MbWZpYnloU2RYdWJmSkFOSkZzUkxnMkJPSFNydnEzK3ZPZ2IxS2J4SFpUWngyY1R6azRjN0w4VExrd0lZSkdSc
mJZZXJNajVPaFVaU3Y4cHZhSDd6SC9hR3ZrNVZoakI2a20vaWsiLCJtYWMiOiIxOTIyZDc4YmYwZmY3ZTExYjg1MjMzNTdmYTMyO
GMxMmRiZGQ3YjJkMThkNjdiNDJkZWUwZWNiYjg5ZjIyNmZlIiwidGFnIjoiIn0%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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites - Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like >link rel="stylesheet" href="//example.com/style.css"/<. Same for scripts >script type="text/javascript"

src="//example.com/code.js"<>/script< The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

MDN: Mixed Content
https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

What is mixed content?
https://web.dev/what-is-mixed-content/

Fixing mixed content
https://web.dev/fixing-mixed-content/

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

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

https://globalgroupny.ssbmultiservices.com/

Possible sensitive directories:

- https://globalgroupny.ssbmultiservices.com/**upload**
- https://globalgroupny.ssbmultiservices.com/**database**

Request

```
GET /upload/ HTTP/1.1
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6IjlrdkVQNXFCWHZQK2ZSMnVtN3R1TUE9PSIsInZhbHVlIjoicTNuUFJGQ0prVktXRzh4SGtyV1V5Zm1NZkRzZD
RSNWVLZ3Z6clRFOURraVdRZWhmU2gxdStMcE04ZHQ2aEQ0Tm5GSkhZcVZrUlBRcFlCV0MxdSt3ck1vZkcvRHlHWTduL0xoTHFUYk
5zenVDRFkraHJtT09uQ25GTWlNWkpJcFYiLCJtYWMiOiJmNzU4MTJmMmU5MDkwM2E0ZWM2ODIxZWUxOTYyZmZiZDZmNjJhMGE5Nm
IxNjIwNmQ4ZDgwNmU2MjQzMGQwZGQ1IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6IjFyelllV3RVWlI1MGt5WmhXbEluSXc9PSIsInZhbHVlIjoia1JVanNrcjlGOWVLaW10e
WI2QjJiQ3FuYkpoK3lHejR1QWd3MUMxZ28yazNHSmFPUkw2bEdYUk9BVmFOS083ejg3YUxKWCszbFdBUkplZ0dlNlZua01pR3J3Q
m5aWVVZM0tjNGoxb1pXNVV1S0xtQUxuOVRmcGt5bnE4OHREWlMiLCJtYWMiOiIyNGNlYmFlZDE4NDc4MmViNmQ1M2M5ZjA2OTg2N
```

```
zAxMTA4MThlMzNmNjhkNGM1MzRlZDg0MDNmNzBmNDNjMjk2IiwidGFnIjoiIn0%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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

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

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://globalgroupny.ssbmultiservices.com/

Possible sensitive files:

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

Request

```
GET /web.config HTTP/1.1
Accept: fegmlsfx/ynbb
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6ImVGWVdHR3JwcWdmYUR4dUhUa01MZ2c9PSIsInZhbHVlIjoiRU1EYysyaGUwSjVCT1UxeGdoeXJPN0hsLzllNE
RtWXlUNy9hUFB0aGRSNkZUbTBlZ0R6QjhlMXlraWN1N0hySkh1c0xXVk1lZTBnbmhSSnlrY3pGUVNUV0FzazBKelNqbXpTd1JHMW
FROFhHV3BnQnpDZDR5WXNqTUcyaTV6QXoiLCJtYWMiOiIwZTZkNTgyYjE0Yzg4MGM3YWU4ZGQ0YmQ1ODA5MDU0ODA2NjQzYjI2Mm
Q4MGEzMGYxZjQ1NzIzN2UxNzVlNWExIiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6InRyV3Mva2FRR2F2bW14WnU1dzFLeUE9PSIsInZhbHVlIjoiRVdvQm9odmVURktLN2EzY
```

```
jQxNFVSTnpabFlLRGt3NHI3cmVBYko4d2ZSOTVFYlR5ZGpDcFBwdGMzb2l5d2NBaWhQT3M5RVRzanFGcDJFR2g1NVZxZyt2YjZYN
VZUTGhUWVFCNEFOUFhicSsza2VaaEpPUXZlL1RoOWY5SGI4d1MiLCJtYWMiOiJlMjI1NTZkODg2ZWRmMjU5OWUwYmUwM2U3YWMwN
zMyOWQ3ZmQyZmM4NWY2ZjgxOGMyODNmYzMyZjA2YTI0YzczIiwidGFnIjoiIn0%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: globalgroupny.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://globalgroupny.ssbmultiservices.com/

Paths without CSP header:

- https://globalgroupny.ssbmultiservices.com/
- https://globalgroupny.ssbmultiservices.com/upload/client-review/
- https://globalgroupny.ssbmultiservices.com/archives
- https://globalgroupny.ssbmultiservices.com/blogs
- https://globalgroupny.ssbmultiservices.com/archives/May%202020
- https://globalgroupny.ssbmultiservices.com/consultation
- https://globalgroupny.ssbmultiservices.com/contact-us
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globalgroupny.ssbmultiservices.com/driving-school
- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
- https://globalgroupny.ssbmultiservices.com/immigration
- https://globalgroupny.ssbmultiservices.com/irs-withholding-calculator
- https://globalgroupny.ssbmultiservices.com/make-payment
- https://globalgroupny.ssbmultiservices.com/privacy-policy
- https://globalgroupny.ssbmultiservices.com/profile
- https://globalgroupny.ssbmultiservices.com/real-estate
- https://globalgroupny.ssbmultiservices.com/real-state-home
- https://globalgroupny.ssbmultiservices.com/tax-form
- https://globalgroupny.ssbmultiservices.com/subscribe
- https://globalgroupny.ssbmultiservices.com/tax-accounting

- https://globalgroupny.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/ Verified

Pages where the content-type header is not specified:

- https://globalgroupny.ssbmultiservices.com/web.config
- https://globalgroupny.ssbmultiservices.com/project/vendor/asm89/stack-cors/LICENSE
- https://globalgroupny.ssbmultiservices.com/project/README.md
- https://globalgroupny.ssbmultiservices.com/project/composer.lock
- https://globalgroupny.ssbmultiservices.com/project/docker-compose.yml

Request

```
GET /web.config HTTP/1.1
Referer: https://globalgroupny.ssbmultiservices.com/
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6InVrMGhRK2h1RzhTQk1iaXNwQzdKTGc9PSIsInZhbHVlIjoiMkNpakk0dHFhb003c2Z1eXQxZEpKMWhMRUlLNX
lSNzdOMzh6ajdRTEZ4YVFrcEpYUlZqdG5FRkNzdXBYMFFHZGUxQTNpMitvMG5HY0QvS1pkdnFhMEIzK0NRK2tOaGdMZEFZOVRIVi
sxWGZOL3dqdjBWR1QzQ2JDT0ZTOHI2UWgiLCJtYWMiOiJkZDdmMzlmMTRmMDNmNDA1ZjZlYzgyNjJhYjhmMzU1MDcyM2FkNTJkNj
ZlZmQ1Y2RiMWU3YmM2ZmI2NTE2ZTY0IiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6IllickVNMkZzVWY1YVhHdTNuQXdVZnc9PSIsInZhbHVlIjoiZnJZMkxYV3FVUmhka3YvR
EtsRzNKRGFyTUtyMkROc2JSMlBhdEFUaXNKU082ckJIQm1VOHVjc2x6WE1xSFZvQXNhTkVGNzB5RlV1cVhaTkxVSCtYZ2w4czdGN
FJJczNrcnI3UHdtNlNCUnlMYkptUDdwNStMa2xOVnF3K2dKakEiLCJtYWMiOiJkODk2MmEzNTBhMTUyOTk4NmRjNjU3MmZkYTIyZ
jM0MTAwOTRiZjI1NDk1NzNkZjcxMzBhM2M5YTRkMzczODk5IiwidGFnIjoiIn0%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: globalgroupny.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://globalgroupny.ssbmultiservices.com/

Emails found:

- https://globalgroupny.ssbmultiservices.com/
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/archives
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/blogs
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/archives/May%202020
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/consultation
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/contact-us
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/driving-school
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/immigration
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/irs-withholding-calculator
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/make-payment
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/make-payment
  abc@yahoo.com
- https://globalgroupny.ssbmultiservices.com/privacy-policy
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/profile
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/real-estate
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/real-state-home
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/tax-form
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/subscribe
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/tax-accounting
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/tax-rates
  rahmangfs@yahoo.com
- https://globalgroupny.ssbmultiservices.com/terms-of-use
  rahmangfs@yahoo.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: globalgroupny.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://globalgroupny.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://globalgroupny.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: globalgroupny.ssbmultiservices.com
Connection: Keep-alive
```

https://globalgroupny.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 4.5.2**
  - URL: https://globalgroupny.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://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://globalgroupny.ssbmultiservices.com/
- https://globalgroupny.ssbmultiservices.com/upload/client-review/
- https://globalgroupny.ssbmultiservices.com/archives
- https://globalgroupny.ssbmultiservices.com/blogs

- https://globalgroupny.ssbmultiservices.com/archives/May%202020
- https://globalgroupny.ssbmultiservices.com/consultation
- https://globalgroupny.ssbmultiservices.com/contact-us
- https://globalgroupny.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://globalgroupny.ssbmultiservices.com/driving-school
- https://globalgroupny.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
- https://globalgroupny.ssbmultiservices.com/immigration
- https://globalgroupny.ssbmultiservices.com/irs-withholding-calculator
- https://globalgroupny.ssbmultiservices.com/make-payment
- https://globalgroupny.ssbmultiservices.com/privacy-policy
- https://globalgroupny.ssbmultiservices.com/profile
- https://globalgroupny.ssbmultiservices.com/real-estate
- https://globalgroupny.ssbmultiservices.com/real-state-home
- https://globalgroupny.ssbmultiservices.com/tax-form
- https://globalgroupny.ssbmultiservices.com/subscribe
- https://globalgroupny.ssbmultiservices.com/tax-accounting
- https://globalgroupny.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b

Request

```
GET / HTTP/1.1
Referer: https://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/

Pages with paths being disclosed:

- https://globalgroupny.ssbmultiservices.com/tax-form **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globalgroupny.ssbmultiservices.com/where-refund **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globalgroupny.ssbmultiservices.com/subscribe-action **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globalgroupny.ssbmultiservices.com/index.php/subscribe-action **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globalgroupny.ssbmultiservices.com/index.php/tax-form **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**
- https://globalgroupny.ssbmultiservices.com/index.php/where-refund **/home/ssbmul5/globalgroupny.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php**

Request

```
POST /tax-form HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://globalgroupny.ssbmultiservices.com/tax-form
Cookie: PHPSESSID=16d0569df9e19f8c2c14ec6faf15c0b6; XSRF-
TOKEN=eyJpdiI6InF0VkYzSjVwMVFDNXJnNUI2TjdTZHc9PSIsInZhbHVlIjoic3RFa2YwU2JVOTcwTVNTbXYvRW1rT1hUUE5QTG
d4SmJmeFI5b2tRaThEOE5SZUU3N2N0WVg4MGRYTEdDWmxSQ2tBdTRlV3VTelEwdVllNmp0S0RIK0R4eEdjTFlKWDNMdndPUzB5YU
dxMURGZmRCTmF6MFhsN1MwZGFlM01ncFIiLCJtYWMiOiI2YjE1YTk4OTdjNWZlYmFkMDg0MzU4NzQ4M2JkMjVhM2YxZWRjNGY5ZD
I5NjU2MDE5ZjM0YTY2ZDgxNjFhZTMzIiwidGFnIjoiIn0%3D;
global_gropuny_session=eyJpdiI6Im5UTWZUeEtpVEFGUjFhcDFEOGk4T1E9PSIsInZhbHVlIjoiR2tZY1Z3NzBKamZXZjhrY
1I0OU5nU09QZlZDVXFQcmcwdGZxUTNIR3dSak0vMkI2UUpNdHp1SkdqYkNJdkh2MVl0M1Rra0pDWjFSZDhuL0RnQStuWjF5L0k2d
01VN3IrUlhkOXMzQXBWN3VxenBnQkN2T2lkNEhXenNzRktIUFgiLCJtYWMiOiI4YzUzMGI5MjEzZTUxYTBhYjU5NWQ3NmJjZDUwM
jRlODIxOWUwODRjZGNiYzM5YTdhYjcwMjBjN2I2ODM5ODNhIiwidGFnIjoiIn0%3D
Content-Length: 41
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: globalgroupny.ssbmultiservices.com
```

```
Connection: Keep-alive

states=https://revenue.alabama.gov/forms/
```

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://globalgroupny.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: globalgroupny.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://globalgroupny.ssbmultiservices.com/

Pages where SRI is not implemented:

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

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

- https://globalgroupny.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://globalgroupny.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: globalgroupny.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://globalgroupny.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
    - May%202020
      - Inputs
        - GET iv, value, mac, tag
    - May%202021
      - Inputs
        - GET iv, value, mac, tag
  - assets
    - 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
  - 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

- blog
  - answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
    - Inputs
      - GET iv, value, mac, tag
  - answers-to-five-common-questions-about-2020-stimulus-payments-b1hgp
    - Inputs
      - GET iv, value, mac, tag
  - answers-to-five-common-questions-about-2020-stimulus-payments-bdhgp
    - Inputs
      - GET iv, value, mac, tag
  - tax-tip-irs-reopens-online-tool-for-non-filers-to-receive-eips-for-children-7si7z
    - Inputs
      - GET iv, value, mac, tag
  - upcoming-tax-deadlines-woxmo
    - Inputs
      - GET iv, value, mac, tag
- 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

blog

answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea

Inputs

GET iv, value, mac, tag

answers-to-five-common-questions-about-2020-stimulus-payments-b1hgp

Inputs

GET iv, value, mac, tag

answers-to-five-common-questions-about-2020-stimulus-payments-bdhgp

Inputs

GET iv, value, mac, tag

tax-tip-irs-reopens-online-tool-for-non-filers-to-receive-eips-for-children-7si7z

Inputs

GET iv, value, mac, tag

upcoming-tax-deadlines-woxmo

Inputs

GET iv, value, mac, tag

real-estate

- Inputs
  - GET iv, value, mac, tag
- luxury-villa-for-sale618958be90e4b
  - Inputs
    - GET iv, value, mac, tag
- luxury-villa-for-sale618958cb7ef3f
  - Inputs
    - GET iv, value, mac, tag

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

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

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

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

- driving-school
  - Inputs
    - GET iv, value, mac, tag

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

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

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

- make-payment
  - Inputs
    - GET iv, value, mac, tag
- privacy-policy
  - Inputs
    - GET iv, value, mac, tag
- profile
  - Inputs
    - GET iv, value, mac, tag
- real-estate
  - Inputs
    - GET iv, value, mac, tag
- real-state-home
  - 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

GET iv, value, mac, tag

POST iv, value, mac, tag

POST states

tax-rates

Inputs

GET iv, value, mac, tag

terms-of-use

Inputs

GET iv, value, mac, tag

video-gallery

Inputs

GET iv, value, mac, tag

where-refund

Inputs

GET iv, value, mac, tag

POST iv, value, mac, tag

POST states

mailman

Inputs

GET iv, value, mac, tag

project

Inputs

GET iv, value, mac, tag

vendor

Inputs

GET iv, value, mac, tag

asm89

stack-cors

src

Inputs

GET iv, value, mac, tag

composer.json

Inputs

GET iv, value, mac, tag

LICENSE

Inputs

GET iv, value, mac, tag

bin

Inputs

GET iv, value, mac, tag

brick

Inputs

GET iv, value, mac, tag

composer

Inputs

GET iv, value, mac, tag

dflydev

Inputs

GET iv, value, mac, tag

doctrine

Inputs

GET iv, value, mac, tag

dragonmantank

Inputs

GET iv, value, mac, tag

egulias

Inputs

GET iv, value, mac, tag

facade

Inputs

GET iv, value, mac, tag

fakerphp

Inputs

GET iv, value, mac, tag

fideloper

Inputs

GET iv, value, mac, tag

filp

Inputs

GET iv, value, mac, tag

fruitcake

Inputs

GET iv, value, mac, tag

graham-campbell

Inputs

GET iv, value, mac, tag

guzzlehttp

Inputs

GET iv, value, mac, tag

hamcrest

Inputs

GET iv, value, mac, tag

laravel

Inputs

GET iv, value, mac, tag

league

Inputs

GET iv, value, mac, tag

mockery

Inputs

GET iv, value, mac, tag

monolog

Inputs

GET iv, value, mac, tag

myclabs

Inputs

GET iv, value, mac, tag

nesbot

Inputs

GET iv, value, mac, tag

nette

Inputs

GET iv, value, mac, tag

nikic

Inputs

GET iv, value, mac, tag

nunomaduro

Inputs

GET iv, value, mac, tag

opis

Inputs

GET iv, value, mac, tag

paypal

Inputs

GET iv, value, mac, tag

phar-io

Inputs

GET iv, value, mac, tag

phpdocumentor

Inputs

GET iv, value, mac, tag

phpoption

Inputs

GET iv, value, mac, tag

phpspec

Inputs

GET iv, value, mac, tag

phpunit

Inputs

GET iv, value, mac, tag

psr

Inputs

GET iv, value, mac, tag

psy

Inputs

GET iv, value, mac, tag

ralouphie

Inputs

GET iv, value, mac, tag

ramsey

Inputs

GET iv, value, mac, tag

sebastian

Inputs

GET iv, value, mac, tag

swiftmailer

Inputs

GET iv, value, mac, tag

symfony

Inputs

GET iv, value, mac, tag

theseer

Inputs

GET iv, value, mac, tag

tijsverkoyen

Inputs

GET iv, value, mac, tag

vlucas

Inputs

GET iv, value, mac, tag

voku

Inputs

GET iv, value, mac, tag

webmozart

Inputs

GET iv, value, mac, tag

autoload.php

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

README.md

Inputs

GET iv, value, mac, tag

real-estate

Inputs

GET iv, value, mac, tag

luxury-villa-for-sale618958be90e4b

Inputs

GET iv, value, mac, tag

luxury-villa-for-sale618958cb7ef3f

Inputs

GET iv, value, mac, tag

upload

Inputs

GET iv, value, mac, tag

client-review

Inputs

GET iv, value, mac, tag

header-footer

Inputs

GET iv, value, mac, tag

post-image

Inputs

GET iv, value, mac, tag

real-state

Inputs

GET iv, value, mac, tag

realstate-post-image

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

archives

Inputs

GET iv, value, mac, tag

blogs

Inputs

GET iv, value, mac, tag

consultation

Inputs

GET iv, value, mac, tag

contact-us

Inputs

POST iv, value, mac, tag

POST _token, email, first_name, last_name, message, phone, subject, submit

GET iv, value, mac, tag

driving-school

Inputs

GET iv, value, mac, tag

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

make-payment

Inputs

GET iv, value, mac, tag

privacy-policy

Inputs

GET iv, value, mac, tag

profile

Inputs

GET iv, value, mac, tag

real-estate

Inputs

GET iv, value, mac, tag

real-state-home

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
    - GET iv, value, mac, tag
    - POST iv, value, mac, tag
    - POST states
- tax-rates
  - Inputs
    - GET iv, value, mac, tag
- terms-of-use
  - Inputs
    - GET iv, value, mac, tag
- video-gallery
  - Inputs
    - GET iv, value, mac, tag


web.config


Inputs