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.

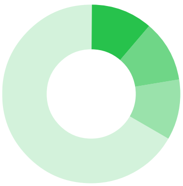
Scan Detail

Target	omkarjewelers.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 3, 2024, 12:33:04 PM GMT+8
Scan Duration	50 minutes
Requests	137645
Average Response Time	33ms
Maximum Response Time	12134ms
Application Build	v23.7.230728157

2	4	19	9
High	Medium	Low	Informational

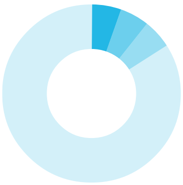
Severity	Vulnerabilities	Instances
High	2	2
Medium	4	4
Low	9	19
Informational	8	9
Total	23	34

Informational



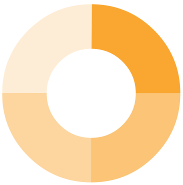
	Instances
🟩 Content Security Policy (CSP) not implement…	1
🟩 Content type is not specified	1
🟩 Email addresses	1
🟩 Others	6

Low Severity



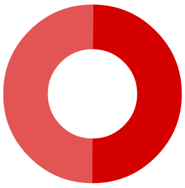
	Instances
🟦 Clickjacking: X-Frame-Options header	1
🟦 Composer installed.json publicly accessible	1
🟦 Cookies with missing, inconsistent or contra…	1
🟦 Others	16

Medium Severity



	Instances
🟧 Development configuration files	1
🟧 Laravel debug mode enabled	1
🟧 Vulnerable JavaScript libraries	1
🟧 Others	1

High Severity



	Instances
🟥 Dotenv .env file	1
🟥 Vulnerable package dependencies [high]	1

Impacts

SEVERITY	IMPACT	
High	1	Dotenv .env file
High	1	Vulnerable package dependencies [high]
Medium	1	Development configuration files
Medium	1	Laravel debug mode enabled
Medium	1	Vulnerable JavaScript libraries
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	HTTP Strict Transport Security (HSTS) not implemented
Low	2	Insecure Inline Frame (iframe)
Low	10	Insecure transition from HTTPS to HTTP in form post
Low	1	Possible sensitive files
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Content type is not specified
Informational	1	Email addresses
Informational	2	Outdated JavaScript libraries
Informational	1	Permissions-Policy header not implemented
Informational	1	Possible server path disclosure (Unix)

SEVERITY	IMPACT	
Informational	1	Reverse proxy detected

Dotenv .env file

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

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

Impact

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

https://omkarjewelers.ssbmultiservices.com/project/ Verified

File: **.env**
Pattern found:

```
APP_ENV=
```

Request

```
GET /project/.env HTTP/1.1
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InUwZ3F4VHVKb2NJb296Qk5EbVJqMnc9PSIsInZhbHVlIjoiV0FBYmdlTzZ0L2txOWZ0MDIzdVVjeHI0VlJPZD
N4b1pRaGJmTkJNUFZsTWVxRVNsWS9ZL1RlM1NCRkVrZEY4b2RFa1VyYUN0S1dicVZ6STc3c3NWZGJBTEdsczZuVXRNbXVteEdHTT
lBY3h1SjhRV2E5eEdka3F0RG5qTSs3ZkgiLCJtYWMiOiIwYzhhN2EzNWU4MGI2ZDI2YTUzYTAxNGMyZjkxN2IwZjY4MGFhOTlkOW
EyMzE4Y2E1ZjNiNGMyMTkyOGJlYmQ4In0%3D;
omkar_jewelers_session=eyJpdiI6InVrUnFvL3h3WldPa2IvemN3RUpRRXc9PSIsInZhbHVlIjoiSE5EOEpjRmdrL3FZb2dkb
WhxQk9LelpneUQ3ajFPM1Q5aVRHQWN1ZVc4V1N5M2RTSWtIK0JhanFkTGF4THRpY0t1TkRUMUtBZVphUU5OWjBJTlFERjV6SGVjO
FJ5SmhPcjNyMUJhMFl1a3YzMmhLRFNjSEFmQlF4aWdITE5KZnMiLCJtYWMiOiJkZjcwNTEzMzEyMDY1ODY4ZmQyMjQzZWFiOWUzY
WQyMmU1ZmFlZWNhMGQzY2I0NTI2ODUwMDc5ZmJiYzQ5Zjc4In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

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://omkarjewelers.ssbmultiservices.com/project/

List of vulnerable **composer** packages:

Package: guzzlehttp/guzzle
Version: 7.2.0
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: 7.2.0
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: 7.2.0
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: 7.2.0
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: 7.2.0
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: 1.7.0
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: 1.7.0
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: league/flysystem
Version: 1.1.3
CVE: CVE-2021-32708
Title: Time-of-check Time-of-use (TOCTOU) Race Condition
Description: Flysystem is an open source file storage library for PHP. The whitespace normalisation using in 1.x and 2.x removes any unicode whitespace. Under certain specific conditions this could potentially allow a malicious user to execute code remotely. The conditions are: A user is allowed to supply the path or filename of an uploaded file, the supplied path or filename is not checked against unicode chars, the supplied pathname checked against an extension deny-list, not an allow-list, the supplied path or filename contains a unicode whitespace char in the extension, the uploaded file is stored in a directory that allows PHP code to be executed. Given these conditions are met a user can

upload and execute arbitrary code on the system under attack. The unicode whitespace removal has been replaced with a rejection (exception). For 1.x users, upgrade to 1.1.4. For 2.x users, upgrade to 2.1.1.

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

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

CWE: CWE-367

References:

- https://github.com/thephpleague/flysystem/commit/f3ad69181b8afed2c9edf7be5a2918144ff4ea32
- https://github.com/thephpleague/flysystem/commit/a3c694de9f7e844b76f9d1b61296ebf6e8d89d74
- https://github.com/thephpleague/flysystem/security/advisories/GHSA-9f46-5r25-5wfm
- https://packagist.org/packages/league/flysystem
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/RNZSWK4GOMJOOHKLZEOE5AQSLC4DNCRZ/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/NWPTENBYKI2IG47GI4DHAACLNRLTWUR5/

Package: symfony/http-kernel

Version: 5.2.1

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://omkarjewelers.ssbmultiservices.com/

Development configuration files:

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

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

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

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

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

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

- https://omkarjewelers.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=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InUwZ3F4VHVKb2NJb296Qk5EbVJqMnc9PSIsInZhbHVlIjoiV0FBYmdlTzZ0L2txOWZ0MDIzdVVjeHI0VlJPZD
N4b1pRaGJmTkJNUFZsTWVxRVNsWS9ZL1RlM1NCRkVrZEY4b2RFa1VyYUN0S1dicVZ6STc3c3NWZGJBTEdsczZuVXRNbXVteEdHTT
lBY3h1SjhRV2E5eEdka3F0RG5qTSs3ZkgiLCJtYWMiOiIwYzhhN2EzNWU4MGI2ZDI2YTUzYTAxNGMyZjkxN2IwZjY4MGFhOTlkOW
EyMzE4Y2E1ZjNiNGMyMTkyOGJlYmQ4In0%3D;
omkar_jewelers_session=eyJpdiI6InVrUnFvL3h3WldPa2IvemN3RUpRRXc9PSIsInZhbHVlIjoiSE5EOEpjRmdrL3FZb2dkb
WhxQk9LelpneUQ3ajFPM1Q5aVRHQWN1ZVc4V1N5M2RTSWtIK0JhanFkTGF4THRpY0t1TkRUMUtBZVphUU5OWjBJTlFERjV6SGVjO
FJ5SmhPcjNyMUJhMFl1a3YzMmhLRFNjSEFmQlF4aWdITE5KZnMiLCJtYWMiOiJkZjcwNTEzMzEyMDY1ODY4ZmQyMjQzZWFiOWUzY
WQyMmU1ZmFlZWNhMGQzY2I0NTI2ODUwMDc5ZmJiYzQ5Zjc4In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Laravel debug mode enabled

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

Impact

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

https://omkarjewelers.ssbmultiservices.com/

Request

```
PUT /index.php HTTP/1.1
Cookie: PHPSESSID=77c2185b74c3f2845d6067aaa73c3ed9; XSRF-
TOKEN=eyJpdiI6IkY4KzNIRmNkKyswVmdtVDY3ZXUzZWc9PSIsInZhbHVlIjoiR3VaNEFBLzVjQ0xEUUNRclRyc0gweWRLSmRiL0
ZHOXpFQXYwSSs3MjBTcWExZnRyZlFEWDVzMmJ6TWErbytqK2VXdW5lTklYMVA3REtZU0ViSkloMnpUTWt6RnZDT0NkQVE2QWhuWn
F6Tis0VVdQSWV4SThPTDdWN3dkSEUya0MiLCJtYWMiOiI0NjZkM2FmODllYmVkODk0Nzc4OWU2NWE3YWQ2YjMxMDkwYTlkODM4NW
IwYmFhODJkMmZmYzE2MTcwODA4ZTdiIn0%3D;
omkar_jewelers_session=eyJpdiI6Ikc2WVBHWDV5ZDlOUWN0WFdERnF4c1E9PSIsInZhbHVlIjoicFhzelFnS0xlNzd1TU1MQ
W9tc2h6RzVGdWZwc01tVkJqZEVQNmIvOEZ6a1FtbDduZHpqVlROSGtrM05QMUQ3UlBqQjBJSEoxS2dKVk5SZWZNempQa0tWNnhHd
zY4dGczR2x5dnhEVEovM0pNWUdrQ0kyQmNpdWl3elF2dHd0SWgiLCJtYWMiOiI0YmFkZjA3ZmYyNDQzNDhlY2RmOWU3MzM1ZTgzM
GE2MzljMGFjNzE3OGQzMmUzOTdiMGM2Nzc1Y2VhZmQyNzg0In0%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: omkarjewelers.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 JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

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

- jQuery 2.2.4
  - URL: https://omkarjewelers.ssbmultiservices.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428

- https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

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

Recommendation

Upgrade to the latest version.

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://omkarjewelers.ssbmultiservices.com/project/

List of vulnerable **composer** packages:

Package: laravel/framework
Version: 8.22.0
CVE: CVE-2021-21263
Title: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
Description: Laravel is a web application framework. Versions of Laravel before 6.20.11, 7.30.2 and 8.22.1 contain a query binding exploitation. This same exploit applies to the illuminate/database package which is used by Laravel. If a request is crafted where a field that is normally a non-array value is an array, and that input is not validated or cast to its expected type before being passed to the query builder, an unexpected number of query bindings can be added to the query. In some situations, this will simply lead to no results being returned by the query builder; however, it is possible certain queries could be affected in a way that causes the query to return unexpected results.
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:L/A:N

CWE: CWE-89
References:

- https://packagist.org/packages/illuminate/database
- https://github.com/laravel/framework/security/advisories/GHSA-3p32-j457-pg5x
- https://github.com/laravel/framework/pull/35865
- https://packagist.org/packages/laravel/framework
- https://blog.laravel.com/security-laravel-62011-7302-8221-released

Package: laravel/framework
Version: 8.22.0
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: 5.2.1
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://omkarjewelers.ssbmultiservices.com/

Paths without secure XFO header:

- https://omkarjewelers.ssbmultiservices.com/
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://omkarjewelers.ssbmultiservices.com/project/vendor/autoload.php
- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux

- https://omkarjewelers.ssbmultiservices.com/upload/category-image/
- https://omkarjewelers.ssbmultiservices.com/about-us
- https://omkarjewelers.ssbmultiservices.com/all-categories
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://omkarjewelers.ssbmultiservices.com/all-products
- https://omkarjewelers.ssbmultiservices.com/contact-us
- https://omkarjewelers.ssbmultiservices.com/custom-jewelry
- https://omkarjewelers.ssbmultiservices.com/faq
- https://omkarjewelers.ssbmultiservices.com/privacy-policy
- https://omkarjewelers.ssbmultiservices.com/services
- https://omkarjewelers.ssbmultiservices.com/terms-of-use
- https://omkarjewelers.ssbmultiservices.com/index.php
- https://omkarjewelers.ssbmultiservices.com/products/others-ojzfv
- https://omkarjewelers.ssbmultiservices.com/index.php/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/cgi-sys/
- https://omkarjewelers.ssbmultiservices.com/database/

Request

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

Request

```
GET /project/vendor/composer/installed.json HTTP/1.1
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InUwZ3F4VHVKb2NJb296Qk5EbVJqMnc9PSIsInZhbHVlIjoiV0FBYmdlTzZ0L2txOWZ0MDIzdVVjeHI0VlJPZD
N4b1pRaGJmTkJNUFZsTWVxRVNsWS9ZL1RlM1NCRkVrZEY4b2RFa1VyYUN0S1dicVZ6STc3c3NWZGJBTEdsczZuVXRNbXVteEdHTT
lBY3h1SjhRV2E5eEdka3F0RG5qTSs3ZkgiLCJtYWMiOiIwYzhhN2EzNWU4MGI2ZDI2YTUzYTAxNGMyZjkxN2IwZjY4MGFhOTlkOW
EyMzE4Y2E1ZjNiNGMyMTkyOGJlYmQ4In0%3D;
omkar_jewelers_session=eyJpdiI6InVrUnFvL3h3WldPa2IvemN3RUpRRXc9PSIsInZhbHVlIjoiSE5EOEpjRmdrL3FZb2dkb
```

```
WhxQk9LelpneUQ3ajFPM1Q5aVRHQWN1ZVc4V1N5M2RTSWtIK0JhanFkTGF4THRpY0t1TkRUMUtBZVphUU5OWjBJTlFERjV6SGVjO
FJ5SmhPcjNyMUJhMFl1a3YzMmhLRFNjSEFmQlF4aWdITE5KZnMiLCJtYWMiOiJkZjcwNTEzMzEyMDY1ODY4ZmQyMjQzZWFiOWUzY
WQyMmU1ZmFlZWNhMGQzY2I0NTI2ODUwMDc5ZmJiYzQ5Zjc4In0%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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://omkarjewelers.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=77c2185b74c3f2845d6067aaa73c3ed9; 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://omkarjewelers.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=dcb555169544a82465235243a05acc4e; 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://omkarjewelers.ssbmultiservices.com/_ignition

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=ceed8df39226cfadfc52d97e6cf65e9c; 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://omkarjewelers.ssbmultiservices.com/cgi-sys/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=8adac7685311a85f91647f5cf617b908; 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://omkarjewelers.ssbmultiservices.com/subscribe

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=12115d5a6eb37da10c49c8862bd2f30e; 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://omkarjewelers.ssbmultiservices.com/database/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d26586053d8368676562c4a56fbd3ac4; 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://omkarjewelers.ssbmultiservices.com/product

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=08e1d8c7fc999fc33bcf26a6b7999d0b; 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://omkarjewelers.ssbmultiservices.com/products

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=a75f80f5558f712104d3037814311e11; 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://omkarjewelers.ssbmultiservices.com/contact-us

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=227ac480df08bb8b052b2b5496461e77; 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://omkarjewelers.ssbmultiservices.com/mailman/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=35f3bf6faa63d95f1c526d55124886fe; 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://omkarjewelers.ssbmultiservices.com/_ignition/health-check

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d365b66ce7ef5c05a46c28afc4353129; 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://omkarjewelers.ssbmultiservices.com/about-us

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=e4624d9661944042e1f9fd35c7d97194; 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://omkarjewelers.ssbmultiservices.com/all-categories

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=63272beda114ba435242615c252496fc; 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://omkarjewelers.ssbmultiservices.com/all-products

  Cookie was set with:

```
Set-Cookie: PHPSESSID=b30f776967235c8c3866215a6b380fc0; 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://omkarjewelers.ssbmultiservices.com/faq

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=d6d876705cec0d871bc93a2fab25a833; 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://omkarjewelers.ssbmultiservices.com/index.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=76a7a32fd89ff5c03bf1b9de20026398; 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://omkarjewelers.ssbmultiservices.com/privacy-policy

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=06d95d4697a7afc309deaead75d055da; 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://omkarjewelers.ssbmultiservices.com/services

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=35585f2d1458e50d7c5d361413123e16; 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://omkarjewelers.ssbmultiservices.com/subscribe

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=ccd9e0c2ae2f98db02d301c01f86fe01; 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://omkarjewelers.ssbmultiservices.com/terms-of-use

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=9d3690e3b9a4e962b6ff2c80377ce58a; 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://omkarjewelers.ssbmultiservices.com/custom-jewelry

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=14cee9b7bec7bde63e59b5dce51f2dc7; 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://omkarjewelers.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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=77c2185b74c3f2845d6067aaa73c3ed9; path=/
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkY4KzNIRmNkKyswVmdtVDY3ZXUzZWc9PSIsInZhbHVlIjoiR3VaNEFBLzVjQ0xEUUN
RclRyc0gweWRLSmRiL0ZHOXpFQXYwSSs3MjBTcWExZnRyZlFEWDVzMmJ6TWErbytqK2VXdW5lTklYMVA3
REtZU0ViSkloMnpUTWt6RnZDT0NkQVE2QWhuWnF6Tis0VVdQSWV4SThPTDdWN3dkSEUya0MiLCJtYWMiO
iI0NjZkM2FmODllYmVkODk0Nzc4OWU2NWE3YWQ2YjMxMDkwYTlkODM4NWIwYmFhODJkMmZmYzE2MTcwOD
A4ZTdiIn0%3D; expires=Wed, 03-Jan-2024 06:33:05 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikoyd3FtUGxiL3pKMXRvWU5XV1Q5WlE9PSIsInZhbHVlIjoiTzN5azBJNkZwTUhVL2w
3Ym56blFZbHRiak9CTE1veUJjZ29GL3htdmk2SmxPQU5GVGNySGVEdVpWdUJCZFZScmdoS3JBd1ZZUmp2
OUFLMDl6U3hpWGN5dm5PTWNFRTM4eUVwUkE4a1MyV05OeGZGWTV1QXMwbll1MGd4NzBZcDEiLCJtYWMiO
iI0YzQwMTJmMDQyOWQ5MmRkOTFjNmY3ZmVjNDNiMDM0OGI0NWJmZmZlMDIyNWU4NGUyZTc5ZTQwMjljND
```

```
QwMmQzIn0%3D; expires=Wed, 03-Jan-2024 06:34:15 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklnTkxxbkllWHZBdEVrakgydkE2NHc9PSIsInZhbHVlIjoiblMyQjlJSXNRTSs1aU5
LSnVSQ21IWGYwRHlMc2syRENTM1h3a1RtR08rZDhIdEpPS0llaTU2STd0ekJIYmxMRzlLUEs2T2VEOGhY
RldlenJMVFp5Vlh3SU9pYXNlSVllcXJZSUtxRnBmYkhZT284YTdTWHZSYUFXdll3UjMvcVciLCJtYWMiO
iI5NjMzMGE4NjI0YTdiODgxZTQ2YTU3MzAyYTBjMjFmNzIzYWY4ZDJkMDM3MjM3YTI1MjRjMGZiMjk2Ym
YyZDljIn0%3D; expires=Wed, 03-Jan-2024 06:36:50 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InUwZ3F4VHVKb2NJb296Qk5EbVJqMnc9PSIsInZhbHVlIjoiV0FBYmdlTzZ0L2txOWZ
0MDIzdVVjeHI0VlJPZDN4b1pRaGJmTkJNUFZsTWVxRVNsWS9ZL1RlM1NCRkVrZEY4b2RFa1VyYUN0S1di
cVZ6STc3c3NWZGJBTEdsczZuVXRNbXVteEdHTTlBY3h1SjhRV2E5eEdka3F0RG5qTSs3ZkgiLCJtYWMiO
iIwYzhhN2EzNWU4MGI2ZDI2YTUzYTAxNGMyZjkxN2IwZjY4MGFhOTlkOWEyMzE4Y2E1ZjNiNGMyMTkyOG
JlYmQ4In0%3D; expires=Wed, 03-Jan-2024 06:37:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkdQck1QbVNZcUxWcFBPa2F3Zm53N1E9PSIsInZhbHVlIjoiUG50WWh2QS9zV3g2OWF
NNXlwMkpRQnZ4elBhRWxuL0g3bWhlUi8wNTFXMWFCV094UHRsL2lXck9aRnZVSkpScVMxTlhVSHByWVNp
M2gySEdUOU9nZ3lwdDBXYlNJa3loQU9CdFNsNWJFc2pKdng1T2V1V2NYdUdpZk1UN2xhbnYiLCJtYWMiO
iIyMmVlMzg2MjRjNDQ2MmUyZDc2NjVjZTQ3OTgwMzQ2OGUyY2Q4Njc5ZTAxMjI5MGJkNjg5NTM4OWEyZj
U4NDU3In0%3D; expires=Wed, 03-Jan-2024 06:34:24 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjZzSkdTZEpWeG1NdFc0NjNGS0dNL1E9PSIsInZhbHVlIjoiRnVnSFlEVHB2amhXZ2R
UOVRZM083eXNJcGZwRVF5V0NtWEZWd3N1Zi9BNEw4eWJ2bUJQcnhoTVBqcThTcHZYdWF0c08yOVpLcFc5
cUd4OE1zWjVJWWRySlVkNWNlaStDK21iZ0lyYnNKMGk0OTBnZ2owM3ZWVVhIaEFQa2twc2MiLCJtYWMiO
iIwZjIyN2RiNjc3YzFlMjRlYTUxMjQ5YTQ1MzQzNTk5NzFhNDcwOWZjMzBmYTkxZGI0OGMwODU4Mzk2OD
```

```
c2YmFjIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImwxRWdiUllIRFhocHppdTBFRmJBY0E9PSIsInZhbHVlIjoiQkoyUytyVGV4QUVncGh
OWTMxeUZWN2R1Nm1LektwSUdBQlpSOVFLSDVMMzVDMzVuRGhPYy9SdFpaMGk1bFpaN1ZUUEFyZ3BDV04r
cDBZRlNudlFId05GZ0M5Rmlya0kzcG5Reit0MHBpcVdEYVpLRXJJTjZkU2pHci9ldTBFeFEiLCJtYWMiO
iJlNDc1OTI5MDVlZDA0YmQzYmIzNzMzNWQwZDQ3MmYzMmVhZDgwYjdmMTdiMTEzMGY0OTI4ZTM3NDFlNm
E5YjdlIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlBKVEhUUm11a01hZnFiWHYvbVQvOGc9PSIsInZhbHVlIjoiMVdKcGp2Z1dTUWU4VGR
vT0tnQkdsQnE1SExlM2tRZGtBVzdWRVVQSTFDRDd0ZEJDK21iaTNRZCtOQ3hzZTVHWUU1NDhjd0JOUkZ6
VDlkWDNGQ1Z2K3JaNU1oNG1ZNzFuQlhzdmJtY0UrRnQ0Zi9TZXM0dk44NjZLNkpKYVR2MkYiLCJtYWMiO
iI3Mjk4MGZkNjgzMWE4MGMwNDgxYzRkMWZhYTFjNWEzY2IzNzE1NjlkOGEwNmI0MWVjMmY0NTNhNWM5OG
U2ZDZlIn0%3D; expires=Wed, 03-Jan-2024 06:38:40 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IndiYUlaOWNiVFVJVUdoLzVIdkV0bUE9PSIsInZhbHVlIjoiVCtqY0xnTGJ4R2IvdkN
kNHlBSkkxRUpzK25Rc1ZxSXNZSHJ3d2dqK1Z1bHJReEhCaGZtMlZwaktnbHdOZGJxQVh6ZnZicjc1dUND
NU9PZStDM3EyanNtVXplL2p2Wkg3WENCeWh3bVFHVnpZaThRVTdzL1BZNzdoU1plakdyY1MiLCJtYWMiO
iI0NzMzMWVkZTQwY2ZkZGI1NDg1NWViOWMyMTY1ODQ3OTJkMmNjODJiOWYxNTBlNzVjYTZjZTNjYWZjNm
YwZmVjIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikl2emMvYVVCVUtHVVprcGFuTFBjbWc9PSIsInZhbHVlIjoiOFRKbW9aanRrd3Bjd1N
nbk40WHkxbk83eFoyYlJmUnVBQXBPcE9za1pJU3hHdVAwVC9oSGRMYXc1NlhJK1pFdldvOUVtajI2c0hn
TFNxT0hSQUhQYW5IQW9uT1g4eUJyWkZ6WUdzZzdJNU5hS2pSYUxBU25Ecm9QelRxWXBWMTMiLCJtYWMiO
iIzNTQyYTAzMjA1Y2M4OWQyNTQ1NmMyOTk4YjM0YjJhNTI3YjEyNzQ5NzM2ZGY1MWNiMzU0NTFmZTc4Nz
```

```
g3ZjMzIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/all-categories

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpyZ3ZWL1ZmOTlMWnhNcW5jS2lsVnc9PSIsInZhbHVlIjoiMWFOVmFpY3FpRCsvN1V
KK2hQZDJBRWxUVWNZRW1uc3V5VXNoV3k3bGlnY0N3dXhnNTYxY3F1aW1nR2xyTFpRSDJpd2Q4VU1ua1JO
amRXVC9lSVRwdWRHc1FVTkRaOGZJVnBPZmtrTHNybHI0KzlLNDcxcWcxOWtuakpXMWhuaHAiLCJtYWMiO
iI1NGIxNzdmZTQ3YmIwOTRiNzM5NTZkM2FjZmUwYjc1MzNjODQ3NzdjYTBiNDM3YjExMTE5NGM1MjYyOT
U3NzcwIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Im02N0QyNERPOXFzeC9IaW9TdHdUaVE9PSIsInZhbHVlIjoiUmRxL0t4ci80Uk84QlJ
HMnN1VmNyckhySVQ4d3pqWWRhUHB1NzhQU2k5d3JWZXJqQ0IwTzA0WnFKcjFFVzBSb3M1dGJIcnd1VlYz
d3FNMVdIVXdHR0ZkWWZPL28xNm00U1ZOQk9RUDhmWCtXRGZySm1wcXNaY0JSN3lNdy9oSVUiLCJtYWMiO
iI1YzY0MTc1YWZlNTllNDkzNzc3ZDU1ODA0MTVhMGYwNzQ1ZGM5MmU3Yzc0MjU2ZTM1ZGRkOTk0YWU5OW
YyZDgxIn0%3D; expires=Wed, 03-Jan-2024 06:39:08 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/all-products

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Imo2TmYyWlJoL3JFdm55VWE0UER4SFE9PSIsInZhbHVlIjoiY3RjQ0YxYW9ESG9OamZ
iUisxWnlhRG03aGE1YkZQZ1UyVGc1SHQ1TmxHdDBYVHNYY1VZWnE0ZWduNGh0YXBNYWlvdEFTNE5uZi9S
VnhnNlZSTnV5NE5xVVZnK1ZCalpmK1EzbG9XV1hGRmZKQmR2UXB6UExNNXBGOHFIY0dPWjgiLCJtYWMiO
iIzOTUxM2NjNTI2ZjY1YzQyNmFiOTY0YjUxM2ZjYWZmYjRiNWMwMDBlNTUyYTdiOWZmNTY3NDc4YTlkOD
Q5YTM5In0%3D; expires=Wed, 03-Jan-2024 06:39:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImxoVlVhZGJTM3R4dm5ETHBqL1VTNnc9PSIsInZhbHVlIjoiTlE3eGdyQmg4TFZYbGp
QV2xXSHd6cTV2SnQwSXNRWG5wdG0zVTRYOUJMbEdKSGRXRlNhOUJVUktZQlY0cHJCRmFrRUt1N2ZEWUdZ
dHpLSWc0NzNMSjZkU0g1OEJycmQ2NGdHSTZ2OVJ0WGdFZWJ4UFZNdEZkWmZyOHFtSzZCN3kiLCJtYWMiO
iI4MTA5YmE0ZWQyZWM3YTM0N2Q1NjZlMzBiYjAzMTAwY2FjZmNmMDE2ZjA2ZTA0YzZiNTRiOWE3YmViZj
```

```
g3N2JjIn0%3D; expires=Wed, 03-Jan-2024 06:39:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/custom-jewelry

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjZwVCs0MHJKSm9yYjZtVmticlZEY1E9PSIsInZhbHVlIjoibml3aE5pYzhpY3RIR2x
VRDhiVnJVMDVvYkVlMWpNTzhhN09CcWJNQ0VaVlk1ejZuTytNQmxraEZSSkR6NjAzMFJDUVZ5V0p5NG5y
TXZEd3MvVWljVVhZeVYrVzZzWGZibHdzY01MSFpwMHBGeVppdmJLRnVHbkRyVFdaNUh2SDMiLCJtYWMiO
iJmYmNjODEzNjIwYmZhODcwOWUxYzA3NDhjNGRlMTAwNDMxZGEwZjBlYmFjZGFmNGZkMjYyNDhlZDllOD
E5NjQxIn0%3D; expires=Wed, 03-Jan-2024 06:39:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/faq

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkRVeUNIZW1ublhNY2k0L2V3dlRrWVE9PSIsInZhbHVlIjoiT2QwTGUwak5tWnBEd2M
zWkR6bXZRRTlpWklaQ0ZVcUN4KzZkNUhqOGN2dGljMm5wNk5PUnhnSkMrNTJOSUdNWCtzNlpQTlFaT1dY
djRpTnJFckdWTHJsK0NHR1NpcEY2V3FvUnd4WThkUnYwYTJqSTVBYW04TnFaV0lQTnJyOSsiLCJtYWMiO
iI5NjhmMzNkZTA4NGFjMDYzYmZlOWUxYjVmODk4ZDE3OWQ5MGRlNTY4NmUwMzJmYzI1ZTMzOTJiNDY2MD
k3OTFhIn0%3D; expires=Wed, 03-Jan-2024 06:39:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InJOZGs0NEFacDRwdEltNlR0Zlc1cXc9PSIsInZhbHVlIjoiSHp6QllLTy83NkxVZmt
rVHlXcGdPSXN4a2JzYlIyTTM1UjRiL0VJbG9VTWNtSlJFZm1ydXhwK3RmZHF3MWkyNDl0eWo0WWc0MTVQ
dVRWVmlJTXlDWXM1eHltRUlBTTQ5OVFiVzR3VU9aYmphbXVjWTVnMmtCdlFTRXkvWjQ5UnMiLCJtYWMiO
iIzYzQ2OWQzMjk5OGRlNWJjNjY4NzAwNDU0MDUxN2FkNzY1YTI5YzlmYWJmMjg4Nzc2YjNlZmRkNTE5Nz
YxNTE3In0%3D; expires=Wed, 03-Jan-2024 06:39:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/services

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjRFL2lZbXorS2VGVHRwNzkrcDd0c0E9PSIsInZhbHVlIjoiUU9rZ3F4aHJTcVIzenY
rOFdKUGdCUjNVRlhaTndBeVJ0UTIrNTRtS1F0T09IZGFzRVd0VnpoZCtFaVNQYk5jempwZU9VY21UcG5T
NzR3dGxxS2NHbTVJanVNdllMK0psaFhpVTF6QWVCV3g2K2JxY1BYUjVOaXd0bjJKcHN6VnYiLCJtYWMiO
iI2OTUyYzA0YmE4OWFhMWIyNTgzNDNjNWYyY2VjNjc3ODRjZDRiYWMzM2JkNGU4NjM2NjQ5NTM5MzI4MD
```

```
E2YTRjIn0%3D; expires=Wed, 03-Jan-2024 06:39:12 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/terms-of-use

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkwxUitqc3ppT3hGdm1QZEU2bmJEYkE9PSIsInZhbHVlIjoic1NtZ3BuYmFkRHVrLzF
QekZFbGk3S2FkbGgxRDNjZU5zNzU5U3ZROWdJY3ZCOHdUWG5QMDR2SHN6Y2lVRjhRejkyU1FCV3dIMlJk
ZTdqZnAxbmZFL0VEUVVjWVhKREZyeUxBdWU2U3UwQVZDejQzOFgxaEYwUE1JMkIzVllxMVYiLCJtYWMiO
iI5ZjdmNmIyZDY1MWYxMmY4YWI0YTVhZGRhZjMwODdlYjVkY2NiZmZlMDFiMzY2OWE1ZjQ1NzlmMjZmMz
M4Y2YwIn0%3D; expires=Wed, 03-Jan-2024 06:39:29 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlB5NmUyazJzeit3S1hiUzY2TTNxdHc9PSIsInZhbHVlIjoiNlB2amZubkdYbDVCbmh
GdlRKWDVISjUzZndUK1RIbDB4ZmRBOGdLR1UvdDVESFljZDN3UFl2S05KSk1sWmRCWWFRQ3pLNVp3OUNO
K2RjTFJDTnd6S2NpQVlYdUU3S3F3SSswY2hsZ1liaTgzSGNJVlZ1Wkh6WkViS2sxNG1Yd0MiLCJtYWMiO
iIzYmZiN2MwNjdmM2ExNWI2MzU4ZmQ1YWNiZmU5MzAzZWI4YzY3NzM0ZmYzNGVjYmRjYmNmOTA5MzAxOT
E5MDQ2In0%3D; expires=Wed, 03-Jan-2024 06:39:30 GMT; Max-Age=7200; path=/;
samesite=lax
```

Request

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

Cookies without Secure flag set:

- https://omkarjewelers.ssbmultiservices.com/

  ```
  Set-Cookie: PHPSESSID=77c2185b74c3f2845d6067aaa73c3ed9; path=/
  ```

- https://omkarjewelers.ssbmultiservices.com/

  ```
  Set-Cookie: XSRF-
  TOKEN=eyJpdiI6IkY4KzNIRmNkKyswVmdtVDY3ZXUzZWc9PSIsInZhbHVlIjoiR3VaNEFBLzVjQ0xEUUN
  RclRyc0gweWRLSmRiL0ZHOXpFQXYwSSs3MjBTcWExZnRyZlFEWDVzMmJ6TWErbytqK2VXdW5lTklYMVA3
  REtZU0ViSkloMnpUTWt6RnZDT0NkQVE2QWhuWnF6Tis0VVdQSWV4SThPTDdWN3dkSEUya0MiLCJtYWMiO
  iI0NjZkM2FmODllYmVkODk0Nzc4OWU2NWE3YWQ2YjMxMDkwYTlkODM4NWIwYmFhODJkMmZmYzE2MTcwOD
  A4ZTdiIn0%3D; expires=Wed, 03-Jan-2024 06:33:05 GMT; Max-Age=7200; path=/;
  samesite=lax
  ```

- https://omkarjewelers.ssbmultiservices.com/

  ```
  Set-Cookie:
  omkar_jewelers_session=eyJpdiI6Ikc2WVBHWDV5ZDlOUWN0WFdERnF4c1E9PSIsInZhbHVlIjoicF
  hzelFnS0xlNzd1TU1MQW9tc2h6RzVGdWZwc01tVkJqZEVQNmIvOEZ6a1FtbDduZHpqVlROSGtrM05QMUQ
  3UlBqQjBJSEoxS2dKVk5SZWZNempQa0tWNnhHdzY4dGczR2x5dnhEVEovM0pNWUdrQ0kyQmNpdWl3elF2
  dHd0SWgiLCJtYWMiOiI0YmFkZjA3ZmYyNDQzNDhlY2RmOWU3MzM1ZTgzMGE2MzljMGFjNzE3OGQzMmUzO
  TdiMGM2Nzc1Y2VhZmQyNzg0In0%3D; expires=Wed, 03-Jan-2024 06:33:05 GMT; Max-
  Age=7200; path=/; httponly; samesite=lax
  ```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikoyd3FtUGxiL3pKMXRvWU5XV1Q5WlE9PSIsInZhbHVlIjoiTzN5azBJNkZwTUhVL2w
3Ym56blFZbHRiak9CTE1veUJjZ29GL3htdmk2SmxPQU5GVGNySGVEdVpWdUJCZFZScmdoS3JBd1ZZUmp2
OUFLMDl6U3hpWGN5dm5PTWNFRTM4eUVwUkE4a1MyV05OeGZGWTV1QXMwbll1MGd4NzBZcDEiLCJtYWMiO
iI0YzQwMTJmMDQyOWQ5MmRkOTFjNmY3ZmVjNDNiMDM0OGI0NWJmZmZlMDIyNWU4NGUyZTc5ZTQwMjljND
QwMmQzIn0%3D; expires=Wed, 03-Jan-2024 06:34:15 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Ik5heVdPRk5lSmthYzdCOC80VUI3SEE9PSIsInZhbHVlIjoieE
Vod1h0R2FWVVlSU3lwZ2xsczJiUnZHZDROVDZoS1pyd3NjRTU1YjdDOTFueXNsUTRhbU5oVnpMc0VMSXl
UZFhDSU9FRTc2QytkN1N4U2dqRTNUZktBQWhIbk1yZERwQi9qY0JrMUN2S3VIcmxqU2ZaT2JjcHcxMXhH
T01uOWciLCJtYWMiOiIwZmZiM2U0YTZmZGE0NTRhNDljZjU4NDI2ZTY5MzkyYmE1NjFkNDIzOTk4MWMxZ
TA3Zjk5Y2I4YjEwZWFjZWFjIn0%3D; expires=Wed, 03-Jan-2024 06:34:15 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IklnTkxxbkllWHZBdEVrakgydkE2NHc9PSIsInZhbHVlIjoiblMyQjlJSXNRTSs1aU5
LSnVSQ21IWGYwRHlMc2syRENTM1h3a1RtR08rZDhIdEpPS0llaTU2STd0ekJIYmxMRzlLUEs2T2VEOGhY
RldlenJMVFp5Vlh3SU9pYXNlSVllcXJZSUtxRnBmYkhZT284YTdTWHZSYUFXdll3UjMvcVciLCJtYWMiO
iI5NjMzMGE4NjI0YTdiODgxZTQ2YTU3MzAyYTBjMjFmNzIzYWY4ZDJkMDM3MjM3YTI1MjRjMGZiMjk2Ym
YyZDljIn0%3D; expires=Wed, 03-Jan-2024 06:36:50 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Ik9FazJRQkhBeEg5Q25mVE9tUTVHVkE9PSIsInZhbHVlIjoiWm
5GM0J0K0tSS1g1MEttSlh4QVZuRnBKQUpkTzNySE9Tc2J5NXlJcldjcm55WnFDZDFXcXdZUHB4TzJvcit
ZaWNrSHNGWkxNSmNSQjYyUWNkQWREVmNhbVpaYUN1TXhndlJCN1lneTNWSFprL2dHRE1ibGNSdjRySjlH
OC9zR1MiLCJtYWMiOiI5MGVmOWE4N2M1Y2U0OWViNzNmMjEzNDljYTc4NWE1ZDhmZjVkMmI3NDViNDM3Z
mI4MTEyYzJlYzcyZTA4NDNjIn0%3D; expires=Wed, 03-Jan-2024 06:36:50 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InUwZ3F4VHVKb2NJb296Qk5EbVJqMnc9PSIsInZhbHVlIjoiV0FBYmdlTzZ0L2txOWZ
0MDIzdVVjeHI0VlJPZDN4b1pRaGJmTkJNUFZsTWVxRVNsWS9ZL1RlM1NCRkVrZEY4b2RFa1VyYUN0S1di
cVZ6STc3c3NWZGJBTEdsczZuVXRNbXVteEdHTTlBY3h1SjhRV2E5eEdka3F0RG5qTSs3ZkgiLCJtYWMiO
iIwYzhhN2EzNWU4MGI2ZDI2YTUzYTAxNGMyZjkxN2IwZjY4MGFhOTlkOWEyMzE4Y2E1ZjNiNGMyMTkyOG
JlYmQ4In0%3D; expires=Wed, 03-Jan-2024 06:37:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6InVrUnFvL3h3WldPa2IvemN3RUpRRXc9PSIsInZhbHVlIjoiSE
5EOEpjRmdrL3FZb2dkbWhxQk9LelpneUQ3ajFPM1Q5aVRHQWN1ZVc4V1N5M2RTSWtIK0JhanFkTGF4THR
pY0t1TkRUMUtBZVphUU5OWjBJTlFERjV6SGVjOFJ5SmhPcjNyMUJhMFl1a3YzMmhLRFNjSEFmQlF4aWdI
TE5KZnMiLCJtYWMiOiJkZjcwNTEzMzEyMDY1ODY4ZmQyMjQzZWFiOWUzYWQyMmU1ZmFlZWNhMGQzY2I0N
TI2ODUwMDc5ZmJiYzQ5Zjc4In0%3D; expires=Wed, 03-Jan-2024 06:37:22 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkdQck1QbVNZcUxWcFBPa2F3Zm53N1E9PSIsInZhbHVlIjoiUG50WWh2QS9zV3g2OWF
NNXlwMkpRQnZ4elBhRWxuL0g3bWhlUi8wNTFXMWFCV094UHRsL2lXck9aRnZVSkpScVMxTlhVSHByWVNp
M2gySEdUOU9nZ3lwdDBXYlNJa3loQU9CdFNsNWJFc2pKdng1T2V1V2NYdUdpZk1UN2xhbnYiLCJtYWMiO
iIyMmVlMzg2MjRjNDQ2MmUyZDc2NjVjZTQ3OTgwMzQ2OGUyY2Q4Njc5ZTAxMjI5MGJkNjg5NTM4OWEyZj
U4NDU3In0%3D; expires=Wed, 03-Jan-2024 06:34:24 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IitjSGpkTVY5cDB5eTYybnRMbWJ1RVE9PSIsInZhbHVlIjoiNF
pZbGgxbTVTQU90VDNjb0xQeE13NTl5TWFkb1YyTGp6aXo3UHdPSHQ2Sm91MW1QczQrRXZvVmxhaHVlZUN
qa2E4K0wwMkNuc28rakNPZExBUFgvZjBPUDFYbFNUd1NJSklGalFhclpMazh1SEs4QnJDeFBOVE1JSlVh
REhpdm8iLCJtYWMiOiIyNTlmYTcyZjU2ZDYwY2M3NGU3YWQ4NTY5ZWY2M2UwZDcwZmZmYmU1Y2NiNDQ4Z
jExZDM5YzNjYWU4ZTEwZmY0In0%3D; expires=Wed, 03-Jan-2024 06:34:24 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjZzSkdTZEpWeG1NdFc0NjNGS0dNL1E9PSIsInZhbHVlIjoiRnVnSFlEVHB2amhXZ2R
UOVRZM083eXNJcGZwRVF5V0NtWEZWd3N1Zi9BNEw4eWJ2bUJQcnhoTVBqcThTcHZYdWF0c08yOVpLcFc5
cUd4OE1zWjVJWWRySlVkNWNlaStDK21iZ0lyYnNKMGk0OTBnZ2owM3ZWVVhIaEFQa2twc2MiLCJtYWMiO
iIwZjIyN2RiNjc3YzFlMjRlYTUxMjQ5YTQ1MzQzNTk5NzFhNDcwOWZjMzBmYTkxZGI0OGMwODU4Mzk2OD
c2YmFjIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IjR1TE1rOGtKQm1xb0U4czVzOGJua1E9PSIsInZhbHVlIjoibH
ZhUVpzbmZPMDNEL1BYbEJTUHA4UGFSNHE1dkVQOHl3TittcStPckorRVhyYjV6eVlRa29PVTdRTVJPSm9
0czR2czFvYms1cGd3djNTME1Ia1FwT2l0ejJGRUk2bWlxajkxYjg3VXRpQXNJUzkvTkV3VDNLVkxlV0xo
dmM0WGkiLCJtYWMiOiI4Zjc5ZmZmYTJjNWY0NTVlMDdhMDgzMTRkZDBjY2JlYTMwOGNkZjUzYjc2MmYxN
DUyODBmMzVjNzQ0NTFjZWFhIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImwxRWdiUllIRFhocHppdTBFRmJBY0E9PSIsInZhbHVlIjoiQkoyUytyVGV4QUVncGh
OWTMxeUZWN2R1Nm1LektwSUdBQlpSOVFLSDVMMzVDMzVuRGhPYy9SdFpaMGk1bFpaN1ZUUEFyZ3BDV04r
cDBZRlNudlFId05GZ0M5Rmlya0kzcG5Reit0MHBpcVdEYVpLRXJJTjZkU2pHci9ldTBFeFEiLCJtYWMiO
iJlNDc1OTI5MDVlZDA0YmQzYmIzNzMzNWQwZDQ3MmYzMmVhZDgwYjdmMTdiMTEzMGY0OTI4ZTM3NDFlNm
E5YjdlIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Ii9YUU9MZU9mVTBXL084U1hpSkpEbUE9PSIsInZhbHVlIjoiRn
cwYXNtTzJhcHozdmJnb0hHNmpjcmxXZTJNQ1VpUWkzSVNVdjRUeVZyL3NLOUQxamJ5MmNiOTJPM3FZTHd
hYzdPamo1ZDFJbms0eFRyUzVWT09BTzRjNTJZczdQR29UTlVIc29ZQzZKWDRpbDZWNWNSY2JhRUNNZzVh
YVh6SG0iLCJtYWMiOiIxYTk1YTExODVjNjVhYjA4YTM3NzAzZTlhZmFlMDU3YjNkNzQyMjczNzAyZmExN
TFlM2NlYWY4YzQ1ZmU0ZGRlIn0%3D; expires=Wed, 03-Jan-2024 06:38:33 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlBKVEhUUm11a01hZnFiWHYvbVQvOGc9PSIsInZhbHVlIjoiMVdKcGp2Z1dTUWU4VGR
vT0tnQkdsQnE1SExlM2tRZGtBVzdWRVVQSTFDRDd0ZEJDK21iaTNRZCtOQ3hzZTVHWUU1NDhjd0JOUkZ6
VDlkWDNGQ1Z2K3JaNU1oNG1ZNzFuQlhzdmJtY0UrRnQ0Zi9TZXM0dk44NjZLNkpKYVR2MkYiLCJtYWMiO
iI3Mjk4MGZkNjgzMWE4MGMwNDgxYzRkMWZhYTFjNWEzY2IzNzE1NjlkOGEwNmI0MWVjMmY0NTNhNWM5OG
U2ZDZlIn0%3D; expires=Wed, 03-Jan-2024 06:38:40 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Ik5mNjNRaFQ3QnN6bGdmdmVCVThjN0E9PSIsInZhbHVlIjoicC
s1aFloeVhiV1NPY01PSHZRNVRQLzdIV3J4R3RxUExWTm1CNjBNbFJIVllRTXZpQUl6NUthZytsQnhvL3Q
yY0M0VXZrek1qTW83NTlJcGNTRWo5UldheUVPUlNoSnRZcldJejVMcXBSQ1dHSnI4amNKTXp1c0xnZVVa
YUovemIiLCJtYWMiOiJjNTdmZGYwYzhjNTkzNmMyYTBmMTc3NWQ4YzMwMDRiYzkyZmNiZjdkZWVmZGI5M
2RiZDM5NTk5MjliNThkN2NkIn0%3D; expires=Wed, 03-Jan-2024 06:38:40 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IndiYUlaOWNiVFVJVUdoLzVIdkV0bUE9PSIsInZhbHVlIjoiVCtqY0xnTGJ4R2IvdkN
kNHlBSkkxRUpzK25Rc1ZxSXNZSHJ3d2dqK1Z1bHJReEhCaGZtMlZwaktnbHdOZGJxQVh6ZnZicjc1dUND
NU9PZStDM3EyanNtVXplL2p2Wkg3WENCeWh3bVFHVnpZaThRVTdzL1BZNzdoU1plakdyY1MiLCJtYWMiO
iI0NzMzMWVkZTQwY2ZkZGI1NDg1NWViOWMyMTY1ODQ3OTJkMmNjODJiOWYxNTBlNzVjYTZjZTNjYWZjNm
YwZmVjIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://omkarjewelers.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Imd3WWpKeHFIakVpT0ljY2pOYUx0bHc9PSIsInZhbHVlIjoiYm
ZsVVdTUDM0L2p6SWdXMnltb0szaGZQK3FQa1h5QnhpVXdTMXBsRTRPaVptLzhSdnRBN2RQc1llTWR3YVd
sTkllU1JOemFQRWZaSHNzVEYycWtHVlBCMjJvT3NLWEtUYVFjVjMrR2xSZjJZSldUUlhISlp4aEdESnlM
UEo4S1AiLCJtYWMiOiIwNzUwY2FlOWIwYThkOWQzMjAxOTYxMGZlOWZlMWU3ODMxYzA4ZDk3NzAzMWZkO
DhjZTA5N2I4NzEwN2JiZTVjIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikl2emMvYVVCVUtHVVprcGFuTFBjbWc9PSIsInZhbHVlIjoiOFRKbW9aanRrd3Bjd1N
nbk40WHkxbk83eFoyYlJmUnVBQXBPcE9za1pJU3hHdVAwVC9oSGRMYXc1NlhJK1pFdldvOUVtajI2c0hn
TFNxT0hSQUhQYW5IQW9uT1g4eUJyWkZ6WUdzZzdJNU5hS2pSYUxBU25Ecm9QelRxWXBWMTMiLCJtYWMiO
iIzNTQyYTAzMjA1Y2M4OWQyNTQ1NmMyOTk4YjM0YjJhNTI3YjEyNzQ5NzM2ZGY1MWNiMzU0NTFmZTc4Nz
g3ZjMzIn0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IkR3MXRSU3JuRmQ2OHZjNTNNSkMyN0E9PSIsInZhbHVlIjoibT
JGaFJ2b05qU2l4a0ViUmhrdThhcU5wYWtoTzZGZ1p4d3orVjZuZnN4S016ZzJOM2xzMkdEcml0ZTJmbFV
nSlMrd1RBTHNDWTR3UFpXcXpaSjBmM0JCTzR5dk1UQ2ZQeE1TM09sbnJtTHBQRm1Eb0c2MkJVZ3o3d21Z
Mkg5ZWYiLCJtYWMiOiJjNzkwYzcwMWUyZjQwODE3OWJhOGI0YzAzOWJiM2VkOTllYTY0ZmQ0YWNmNzFkZ
WQ5ZTM1OWNjNGZkMGM3ZWI0In0%3D; expires=Wed, 03-Jan-2024 06:38:53 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

Request

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

Recommendation

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

HTTP Strict Transport Security (HSTS) not implemented

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

Impact

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

https://omkarjewelers.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://omkarjewelers.ssbmultiservices.com/
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://omkarjewelers.ssbmultiservices.com/project/vendor/autoload.php
- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/upload/category-image/
- https://omkarjewelers.ssbmultiservices.com/about-us
- https://omkarjewelers.ssbmultiservices.com/all-categories
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://omkarjewelers.ssbmultiservices.com/all-products
- https://omkarjewelers.ssbmultiservices.com/contact-us
- https://omkarjewelers.ssbmultiservices.com/custom-jewelry
- https://omkarjewelers.ssbmultiservices.com/faq
- https://omkarjewelers.ssbmultiservices.com/privacy-policy
- https://omkarjewelers.ssbmultiservices.com/services
- https://omkarjewelers.ssbmultiservices.com/terms-of-use
- https://omkarjewelers.ssbmultiservices.com/index.php
- https://omkarjewelers.ssbmultiservices.com/products/others-ojzfv
- https://omkarjewelers.ssbmultiservices.com/index.php/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/cgi-sys/
- https://omkarjewelers.ssbmultiservices.com/database/

Request

```
GET / HTTP/1.1
Referer: https://omkarjewelers.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: omkarjewelers.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://omkarjewelers.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://omkarjewelers.ssbmultiservices.com/
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6Im02N0QyNERPOXFzeC9IaW9TdHdUaVE9PSIsInZhbHVlIjoiUmRxL0t4ci80Uk84QlJHMnN1VmNyckhySVQ4d3
pqWWRhUHB1NzhQU2k5d3JWZXJqQ0IwTzA0WnFKcjFFVzBSb3M1dGJIcnd1VlYzd3FNMVdIVXdHR0ZkWWZPL28xNm00U1ZOQk9RUD
hmWCtXRGZySm1wcXNaY0JSN3lNdy9oSVUiLCJtYWMiOiI1YzY0MTc1YWZlNTllNDkzNzc3ZDU1ODA0MTVhMGYwNzQ1ZGM5MmU3Yz
c0MjU2ZTM1ZGRkOTk0YWU5OWYyZDgxIn0%3D;
omkar_jewelers_session=eyJpdiI6ImMwamZTaDJvSTA2UjdYOG9vZm9STUE9PSIsInZhbHVlIjoidWhXY3IzUTRzVTliV0x6O
UxXaWFadUltamttN3NOdWNBbXBabndxSEpMa3JoTmhaTUFGVjVmRXhMU3cxNWM4NkU0UE5FZTFoNTNRZlJVK2wvZWdhcHk0UWMzR
25qQzJLWGt2Z1ZCQlMwMUZBY2N3YitiYmhIMVdkWTlPUk42YnMiLCJtYWMiOiJiZTYyMDc1ZjZiMzI2ODg1MjgxMjhjZGRkZGQ4M
TZkZjk2NjQwMGUzYzQ4YzFkY2Y2YWQ2ZTBiNDU1ZTE2Mjc0In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/custom-jewelry Verified

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

Request

```
GET /custom-jewelry HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6Im02N0QyNERPOXFzeC9IaW9TdHdUaVE9PSIsInZhbHVlIjoiUmRxL0t4ci80Uk84QlJHMnN1VmNyckhySVQ4d3
pqWWRhUHB1NzhQU2k5d3JWZXJqQ0IwTzA0WnFKcjFFVzBSb3M1dGJIcnd1VlYzd3FNMVdIVXdHR0ZkWWZPL28xNm00U1ZOQk9RUD
hmWCtXRGZySm1wcXNaY0JSN3lNdy9oSVUiLCJtYWMiOiI1YzY0MTc1YWZlNTllNDkzNzc3ZDU1ODA0MTVhMGYwNzQ1ZGM5MmU3Yz
c0MjU2ZTM1ZGRkOTk0YWU5OWYyZDgxIn0%3D;
omkar_jewelers_session=eyJpdiI6ImMwamZTaDJvSTA2UjdYOG9vZm9STUE9PSIsInZhbHVlIjoidWhXY3IzUTRzVTliV0x6O
UxXaWFadUltamttN3NOdWNBbXBabndxSEpMa3JoTmhaTUFGVjVmRXhMU3cxNWM4NkU0UE5FZTFoNTNRZlJVK2wvZWdhcHk0UWMzR
25qQzJLWGt2Z1ZCQlMwMUZBY2N3YitiYmhIMVdkWTlPUk42YnMiLCJtYWMiOiJiZTYyMDc1ZjZiMzI2ODg1MjgxMjhjZGRkZGQ4M
TZkZjk2NjQwMGUzYzQ4YzFkY2Y2YWQ2ZTBiNDU1ZTE2Mjc0In0%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: omkarjewelers.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

Insecure transition from HTTPS to HTTP in form post

This secure (https) page contains a form that is posting to an insecure (http) page. This could confuse users who may think their data is encrypted when in fact it's not.

Impact

Possible information disclosure.

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6Im02N0QyNERPOXFzeC9IaW9TdHdUaVE9PSIsInZhbHVlIjoiUmRxL0t4ci80Uk84QlJHMnN1VmNyckhySVQ4d3
pqWWRhUHB1NzhQU2k5d3JWZXJqQ0IwTzA0WnFKcjFFVzBSb3M1dGJIcnd1VlYzd3FNMVdIVXdHR0ZkWWZPL28xNm00U1ZOQk9RUD
hmWCtXRGZySm1wcXNaY0JSN3lNdy9oSVUiLCJtYWMiOiI1YzY0MTc1YWZlNTllNDkzNzc3ZDU1ODA0MTVhMGYwNzQ1ZGM5MmU3Yz
c0MjU2ZTM1ZGRkOTk0YWU5OWYyZDgxIn0%3D;
omkar_jewelers_session=eyJpdiI6ImMwamZTaDJvSTA2UjdYOG9vZm9STUE9PSIsInZhbHVlIjoidWhXY3IzUTRzVTliV0x6O
UxXaWFadUltamttN3NOdWNBbXBabndxSEpMa3JoTmhaTUFGVjVmRXhMU3cxNWM4NkU0UE5FZTFoNTNRZlJVK2wvZWdhcHk0UWMzR
25qQzJLWGt2Z1ZCQlMwMUZBY2N3YitiYmhIMVdkWTlPUk42YnMiLCJtYWMiOiJiZTYyMDc1ZjZiMzI2ODg1MjgxMjhjZGRkZGQ4M
TZkZjk2NjQwMGUzYzQ4YzFkY2Y2YWQ2ZTBiNDU1ZTE2Mjc0In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /index.php/contact-us HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/index.php
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6IlhKZ0NGSGpRM3c4VkMyVWdnSEI1dVE9PSIsInZhbHVlIjoic3JGWHhzV2NoWktlcTRocUZFcEpEVm1KcWtxcE
NnSkdKbGowajJycDVsQXdzMXdINUxWTmVEbVVKUzRWWFlQOWdTNmlkanBNV3hTZWZoNDVTOFRYSm0vRTVDTEJjRDJnaUVvSHBEa3
hycEJIRXpCK1V1b2VyOFgwKzFnaWMxMnYiLCJtYWMiOiI5ZmI1YjI5NzAzYzUxNDc4YTM4YTdjYmFhZDg0ZjE3ZmEwNGE0OTMzOG
FmZjhhZDNkNGExYjU1NTBmY2Y3YWFlIn0%3D;
```

```
omkar_jewelers_session=eyJpdiI6Ind5ZUI2VXFpUE5wZUFuWUYzdlVZemc9PSIsInZhbHVlIjoiaThHK25IVnVEMjIwSGhUM
kxhNGM5MzYwekhmdXMrN3JWcWVHREdNS2ZML1F3ZGJscnRxbEtoVUhuOVRKbTB2ZDE0ZXF1ekRzSlp0SGkzeCtqSC82RlFYTXliU
FdNZXlWaWtHOVg3OVdzSjRDamFEMjYrMGZqYnFMZWRWR08rZXgiLCJtYWMiOiIxZTcwMGQ0OGEwODE5MTJkODZiYTFjMGNlZmRhY
jc4Nzg5ZDc5OTE5MGJkMGVkNmMyNjgxY2FiNTk5YjhlMjdmIn0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us?q=1 HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InVpVWFQQ3FrZ1pMSUVZam1jT0Jrdnc9PSIsInZhbHVlIjoiZFVEZ0ZIKzAxMi9LeXk5aFZpWjJRNVo3dlFLZ3
FDZXcwZzVocEN1V1BrZlQwekpqMWxpZFowYUtEWVVxcXdmYXNhMzlNc1IxdTBBNWg2Q1BtY1EvL1RsRm44VEFSSzI0SWd2L3F5SE
psWDFQSjZDK2JVdWEyM3dPUngwSVpZaTUiLCJtYWMiOiJmMjM3YTdmM2MzNDQ3ZGEyOTAwMjA0MDA5NjMzY2U5Mjg0N2FmZjBiM2
U4MWQ1NWY2M2UwNDJhMDY1NWQwMDBmIn0%3D;
omkar_jewelers_session=eyJpdiI6IlZiR3hyWlpUVzNsYWRiaE5YMSt5WVE9PSIsInZhbHVlIjoiWXFxVDhCcmY1Q0JqNmJFS
E13anZZOGVJNEtBd01iTnl2NUdTTkhXbXd3cUh4VFhTN2J1VjJBTDJ0YU1HNSs0aWRnS0R2aFFvb2FIY21RM0pmZmFzWU5vQzFnN
ktJOEhCdXJzYVk3T0JXY3pTa1BpbFp2RUJ1eW94OGpzbGtnVGciLCJtYWMiOiI3NjAyZjIyYTBkMDM2MmY0ZGVlYzg1ODc2Yjg3Z
mVhYTAzMzk2YTcwNmU2YWVkYWQ0NTU3OWNlMmM3YzRlMmFlIn0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us? HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6Ii84R04vMGp0UzU2MHYxL1o4UW1ZR3c9PSIsInZhbHVlIjoiaCtCNy9CeHVCQWZsVkZlSm5tZCtySFN6VzFMTF
hYR3d3UXRDMEdLTk9DTkF0YlIzdVBsOHVhZmFjd1VaOCtGWDRLaGRIRlVWZU1JYUVGell6V1dyVy90bitQeXd6OEhmUytpbUo3d2
FjdzVDZEZrTXRQcTgvaDVBdExYRWpJYTMiLCJtYWMiOiI1MTMxMWJhNzlmZGM0NGUwYTNlNGJlYjgxODA0YjdmYTgxMmQ3MTQzNm
E2NDQxOGIzYWQ5OTMxMTNiNjFmNzJkIn0%3D;
omkar_jewelers_session=eyJpdiI6InFRU1V0eS9ZSW1tb2lJQXRuc0VjRkE9PSIsInZhbHVlIjoiWUYwK3lvbFNrQ0JlUVkrO
ENRN2oyb2pqTzBMTFA4eW0xZERmbTg2KzhEdlppeUgzVXUwaHhmdzdGdjN2YjJrRWNuL2pjcWI3YUJ1ckcvTk9PbHRnK01pWVFMT
XdLbzM1SXRteWxyeWRMUER4YklUVVBlQ2Z4MFhsdE1MZmtQUk8iLCJtYWMiOiJhNWI0OTk4Yjk5NTk0MTc4NGMxY2FiZGMxMTE5M
```

```
jU3Zjk4MTVhOTA2MmRlM2E2YjgwZWU3YTU5OWQ3MzkxNzM3In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us?check_1=accept_1 HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6Ii9kSDYyYldKU1Rna3JvRm5ib3RPbkE9PSIsInZhbHVlIjoiTE9jaWwrcWxxTFFvK2RkUzgyRnZ0NDhmQ1hSZm
FzS2NzaW1Mb3FhRTZZYW9jNXNuSHpwcDV4ZGZsWVFUWkxIMExHZStwZUNNSkVyMm5ZVDA2N2wrVS9XUmZBMUlKeE16ZlFRVjJXVm
hkSjFjYTVzZ3FaS1piNm51WHpzYnFLQUwiLCJtYWMiOiI3NGRlZDEyNTNkNGNjMjYxMjUxNGU3MGJlY2UwMzhlZTY4ZDNiMWQzOG
Y1NTJkYzI0Y2Q3MWY2MmFhZjNjOTZiIn0%3D;
omkar_jewelers_session=eyJpdiI6IkZ0Mzl0ZzZmTmJOVEE0enJDSS9yZkE9PSIsInZhbHVlIjoieFo3V3cwMm1hcEZmekRZT
GtEQktwWENKd0Y0MkZNeVFDMTNNbHdrWU8xS0lmTFBOTGsvTGxNdUVNTFJrUFZQMG5Rd1VRd1BvNzlneDJrOXBFMG1MWlRMY3Iwe
kZnVjliNmNQUGtZRzlZa0xUSGwvMnI3NDdzV3dBa29RUWVsQk8iLCJtYWMiOiJiMTU1OTdhYzRjNzY4NmZjZGZkNmZhNjE3MGY5N
2Y1ZjEwY2ZhMTg0ODgxZTc1ODRhNjFmZGQwYzY5MjgwODg2In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /index.php/contact-us?q=1 HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/index.php/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6IkxQQUtFbS8rclhSN0MvQVdZZ0xYQWc9PSIsInZhbHVlIjoiUWNQa0kxWWxIa3BTR1ZCOVFqTTVDSFp4eHFqV2
dQZThUSlQwODVIU2lnUUZPZno3eHdWOEhBSW5pSitGblN4akE4Z2o0YUQvWUQ5SEVEbjI4VkxxR2ZaTmpSeHQrajVwVWNNMmd0OE
ZhLzRHd08zY2RQYkxYNUZESGlwbDhPNloiLCJtYWMiOiI1YjBiZWE3MGQ2MmZmM2U4YTc3ZDQ4MjhkMTRmZmM2ZTNiNGQwNTVlN2
I0NTZhZjRiOWE4NjEzMTNhNTM3MTFlIn0%3D;
omkar_jewelers_session=eyJpdiI6IkxiSTU5TDM4VmlGNUFWTmtrVXIzK1E9PSIsInZhbHVlIjoiTU1UcC9QR0hFSE5Nc1Z0S
nZ0WTFueWxWQXVSbmtsVTZXcXJOUjdRcjVFalJ1bS8rRmVkbnRqQjZObXhwaXZNbmhQTGJSVHhqQmZ5MldxdFk4ZG9uV3hEV0VGR
FcyK2NiYnN5Y0lHM1M3WW5uek84Zk9JVHRUKzd4UmNLWkFJV3EiLCJtYWMiOiIyZTA0YjQ0YmExOGM5YTFiNmYxMGNmZWU5MjFjN
mY0NzBjZTI4MDFjMmM2Y2M5Nzc1ZTQzMDdlZDU0OWEzOGY3In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /index.php/contact-us? HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/index.php/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InRvdzN2TktqYjV5MjRWajNlbThwT2c9PSIsInZhbHVlIjoiL0VwUXRUMFhJV2xuc1ZZN3drQ0svM3ZVNkR1ZE
9pR05VS01URXhuR0c0MHh5ZHJGUFY1OFBZbFhucHFZd3Z6R2JOcWtiQzhVNnVBb3A5TGk0VzMwUk4vR3J5dzlPT3BsVXh4NnZWNT
lKQ3hycTQwQXZEeitNeDcyaXJYd2FkRnMiLCJtYWMiOiJkOTM2MGZjN2Y3YzE0Yjk3NGJlMDE3NTNjODlkY2FjYmJlOTEzNzI0ZD
UyODI4Y2E5YmIyZDFhNmE5NTRlZTc1In0%3D;
omkar_jewelers_session=eyJpdiI6Ilg1V2h4Q2puL0poV1JSR2V6N28wR3c9PSIsInZhbHVlIjoiOEpyQlNjZUFKcGpsRzFNa
mFwelR5OHkxWlFUYXRuZmJYai9US0lpZGtsSjhNOWw1eHZ3NGQwSGN3SUUrRzRIS0JGNExzanBmQ0pJUzNpMXR2RE1OZ0kzYXFSM
VpNcmZPRDV5NDZSUXlVOElXNlQ4Mm9JV3BjNTBvc0t3SmNUeUYiLCJtYWMiOiI2YWRiYzg3NjU0ZWM3OTBiNDllNDM5MWQ1NTY1O
TU0YWI3YTBlOWJhMzcxMDBmYmVhNmI1YTk0ZjI5OWYzYjg1In0%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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /index.php/contact-us?check_1=accept_1 HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/index.php/contact-us
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6InRvdzN2TktqYjV5MjRWajNlbThwT2c9PSIsInZhbHVlIjoiL0VwUXRUMFhJV2xuc1ZZN3drQ0svM3ZVNkR1ZE
9pR05VS01URXhuR0c0MHh5ZHJGUFY1OFBZbFhucHFZd3Z6R2JOcWtiQzhVNnVBb3A5TGk0VzMwUk4vR3J5dzlPT3BsVXh4NnZWNT
lKQ3hycTQwQXZEeitNeDcyaXJYd2FkRnMiLCJtYWMiOiJkOTM2MGZjN2Y3YzE0Yjk3NGJlMDE3NTNjODlkY2FjYmJlOTEzNzI0ZD
UyODI4Y2E5YmIyZDFhNmE5NTRlZTc1In0%3D;
omkar_jewelers_session=eyJpdiI6Ilg1V2h4Q2puL0poV1JSR2V6N28wR3c9PSIsInZhbHVlIjoiOEpyQlNjZUFKcGpsRzFNa
mFwelR5OHkxWlFUYXRuZmJYai9US0lpZGtsSjhNOWw1eHZ3NGQwSGN3SUUrRzRIS0JGNExzanBmQ0pJUzNpMXR2RE1OZ0kzYXFSM
VpNcmZPRDV5NDZSUXlVOElXNlQ4Mm9JV3BjNTBvc0t3SmNUeUYiLCJtYWMiOiI2YWRiYzg3NjU0ZWM3OTBiNDllNDM5MWQ1NTY1O
TU0YWI3YTBlOWJhMzcxMDBmYmVhNmI1YTk0ZjI5OWYzYjg1In0%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: omkarjewelers.ssbmultiservices.com
```

```
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/
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
Cookie: XSRF-
TOKEN=eyJpdiI6IlFPajZMMmowRHhEUldpYWl2OTdhNnc9PSIsInZhbHVlIjoiU3AvektHeWpvbGVsK0dzMU1mcklLNlBITmhrcW
RIU0tNMXBRV3VheGR4YjlrRG5xUDJXOEVJQ0RsdnJxQjh2Rjh3L1dXbmpaYlIyNmNwaUNIVGVVQmVpSzI4S2dnV3Z6QWxyUEhIRU
RFbW9hRk9EYmdBdGNrSjUyVnBEM0t0SmEiLCJtYWMiOiI3YWFmZjI3MzEzOTQ4NDliNDU1MTI2NWU2OWQ0NjFlYjNmNGQzZWM2Mm
JkOTQxMzMzYWE4Mzc4MjRjYmM3MWFlIn0=;
omkar_jewelers_session=eyJpdiI6IjFta09zR1VZa3Z4OUlVOVpLc1BsQkE9PSIsInZhbHVlIjoia2FZYVJwTWFWSzBQUTg1Z
EdNSmV4dFkxdDZSZjUvUGpLNnd3bllZOTFmMHhCWUhUczR2bmJyOWgySXc2Q1VPNlRheVFNengrZjl1K0hzdk16WFA3dkdtZzRnb
GovTEc0dlB5Rjd6ZXhtRVdmcG9KNWJKOWVmdTBGRVdGa212dHAiLCJtYWMiOiJhY2VhNjFlNDExZjAyYmRhNTlkNTA2ZGFlYzA4N
GU4ODRlY2VkYWUzNzJmMGUyOTRmN2NmNzMxM2QzMmJkYzFlIn0=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

https://omkarjewelers.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /index.php/contact-us HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/index.php
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
Cookie: XSRF-
TOKEN=eyJpdiI6IlFPajZMMmowRHhEUldpYWl2OTdhNnc9PSIsInZhbHVlIjoiU3AvektHeWpvbGVsK0dzMU1mcklLNlBITmhrcW
RIU0tNMXBRV3VheGR4YjlrRG5xUDJXOEVJQ0RsdnJxQjh2Rjh3L1dXbmpaYlIyNmNwaUNIVGVVQmVpSzI4S2dnV3Z6QWxyUEhIRU
RFbW9hRk9EYmdBdGNrSjUyVnBEM0t0SmEiLCJtYWMiOiI3YWFmZjI3MzEzOTQ4NDliNDU1MTI2NWU2OWQ0NjFlYjNmNGQzZWM2Mm
JkOTQxMzMzYWE4Mzc4MjRjYmM3MWFlIn0=;
omkar_jewelers_session=eyJpdiI6IjFta09zR1VZa3Z4OUlVOVpLc1BsQkE9PSIsInZhbHVlIjoia2FZYVJwTWFWSzBQUTg1Z
EdNSmV4dFkxdDZSZjUvUGpLNnd3bllZOTFmMHhCWUhUczR2bmJyOWgySXc2Q1VPNlRheVFNengrZjl1K0hzdk16WFA3dkdtZzRnb
GovTEc0dlB5Rjd6ZXhtRVdmcG9KNWJKOWVmdTBGRVdGa212dHAiLCJtYWMiOiJhY2VhNjFlNDExZjAyYmRhNTlkNTA2ZGFlYzA4N
GU4ODRlY2VkYWUzNzJmMGUyOTRmN2NmNzMxM2QzMmJkYzFlIn0=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

The form target should point to a secure (https) page.

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://omkarjewelers.ssbmultiservices.com/

Possible sensitive files:

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

Request

```
GET /web.config HTTP/1.1
Accept: btalusct/rckh
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6IkY2cTNtZlhKR1dmcmtCQjhhNURoTlE9PSIsInZhbHVlIjoiTzNUWXAwZGlSZHBJdUZvWmRId3ZWb1BCR1dkTT
lDZmlDQk05YTZLZ2M0NkhmR3BqLytGaGFmVGVIc0IvU2JYMER6cUhWQXNLaVEyc3duRXBJQVpJdW1VZ2ZNWTNoZ2FsSGlzQ3BQcX
ZzMzdHaXBLSnR4YTkrcEdaTENaYTdRL2wiLCJtYWMiOiJhNTgyZWNmMGQxYTFiNGViY2VjNjI3MWMxY2MzYWYwNWVkNjc3OWNkYj
AxMDJlMWVkNjRiN2RjMDgxYzAwMDI2In0%3D;
omkar_jewelers_session=eyJpdiI6IjA2aHRvRmhWN1Zpb3R5WkM5dTcrc0E9PSIsInZhbHVlIjoiWE4vOWlUZlZrLy9vK0Q1M
y96R3R3OVAwOHpNT25TYlBzMTd1ZDlYQjdqQno4bEVaL0lKNVVOUjRoMFp3SVBCK3owcUNZM2s2aERlNEhPbnV0S1NMRjNFRTlpV
VRoWmFkRE9Talk5OFJKdU9US2xOcWdZR050c3pCUnR0NCs4dVoiLCJtYWMiOiIyYmE2NzI5ZGQ4ZjU0ZWYzYjg4MzQ0OTBjMjY2M
zE1YWUyNGI5OGEzODcxNWYxZjU0MThhYTNhODBmZDFkMzcyIn0%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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/

Paths without CSP header:

- https://omkarjewelers.ssbmultiservices.com/
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://omkarjewelers.ssbmultiservices.com/project/vendor/autoload.php

- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/upload/category-image/
- https://omkarjewelers.ssbmultiservices.com/about-us
- https://omkarjewelers.ssbmultiservices.com/all-categories
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://omkarjewelers.ssbmultiservices.com/all-products
- https://omkarjewelers.ssbmultiservices.com/contact-us
- https://omkarjewelers.ssbmultiservices.com/custom-jewelry
- https://omkarjewelers.ssbmultiservices.com/faq
- https://omkarjewelers.ssbmultiservices.com/privacy-policy
- https://omkarjewelers.ssbmultiservices.com/services
- https://omkarjewelers.ssbmultiservices.com/terms-of-use
- https://omkarjewelers.ssbmultiservices.com/index.php
- https://omkarjewelers.ssbmultiservices.com/products/others-ojzfv
- https://omkarjewelers.ssbmultiservices.com/index.php/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/cgi-sys/
- https://omkarjewelers.ssbmultiservices.com/database/

Request

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

Pages where the content-type header is not specified:

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

Request

```
GET /web.config HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/
Cookie: PHPSESSID=6130381984d9af259fc9956fa6a0f350; XSRF-
TOKEN=eyJpdiI6IjRFL2lZbXorS2VGVHRwNzkrcDd0c0E9PSIsInZhbHVlIjoiUU9rZ3F4aHJTcVIzenYrOFdKUGdCUjNVRlhaTn
dBeVJ0UTIrNTRtS1F0T09IZGFzRVd0VnpoZCtFaVNQYk5jempwZU9VY21UcG5TNzR3dGxxS2NHbTVJanVNdllMK0psaFhpVTF6QW
```

```
VCV3g2K2JxY1BYUjVOaXd0bjJKcHN6VnYiLCJtYWMiOiI2OTUyYzA0YmE4OWFhMWIyNTgzNDNjNWYyY2VjNjc3ODRjZDRiYWMzM2
JkNGU4NjM2NjQ5NTM5MzI4MDE2YTRjIn0%3D;
omkar_jewelers_session=eyJpdiI6Imd1SS9YRUR4SlNnZWZsck56c0hNUGc9PSIsInZhbHVlIjoiY2ZxZDVZZlo5SFdZSXBDN
UloSWdwOVovNXA3WDFIUVRTMThHb0N5THhmcWlicVRRcDAzMnpQbnlVWWFScHo0Y2FzbzN5bHBIRFhsNHpMTzhmQnNmL0k2MExDZ
HJ1azVFbUdOeWRqTWZ1ODdrT1NLWTRheTBiNnI2U0pYRWU3bi8iLCJtYWMiOiJjODg4ODgyOTJkM2VjYzg4MTQzYjQ2ZmU2NmZjM
mEwOTMzODVlMDE1ZTgzZTNiNWVhODk5YmRiZTA4NTE5MGJiIn0%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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/

Emails found:

- https://omkarjewelers.ssbmultiservices.com/
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/subscribe
  crm@bijoytech.com
- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/about-us
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/all-categories
  pulakeshroyny@gmail.com

- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/all-products
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/contact-us
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/custom-jewelry
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/faq
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/privacy-policy
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/services
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/terms-of-use
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/index.php
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/products/others-ojzfv
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/index.php/subscribe
  crm@bijoytech.com
- https://omkarjewelers.ssbmultiservices.com/index.php/products/gold-bangles-cjvux
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/index.php/product/gold-bangles-1-dlcozaecw5
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-2-bqihs4kieh
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/index.php/products/others-ojzfv
  pulakeshroyny@gmail.com
- https://omkarjewelers.ssbmultiservices.com/products/gold-earrings-ywdzz
  pulakeshroyny@gmail.com

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.0.0 Safari/537.36
Host: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 3.3.7**
  - URL: https://omkarjewelers.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://omkarjewelers.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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive
```

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

- **Modernizr 2.7.1**
  - URL: https://omkarjewelers.ssbmultiservices.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.

- References:
  - https://github.com/Modernizr/Modernizr/releases

Request

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

Locations without Permissions-Policy header:

- https://omkarjewelers.ssbmultiservices.com/
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://omkarjewelers.ssbmultiservices.com/project/vendor/autoload.php
- https://omkarjewelers.ssbmultiservices.com/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/upload/category-image/
- https://omkarjewelers.ssbmultiservices.com/about-us
- https://omkarjewelers.ssbmultiservices.com/all-categories
- https://omkarjewelers.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://omkarjewelers.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://omkarjewelers.ssbmultiservices.com/all-products
- https://omkarjewelers.ssbmultiservices.com/contact-us
- https://omkarjewelers.ssbmultiservices.com/custom-jewelry
- https://omkarjewelers.ssbmultiservices.com/faq
- https://omkarjewelers.ssbmultiservices.com/privacy-policy

- https://omkarjewelers.ssbmultiservices.com/services
- https://omkarjewelers.ssbmultiservices.com/terms-of-use
- https://omkarjewelers.ssbmultiservices.com/index.php
- https://omkarjewelers.ssbmultiservices.com/products/others-ojzfv
- https://omkarjewelers.ssbmultiservices.com/index.php/products/gold-bangles-cjvux
- https://omkarjewelers.ssbmultiservices.com/cgi-sys/
- https://omkarjewelers.ssbmultiservices.com/database/

Request

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

Pages with paths being disclosed:

- https://omkarjewelers.ssbmultiservices.com/subscribe
  /home/ssbmul5/omkarjewelers.ssbmultiservices.com/project/vendor/swiftmailer/swiftmailer/lib/classes/Swift/Transport/Esmtp/AuthHandler.php
- https://omkarjewelers.ssbmultiservices.com/index.php/subscribe
  /home/ssbmul5/omkarjewelers.ssbmultiservices.com/project/vendor/swiftmailer/swiftmailer/lib/classes/Swift/Transport/Esmtp/AuthHandler.php
- https://omkarjewelers.ssbmultiservices.com/subscribe
  /home/ssbmul5/omkarjewelers.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php
- https://omkarjewelers.ssbmultiservices.com/index.php/subscribe
  /home/ssbmul5/omkarjewelers.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php

Request

```
POST /subscribe HTTP/1.1
Referer: https://omkarjewelers.ssbmultiservices.com/
Cookie: PHPSESSID=77c2185b74c3f2845d6067aaa73c3ed9; XSRF-
TOKEN=eyJpdiI6IkY4KzNIRmNkKyswVmdtVDY3ZXUzZWc9PSIsInZhbHVlIjoiR3VaNEFBLzVjQ0xEUUNRclRyc0gweWRLSmRiL0
ZHOXpFQXYwSSs3MjBTcWExZnRyZlFEWDVzMmJ6TWErbytqK2VXdW5lTklYMVA3REtZU0ViSkloMnpUTWt6RnZDT0NkQVE2QWhuWn
F6Tis0VVdQSWV4SThPTDdWN3dkSEUya0MiLCJtYWMiOiI0NjZkM2FmODllYmVkODk0Nzc4OWU2NWE3YWQ2YjMxMDkwYTlkODM4NW
IwYmFhODJkMmZmYzE2MTcwODA4ZTdiIn0%3D;
omkar_jewelers_session=eyJpdiI6Ikc2WVBHWDV5ZDlOUWN0WFdERnF4c1E9PSIsInZhbHVlIjoicFhzelFnS0xlNzd1TU1MQ
W9tc2h6RzVGdWZwc01tVkJqZEVQNmIvOEZ6a1FtbDduZHpqVlROSGtrM05QMUQ3UlBqQjBJSEoxS2dKVk5SZWZNempQa0tWNnhHd
zY4dGczR2x5dnhEVEovM0pNWUdrQ0kyQmNpdWl3elF2dHd0SWgiLCJtYWMiOiI0YmFkZjA3ZmYyNDQzNDhlY2RmOWU3MzM1ZTgzM
GE2MzljMGFjNzE3OGQzMmUzOTdiMGM2Nzc1Y2VhZmQyNzg0In0%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
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: omkarjewelers.ssbmultiservices.com
Connection: Keep-alive

_token=LHaffTRBwJBGpvijL28H2ibyL0VUL3CBw4hW4qZd&email=testing%40example.com
```

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://omkarjewelers.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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com/

Pages where SRI is not implemented:

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

Request

```
GET / HTTP/1.1
Referer: https://omkarjewelers.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: omkarjewelers.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://omkarjewelers.ssbmultiservices.com
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
  - _ignition
    - Inputs
      - GET iv, value, mac
    - health-check
      - Inputs
        - GET iv, value, mac
  - assets
    - Inputs
      - GET iv, value, mac
    - admin
      - Inputs
        - GET iv, value, mac
    - front
      - Inputs
        - GET iv, value, mac
      - css
        - icon_fonts
          - css
            - all_icons.min.css
          - font
            - Inputs
              - GET iv, value, mac
        - animate.min.css
        - bootstrap.min.css
        - custom.css
        - magnific-popup.min.css
        - menu.css

            - responsive.css
            - style.css
        - fonts
            - Inputs
                - GET iv, value, mac
        - img
            - Inputs
                - GET iv, value, mac
        - js
            - bootstrap-portfilter.min.js
            - common_scripts_min.js
            - functions.js
            - jquery-2.2.4.min.js
            - modernizr.js
            - validate.js
            - video_header.js
        - fonts
            - Inputs
                - GET iv, value, mac
    - logo
        - Inputs
            - GET iv, value, mac
    - sweet-alert.min.js
- cgi-sys
    - Inputs
        - GET iv, value, mac
- database
    - Inputs
        - GET iv, value, mac
- index.php
    - Inputs
        - GET iv, value, mac
    - product

- Inputs
  - GET iv, value, mac
- gold-bangles-1-dlcozaecw5
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-bangles-2-bqihs4kieh
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-earring-1-gehy0lwwrc
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-earring-2-rulpfdv2gj
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-1-vbhe59cvkb
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-2-xi4ooxiypl
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-3-q8g7hrmqrv
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-4-eov9o7zbmj
  - Inputs
    - GET iv, value, mac

        - GET check_2, check_1, q
  - gold-pendants-1-vvxaidwlbn
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-pendants-2-y3xjcwv09q
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
- products
  - Inputs
    - GET iv, value, mac
  - gold-bangles-cjvux
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-earrings-ywdzz
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-necklace-yhza4
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-pendants-ieyji
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - others-ojzfv
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
- about-us

- Inputs
  - GET iv, value, mac
  - GET check_2, check_1, q
- all-categories
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- all-products
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- contact-us
  - Inputs
    - GET iv, value, mac
    - GET check_2, q, check_1
    - POST iv, value, mac
    - POST _token, calculation, email, f_name, first_num, l_name, message, phone, second_num
- custom-jewelry
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- faq
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- privacy-policy
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- product
  - Inputs
    - GET iv, value, mac
- products

    - Inputs
      - GET iv, value, mac
  - services
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - subscribe
    - Inputs
      - GET iv, value, mac
      - POST iv, value, mac
      - POST _token, email
  - terms-of-use
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
- mailman
  - Inputs
    - GET iv, value, mac
  - archives
    - Inputs
      - GET iv, value, mac
- product
  - Inputs
    - GET iv, value, mac
  - gold-bangles-1-dlcozaecw5
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-bangles-2-bqihs4kieh
    - Inputs
      - GET iv, value, mac
      - GET check_2, check_1, q
  - gold-earring-1-gehy0lwwrc

- Inputs
  - GET iv, value, mac
  - GET check_2, check_1, q
- gold-earring-2-rulpfdv2gj
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-1-vbhe59cvkb
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-2-xi4ooxiypl
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-3-q8g7hrmqrv
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-4-eov9o7zbmj
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-pendants-1-vvxaidwlbn
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-pendants-2-y3xjcwv09q
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q

- products
  - Inputs

- GET iv, value, mac

- gold-bangles-cjvux
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-earrings-ywdzz
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-necklace-yhza4
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- gold-pendants-ieyji
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- others-ojzfv
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q

- project
  - Inputs
    - GET iv, value, mac
  - config
    - Inputs
      - GET iv, value, mac
  - database
    - Inputs
      - GET iv, value, mac
  - resources
    - Inputs
      - GET iv, value, mac

- storage
  - Inputs
    - GET iv, value, mac
- tests
  - Inputs
    - GET iv, value, mac
- vendor
  - Inputs
    - GET iv, value, mac
  - bin
    - Inputs
      - GET iv, value, mac
  - autoload.php
    - Inputs
      - GET iv, value, mac
- .env
  - Inputs
    - GET iv, value, mac
- composer.json
  - Inputs
    - GET iv, value, mac
- composer.lock
  - Inputs
    - GET iv, value, mac
- docker-compose.yml
  - Inputs
    - GET iv, value, mac
- package.json
  - Inputs
    - GET iv, value, mac
- upload
  - Inputs
    - GET iv, value, mac

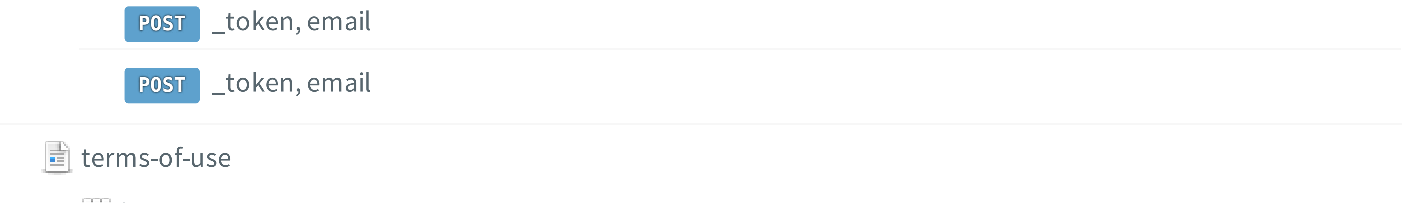
- about-us-image
  - Inputs
    - GET iv, value, mac
- category-image
  - Inputs
    - GET iv, value, mac
- client-review-image
  - Inputs
    - GET iv, value, mac
- header-footer
  - Inputs
    - GET iv, value, mac
- home-intro
  - Inputs
    - GET iv, value, mac
- pages-banner-video
  - Inputs
    - GET iv, value, mac
- product-image
  - Inputs
    - GET iv, value, mac
- service-image
  - Inputs
    - GET iv, value, mac

- _ignition
  - Inputs
    - GET iv, value, mac
- about-us
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- all-categories
  - Inputs
    - GET iv, value, mac

- GET check_2, check_1, q

- all-products
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- contact-us
  - Inputs
    - GET iv, value, mac
    - GET check_2, q, check_1
    - POST iv, value, mac
    - POST _token, calculation, email, f_name, first_num, l_name, message, phone, second_num
- custom-jewelry
  - Inputs
    - GET iv, value, mac
    - GET check_2, check_1, q
- faq
  - #fragments
    - collapseOne_doc
    - collapseOne_preorder
    - collapseOne_pricing
    - collapseOne_printing
    - collapseOne_privacy
    - collapseOne_register
    - collapseOne_works
    - collapseThree_doc
    - collapseThree_preorder
    - collapseThree_pricing
    - collapseThree_printing
    - collapseThree_privacy
    - collapseThree_register
    - collapseThree_works
    - collapseTwo_doc
    - collapseTwo_preorder

        - collapseTwo_pricing
        - collapseTwo_printing
        - collapseTwo_privacy
        - collapseTwo_register
        - collapseTwo_works
    - Inputs
        - GET iv, value, mac
        - GET check_2, check_1, q
- index.php
    - Inputs
        - GET iv, value, mac
        - GET check_2, check_1, q
- privacy-policy
    - Inputs
        - GET iv, value, mac
        - GET check_2, check_1, q
- product
    - Inputs
        - GET iv, value, mac
- products
    - Inputs
        - GET iv, value, mac
- robots.txt
    - Inputs
        - GET iv, value, mac
- services
    - Inputs
        - GET iv, value, mac
        - GET check_2, check_1, q
- subscribe
    - Inputs
        - GET iv, value, mac
        - POST iv, value, mac



POST _token, email

POST _token, email

terms-of-use