Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 2

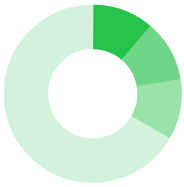
One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Scan Detail

Target	jewellery.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 14, 2024, 8:23:59 PM GMT+8
Scan Duration	40 minutes
Requests	9026
Average Response Time	309ms
Maximum Response Time	19665ms
Application Build	v23.7.230728157

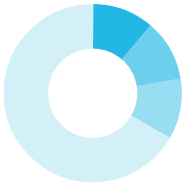
Severity	Vulnerabilities	Instances
High	0	0
Medium	2	2
Low	8	9
Informational	8	9
Total	18	20

Informational



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

Low Severity



	Instances
Clickjacking: X-Frame-Options header	1
Cookies with missing, inconsistent or contra…	1
Cookies without HttpOnly flag set	1
Others	6

Medium Severity

	Instances
Directory listings	1
Vulnerable JavaScript libraries	1

Impacts

SEVERITY	IMPACT	
Medium	1	Directory listings
Medium	1	Vulnerable JavaScript libraries
Low	1	Clickjacking: X-Frame-Options header
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	1	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	1	HTTP Strict Transport Security (HSTS) not following best practices
Informational	2	Outdated JavaScript libraries
Informational	1	Permissions-Policy header not implemented
Informational	1	Reverse proxy detected
Informational	1	Subresource Integrity (SRI) not implemented

Directory listings

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

Impact

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

https://jewellery.ssbmultiservices.com/ Verified

Folders with directory listing enabled:

- https://jewellery.ssbmultiservices.com/assets/
- https://jewellery.ssbmultiservices.com/assets/front/css/
- https://jewellery.ssbmultiservices.com/assets/front/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://jewellery.ssbmultiservices.com/assets/front/js/
- https://jewellery.ssbmultiservices.com/upload/
- https://jewellery.ssbmultiservices.com/upload/category-image/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://jewellery.ssbmultiservices.com/upload/header-footer/
- https://jewellery.ssbmultiservices.com/upload/home-intro/

Request

```
GET /assets/ HTTP/1.1
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6InlGcjM3UEYwRTRtbUNONGR1NDZnNmc9PSIsInZhbHVlIjoidldCUG5KazlSZFMzM0lrNHNEUURuTHVFWWQ3Tk
pHRkFhaGhhMU9od0wxVk5mcCtWZWc3K09WU1k2VUN6dUJ1VDRuUUhpSmhlUDIwdGczb09ac2ZJbHU3a1pOOE9QTGZKNTFEV0lVZm
M4akVLczE0WlRHWFJ6dGVtR1gwQWxSKzEiLCJtYWMiOiJmYWY3MmQxOGMxZmEwYTM1YTE3Mjg1MjU2ODYxNDE1ZmUzNWU5ZDA3Nj
lmZmJjNTBmYmZjMzQ5NDFmMDE5YzE5In0%3D;
omkar_jewelers_session=eyJpdiI6IkpqekFyKzdxK3piT0RHVmE4WTFPTnc9PSIsInZhbHVlIjoiTTVCeWVHNGoyZWhqNWhLW
GN1Nyt4bjQ2ekhZSStUa3MwM3FocXJYS3I1dmJJWjhDMXlBR0N1RnZjOHBKM0Q1dU5oTzkxK0d3RHpHanh6d3E2bmhhYkJURUVDY
Xd4WEI0Vms1Y25pT2J1MGQzSjhmSVNja1V1L3NaRDlaa2dZekMiLCJtYWMiOiIzYjZkMjYwZDBiZDZiYzg1Yjc1YTAzODYwNmVjZ
GJmNjk4YjY1MWM4Nzc4MzM5YmIwYjgwNWJkODlkOTc5OTc5In0%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: jewellery.ssbmultiservices.com
```

```
Connection: Keep-alive
```

Recommendation

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

References

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

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://jewellery.ssbmultiservices.com/ Confidence: 95%

- **jQuery 2.2.4**
  - URL: https://jewellery.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://jewellery.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: jewellery.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

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://jewellery.ssbmultiservices.com/

Paths without secure XFO header:

- https://jewellery.ssbmultiservices.com/upload/category-image/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://jewellery.ssbmultiservices.com/upload/header-footer/
- https://jewellery.ssbmultiservices.com/upload/home-intro/
- https://jewellery.ssbmultiservices.com/product

Request

```
GET /upload/category-image/ HTTP/1.1
Referer: https://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6InVFZklPaUM0QVJxVDBtT1MxcDJTWmc9PSIsInZhbHVlIjoiWDdoMlVsTURYaGlKb2lKZmV1aVZ2azd4YXlQck
NwY3p1TEJvaGt5Uy9raGJUb0lSaVdleEdXZGRaMzRWSzlFN1BjcTZEd3BiZDNOYWtNNGtBTkUxK05mRmlqeE1IenRYK2tmcDRtTF
BXc0tmc2hpZWh6Z1B5ZzAxOHF6R2JrZHoiLCJtYWMiOiJmZGZiMzI3NDUyM2MxY2FlNDFlODgzMjk2Mjc0ODExMGE4OWM2ZjM2YT
g5YTAzNTliNGFmMDFjNGFjMzgxNzg3In0%3D;
omkar_jewelers_session=eyJpdiI6IjhNRkV6NEVoZmVLRUIzRE9NZGVFVGc9PSIsInZhbHVlIjoiSld0QUFCV2xtUU5ZY3lBT
kZuZGM4VnBlUS8yc0pRTFk3WVFVdGFYU0RiUXpKK0VONjRHSGVxR1YzNDVQcW5PSXUvZHhxeHlVcnkyM2EzbVBnSVVGSVRWMHZ1S
mIyS1JJV0ZESTdsSmtoYmMxQ2FUdFA3azBFcVJwUlFoK1FpQjgiLCJtYWMiOiJlMDg0NTJhNDRhM2M1YmFjYjU0NmIwZmRmYzEyZ
DBiNTYwMGQ4YzdiY2JlN2JmODYyNmI1NGUyNzExYTllNWIxIn0%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: jewellery.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

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://jewellery.ssbmultiservices.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://jewellery.ssbmultiservices.com/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; 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://jewellery.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: jewellery.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://jewellery.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; path=/
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjEwdGlwMkpRTU45WGVtY3V6eFQvemc9PSIsInZhbHVlIjoiMFc5Sy96NjNiZndnaUp
VajBxTjJBYWorYmQzL2xlNTh1eEF5c1FBNXI5NC9qZjZrbkJJd3hLOHNmb2l0L283T0xmM1kySTlSTVpM
R3pVeG1kUlhDTm9ITHRFeitsRFVzRzY2K2NJNTluTmZEMEpsc0FSYnB2NXdMV3E4R09QT1AiLCJtYWMiO
iI4NDU2MTQ3MTg4YmNlZWU1NzAxZGJmNjhhNWM2NDI0ZjI5NWY3ZmM2OTI5ODZiNzYwZmY3NWNlNWQ2Ym
M1MDdjIn0%3D; expires=Sun, 14-Jan-2024 14:24:01 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlGcjM3UEYwRTRtbUNONGR1NDZnNmc9PSIsInZhbHVlIjoidldCUG5KazlSZFMzM0l
rNHNEUURuTHVFWWQ3TkpHRkFhaGhhMU9od0wxVk5mcCtWZWc3K09WU1k2VUN6dUJ1VDRuUUhpSmhlUDIw
dGczb09ac2ZJbHU3a1pOOE9QTGZKNTFEV0lVZmM4akVLczE0WlRHWFJ6dGVtR1gwQWxSKzEiLCJtYWMiO
iJmYWY3MmQxOGMxZmEwYTM1YTE3Mjg1MjU2ODYxNDE1ZmUzNWU5ZDA3NjlmZmJjNTBmYmZjMzQ5NDFmMD
E5YzE5In0%3D; expires=Sun, 14-Jan-2024 14:25:06 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkJKaUdhY1AxRTlKZVRzNTBXYmtCMEE9PSIsInZhbHVlIjoiYXcyZXZQY3l5a0JyeE5
kbUVseEZTcndJZEc1RFUwbW81aDJtV0RvV3RJZ2RFR01EcjlZN2JVTVRDUW9COTlhSTVISzVPbzZNREtP
OGxQUXJqbHovalQwVGUzdVUwUktIVzlNQXJkMXFTWkJ6M2xxeWhGZjlKeHNzTzlBc1pMTmQiLCJtYWMiO
iJiZjJhMTZhZTQ3M2UzZTcwZDA0NDE3NjMxNWIxNTRhMGNmODhjNDhkMDk0ODJiZTc3M2M4YWJkODE1Y2
Y5MDMwIn0%3D; expires=Sun, 14-Jan-2024 14:25:21 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImoxUldtYUYxVG9mUDR3Q3o3djlHaWc9PSIsInZhbHVlIjoibTc1ZVhlQktETVp5emo
zdDlTNjJMNnhJaXhXSW4xUHc3T05pWkMweVlWS1B4Wk5xVmNaaGVTQitCQTllMXk5dFVVSVdBYm9uNUFL
```

```
aHVMSklUT0czMlJGWlM3TUsrb1ZLYy9LK2c3bUpYZnA3cm5udCtBbldOMVBBemFkaGw2WDIiLCJtYWMiO
iJhMTQwMGIxYTgwOGZkZGI1ZjVjZGI4YWQwN2MyZTMwZWM2YWMzY2M5ZTRjMzZlZWI1OTg0NGRjYWNhYT
AwN2U2In0%3D; expires=Sun, 14-Jan-2024 14:51:17 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InVFZklPaUM0QVJxVDBtT1MxcDJTWmc9PSIsInZhbHVlIjoiWDdoMlVsTURYaGlKb2l
KZmV1aVZ2azd4YXlQckNwY3p1TEJvaGt5Uy9raGJUb0lSaVdleEdXZGRaMzRWSzlFN1BjcTZEd3BiZDNO
YWtNNGtBTkUxK05mRmlqeE1IenRYK2tmcDRtTFBXc0tmc2hpZWh6Z1B5ZzAxOHF6R2JrZHoiLCJtYWMiO
iJmZGZiMzI3NDUyM2MxY2FlNDFlODgzMjk2Mjc0ODExMGE4OWM2ZjM2YTg5YTAzNTliNGFmMDFjNGFjMz
gxNzg3In0%3D; expires=Sun, 14-Jan-2024 14:51:28 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImJ3NUF0SjFac1EwY1VIOGJSN05ibVE9PSIsInZhbHVlIjoiQXJCWGJ5L2FJV1MyN0x
CeThCd1Q5cU5XMGVmbmxVelIxZlpSK2ZxRGViWjdLZnJUbkduSHdHR1RtT1dMNGQrK0hleTNqZDVxM0Na
YzY5M1c5N1FZVjBmQjgvakN1Z1Y0MVo5TFBicVRuejJWM0hrM2N3d25UMmJoQVpiSytqZnYiLCJtYWMiO
iIyNmYxZGJhM2E1MDY3NzNmZjllMjJkY2I5OWY2YzM2MGRmYjMzZmZlOWNhMDk4YjI1NjlkYmFhMDFlND
g5MDQ5In0%3D; expires=Sun, 14-Jan-2024 14:51:35 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkFDbFNIVnh5NWFrSkE2LzJzWis3WlE9PSIsInZhbHVlIjoiZk1VdE40bEwwdE5mbC8
2Y2VnSGVFQ0x4RjE3SGNrQlJvc3NYS3lHbCt6RFkrMjNhQlUxcnRaOUVrbEppeitlbEI5YXF0WWtzSUdk
VjBRUFFzUFlJRU40bkh1NVN5UjFZQUNTZm1NeW5QRHdyUVJzbWVMOEdVTExHU01OR3hvRkEiLCJtYWMiO
iIyY2E2YmMxMTlmYWQ2ZjY4MjU3MzAyYzc4MmY5MGQ2MDg4ZjIwNWY1NGZkZmZkMWFiZGE1YTRmYTVjYj
MyZDNlIn0%3D; expires=Sun, 14-Jan-2024 14:52:12 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlloOUQ3SmJEckszdXZ2Y1ozMi9nb1E9PSIsInZhbHVlIjoiakIreVdoYVZqQlZFYlJ
rVmRpL3lhY1Jmd3lFUEJCRDZaVCs0R0IyYWJnN2Rpc3RWdGFsYk90bnVHc0s5emR5Q053RlhOVFdQOERV
```

```
SGJDWm5kUVU3cnZ1QzJWZW5icnc5N1JLeUZoaHhURzhBcjRRZmdHRmZhUVBCS3lHUVNEV3UiLCJtYWMiO
iI0OTIxNWUxMzc5NWMxNmJlMDA3ZWNmNzgwM2ZkZWMxYjM2YmM3ZWFiZjFhYWUxZDZlMThlMGJiOGYxZG
Y5OGU2In0%3D; expires=Sun, 14-Jan-2024 14:52:13 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InBYT1I4RnFyTk9wVjVTZXI3YWJwZnc9PSIsInZhbHVlIjoiSEFlczhpaVRWSi9lM3F
mQ0loN3NDQmVKVnlZZzFTVi9MSmdPcjNRYkNPRUlBZFFYeWt4OWVjdVIwSkxTdmRtVERnblFQYWo4dkIv
VGpNUk8ySTlmakhtTlRNUzFtZk1SU2pFdkVrRDgvY2hwek9XM0ovbTdSSFZvRkR1WTBRcUQiLCJtYWMiO
iI2YmIyMDNmNDU3YjVkYTBlZjU0OTcwNWU0Njk1NWNmOGJhZTE2NWM3MjY4MDk5ODQzYzQwYzUxOGQyNG
RmMTI5In0%3D; expires=Sun, 14-Jan-2024 14:52:21 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJiRVdtYXFNRS9ldm8xbXlUeVN3NkE9PSIsInZhbHVlIjoiUjd6R0JkQ2NINDZDd1d
5aHRKOGwrOXNCQmErU2Z4U0ZrMWRaL0s1MHpsd0ljK0JqVXd6RmhKaXdRakVrd2RFa1JTRTZ4WTFraDJX
N3B4NmlnbUVJUGFyRkVnU294bXdRcUhWWWE2OGxiTjFDSitLZEgrRFR3MGluRm5FeWc4Q0siLCJtYWMiO
iI4MWJjZGQzN2Y0MTdkY2QwYWJkNTAwMmJjMWMzMTkyMTI0MTdhYTdhZmE4ZjdmMDhhZTU2NjhiMjlhNT
Q1NzFiIn0%3D; expires=Sun, 14-Jan-2024 14:52:41 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJjN3JRNDZVenpuMmhTcEoweXFqbXc9PSIsInZhbHVlIjoiMC9naGlhZUdoZjdDZnh
Cc1FIc2ZNMHZZZlNDbGRXL3NORmMvOWk2Nlg4dWJubUhyUVBhdTI1SjFMUy9FSFFoQWcwUkRMMWtPVWZ5
U2RTQ0RnSlhBVDRrVHB1cnBua2xhS291NFNVODNrNTJkL1RGd0ZzOG1VczNyTFdzZEtxS2YiLCJtYWMiO
iIzYjNlYWQ5NmU2NjM4NGRiMTNlMmZkNmVjNWY5NDQyMjRiZTkwMzNmMzEzNTFjYzcyNWU3OGQyNjViM2
I2YmQ1In0%3D; expires=Sun, 14-Jan-2024 14:52:42 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImluelFRVUZ6TXlxQ2tDS0ZYdmZUU0E9PSIsInZhbHVlIjoiemNPR3NhcW1Rb2kwVnp
6N3hOQjFYV3RJZWxZQUxwWVBrWU8xbFNYZ2hNM0FabkFwT1dvdk1RRWpqTFBBb1dFdW50RVZNYkhPdk1E
```

```
SGZaQXlGUGZNZWpKQTZzUGpPNS9uanlLVzkrN2RUMFUrdWJIY3piNW9yVHhGcjJ0TzE0a24iLCJtYWMiO
iI1ZDczM2FjYTI3Y2UzZWU2MWRjY2U4NzczNDY1MTFmODhmNGM5M2Q5OTg2NTRmYjFlNGMxNjAwNGNlNT
BmNjBlIn0%3D; expires=Sun, 14-Jan-2024 14:52:42 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjJ5dndvb1VRV1M1bHBHUDFTRk1LS1E9PSIsInZhbHVlIjoiQ0lnYWpsUnN2NEVlRHp
neWltY09EbkJaTEJYOFk2ejFQbWJkbTQxV2R1cVNGTGVQbUJpc3Boa3FxMlpIZjNCZG5kL2J3WFd5MEg0
SWtWcytBV1d5V2pyTFl6VXc5d0lXcXNNdzVuV29KbE92d2J5cms2Z3hrTWRUVHdpckU3UmoiLCJtYWMiO
iIyMjdjOWQ2MWFhNzFlMTJjMTg3YzMwOGJlNzRmYzdjOWE0ZDU0YmZmMDY2Nzc1YjEzMjJiYTEwMmExMj
EzNDAzIn0%3D; expires=Sun, 14-Jan-2024 14:52:42 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InRId2ZwQ1MwSk9yemkvZnRkY2lzV2c9PSIsInZhbHVlIjoiRUpVWm5NK2NQcTdiT2h
qRWVNeGR6N2NHSk1NMzRzSGVxSHBaZlhuV2JZdDd1OEV6K25SclJLemphS2tPMGlUNFR0SFBwVFdPbTQ4
QkxnNUdRYWo0K1ZFVU55QTJIVngrSkpZWG1VOUJ5eU81YTZyeThqZ29pUzBJY2o0bnYxZmoiLCJtYWMiO
iIzZmEwZDdiMGVmOGM0ZTA0ODJiZjVjMzc3M2ZiZDM5YTczZmYyZDJkZjk0ZjM1YmExZDViMTcwMTgxN2
Q4NjlkIn0%3D; expires=Sun, 14-Jan-2024 14:52:43 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkNObzZZWUcyTnZyci85OFg2WExmV1E9PSIsInZhbHVlIjoiY1JRbGdvMTRTYXI5R05
KV0JOK3ZlT1FKVVA0OGppUmZQbFgrVGI2N3ZKR2t6a1Q3RWEvRTNLWTJWeC9GcXByMTdpYi9EcVYxRjBy
MXFJS3FyQTlHZW43NHpnYXpvK2Z2cmZyTXZHakJaTWdJYUhKNW0zVnpiVGxtMWlJWWZnOUciLCJtYWMiO
iJiNmZjY2Y5OGNjOWM0YWJjMWIzZGM4MTFkYTE2NzI3ZWNjZDgwMGM2ZGFiYThhZjRlOTBlMWZjY2RkYz
E1MDQ4In0%3D; expires=Sun, 14-Jan-2024 14:52:43 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkpYUnRaMkRmZzRRN0hJUzBDd3ZrOVE9PSIsInZhbHVlIjoiUjg5OFBwYVVSWnZ2VlZ
JVTEwRWtTclpsdkZJSFBPSnBVMmo3TkhuNy9ONVBlbVlYTnpEZ1FxMjBQRnAxQXN3V0hLQ1owS3dZOTRY
```

```
ZWpqb3Q1dnh6ZlM2Q2pxbEpGRmE4bnlpdk1ZT0N2WWZvVFBHNnFIVzRDV0hhbXZoMC91NUoiLCJtYWMiO
iJmOWNjZDIzZmU4NjJjY2FkZjUyYWU5MTBmZjliM2EzMTM1YjEzMDM5ODljZTRjZWRkY2JmMDgwODI4OD
ZhZGI2In0%3D; expires=Sun, 14-Jan-2024 14:53:00 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ilp6ckJIQ1VyNk93Tk9tVE1lU2xYN0E9PSIsInZhbHVlIjoiYUN1SWViYUNZczkrWmJ
WNXZkN0J5S1Npam5odnFhbzNQNkRoWVAwT0pPY3N1dVd0bEhVQ3FGUzU2bExORVl6anpQNEFxcmJNWklR
ZG5JTlZPN1gvS21PSlV6aGhETGp0amMzM1I1V0NTaVVLc0VURFhIeCtVOE9Sa011Z2x4ZHkiLCJtYWMiO
iIwZDViZWYwYjFhNGFmYTU4YTRkNTE4ZDVmNWUxNzk5YTU3YmE3YTk2YTZkYmYyOGM5NzRjYmViY2IyMT
kyYTgxIn0%3D; expires=Sun, 14-Jan-2024 14:53:01 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/products/others-ojzfv

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ii9VVjJqY0gxMmV4czZ1ZFdiTHdTT1E9PSIsInZhbHVlIjoiSWtLcXkzeHZLVXZnWER
ybUR5VCtob2RsaGdDZzhtcTUvWUJUQjdLRHQxQkJSUGJZRTZ2WGhYYVBYZ3dEdS9HVCtNcEkvaHM4M2Ry
Tk9CTFVlQ2FZZFoxc29oU2o4V1FWYjB5TUdjYm8xTVJHZ01Vbk9qTkFxckhDcWFiUEZTcVkiLCJtYWMiO
iJjZTVkYzEzZTcxYzk5ZmI1MDQyYjY3YWM2Y2Y5ZWU1NTAxYWViNzI4NGM3YmQ5ZTU5YjI1MDNkYjU2YT
djNDJiIn0%3D; expires=Sun, 14-Jan-2024 14:53:01 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImlxcWFJN1h0UzhZRWltaWx5T1phQkE9PSIsInZhbHVlIjoiNUJvNU1kVTFtMEQzWUt
1RXNKMXJEQVF3Q0xoQ25tQUpRRW1RZXJ0ZlJnUWt2MGhwV08vbUtaUmdrdG5TMTEwUUJUMzVSbGpsbU0y
VjNWb3FZN3RXSlFBNm1RM2VNSXVDdW16bWNEYUxZTmxudVVIdlNNS3JpaHFqMEhzVkN0MUwiLCJtYWMiO
iI1MWRmYjg4MTRkN2VlYjU0NTU2Y2M2YmE2MzNiY2ZkNmJjZjNhMDI4YmNhMmUzYWJhMjVkNjQ2MTU0Yz
hlN2U0In0%3D; expires=Sun, 14-Jan-2024 14:53:07 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkRFT2lIaGRPN21uRWZzL01JdzBJQkE9PSIsInZhbHVlIjoiRndUQVZTa2VFb0JKRk0
vSlkwSTRDUjVLU1J1STYyOTZ3MnZBYUtwdUs4WlNrOVgyMnNrdjNzREpPK3h4UDh1QXFuemprOGRrVVJG
```

```
SW1FVmVkaWdNYlhUYzNiSTF3L0VNL2VKV2RmWFpZNUhJM2JQWm44bnZxdzc0ejJNRjA3RHciLCJtYWMiO
iI2MGQ1NzRkNzBiMTRmOWUwMWFmODQ3MmUzM2JhMjc4YThmMGQ4YzRkZDdmYTJkYTY2ZmQ3M2EwZDk0Ym
ZhMzFkIn0%3D; expires=Sun, 14-Jan-2024 14:53:10 GMT; Max-Age=7200; path=/;
samesite=lax
```

Request

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

Cookies without Secure flag set:

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; path=/
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjEwdGlwMkpRTU45WGVtY3V6eFQvemc9PSIsInZhbHVlIjoiMFc5Sy96NjNiZndnaUp
VajBxTjJBYWorYmQzL2xlNTh1eEF5c1FBNXI5NC9qZjZrbkJJd3hLOHNmb2l0L283T0xmM1kySTlSTVpM
R3pVeG1kUlhDTm9ITHRFeitsRFVzRzY2K2NJNTluTmZEMEpsc0FSYnB2NXdMV3E4R09QT1AiLCJtYWMiO
iI4NDU2MTQ3MTg4YmNlZWU1NzAxZGJmNjhhNWM2NDI0ZjI5NWY3ZmM2OTI5ODZiNzYwZmY3NWNlNWQ2Ym
M1MDdjIn0%3D; expires=Sun, 14-Jan-2024 14:24:01 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IkE2YXF5WjQ4ODdDbWJJUFdRekk0Znc9PSIsInZhbHVlIjoiNk
tKUEgrSThsVEU2YldaeGEyRlE2dEk5dWRNTGJUbE5FTHdkd1FvMFRlSDJyNURHOTBOdkFoaERqOEs2cWV
HOFhNTk9KdUppM0pPOGFHS2w0MUk4MUtJczlta0FxdmI4L211SmxkYkd5RURLN2sxNlBtSWcrUVNUYkw3
dXIyZjciLCJtYWMiOiJlOTNkZmI1YzYyZWNkMzY5MWQzNWM3ZGY3MjViYTJhNmFkY2NiMzIwY2RmMTJkN
zhlOTkxYzczNzZmOWZlMmUyIn0%3D; expires=Sun, 14-Jan-2024 14:24:01 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlGcjM3UEYwRTRtbUNONGR1NDZnNmc9PSIsInZhbHVlIjoidldCUG5KazlSZFMzM0l
rNHNEUURuTHVFWWQ3TkpHRkFhaGhhMU9od0wxVk5mcCtWZWc3K09WU1k2VUN6dUJ1VDRuUUhpSmhlUDIw
dGczb09ac2ZJbHU3a1pOOE9QTGZKNTFEV0lVZmM4akVLczE0WlRHWFJ6dGVtR1gwQWxSKzEiLCJtYWMiO
iJmYWY3MmQxOGMxZmEwYTM1YTE3Mjg1MjU2ODYxNDE1ZmUzNWU5ZDA3NjlmZmJjNTBmYmZjMzQ5NDFmMD
E5YzE5In0%3D; expires=Sun, 14-Jan-2024 14:25:06 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IkpqekFyKzdxK3piT0RHVmE4WTFPTnc9PSIsInZhbHVlIjoiTT
VCeWVHNGoyZWhqNWhLWGN1Nyt4bjQ2ekhZSStUa3MwM3FocXJYS3I1dmJJWjhDMXlBR0N1RnZjOHBKM0Q
1dU5oTzkxK0d3RHpHanh6d3E2bmhhYkJURUVDYXd4WEI0Vms1Y25pT2J1MGQzSjhmSVNja1V1L3NaRDla
a2dZekMiLCJtYWMiOiIzYjZkMjYwZDBiZDZiYzg1Yjc1YTAzODYwNmVjZGJmNjk4YjY1MWM4Nzc4MzM5Y
mIwYjgwNWJkODlkOTc5OTc5In0%3D; expires=Sun, 14-Jan-2024 14:25:06 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkJKaUdhY1AxRTlKZVRzNTBXYmtCMEE9PSIsInZhbHVlIjoiYXcyZXZQY3l5a0JyeE5
kbUVseEZTcndJZEc1RFUwbW81aDJtV0RvV3RJZ2RFR01EcjlZN2JVTVRDUW9COTlhSTVISzVPbzZNREtP
OGxQUXJqbHovalQwVGUzdVUwUktIVzlNQXJkMXFTWkJ6M2xxeWhGZjlKeHNzTzlBc1pMTmQiLCJtYWMiO
iJiZjJhMTZhZTQ3M2UzZTcwZDA0NDE3NjMxNWIxNTRhMGNmODhjNDhkMDk0ODJiZTc3M2M4YWJkODE1Y2
Y5MDMwIn0%3D; expires=Sun, 14-Jan-2024 14:25:21 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6ImQrQU54RUZXaFJMMlVBUWxYK0IxZUE9PSIsInZhbHVlIjoiZU
5TLyt1clN0Wm1Ud082M1hBQ2hENStZOWljQ1NsUDN2U3JqYWpNaDlkM2swdkZvb25Ud25MQ3A1TTJYRWY
2aE02UE1XbFpoaWlCVXA1UDFjYnFialFGMmhvRm1QbVg0MWdXODlOZlE5MjltODNZdSsrUG13Tno1V1N4
VEVEZm4iLCJtYWMiOiI3MzFkMzkzYjg3ODAzZjQ1MWMyZjI5N2YzMDM2MzkxMzEyMjg2YWU1ZmIwYmRlY
2I2ZmUyYjZiYjA3ZmRjY2FmIn0%3D; expires=Sun, 14-Jan-2024 14:25:21 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImoxUldtYUYxVG9mUDR3Q3o3djlHaWc9PSIsInZhbHVlIjoibTc1ZVhlQktETVp5emo
zdDlTNjJMNnhJaXhXSW4xUHc3T05pWkMweVlWS1B4Wk5xVmNaaGVTQitCQTllMXk5dFVVSVdBYm9uNUFL
aHVMSklUT0czMlJGWlM3TUsrb1ZLYy9LK2c3bUpYZnA3cm5udCtBbldOMVBBemFkaGw2WDIiLCJtYWMiO
iJhMTQwMGIxYTgwOGZkZGI1ZjVjZGI4YWQwN2MyZTMwZWM2YWMzY2M5ZTRjMzZlZWI1OTg0NGRjYWNhYT
AwN2U2In0%3D; expires=Sun, 14-Jan-2024 14:51:17 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6InBzSHU5L1JyZFE3cXdWKzhCL2svZ0E9PSIsInZhbHVlIjoiMz
BpcTV3NXRTVW5hQnlTSnhUanNacGplY3Z5bGNVMHpRNFpCaDB2QmVVRFE0V1owQUJZbGdacUM5azFGMDZ
hc0RSVjQydDhSYmUrNysycDVkVXRTSmlybkJ4bkFMYW82OC9tcGRsaU56NG9aTHZqaWVwTVEzQm8rdERv
aEN1aDEiLCJtYWMiOiI4OGY2YTJhZGM5MzQxN2E4OTQzMWI2MzZhNWMwYmZhMWFhMzdkM2ZmYjFjYmQ0N
zg4NzI0YjIzMzI5ODIwY2IzIn0%3D; expires=Sun, 14-Jan-2024 14:51:17 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InVFZklPaUM0QVJxVDBtT1MxcDJTWmc9PSIsInZhbHVlIjoiWDdoMlVsTURYaGlKb2l
KZmV1aVZ2azd4YXlQckNwY3p1TEJvaGt5Uy9raGJUb0lSaVdleEdXZGRaMzRWSzlFN1BjcTZEd3BiZDNO
YWtNNGtBTkUxK05mRmlqeE1IenRYK2tmcDRtTFBXc0tmc2hpZWh6Z1B5ZzAxOHF6R2JrZHoiLCJtYWMiO
iJmZGZiMzI3NDUyM2MxY2FlNDFlODgzMjk2Mjc0ODExMGE4OWM2ZjM2YTg5YTAzNTliNGFmMDFjNGFjMz
gxNzg3In0%3D; expires=Sun, 14-Jan-2024 14:51:28 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IjhNRkV6NEVoZmVLRUIzRE9NZGVFVGc9PSIsInZhbHVlIjoiSl
d0QUFCV2xtUU5ZY3lBTkZuZGM4VnBlUS8yc0pRTFk3WVFVdGFYU0RiUXpKK0VONjRHSGVxR1YzNDVQcW5
PSXUvZHhxeHlVcnkyM2EzbVBnSVVGSVRWMHZ1SmIyS1JJV0ZESTdsSmtoYmMxQ2FUdFA3azBFcVJwUlFo
K1FpQjgiLCJtYWMiOiJlMDg0NTJhNDRhM2M1YmFjYjU0NmIwZmRmYzEyZDBiNTYwMGQ4YzdiY2JlN2JmO
DYyNmI1NGUyNzExYTllNWIxIn0%3D; expires=Sun, 14-Jan-2024 14:51:28 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImJ3NUF0SjFac1EwY1VIOGJSN05ibVE9PSIsInZhbHVlIjoiQXJCWGJ5L2FJV1MyN0x
CeThCd1Q5cU5XMGVmbmxVelIxZlpSK2ZxRGViWjdLZnJUbkduSHdHR1RtT1dMNGQrK0hleTNqZDVxM0Na
YzY5M1c5N1FZVjBmQjgvakN1Z1Y0MVo5TFBicVRuejJWM0hrM2N3d25UMmJoQVpiSytqZnYiLCJtYWMiO
iIyNmYxZGJhM2E1MDY3NzNmZjllMjJkY2I5OWY2YzM2MGRmYjMzZmZlOWNhMDk4YjI1NjlkYmFhMDFlND
g5MDQ5In0%3D; expires=Sun, 14-Jan-2024 14:51:35 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6ImszSGJtY2ZLbmZET3VpcitHRWtESGc9PSIsInZhbHVlIjoidG
Y5MVhiNlVydWU3amp6cU9iZmVFZ0tvT0kxUXU3WGM2SGpOak9BRk4rRUNINnJweHpWMlhpWXVNRTdQRk9
lWkhyVElqMkE1RytLQVVPM2Y5S1B3cmlGUnN0SWZaa3hWaXVjdFlNZFI0SUJuVmhCZSt0cm5LRGo3TDRo
RnJ3L3AiLCJtYWMiOiIxZmExNWZjYjBjNTU0ZWJmYzEzZmFlMDk5ZWJiMjM2YTBlYTc5NTA3ZmI0NDljM
DY4ZGY4ZWNhM2U3MTJlZDNlIn0%3D; expires=Sun, 14-Jan-2024 14:51:35 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkFDbFNIVnh5NWFrSkE2LzJzWis3WlE9PSIsInZhbHVlIjoiZk1VdE40bEwwdE5mbC8
2Y2VnSGVFQ0x4RjE3SGNrQlJvc3NYS3lHbCt6RFkrMjNhQlUxcnRaOUVrbEppeitlbEI5YXF0WWtzSUdk
VjBRUFFzUFlJRU40bkh1NVN5UjFZQUNTZm1NeW5QRHdyUVJzbWVMOEdVTExHU01OR3hvRkEiLCJtYWMiO
iIyY2E2YmMxMTlmYWQ2ZjY4MjU3MzAyYzc4MmY5MGQ2MDg4ZjIwNWY1NGZkZmZkMWFiZGE1YTRmYTVjYj
MyZDNlIn0%3D; expires=Sun, 14-Jan-2024 14:52:12 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6InNNeEV2NmRxZFNXVm0rcDJiQkdxUXc9PSIsInZhbHVlIjoiUz
Zid3Rya1hWdVgrTWVXWnE5ZVRFeE5POHlCbHUrbWhCeTluTThTdEZzVGZiN0pJUTJsOFlJclNQc0ZkZkQ
3ZWJES21RV01NVlk1YkUwZytROENwaVBpdS9SZndpb2Rna1RTcHN2cS9mSmhnZTJhbGt5UThvS2c5eVJv
QUhzR3IiLCJtYWMiOiJiZjM2OGM3MTMwZDM4Mzg3YTllNzBhOTY2MTk4ZDkxZjcxM2IwNDdiMTU5YjczZ
Tc5ZmVkMWQ0NjMyZDFlMWYzIn0%3D; expires=Sun, 14-Jan-2024 14:52:12 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlloOUQ3SmJEckszdXZ2Y1ozMi9nb1E9PSIsInZhbHVlIjoiakIreVdoYVZqQlZFYlJ
rVmRpL3lhY1Jmd3lFUEJCRDZaVCs0R0IyYWJnN2Rpc3RWdGFsYk90bnVHc0s5emR5Q053RlhOVFdQOERV
SGJDWm5kUVU3cnZ1QzJWZW5icnc5N1JLeUZoaHhURzhBcjRRZmdHRmZhUVBCS3lHUVNEV3UiLCJtYWMiO
iI0OTIxNWUxMzc5NWMxNmJlMDA3ZWNmNzgwM2ZkZWMxYjM2YmM3ZWFiZjFhYWUxZDZlMThlMGJiOGYxZG
Y5OGU2In0%3D; expires=Sun, 14-Jan-2024 14:52:13 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://jewellery.ssbmultiservices.com/

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6Impybm1FeVBIY2kvV2hSTFUzbEZTRGc9PSIsInZhbHVlIjoidG
hNS1lDN2wrRXNYTkFuMW5QWU9pWUt2M3JJRTlFbHJQaXBoMHdNNnJ6Q05VOHcvT0k2Vjlua25yMkRIdXh
VUHFwV1RpU0JTSFdUVy9HeFlFUWVDZ1Y1Q054cWpSR21iSEErUXVsU1hhQ0JDOFcvSHVxMVBoQnRFck9o
NXRKVkEiLCJtYWMiOiJiMGE2NTA5MGJiMzMzNjAyZDk0NmNhZWEzZWI2YjNmMjExYWFmYTllY2NiNWM3Z
GY4MmYxZDg1Y2JjMTg4OTczIn0%3D; expires=Sun, 14-Jan-2024 14:52:13 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InBYT1I4RnFyTk9wVjVTZXI3YWJwZnc9PSIsInZhbHVlIjoiSEFlczhpaVRWSi9lM3F
mQ0loN3NDQmVKVnlZZzFTVi9MSmdPcjNRYkNPRUlBZFFYeWt4OWVjdVIwSkxTdmRtVERnblFQYWo4dkIv
VGpNUk8ySTlmakhtTlRNUzFtZk1SU2pFdkVrRDgvY2hwek9XM0ovbTdSSFZvRkR1WTBRcUQiLCJtYWMiO
iI2YmIyMDNmNDU3YjVkYTBlZjU0OTcwNWU0Njk1NWNmOGJhZTE2NWM3MjY4MDk5ODQzYzQwYzUxOGQyNG
RmMTI5In0%3D; expires=Sun, 14-Jan-2024 14:52:21 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6IkNGQVFzYUVOWFJEeHBaQjBBOVl6WEE9PSIsInZhbHVlIjoiK1
F4QmVhVi9Nd2h4czQ1SGFLTkw4ODZWOFk5dGZsR0JUbmpOeGRqNnRCQlF0eHZBOW80eEhpR1ZzZmtHaCt
1bWhRT2VsMmkzdnFsek9lem8xcjlvVjVmak83QWVabTFlYlYySU5taTdxWENDR0xaeWMrS2xQSk11WHAr
NzFJa2giLCJtYWMiOiIzYzBlMmJlMDI1MWQxNWIxODEzMWExMDBlYTQ5OWNhZWUxOWVkZjQzODg5MmE2M
mNiMGYyNmMzNzcxYzQxNjFjIn0%3D; expires=Sun, 14-Jan-2024 14:52:21 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlJiRVdtYXFNRS9ldm8xbXlUeVN3NkE9PSIsInZhbHVlIjoiUjd6R0JkQ2NINDZDd1d
5aHRKOGwrOXNCQmErU2Z4U0ZrMWRaL0s1MHpsd0ljK0JqVXd6RmhKaXdRakVrd2RFa1JTRTZ4WTFraDJX
N3B4NmlnbUVJUGFyRkVnU294bXdRcUhWWWE2OGxiTjFDSitLZEgrRFR3MGluRm5FeWc4Q0siLCJtYWMiO
iI4MWJjZGQzN2Y0MTdkY2QwYWJkNTAwMmJjMWMzMTkyMTI0MTdhYTdhZmE4ZjdmMDhhZTU2NjhiMjlhNT
Q1NzFiIn0%3D; expires=Sun, 14-Jan-2024 14:52:41 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
omkar_jewelers_session=eyJpdiI6InFya05GRGRtSzNnWmJYdks1TFlBV2c9PSIsInZhbHVlIjoibH
BUV3RzUDRieGdxMXlaT1pob2haQjNTZVR3eUR5NC9CdnZMUkNKUXB2ZWZlYnZNSHhKWG5rdC9vTUdrR0d
BUGVCSVU0U2JjUkNTYWswako5dFJHaVlGckhUbkJQU0FlTWFReDJoeCt0N1NUU21QcjBQY21OemdXaVRu
NmdZcUgiLCJtYWMiOiI4ZjQwZTMyNjI1ZTlmZDYxZGJjOGJmNWMyZWE2ZjI2NDczNzcxNTM4ZDk2ZjlhM
zVkM2Q4ZjE5MWUwYTI1MDEzIn0%3D; expires=Sun, 14-Jan-2024 14:52:41 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

Request

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

URLs where HSTS is not enabled:

- https://jewellery.ssbmultiservices.com/upload/category-image/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://jewellery.ssbmultiservices.com/upload/header-footer/
- https://jewellery.ssbmultiservices.com/upload/home-intro/
- https://jewellery.ssbmultiservices.com/product

Request

```
GET /upload/category-image/ HTTP/1.1
Referer: https://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6InVFZklPaUM0QVJxVDBtT1MxcDJTWmc9PSIsInZhbHVlIjoiWDdoMlVsTURYaGlKb2lKZmV1aVZ2azd4YXlQck
NwY3p1TEJvaGt5Uy9raGJUb0lSaVdleEdXZGRaMzRWSzlFN1BjcTZEd3BiZDNOYWtNNGtBTkUxK05mRmlqeE1IenRYK2tmcDRtTF
BXc0tmc2hpZWh6Z1B5ZzAxOHF6R2JrZHoiLCJtYWMiOiJmZGZiMzI3NDUyM2MxY2FlNDFlODgzMjk2Mjc0ODExMGE4OWM2ZjM2YT
g5YTAzNTliNGFmMDFjNGFjMzgxNzg3In0%3D;
```

```
omkar_jewelers_session=eyJpdiI6IjhNRkV6NEVoZmVLRUIzRE9NZGVFVGc9PSIsInZhbHVlIjoiSld0QUFCV2xtUU5ZY3lBT
kZuZGM4VnBlUS8yc0pRTFk3WVFVdGFYU0RiUXpKK0VONjRHSGVxR1YzNDVQcW5PSXUvZHhxeHlVcnkyM2EzbVBnSVVGSVRWMHZ1S
mIyS1JJV0ZESTdsSmtoYmMxQ2FUdFA3azBFcVJwUlFoK1FpQjgiLCJtYWMiOiJlMDg0NTJhNDRhM2M1YmFjYjU0NmIwZmRmYzEyZ
DBiNTYwMGQ4YzdiY2JlN2JmODYyNmI1NGUyNzExYTllNWIxIn0%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: jewellery.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://jewellery.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://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6IjdVTE9EWFRmWWZFb1Fzd3NHd29qUkE9PSIsInZhbHVlIjoiMjUxbWdSU0RycWN5U0djdVRqWG9KTkFERmR0M1
I4eExiVGdKRW1BSS9ENzlsczlxd2dpd1p0cStBRDRIdWZvNmhyVW9Wbi8zOGwycHZ0T2ZjMGt3ZWdORlZ5SGNMcGNTS0EyNEU1UV
p2S2FrYUhnT3FXMHMva0hpcnA4aWUvSloiLCJtYWMiOiIyYjM4MDM0ZDQzNzZjMDUwZTMyNDY2ZTM4MTQ2ZDRhYjA4YWEwMGYxMG
QwN2NlMDg2NjA1YzRiNmEwMGQ3MWFmIn0%3D;
omkar_jewelers_session=eyJpdiI6IkpYQzNHTlNRQ0FneTlVZzgzZTFBTWc9PSIsInZhbHVlIjoiQ05KWWoyNkR5ZjhJWWNMb
XZXQmV3aitqdW5NV3BhYTEySWdvSjV4RU5udlluNGMxS2VJR1dxeFZ5VU45akpBTTFBdml5Z1RNRG5GYkE5TjhzNEgyVGt2YTlLe
Xd3L1ZqbExIcDJsRUcrUmFjL3RMR2ttZTBGU0NIMjJaaU1ycm8iLCJtYWMiOiI1Zjg5YzVkM2UxNTA5ODk1NmQzM2VlMGIyODg2O
GVlYzUwNDM4ZDgwNzZlMDMyOGYzMmY2M2E0MGQ3MjMzMTI0In0%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: jewellery.ssbmultiservices.com
Connection: Keep-alive
```

https://jewellery.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://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6IjdVTE9EWFRmWWZFb1Fzd3NHd29qUkE9PSIsInZhbHVlIjoiMjUxbWdSU0RycWN5U0djdVRqWG9KTkFERmR0M1
I4eExiVGdKRW1BSS9ENzlsczlxd2dpd1p0cStBRDRIdWZvNmhyVW9Wbi8zOGwycHZ0T2ZjMGt3ZWdORlZ5SGNMcGNTS0EyNEU1UV
p2S2FrYUhnT3FXMHMva0hpcnA4aWUvSloiLCJtYWMiOiIyYjM4MDM0ZDQzNzZjMDUwZTMyNDY2ZTM4MTQ2ZDRhYjA4YWEwMGYxMG
QwN2NlMDg2NjA1YzRiNmEwMGQ3MWFmIn0%3D;
omkar_jewelers_session=eyJpdiI6IkpYQzNHTlNRQ0FneTlVZzgzZTFBTWc9PSIsInZhbHVlIjoiQ05KWWoyNkR5ZjhJWWNMb
XZXQmV3aitqdW5NV3BhYTEySWdvSjV4RU5udlluNGMxS2VJR1dxeFZ5VU45akpBTTFBdml5Z1RNRG5GYkE5TjhzNEgyVGt2YTlLe
Xd3L1ZqbExIcDJsRUcrUmFjL3RMR2ttZTBGU0NIMjJaaU1ycm8iLCJtYWMiOiI1Zjg5YzVkM2UxNTA5ODk1NmQzM2VlMGIyODg2O
GVlYzUwNDM4ZDgwNzZlMDMyOGYzMmY2M2E0MGQ3MjMzMTI0In0%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: jewellery.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://jewellery.ssbmultiservices.com/

http://maps.google.com/maps

Request

```
GET /contact-us HTTP/1.1
Referer: https://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6IjdVTE9EWFRmWWZFb1Fzd3NHd29qUkE9PSIsInZhbHVlIjoiMjUxbWdSU0RycWN5U0djdVRqWG9KTkFERmR0M1
I4eExiVGdKRW1BSS9ENzlsczlxd2dpd1p0cStBRDRIdWZvNmhyVW9Wbi8zOGwycHZ0T2ZjMGt3ZWdORlZ5SGNMcGNTS0EyNEU1UV
p2S2FrYUhnT3FXMHMva0hpcnA4aWUvSloiLCJtYWMiOiIyYjM4MDM0ZDQzNzZjMDUwZTMyNDY2ZTM4MTQ2ZDRhYjA4YWEwMGYxMG
QwN2NlMDg2NjA1YzRiNmEwMGQ3MWFmIn0%3D;
omkar_jewelers_session=eyJpdiI6IkpYQzNHTlNRQ0FneTlVZzgzZTFBTWc9PSIsInZhbHVlIjoiQ05KWWoyNkR5ZjhJWWNMb
XZXQmV3aitqdW5NV3BhYTEySWdvSjV4RU5udlluNGMxS2VJR1dxeFZ5VU45akpBTTFBdml5Z1RNRG5GYkE5TjhzNEgyVGt2YTlLe
Xd3L1ZqbExIcDJsRUcrUmFjL3RMR2ttZTBGU0NIMjJaaU1ycm8iLCJtYWMiOiI1Zjg5YzVkM2UxNTA5ODk1NmQzM2VlMGIyODg2O
GVlYzUwNDM4ZDgwNzZlMDMyOGYzMmY2M2E0MGQ3MjMzMTI0In0%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: jewellery.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://jewellery.ssbmultiservices.com/

Possible sensitive files:

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

Request

```
GET /web.config HTTP/1.1
Accept: neagryas/ckmq
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6IjZoQmZYWXhaNW8veFBtVjArMXFZQ3c9PSIsInZhbHVlIjoiT1NybmM5dm44Z0VlZmlNMDNEcVZRT3BLWEJDMk
tqV0NUcXRDSVBvaVEwQW41VVFrdDFrVTM5MDRpdlVoS1IvVzJnOXVxNVF1TzdxRHhkYS8raTRFSmxLU1l6dGJnQmN6UUVEVUtVMk
VoM1oyYld2Vko2ZlJTWURFMnJiNUtCUzYiLCJtYWMiOiJlY2Q4N2I4MzlmNjVlNDcxMDM2ZjAzNjcyNWZhMjFjOTNmZThkNzUzOG
NjMGEzMzhmODg5NDQzNzcyMGRhZjYwIn0%3D;
omkar_jewelers_session=eyJpdiI6InpQTzFZZzEySWU5NGpCalprMnVGS1E9PSIsInZhbHVlIjoicFNUaHh6QlBYNVdtOE9ye
lJLRG1qTTUzMk9aUVRCZ211V1hGNHEyTFhVQkRpRjBnYTY5QlA0aVpNSFRPd1pON1RKZ3FYczBzV21UbEd4b3ltU2czV0NFM2F1V
HB3cW1IN1pFMzVpSkJ0Znhsd1VhTW9BNkdqVXQrS3EvN2VKM28iLCJtYWMiOiJmODQ5ZmZkYWJjYjcxYjYyMzlmYjExZjI2MTQ1N
jkzNjdjNzFhNWZlZmM3Y2IwZDU4NzBhNjUwODgzYWZmN2I5In0%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: jewellery.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://jewellery.ssbmultiservices.com/

Paths without CSP header:

- https://jewellery.ssbmultiservices.com/
- https://jewellery.ssbmultiservices.com/products/gold-bangles-cjvux
- https://jewellery.ssbmultiservices.com/upload/category-image/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://jewellery.ssbmultiservices.com/about-us

- https://jewellery.ssbmultiservices.com/all-categories
- https://jewellery.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://jewellery.ssbmultiservices.com/all-products
- https://jewellery.ssbmultiservices.com/contact-us
- https://jewellery.ssbmultiservices.com/custom-jewelry
- https://jewellery.ssbmultiservices.com/faq
- https://jewellery.ssbmultiservices.com/privacy-policy
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://jewellery.ssbmultiservices.com/services
- https://jewellery.ssbmultiservices.com/terms-of-use
- https://jewellery.ssbmultiservices.com/products/others-ojzfv
- https://jewellery.ssbmultiservices.com/upload/header-footer/
- https://jewellery.ssbmultiservices.com/upload/home-intro/
- https://jewellery.ssbmultiservices.com/product
- https://jewellery.ssbmultiservices.com/index.php
- https://jewellery.ssbmultiservices.com/products/gold-earrings-ywdzz

Request

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

Pages where the content-type header is not specified:

- https://jewellery.ssbmultiservices.com/web.config

Request

```
GET /web.config HTTP/1.1
Referer: https://jewellery.ssbmultiservices.com/
Cookie: PHPSESSID=ebe0c3e6886dc458a16f9206423f61cb; XSRF-
TOKEN=eyJpdiI6IjJ5dndvb1VRV1M1bHBHUDFTRk1LS1E9PSIsInZhbHVlIjoiQ0lnYWpsUnN2NEVlRHpneWltY09EbkJaTEJYOF
k2ejFQbWJkbTQxV2R1cVNGTGVQbUJpc3Boa3FxMlpIZjNCZG5kL2J3WFd5MEg0SWtWcytBV1d5V2pyTFl6VXc5d0lXcXNNdzVuV2
9KbE92d2J5cms2Z3hrTWRUVHdpckU3UmoiLCJtYWMiOiIyMjdjOWQ2MWFhNzFlMTJjMTg3YzMwOGJlNzRmYzdjOWE0ZDU0YmZmMD
Y2Nzc1YjEzMjJiYTEwMmExMjEzNDAzIn0%3D;
omkar_jewelers_session=eyJpdiI6IkJ1WUk4SDdyTEhJVUhnQy90dlBIS0E9PSIsInZhbHVlIjoiVmdCYVJROVFHaUNSZjJPc
GR5K1JuSEVkUGMrREdOQ3NBdmllbHJyWXpDZXpjUE94U3lYN0NobjRnVDFBZTBSM2pNQU8xMzl6aXF6UXZobHhoYjlHUWhqSWhLM
GVoNTk4S3Y2UmYydUp5RzV5TnFjanJrWlQ4QUpZQUUwSHhJWEMiLCJtYWMiOiI5MjA0Yjc1YWRmMjFmODY4YjNiZmY5MmRlNjk1Y
TlkOTY4ZTE4Y2U0YmI1OTU0MDBjNjc2NjczNDU3ZDk2NjJiIn0%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: jewellery.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://jewellery.ssbmultiservices.com/

Emails found:

- https://jewellery.ssbmultiservices.com/
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/products/gold-bangles-cjvux
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/about-us
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/all-categories
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/all-products
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/contact-us
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/custom-jewelry
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/faq
  pulakeshroyny@gmail.com

- https://jewellery.ssbmultiservices.com/privacy-policy
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/services
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/terms-of-use
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/products/others-ojzfv
  pulakeshroyny@gmail.com
- https://jewellery.ssbmultiservices.com/index.php
  pulakeshroyny@gmail.com
- https://jewellery.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: jewellery.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

HTTP Strict Transport Security (HSTS) not following best practices

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

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

https://jewellery.ssbmultiservices.com/

URLs where HSTS configuration is not according to best practices:

- https://jewellery.ssbmultiservices.com/ - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/products/gold-bangles-cjvux - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/about-us - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/all-categories - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5 - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/all-products - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/contact-us - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/custom-jewelry - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/faq - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/privacy-policy - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/services - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/terms-of-use - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/products/others-ojzfv - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/index.php - max-age is less that 1 year (31536000);
- https://jewellery.ssbmultiservices.com/products/gold-earrings-ywdzz - max-age is less that 1 year (31536000);

Request

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

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org
https://hstspreload.org/

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

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://jewellery.ssbmultiservices.com/ Confidence: 95%

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

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

- **Modernizr 2.7.1**
  - URL: https://jewellery.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://jewellery.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: jewellery.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://jewellery.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://jewellery.ssbmultiservices.com/
- https://jewellery.ssbmultiservices.com/products/gold-bangles-cjvux
- https://jewellery.ssbmultiservices.com/upload/category-image/
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/font/
- https://jewellery.ssbmultiservices.com/about-us
- https://jewellery.ssbmultiservices.com/all-categories
- https://jewellery.ssbmultiservices.com/product/gold-bangles-1-dlcozaecw5
- https://jewellery.ssbmultiservices.com/all-products
- https://jewellery.ssbmultiservices.com/contact-us
- https://jewellery.ssbmultiservices.com/custom-jewelry
- https://jewellery.ssbmultiservices.com/faq
- https://jewellery.ssbmultiservices.com/privacy-policy
- https://jewellery.ssbmultiservices.com/assets/front/css/icon_fonts/css/
- https://jewellery.ssbmultiservices.com/services
- https://jewellery.ssbmultiservices.com/terms-of-use
- https://jewellery.ssbmultiservices.com/products/others-ojzfv
- https://jewellery.ssbmultiservices.com/upload/header-footer/
- https://jewellery.ssbmultiservices.com/upload/home-intro/
- https://jewellery.ssbmultiservices.com/product
- https://jewellery.ssbmultiservices.com/index.php
- https://jewellery.ssbmultiservices.com/products/gold-earrings-ywdzz

Request

```
GET / HTTP/1.1
Referer: https://jewellery.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: jewellery.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/

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://jewellery.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: jewellery.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://jewellery.ssbmultiservices.com/

Pages where SRI is not implemented:

- https://jewellery.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://jewellery.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: jewellery.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://jewellery.ssbmultiservices.com
  - assets
    - front
      - css
        - icon_fonts
          - css
            - all_icons.css
            - all_icons.min.css
            - fontello-codes.css
            - icon_set_1.css
            - icon_set_2.css
          - font
        - animate.min.css
        - bootstrap.min.css
        - custom.css
        - magnific-popup.min.css
        - menu.css
        - responsive.css
        - style.css
      - img
      - js
        - bootstrap-portfilter.min.js
        - common_scripts_min.js
        - functions.js
        - jquery-2.2.4.min.js
        - modernizr.js
        - validate.js
        - video_header.js
    - logo
    - sweet-alert.min.js
  - index.php

- products
  - gold-bangles-cjvux
  - gold-earrings-ywdzz
  - gold-necklace-yhza4
  - gold-pendants-ieyji
  - others-ojzfv
- about-us
- all-categories
- all-products
- contact-us
- custom-jewelry
- faq
- privacy-policy
- services
- subscribe
- terms-of-use

- product
  - gold-bangles-1-dlcozaecw5
  - gold-bangles-2-bqihs4kieh
  - gold-earring-1-gehy0lwwrc
  - gold-earring-2-rulpfdv2gj
  - gold-necklace-1-vbhe59cvkb
  - gold-necklace-2-xi4ooxiypl
  - gold-necklace-3-q8g7hrmqrv
  - gold-necklace-4-eov9o7zbmj
  - gold-pendants-1-vvxaidwlbn
  - gold-pendants-2-y3xjcwv09q

- products
  - gold-bangles-cjvux
  - gold-earrings-ywdzz
  - gold-necklace-yhza4
  - gold-pendants-ieyji
  - others-ojzfv

- upload
  - about-us-image
  - category-image
  - client-review-image
  - header-footer
  - home-intro
  - pages-banner-video
  - product-image
  - service-image
- about-us
- all-categories
- all-products
- contact-us
- custom-jewelry
- 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

- index.php
- privacy-policy
- product
- services
- subscribe
- terms-of-use
- web.config