Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 3

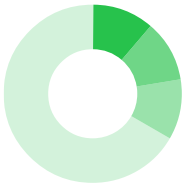
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	https://karnafullytravel.ssbmultiservices.com/
Scan Type	Full Scan
Start Time	Feb 10, 2024, 11:45:58 PM GMT+8
Scan Duration	2 hours
Requests	225094
Average Response Time	33ms
Maximum Response Time	29844ms
Application Build	v23.7.230728157

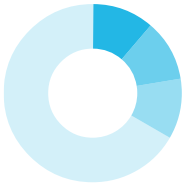
Severity	Vulnerabilities	Instances
High	1	1
Medium	1	1
Low	6	9
Informational	8	9
Total	16	20

Informational



	Instances
Content Security Policy (CSP) not implement…	1
Email addresses	1
File uploads	1
Others	6

Low Severity



	Instances
Clickjacking: X-Frame-Options header	1
Cookies without HttpOnly flag set	1
Cookies without Secure flag set	1
Others	6

Medium Severity

	Instances
Directory listings	1

High Severity

	Instances
Possible database backup	1

Impacts

SEVERITY	IMPACT	
High	1	Possible database backup
Medium	1	Directory listings
Low	1	Clickjacking: X-Frame-Options header
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	3	Passive Mixed Content over HTTPS
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Email addresses
Informational	1	File uploads
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

Possible database backup

Manual confirmation is required for this alert.

One or more possible database backups were identified. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.

Impact

These file(s) may disclose sensitive information. This information can be used to launch further attacks.

https://karnafullytravel.ssbmultiservices.com/

Pages with possible database backups:

-

Request

```
GET /karnafullytravel.zip HTTP/1.1
Range: bytes=0-99999
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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Sensitive files such as database backups should never be stored in a directory that is accessible to the web server. As a workaround, you could restrict access to these file(s).

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://karnafullytravel.ssbmultiservices.com/ Verified

Folders with directory listing enabled:

- https://karnafullytravel.ssbmultiservices.com/upload/brand-slide/
- https://karnafullytravel.ssbmultiservices.com/upload/hajj-umrah/
- https://karnafullytravel.ssbmultiservices.com/upload/logo/
- https://karnafullytravel.ssbmultiservices.com/upload/slider/
- https://karnafullytravel.ssbmultiservices.com/upload/travel/
- https://karnafullytravel.ssbmultiservices.com/upload/about-us/
- https://karnafullytravel.ssbmultiservices.com/upload/posts/
- https://karnafullytravel.ssbmultiservices.com/upload/documents/
- https://karnafullytravel.ssbmultiservices.com/upload/hot-deal/
- https://karnafullytravel.ssbmultiservices.com/upload/photo-gallery/
- https://karnafullytravel.ssbmultiservices.com/upload/where-to-sleep/
- https://karnafullytravel.ssbmultiservices.com/upload/tourist_attractions/

Request

```
GET /upload/brand-slide/ HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6InNtZ3V0RzhnQktYY3ZPSkpiazBqalE9PSIsInZhbHVlIjoiUkpWSUViMFQvUHJLYUtHWVpHOHdlMlpaZW8rRm
tkbUY3b1UxMmM5YmRyekVUS2hEVVg2akI1YmVRa1dOdmJmcUpOelhpQzVNMmZLZ2NPU2tONzNKdnorNm1yRkp1V0ZEQzdRM3VhNC
t3UExOUDhMWnFxNGYvWUtqbjFoVm1RWWEiLCJtYWMiOiIyOGY1YmM1ZjlmZjM2MGVkN2JhYTQ3Y2Q2MjE5N2JlZGViYjgyYWVmMT
lmMDc2MmM5NDg2YmEzNDVlOTBkNjRkIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IktFMkxHVTB3amJKWVZrY25XNTVBNmc9PSIsInZhbHVlIjoiSFpESGxaR0Y3Zl
plU3p6RFNEbEFLYmR2SmhzWGw0Z09ucXgzMUt6Z256WmljUTZHaStXdjlnRUh5RUVVeVdNM2VmUDRVMXVPTW9TSnNPSEdxTjJYa3
JKTVd2bTNFMUZmNE5uOW5sZ1R4c094M3Z5UHpzaXJBQXVXbkhNaTF3MmkiLCJtYWMiOiJhNzZlYWE2ZjM2YTJiNDU1MDg4MTBhN2
RjMjlmN2I3MmE4NjU3NjVmNjI2ZTMxZTQ1ZmVkNjc4MWJmYjg0YTE1In0%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: karnafullytravel.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

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://karnafullytravel.ssbmultiservices.com/

Paths without secure XFO header:

- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/all.css
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/css/toastr.min.css
- https://karnafullytravel.ssbmultiservices.com/upload/brand-slide/
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://karnafullytravel.ssbmultiservices.com/cgi-sys/
- https://karnafullytravel.ssbmultiservices.com/mailman/
- https://karnafullytravel.ssbmultiservices.com/upload/hajj-umrah/
- https://karnafullytravel.ssbmultiservices.com/assets/website/css/style.css
- https://karnafullytravel.ssbmultiservices.com/single-package
- https://karnafullytravel.ssbmultiservices.com/single-travels

- https://karnafullytravel.ssbmultiservices.com/single-blog
- https://karnafullytravel.ssbmultiservices.com/mailman/archives/
- https://karnafullytravel.ssbmultiservices.com/upload/logo/
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/js/toastr.min.js
- https://karnafullytravel.ssbmultiservices.com/upload/slider/
- https://karnafullytravel.ssbmultiservices.com/password
- https://karnafullytravel.ssbmultiservices.com/assets/front/grid-gallery/GridHorizontal.js
- https://karnafullytravel.ssbmultiservices.com/upload/travel/
- https://karnafullytravel.ssbmultiservices.com/upload/about-us/
- https://karnafullytravel.ssbmultiservices.com/assets/front/owl-carousel/owl.carousel.min.css
- https://karnafullytravel.ssbmultiservices.com/upload/posts/

Request

```
GET /assets/front/fonts/fontawesome/css/all.css HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijg2NndyVkVkYjY2cXVoMmtTQmxkbWc9PSIsInZhbHVlIjoiMmJpQ3dGUTF6YytPanE2NW0vb3ZYamlJMS9rVH
RnWkRUSU1KSXNnUEhsK3BxajVKQ3FxMW03VTRZSlYyV1RuSVhyeEhVeVhNREJFNkhtLzdRWUY1R0hPSFBvem1pSW0rMnFGL0dSb0
lCZlYzZ3RnUEJibTk3V3lDeVZuN3dQNEwiLCJtYWMiOiJhZDU2MWYxMDExYmRiOWZkYTllYTMxMGExZDhkMDJjMTliMmQ1ZmI5Mz
AxODg2N2ZiMTgwZGE2YjY0ODZlMjgyIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IkFadUJwZm9BcCtpcVhaNVMrZWdHK3c9PSIsInZhbHVlIjoibFVOUmdPNDNuVm
xnTWdPanFLS0pDWldlcERadXR2WEo4cDBKVG4rZWNtSHhIaTVZeXFmSEJnWkd6VVVVMkl5SXpMYm5uR3BDVHhMSldFeENZdncvUz
RwRUVtMkwvcFRBT0NWeWd5S0E4UVNTWElrNkhGakJEUWg1YVJ1aFBWS3YiLCJtYWMiOiI4MjNmODdlYzUxODFlOGFiZDEwOTc2ZD
M2ZDc4YTg2ZmZlZWQ2Yjc3ZjllNmUzMGY4YzQ3MDMyOWZlZGUzNTZmIn0%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: karnafullytravel.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 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://karnafullytravel.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://karnafullytravel.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ijg2NndyVkVkYjY2cXVoMmtTQmxkbWc9PSIsInZhbHVlIjoiMmJpQ3dGUTF6YytPanE
2NW0vb3ZYamlJMS9rVHRnWkRUSU1KSXNnUEhsK3BxajVKQ3FxMW03VTRZSlYyV1RuSVhyeEhVeVhNREJF
NkhtLzdRWUY1R0hPSFBvem1pSW0rMnFGL0dSb0lCZlYzZ3RnUEJibTk3V3lDeVZuN3dQNEwiLCJtYWMiO
iJhZDU2MWYxMDExYmRiOWZkYTllYTMxMGExZDhkMDJjMTliMmQ1ZmI5MzAxODg2N2ZiMTgwZGE2YjY0OD
ZlMjgyIn0%3D; expires=Sat, 10-Feb-2024 17:46:00 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImQ5UHNWdUNjQmhMbnlJenhTNjFORGc9PSIsInZhbHVlIjoiQWZMakxaZldaQ29SYmV
OYlBqMG1ZYWw5QVZxK01wdVVaTTNXMnhHTTVjaFY2TnR3STVBaUlXRmxSTmRtT2dXellvQlIrVzdWZ3or
cDVIZG5OQTNFdE5ZTXg1bnNWT01Hd2pCcE9pdEF6L05NcGZFRnBjSXUzSUJGdHZ3TjBFN0EiLCJtYWMiO
iJiNzgxMDIwN2M1YTVhZTVjYzdiNmE2OWFhNmYyOWU3NTIwZWI0YWI2ZmFhZmZjZmZhZWM0MzRjYzNiNj
FhZGY3In0%3D; expires=Sat, 10-Feb-2024 17:47:26 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjRFV2NFS3lOZW94Z3VCVXpOSU8zaXc9PSIsInZhbHVlIjoiN2dFMUJDbm5DZFk1dnh
aZGk2dGFiZHhlTk56T0Q2MTNTUlUrY2lNdGpiVzdpNGxUWGI3TGZMaXhucG1XTE1LdHppMmY1RmI2Y01B
RDNmY3JsaWsxVUlONHVnVzNpNnloVURZYi9FRWdEMGFtL0ZJRURnTXd5ZVFIUEJhcysyc28iLCJtYWMiO
iI5ZjZjNmUyZjM3ZmQ5Y2U4OGRlMDdlOTlhYzA0MWQ2ZjA2YTZlNTE3ZTA3N2M0YTU0YjEyNWQ3YmFmNW
UzMDk1In0%3D; expires=Sat, 10-Feb-2024 17:47:30 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVMMXV2eksvSzdHSEdwMkFlR051cEE9PSIsInZhbHVlIjoiR1pHVmphV0xGa0pIcnl
qRVBjd2tnRDBIZlVESFIyUDZIdU1POFVKMFpob0g4QktzSnN4NFFkNG9rejZIVHpUQUYrRnpvbDJCWGNZ
UnVWYk9BWEZGV0RKUnVYSGoyTFpGV1N5QVhoYWRhbldmRTQ5QlVUSlJGY0poZkg5OTRIb3AiLCJtYWMiO
iIwODVmZmY4MjMyMjgwMjgzNWUxZmE5NmZkMmRmYTYxM2Y5NTZiYTVlNWU5Mjg2YWY1NGRiOWE2NGQ5NT
UxNDYwIn0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InNtZ3V0RzhnQktYY3ZPSkpiazBqalE9PSIsInZhbHVlIjoiUkpWSUViMFQvUHJLYUt
HWVpHOHdlMlpaZW8rRmtkbUY3b1UxMmM5YmRyekVUS2hEVVg2akI1YmVRa1dOdmJmcUpOelhpQzVNMmZL
Z2NPU2tONzNKdnorNm1yRkp1V0ZEQzdRM3VhNCt3UExOUDhMWnFxNGYvWUtqbjFoVm1RWWEiLCJtYWMiO
iIyOGY1YmM1ZjlmZjM2MGVkN2JhYTQ3Y2Q2MjE5N2JlZGViYjgyYWVmMTlmMDc2MmM5NDg2YmEzNDVlOT
BkNjRkIn0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/blog

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkgxRGNjSDhTK1UzaE1hVmZNWVUrNEE9PSIsInZhbHVlIjoia1pQdVV0bVkxQmdZdDM
wVnNaUXp3bHE2SGtaYXFQdE8wSUFWVXgzcFhoMlEwMEdKRnBqU0FOTk1yemRDS2ozcURLVTdQb1YvZ01S
bEhIUnFVM1F1M2tmWmNWbWdaS1RxSXA0U2dmRCsvYmdMdHh1QzFocVI0UUhVdy8vMklRUFkiLCJtYWMiO
iIwODk1MDg4YzJmNGE0NmM5MjcyZmFiODE0ZWVjZjI4YzM1YWIyNzhjZjc1MDRiYWJhZTM1YzczOTE0OT
k3M2I0In0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Im1vcnhvNGF2UjZjN1Z3eXYwbjBiYUE9PSIsInZhbHVlIjoibHZsUzBsRnVtMnhrUmh
pNHdmRUFlNGZ6Z2pVdjg2dDN4SW1LYkJLcDNJT1B0OHFIdURRbE5PNGlnQWpUK2czZ201RlRvNzY1ZHlx
djhjbzQzSlI0dnR2aml1eUdsWWlJTGVKQW5xYjVuMXUzT1c2WEdsOG0wUm94OUNEdGJwZ1kiLCJtYWMiO
iJiMmFkZWU3NzY3YWUwNjE4YzdjNzFjNGM3MjFlOGVkNDgwOWIzMjYzZjliMzNlZDcyNTRjMzA0ZGQzOW
NhMGFmIn0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjN3Q3pKeWJaWjBTa0RLSnljNWEzK0E9PSIsInZhbHVlIjoibVhReFZHSDIrUC9HcTE
4aTNaOERtWGpOb29tNTluTmdseVloSnFtOVlrZSsycXlYSVJHVm03OWdtcjRIR2dGa0VkeVRPdzNuc1Rw
Mk5QL3hxVEc0THdSaFRCMjQvWmxCZ2JBblI1QXkwV1lDam13YWVRU2dXRWVreExidVU1UTciLCJtYWMiO
iJiNWVjYWU4MmU0ZWM4ZmEwMmMyM2ZjNWVkZTQ0ZjEwMDJkMGNjZTRlM2M3YjBlYTVjMDE0ZmEzYTE5OD
A4NmI4In0%3D; expires=Sat, 10-Feb-2024 17:48:00 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Imc4aUR0ZG1XOUVHWERwbFFmRFNFaWc9PSIsInZhbHVlIjoiUXZIdE1EY3BITWlQSC9
xcXRuWXFxWFlNMzlLT2Y2aitzTXdDcms1RGZTQ3QwT2hGaC9JUGpUY1AyS2UwcjYwNTJsNVNJNHc3YS91
SG5ib0NyUTlreENLTDhySDhHcmY3bElkYVBLeHlkWE9qTkNiNHVYdmRRRkVQckpWcnZwSDMiLCJtYWMiO
iI2OTA4OWZmM2E3ODkwZmFiYjdlMGU3YWE0NDkxOWU2YWI0MmVmNTY5ZjcwMjEwNWRiZjVhYjM2MmM1YT
lmMTU4In0%3D; expires=Sat, 10-Feb-2024 17:47:56 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjdMbVRWTmFYOGNQQUxsd2RBbFc5TVE9PSIsInZhbHVlIjoiVTl3d3VrNFZVRFdzK3d
tQW1HY0RoREpLRnZkZ2JFRnpUVnMrOVh6OVQ2dE5iWVNVbDR4aDNkc2tLekd4bk9OeEtWRW1DQVFNdWNq
WENBYmpyd0JYaDJCTnNCcERkZ0VWWklGRDN2NHYwRlNUVGQzRDFUOEg3alNnUHF5Smo5bzAiLCJtYWMiO
iI5MjljY2JlM2MwNjE5YWRlZTdjY2MxYTRlMTNhNDY1M2YxNWY0ODBlZTcyMTdhZmM0M2U5ZWM2Y2YyOD
BhNDNlIn0%3D; expires=Sat, 10-Feb-2024 17:48:10 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjU5UnUzbGlRcUJCbGZLdDZibDBiRVE9PSIsInZhbHVlIjoiSFhJcWFQRDRWMmlucGR
jSUIraS90dSt4NlNsRlJvWWJiQzJrV2J1Qmdvc2o0ZlgwUU14amNwelFLZTI1cVFXSlU1cExBSW5jMlJM
UVYxMk5lV05jZnFkSGpDZVZkRXFHUTlnbXZMVjFiaUZla0Z2enY5alBoVUEvYVhERnA0bXMiLCJtYWMiO
iJiYjJmMTM4Mjg0ZDI5NjZhNzlmNmRlZTMzMWY2ZjFlYjA0OGNkNmZlMDY3MGJlZDNkM2NiNDdlMDRmYW
RhYjQ1In0%3D; expires=Sat, 10-Feb-2024 17:48:10 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ind0Y0Z5NlpQWkFtdTQ4R0ZVaGR0cUE9PSIsInZhbHVlIjoiU09xNEc5dE5BTHd2ME1
BaUxwWXRsVjQ1Mmp4TVFlQWxBWUtOaDJaNjFlS1Y0S01peTNKTUo5cENWM25OYzJRRjFHSTFZeUt1VHlY
WENORWVVSlREUmNQVEErd0FEWWkyaUZNK0tsRXQ3L1YzZC9sMk5OM3Z3WThZd0RSM0VVNHkiLCJtYWMiO
iIyYjg0MmExNTNiZWYzYTdlNTAwOGMzOWJlN2I3ZWUwN2EwZTZhZjVhZTFhMTc1NzA4ODU0NzA5NjhmNj
Q3YWQxIn0%3D; expires=Sat, 10-Feb-2024 17:48:19 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/contact-us/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ii8xeWdTMXR3eGY5TllkQjZCMU03aGc9PSIsInZhbHVlIjoiSG5CeTFNZDI3YnFBd05
XbERseUsvMkJvVFBnWks2TXZ0VWd3K2dvVkpydDJqaEVJVCsyYzNOd21BQXJUK3hmakZjM2JCRFhDQVdB
c1lEMlZpSmk1UExRUjYyQ1krYWdGdlZrcmMxV2JFM2NYZ3l3MUNGQzNPQlRIMWlZU1RGQ0QiLCJtYWMiO
iI5ZTYyNDVlNzdiNzIxMWE4ZjM0MTY4Y2FkMTUxODNkODhhNGMwYWY3NjY3MzllOGZlYjc5MWVjYmM3MT
k1NjI2In0%3D; expires=Sat, 10-Feb-2024 17:48:13 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik1vVWFYaWU3ekNiRFFvbStnT1JsdFE9PSIsInZhbHVlIjoiMGFCcHg5S3duT2ZCZlZ
zZXMwa1lEUytieVBjdDRHcFZhNVk4UUlTaWdkc2RqTDdqWHdEcXJXQlNiWk9rM3lLd0lsRE1rOGtPQ1RK
cnlubjEybXdodmh6R1dBTzl2VnZZM25WcnFZZzgwOWQ1KzY1Zk1KZ0cyeSsveHh1dDFFZnoiLCJtYWMiO
iJmMTczMjA4NjJlNjNhMDU3M2ZlNDU4NTA3MTYzYTcyNjM1MjQxZjNiN2ZkNzkwYWYxYWI5ZDBhYzZhMD
gzOTRkIn0%3D; expires=Sat, 10-Feb-2024 17:52:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/blog

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlRzZ1lVcS9BMmpYcWpGaG1OL0JFYnc9PSIsInZhbHVlIjoiYkV2V1UzZUNNRWRIYld
MY3B6QmtpSGFUSUxkWGgxR1l6ZkRERGExMFpLNnNoRDZNM2tFS1NRcWFydC9QMDM0UzNtMVZFYUltbkRG
N0ZkZzZHTDRhZUd3YitCZ3ZTS1dhYWNUemdWVjlPaHVwSXlXdTVxQ1JoODVDUDMwcEorbmEiLCJtYWMiO
iIyYzQ1MDk3YjcwNmRhMTBjNzdkMDdiZjkyMzIyNjA5ZGZiZjI0Y2Y0YjQyMmNhNzA0Mjg2N2I4MmM4ZD
gyMThjIn0%3D; expires=Sat, 10-Feb-2024 17:52:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/hajj-package

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjBRTGVzazRlSnhKN1JtVEdTUmQ1WUE9PSIsInZhbHVlIjoiWWVPTVNLUDVIQzBQOFQ
yOUVBaHlxbm9zQmxrNFc0Sk1TeVhqV0FXc2hZZUI2b3F4WXZWY1J3aHB6bDhiTFR1TmplVVA0YnkvdlBK
UnJLSWJtbTkrR0NYWXRBbHh1bVdIOVhJYU56Ri9FYjdmWEU4MnpRdU50SEYzdDlLY21OWkoiLCJtYWMiO
iI3N2RmYmY4NDNkYWUxOGRhOTQzMzY0ODYzMzM5ZTNlOGRlZmY5MjhhMWFkMWZjMjY0M2FhZmU2YzAxYT
JmZDYwIn0%3D; expires=Sat, 10-Feb-2024 17:52:11 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/hot-deals

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlNhM0ZQVzk3SmZpK1hxbFRkajRMSGc9PSIsInZhbHVlIjoiZW1xaWd3WDR1MENEL2Z
VSU1oaWRPdUFGQzlQOG51d2ZHZlR6WjhjaFZ3M2dUb2JBWVFPN3QrNmRWbisyTGxhdFVNN2MyeXVvWmdl
bHR4YTI5NWVQLytXakFxbEdESUtkN0lJSXRURnJCbjNQQ1IzdEZ4ZUNVNzJ1VmVYWTZEUmsiLCJtYWMiO
iJiNjA1ZDE4NzNhNDdjMWQ3Y2U2ZTU3NWQwNDlmMWZlMWQwMGQ4ZTc5OGQwOTE2MTkzYzBmNTE5NjNmYW
RiMzJmIn0%3D; expires=Sat, 10-Feb-2024 17:53:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/photo-gallery

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik1PaFQyVmk2MlR0bzZJd25obHFrN3c9PSIsInZhbHVlIjoibkJYTHpZbEY4QzBOck5
VRFNpdUdDVm9mT0wvcTUwd3V3UUYwazZMZXVnM25VMFV6ZUxZOE95ZGlVSjQ3WDJHdjg4YWRTZXVUZ1Vw
UUJYeDNpa2VmWUZqdU9CMFZKcy83ZVZKclJza1YrLzJrSlV2eDBWMDlxb1Z4TERJRWUxbU8iLCJtYWMiO
iIyNWQ4ZWUwZTgzNWM0ZGE4YWQ4NGVkZTIzYjMwZmUwZWRmOWZjNDQ3ZDVlN2IzY2YzMzZlMDUyOTNiOG
E4MGNjIn0%3D; expires=Sat, 10-Feb-2024 17:53:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik1Bb0lqNUNoN005TVViVzVheHg0YUE9PSIsInZhbHVlIjoiZzh5YTVYRVRhQWNIWnh
jLzhxVU5oRXJNektLenVBTVF1enllaitjY29SUVI0OG5ocjJSK1Q4eDR6ZDFTQ0UxK2lYZkh4cU55YlpW
TTRyVEg1b3FxUWZ4KzFhR0orL3NhNm5leHF6a0VYeWFYb0ZQUnBNMUZhS1F6RGVQRjJQUkciLCJtYWMiO
iIwNDNkNWRlNGY2OTRmNmZmNDI1MGRmOWRlZDhhNTNiOTNmNTk1MDdhMmJiNWFiMTVlYWZkNWNmM2IwZj
ExMzhjIn0%3D; expires=Sat, 10-Feb-2024 17:53:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/term-of-use

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ik80MWlDMFdxTGFqemFzbkVybjh1cnc9PSIsInZhbHVlIjoiWkZOaEtQdHhCdnBISmM
5VTU3OTNzaXhHV0d6SUNiN0E2NDk0VVlJSTllanRCUk8wVFRJZlFjY0U5YWpuWG1MbDNucHRkUkNsYjdW
TnJ5V2lyOXpkcEVvNmpVa1JDRlFHdjB0dFFmYVBoMURjL2hYWXNqNWxIUUxwRkZ1cFRkM2UiLCJtYWMiO
iIxOWJkMGZhY2U2MjM1Y2VjMjBlZWJkYjQyZDBhZWRiMWVjZDYyOGM3NTMyMzhlMzNhMTk1NjYxM2ZlNz
kxODFkIn0%3D; expires=Sat, 10-Feb-2024 17:53:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/tourist-attraction

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkZOODZFY3J1ZjBUVWdQKy8ramZtMUE9PSIsInZhbHVlIjoiQ3VWVzVqSFczRGdLaHh
5cUlLS0ZHcjBmU0JmSHU4UVNzeGVLL28rQi9HSzYwa0xabGtNSXlYcjFYMnpZeEVqSzhGQ0ovRXNyekNh
V2k5bXJ6VTNZejRMSmNRbHNENmhUckFFNWFUVWFiMmtnZ1F0QXU4MUJ6bEZFemczZWxMelAiLCJtYWMiO
iJkMzQxNTMzYWExNTVlODA1Yjk2ODQxNmMzNjFmMjZlNzgyODYwOGE4NDg4Zjk0NmVhMDEzOTFlMjA4OW
IwNGY2In0%3D; expires=Sat, 10-Feb-2024 17:53:22 GMT; Max-Age=7200; path=/;
samesite=lax
```

Request

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

Cookies without Secure flag set:

- https://karnafullytravel.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ijg2NndyVkVkYjY2cXVoMmtTQmxkbWc9PSIsInZhbHVlIjoiMmJpQ3dGUTF6YytPanE
2NW0vb3ZYamlJMS9rVHRnWkRUSU1KSXNnUEhsK3BxajVKQ3FxMW03VTRZSlYyV1RuSVhyeEhVeVhNREJF
NkhtLzdRWUY1R0hPSFBvem1pSW0rMnFGL0dSb0lCZlYzZ3RnUEJibTk3V3lDeVZuN3dQNEwiLCJtYWMiO
iJhZDU2MWYxMDExYmRiOWZkYTllYTMxMGExZDhkMDJjMTliMmQ1ZmI5MzAxODg2N2ZiMTgwZGE2YjY0OD
ZlMjgyIn0%3D; expires=Sat, 10-Feb-2024 17:46:00 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6IkFadUJwZm9BcCtpcVhaNVMrZWdHK3c9PSIsInZhbHV
```

```
lIjoibFVOUmdPNDNuVmxnTWdPanFLS0pDWldlcERadXR2WEo4cDBKVG4rZWNtSHhIaTVZeXFmSEJnWkd6
VVVVMkl5SXpMYm5uR3BDVHhMSldFeENZdncvUzRwRUVtMkwvcFRBT0NWeWd5S0E4UVNTWElrNkhGakJEU
Wg1YVJ1aFBWS3YiLCJtYWMiOiI4MjNmODdlYzUxODFlOGFiZDEwOTc2ZDM2ZDc4YTg2ZmZlZWQ2Yjc3Zj
llNmUzMGY4YzQ3MDMyOWZlZGUzNTZmIn0%3D; expires=Sat, 10-Feb-2024 17:46:00 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImQ5UHNWdUNjQmhMbnlJenhTNjFORGc9PSIsInZhbHVlIjoiQWZMakxaZldaQ29SYmV
OYlBqMG1ZYWw5QVZxK01wdVVaTTNXMnhHTTVjaFY2TnR3STVBaUlXRmxSTmRtT2dXellvQlIrVzdWZ3or
cDVIZG5OQTNFdE5ZTXg1bnNWT01Hd2pCcE9pdEF6L05NcGZFRnBjSXUzSUJGdHZ3TjBFN0EiLCJtYWMiO
iJiNzgxMDIwN2M1YTVhZTVjYzdiNmE2OWFhNmYyOWU3NTIwZWI0YWI2ZmFhZmZjZmZhZWM0MzRjYzNiNj
FhZGY3In0%3D; expires=Sat, 10-Feb-2024 17:47:26 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6InYycjRUQ3Jac2UzSG0xTHZjdkRYSnc9PSIsInZhbHV
lIjoiMFcyOE10b3JBaUZPV3FsWWp0OEorTDZPYzhuQWxDMi9Cb2x3emhPRnQzcUJEcEYwNythVVFnaG5Q
ZjRVazBoeklCcGx3Umg3TmdhT3RIUnNpQThxYzBXUXVCM3Zoc2MvYWVCTWdibS9lOFZtdWhxNTV6dkI0e
WIxbmNCeFRmSVYiLCJtYWMiOiI4OGM0MmI3MjVjZTQ4NGNmMjAzOTEyMTM4MzVkMDg4YWQ3OWNkOGNlND
cxNGE3N2ZkOTUwNDZlNGI2MDY4ZDM0In0%3D; expires=Sat, 10-Feb-2024 17:47:26 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjRFV2NFS3lOZW94Z3VCVXpOSU8zaXc9PSIsInZhbHVlIjoiN2dFMUJDbm5DZFk1dnh
aZGk2dGFiZHhlTk56T0Q2MTNTUlUrY2lNdGpiVzdpNGxUWGI3TGZMaXhucG1XTE1LdHppMmY1RmI2Y01B
RDNmY3JsaWsxVUlONHVnVzNpNnloVURZYi9FRWdEMGFtL0ZJRURnTXd5ZVFIUEJhcysyc28iLCJtYWMiO
iI5ZjZjNmUyZjM3ZmQ5Y2U4OGRlMDdlOTlhYzA0MWQ2ZjA2YTZlNTE3ZTA3N2M0YTU0YjEyNWQ3YmFmNW
UzMDk1In0%3D; expires=Sat, 10-Feb-2024 17:47:30 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6InVTU3RZMXUyb1dLa0ptcm5LRTc5ZVE9PSIsInZhbHV
```

```
lIjoia2pBRG5BV3RLRVd4R0xuMGkwczFoNVB5UzVPQk1SUlJCbkxQTHNob21rMnB5N1N6UmxId0VVeks3
RkZaOU85MzNFcmdRK0Fic3ZtMTdhSFFsamJpNHVsVDliT1pFbWM4V2tOcWRYSE13ZnN1cEF6UFFPWG0rM
2FmUnhPT0JxSjciLCJtYWMiOiI3OTE3OWIxNTIxNDU1ZWE3ZjJmNDJjOThlODNkMzQxYWVkMGU0YThiYm
ZjNDM0OGFiNTUyZjU3YmZkZGQyZTJjIn0%3D; expires=Sat, 10-Feb-2024 17:47:30 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVMMXV2eksvSzdHSEdwMkFlR051cEE9PSIsInZhbHVlIjoiR1pHVmphV0xGa0pIcnl
qRVBjd2tnRDBIZlVESFIyUDZIdU1POFVKMFpob0g4QktzSnN4NFFkNG9rejZIVHpUQUYrRnpvbDJCWGNZ
UnVWYk9BWEZGV0RKUnVYSGoyTFpGV1N5QVhoYWRhbldmRTQ5QlVUSlJGY0poZkg5OTRIb3AiLCJtYWMiO
iIwODVmZmY4MjMyMjgwMjgzNWUxZmE5NmZkMmRmYTYxM2Y5NTZiYTVlNWU5Mjg2YWY1NGRiOWE2NGQ5NT
UxNDYwIn0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6ImIvYWg5YXBRSUxJNHM4QUtrdXFaUkE9PSIsInZhbHV
lIjoiT2NNSXZBcnB1eE15NEh6ZVllYnlpa1Vlbk1UQURQODZaUkpVQndjWEI4citHYU1sb3I0TnBTVVhK
a2RWb3JkdTQvNmVQMkNmWUtlL2VCcEh0Zm9XMzFjYUcxT2xYc2o1UEFMQjU0NTA4SkpZV2Z0THdyN2lNY
Ux1d2dWVDJpSHgiLCJtYWMiOiI1ZGQ5Njc2Zjc0OTNmN2E2NzYxZDk0YjZhZmRjNDRlY2I4OWY2ZjRiYj
FkZmJjMWI2ZTkwYzE2NWEzOThiYzczIn0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InNtZ3V0RzhnQktYY3ZPSkpiazBqalE9PSIsInZhbHVlIjoiUkpWSUViMFQvUHJLYUt
HWVpHOHdlMlpaZW8rRmtkbUY3b1UxMmM5YmRyekVUS2hEVVg2akI1YmVRa1dOdmJmcUpOelhpQzVNMmZL
Z2NPU2tONzNKdnorNm1yRkp1V0ZEQzdRM3VhNCt3UExOUDhMWnFxNGYvWUtqbjFoVm1RWWEiLCJtYWMiO
iIyOGY1YmM1ZjlmZjM2MGVkN2JhYTQ3Y2Q2MjE5N2JlZGViYjgyYWVmMTlmMDc2MmM5NDg2YmEzNDVlOT
BkNjRkIn0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/search

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6IktFMkxHVTB3amJKWVZrY25XNTVBNmc9PSIsInZhbHV
```

```
lIjoiSFpESGxaR0Y3ZlplU3p6RFNEbEFLYmR2SmhzWGw0Z09ucXgzMUt6Z256WmljUTZHaStXdjlnRUh5
RUVVeVdNM2VmUDRVMXVPTW9TSnNPSEdxTjJYa3JKTVd2bTNFMUZmNE5uOW5sZ1R4c094M3Z5UHpzaXJBQ
XVXbkhNaTF3MmkiLCJtYWMiOiJhNzZlYWE2ZjM2YTJiNDU1MDg4MTBhN2RjMjlmN2I3MmE4NjU3NjVmNj
I2ZTMxZTQ1ZmVkNjc4MWJmYjg0YTE1In0%3D; expires=Sat, 10-Feb-2024 17:47:34 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/blog

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkgxRGNjSDhTK1UzaE1hVmZNWVUrNEE9PSIsInZhbHVlIjoia1pQdVV0bVkxQmdZdDM
wVnNaUXp3bHE2SGtaYXFQdE8wSUFWVXgzcFhoMlEwMEdKRnBqU0FOTk1yemRDS2ozcURLVTdQb1YvZ01S
bEhIUnFVM1F1M2tmWmNWbWdaS1RxSXA0U2dmRCsvYmdMdHh1QzFocVI0UUhVdy8vMklRUFkiLCJtYWMiO
iIwODk1MDg4YzJmNGE0NmM5MjcyZmFiODE0ZWVjZjI4YzM1YWIyNzhjZjc1MDRiYWJhZTM1YzczOTE0OT
k3M2I0In0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/blog

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6InJTdjJoWlhocGc1cngvNWpvbDFWblE9PSIsInZhbHV
lIjoiWVZMaGdjL0UxdklCenBxZmk1S0ljZXR5U2FTL3pzYmZ1UStvVEVFdWJ0SndVWko2RDhNTWtBL0d1
Skd3K2lTaWlqbmxZZm1ETndGR0xSM2ZPV05HK1huVjF4cHlxK2FXM3hZc0JYczk2aEVPWlROQ1FUNzZKW
DQ2VHlhckd0TVIiLCJtYWMiOiI5YmVlM2U3NjMyMmMxYjU1MzlmN2VlMTE0OGVkN2JiNGFkODkwMjVlZm
VhNzNhZWZlOWU1YmQzNWY4YzAwNDQ5In0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Im1vcnhvNGF2UjZjN1Z3eXYwbjBiYUE9PSIsInZhbHVlIjoibHZsUzBsRnVtMnhrUmh
pNHdmRUFlNGZ6Z2pVdjg2dDN4SW1LYkJLcDNJT1B0OHFIdURRbE5PNGlnQWpUK2czZ201RlRvNzY1ZHlx
djhjbzQzSlI0dnR2aml1eUdsWWlJTGVKQW5xYjVuMXUzT1c2WEdsOG0wUm94OUNEdGJwZ1kiLCJtYWMiO
iJiMmFkZWU3NzY3YWUwNjE4YzdjNzFjNGM3MjFlOGVkNDgwOWIzMjYzZjliMzNlZDcyNTRjMzA0ZGQzOW
NhMGFmIn0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6IjBEU0tQRmhFTmxkRzBXS1E5QzdBd3c9PSIsInZhbHV
```

```
lIjoiK09CVnNacnFJUW9pZzZ6VHA0aS84ZSs2ZTc0T0VjNFY3S1pETXBuRWdWODVYaElGT05ET0Y1UVEz
NUc5QlJlbUwwTWl4aWVjd0EzMUNTbmVuTG1hUlFWZ3BTWllEeVZCTTYzU2ptT0NSc2hncklPclZ6T0xIY
m1oMjdmNkxPNHEiLCJtYWMiOiI4NmFhMjcyYTc5ZWE4MTVkNDEzYjAwNjQ5ZTgzYjY3YjczNzdlZjNjMT
Y5ZmVjOWNjNWQzZWQ0Nzc3ZDdkOGEzIn0%3D; expires=Sat, 10-Feb-2024 17:47:55 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjN3Q3pKeWJaWjBTa0RLSnljNWEzK0E9PSIsInZhbHVlIjoibVhReFZHSDIrUC9HcTE
4aTNaOERtWGpOb29tNTluTmdseVloSnFtOVlrZSsycXlYSVJHVm03OWdtcjRIR2dGa0VkeVRPdzNuc1Rw
Mk5QL3hxVEc0THdSaFRCMjQvWmxCZ2JBblI1QXkwV1lDam13YWVRU2dXRWVreExidVU1UTciLCJtYWMiO
iJiNWVjYWU4MmU0ZWM4ZmEwMmMyM2ZjNWVkZTQ0ZjEwMDJkMGNjZTRlM2M3YjBlYTVjMDE0ZmEzYTE5OD
A4NmI4In0%3D; expires=Sat, 10-Feb-2024 17:48:00 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6Ikc1QUNRWE14aTREUjBSQ1JFbGtXQ1E9PSIsInZhbHV
lIjoic3VrcFcxT0JsQ3ltQkp2SVUzU2VpWXlXbmlVenVVNjk3T1Z5eHVmWGxQME82MlZVRXZGRkEzdXFi
eE1DY3poMU1xSExGaDc0RXpmQzZNaTdqWUN3RERId21XMnJvUmRLWm9Bb0RBVXNJUGM1aXA5dCtCWThNb
FJLMnYrMlc3OW8iLCJtYWMiOiI2Y2U4NDU1NWQ1MTBlZDJhYzM4MWQ1ODIzYjliOGIzZjA3YjQ2NWQ1Zm
RhOTM2ZWUzMmM1MzI1MDhmOTkwODhhIn0%3D; expires=Sat, 10-Feb-2024 17:48:00 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

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

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Imc4aUR0ZG1XOUVHWERwbFFmRFNFaWc9PSIsInZhbHVlIjoiUXZIdE1EY3BITWlQSC9
xcXRuWXFxWFlNMzlLT2Y2aitzTXdDcms1RGZTQ3QwT2hGaC9JUGpUY1AyS2UwcjYwNTJsNVNJNHc3YS91
SG5ib0NyUTlreENLTDhySDhHcmY3bElkYVBLeHlkWE9qTkNiNHVYdmRRRkVQckpWcnZwSDMiLCJtYWMiO
iI2OTA4OWZmM2E3ODkwZmFiYjdlMGU3YWE0NDkxOWU2YWI0MmVmNTY5ZjcwMjEwNWRiZjVhYjM2MmM1YT
lmMTU4In0%3D; expires=Sat, 10-Feb-2024 17:47:56 GMT; Max-Age=7200; path=/;
samesite=lax
```

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

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6InBJN25SdWR1cW8zSnJadGNxaUxMWEE9PSIsInZhbHV
```

```
lIjoiaEpnRDBRVVIrcnpLNGYrYmdVbmhFT1c5RkxFTUZSWmFJQjhlRWQreFY5S05NeUsxeHRjS2lHMG9L
c2RTOWlBbHdiWWczSFRJc0FxUWRNemp4KzhLeDJFRCtuVEdkQVRtd01zMEltaGFicS9tSkhWUzNJdWhnQ
0RKYUp5SERTNUwiLCJtYWMiOiJlMWU0MWVjYzU3NTY0YjUyZTJhMThjNjA3OGIyYTc5MjU3YTgwODY1YT
gwOWVlNWQwOTgwNWQ4OWQ4ZGU5ODMzIn0%3D; expires=Sat, 10-Feb-2024 17:47:56 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjdMbVRWTmFYOGNQQUxsd2RBbFc5TVE9PSIsInZhbHVlIjoiVTl3d3VrNFZVRFdzK3d
tQW1HY0RoREpLRnZkZ2JFRnpUVnMrOVh6OVQ2dE5iWVNVbDR4aDNkc2tLekd4bk9OeEtWRW1DQVFNdWNq
WENBYmpyd0JYaDJCTnNCcERkZ0VWWklGRDN2NHYwRlNUVGQzRDFUOEg3alNnUHF5Smo5bzAiLCJtYWMiO
iI5MjljY2JlM2MwNjE5YWRlZTdjY2MxYTRlMTNhNDY1M2YxNWY0ODBlZTcyMTdhZmM0M2U5ZWM2Y2YyOD
BhNDNlIn0%3D; expires=Sat, 10-Feb-2024 17:48:10 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie:
karnafully_travel_inc_session=eyJpdiI6Iks0c3k2cDYrU0dtQ2hqSnovU2pkalE9PSIsInZhbHV
lIjoiNkpQQ25UWmhuZ0o1U1VZYWdBV2FzK3VsNmpsWjhFTmZXTGtRemFJajZBTWpPd2I1ZFVueHFvaFc5
NXcwL0pLRjA4S3F4cm1FZmpqRG10Q1ltOGZXQ0k0WDVYZkh1MncrS0tEV2d0aGNrekpya2tGNmVsbzRDM
UpqS3Z5YlVQWmQiLCJtYWMiOiI5NjA3M2EzNmY3OTkzZjJhNzg5ZTc4ODdkMGI0ZDM2YmYyMDEzY2Q5Ym
U4ZjFjYjRjYmIzMDJiZTc1MWM1Njg3In0%3D; expires=Sat, 10-Feb-2024 17:48:10 GMT; Max-
Age=7200; path=/; httponly; samesite=lax
```

- https://karnafullytravel.ssbmultiservices.com/booking/message

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjU5UnUzbGlRcUJCbGZLdDZibDBiRVE9PSIsInZhbHVlIjoiSFhJcWFQRDRWMmlucGR
jSUIraS90dSt4NlNsRlJvWWJiQzJrV2J1Qmdvc2o0ZlgwUU14amNwelFLZTI1cVFXSlU1cExBSW5jMlJM
UVYxMk5lV05jZnFkSGpDZVZkRXFHUTlnbXZMVjFiaUZla0Z2enY5alBoVUEvYVhERnA0bXMiLCJtYWMiO
iJiYjJmMTM4Mjg0ZDI5NjZhNzlmNmRlZTMzMWY2ZjFlYjA0OGNkNmZlMDY3MGJlZDNkM2NiNDdlMDRmYW
RhYjQ1In0%3D; expires=Sat, 10-Feb-2024 17:48:10 GMT; Max-Age=7200; path=/;
samesite=lax
```

Request

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

URLs where HSTS is not enabled:

- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/all.css
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/css/toastr.min.css
- https://karnafullytravel.ssbmultiservices.com/upload/brand-slide/
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://karnafullytravel.ssbmultiservices.com/cgi-sys/
- https://karnafullytravel.ssbmultiservices.com/mailman/
- https://karnafullytravel.ssbmultiservices.com/upload/hajj-umrah/
- https://karnafullytravel.ssbmultiservices.com/assets/website/css/style.css
- https://karnafullytravel.ssbmultiservices.com/single-package
- https://karnafullytravel.ssbmultiservices.com/single-travels
- https://karnafullytravel.ssbmultiservices.com/single-blog
- https://karnafullytravel.ssbmultiservices.com/mailman/archives/
- https://karnafullytravel.ssbmultiservices.com/upload/logo/
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/js/toastr.min.js
- https://karnafullytravel.ssbmultiservices.com/upload/slider/
- https://karnafullytravel.ssbmultiservices.com/password
- https://karnafullytravel.ssbmultiservices.com/assets/front/grid-gallery/GridHorizontal.js

- https://karnafullytravel.ssbmultiservices.com/upload/travel/
- https://karnafullytravel.ssbmultiservices.com/upload/about-us/
- https://karnafullytravel.ssbmultiservices.com/assets/front/owl-carousel/owl.carousel.min.css
- https://karnafullytravel.ssbmultiservices.com/upload/posts/

Request

```
GET /assets/front/fonts/fontawesome/css/all.css HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijg2NndyVkVkYjY2cXVoMmtTQmxkbWc9PSIsInZhbHVlIjoiMmJpQ3dGUTF6YytPanE2NW0vb3ZYamlJMS9rVH
RnWkRUSU1KSXNnUEhsK3BxajVKQ3FxMW03VTRZSlYyV1RuSVhyeEhVeVhNREJFNkhtLzdRWUY1R0hPSFBvem1pSW0rMnFGL0dSb0
lCZlYzZ3RnUEJibTk3V3lDeVZuN3dQNEwiLCJtYWMiOiJhZDU2MWYxMDExYmRiOWZkYTllYTMxMGExZDhkMDJjMTliMmQ1ZmI5Mz
AxODg2N2ZiMTgwZGE2YjY0ODZlMjgyIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IkFadUJwZm9BcCtpcVhaNVMrZWdHK3c9PSIsInZhbHVlIjoibFVOUmdPNDNuVm
xnTWdPanFLS0pDWldlcERadXR2WEo4cDBKVG4rZWNtSHhIaTVZeXFmSEJnWkd6VVVVMkl5SXpMYm5uR3BDVHhMSldFeENZdncvUz
RwRUVtMkwvcFRBT0NWeWd5S0E4UVNTWElrNkhGakJEUWg1YVJ1aFBWS3YiLCJtYWMiOiI4MjNmODdlYzUxODFlOGFiZDEwOTc2ZD
M2ZDc4YTg2ZmZlZWQ2Yjc3ZjllNmUzMGY4YzQ3MDMyOWZlZGUzNTZmIn0%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: karnafullytravel.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://karnafullytravel.ssbmultiservices.com/ Verified

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

Request

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

https://karnafullytravel.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://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6InNtZ3V0RzhnQktYY3ZPSkpiazBqalE9PSIsInZhbHVlIjoiUkpWSUViMFQvUHJLYUtHWVpHOHdlMlpaZW8rRm
tkbUY3b1UxMmM5YmRyekVUS2hEVVg2akI1YmVRa1dOdmJmcUpOelhpQzVNMmZLZ2NPU2tONzNKdnorNm1yRkp1V0ZEQzdRM3VhNC
t3UExOUDhMWnFxNGYvWUtqbjFoVm1RWWEiLCJtYWMiOiIyOGY1YmM1ZjlmZjM2MGVkN2JhYTQ3Y2Q2MjE5N2JlZGViYjgyYWVmMT
lmMDc2MmM5NDg2YmEzNDVlOTBkNjRkIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IktFMkxHVTB3amJKWVZrY25XNTVBNmc9PSIsInZhbHVlIjoiSFpESGxaR0Y3Zl
plU3p6RFNEbEFLYmR2SmhzWGw0Z09ucXgzMUt6Z256WmljUTZHaStXdjlnRUh5RUVVeVdNM2VmUDRVMXVPTW9TSnNPSEdxTjJYa3
JKTVd2bTNFMUZmNE5uOW5sZ1R4c094M3Z5UHpzaXJBQXVXbkhNaTF3MmkiLCJtYWMiOiJhNzZlYWE2ZjM2YTJiNDU1MDg4MTBhN2
RjMjlmN2I3MmE4NjU3NjVmNjI2ZTMxZTQ1ZmVkNjc4MWJmYjg0YTE1In0%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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

References

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

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

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

Passive Mixed Content over HTTPS

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

Impact

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

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

The following issues were detected:

- The tag **img** references the resource **http://karnafullytravel.com/upload/photo-gallery/img_1622445122_60b48c42bf86c.jpg**

Request

```
GET /about-us HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijg2NndyVkVkYjY2cXVoMmtTQmxkbWc9PSIsInZhbHVlIjoiMmJpQ3dGUTF6YytPanE2NW0vb3ZYamlJMS9rVH
RnWkRUSU1KSXNnUEhsK3BxajVKQ3FxMW03VTRZSlYyV1RuSVhyeEhVeVhNREJFNkhtLzdRWUY1R0hPSFBvem1pSW0rMnFGL0dSb0
lCZlYzZ3RnUEJibTk3V3lDeVZuN3dQNEwiLCJtYWMiOiJhZDU2MWYxMDExYmRiOWZkYTllYTMxMGExZDhkMDJjMTliMmQ1ZmI5Mz
AxODg2N2ZiMTgwZGE2YjY0ODZlMjgyIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IkFadUJwZm9BcCtpcVhaNVMrZWdHK3c9PSIsInZhbHVlIjoibFVOUmdPNDNuVm
xnTWdPanFLS0pDWldlcERadXR2WEo4cDBKVG4rZWNtSHhIaTVZeXFmSEJnWkd6VVVVMkl5SXpMYm5uR3BDVHhMSldFeENZdncvUz
RwRUVtMkwvcFRBT0NWeWd5S0E4UVNTWElrNkhGakJEUWg1YVJ1aFBWS3YiLCJtYWMiOiI4MjNmODdlYzUxODFlOGFiZDEwOTc2ZD
M2ZDc4YTg2ZmZlZWQ2Yjc3ZjllNmUzMGY4YzQ3MDMyOWZlZGUzNTZmIn0%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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

https://karnafullytravel.ssbmultiservices.com/hajj-package

The following issues were detected:

- The tag **img** references the resource **http://karnafullytravel.com/upload/photo-gallery/img_1622444164_60b48884ef758.jpg**

Request

```
GET /hajj-package HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6Ik1vVWFYaWU3ekNiRFFvbStnT1JsdFE9PSIsInZhbHVlIjoiMGFCcHg5S3duT2ZCZlZzZXMwa1lEUytieVBjdD
RHcFZhNVk4UUlTaWdkc2RqTDdqWHdEcXJXQlNiWk9rM3lLd0lsRE1rOGtPQ1RKcnlubjEybXdodmh6R1dBTzl2VnZZM25WcnFZZz
gwOWQ1KzY1Zk1KZ0cyeSsveHh1dDFFZnoiLCJtYWMiOiJmMTczMjA4NjJlNjNhMDU3M2ZlNDU4NTA3MTYzYTcyNjM1MjQxZjNiN2
ZkNzkwYWYxYWI5ZDBhYzZhMDgzOTRkIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IlpFVzRKOWI0MWFVOHhYclcwSkZCMmc9PSIsInZhbHVlIjoiTXZPL1JoVkxybV
BUUmUwd29VVkZTWGlzb3dOK3gvU0Z4NERkTUpWSmJaTEptZmhOUWhEMG9lZVZOSlh0cmkxSFVGQUxnUnpqOFVCOFk5VUlQeFFpUH
JDVnVZcmo3ejN3dGFITUcvR2UyUUl4a21LTlJpUHNLRldCUktKZDBXdmIiLCJtYWMiOiIxNjQzNzA0ODRkZDRmMzlhNTUyOWU4OD
Q5MjhlNjY4ZjM3N2Q2YjhhNDQ5OWU5YTdhODlkM2MwNWJmOTU0NWEwIn0%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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

https://karnafullytravel.ssbmultiservices.com/umrah-package

The following issues were detected:

- The tag **img** references the resource **http://karnafullytravel.com/upload/photo-gallery/img_1622444135_60b488670e9e6.jpg**

Request

```
GET /umrah-package HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IkZOODZFY3J1ZjBUVWdQKy8ramZtMUE9PSIsInZhbHVlIjoiQ3VWVzVqSFczRGdLaHh5cUlLS0ZHcjBmU0JmSH
U4UVNzeGVLL28rQi9HSzYwa0xabGtNSXlYcjFYMnpZeEVqSzhGQ0ovRXNyekNhV2k5bXJ6VTNZejRMSmNRbHNENmhUckFFNWFUVW
FiMmtnZ1F0QXU4MUJ6bEZFemczZWxMelAiLCJtYWMiOiJkMzQxNTMzYWExNTVlODA1Yjk2ODQxNmMzNjFmMjZlNzgyODYwOGE4ND
```

```
g4Zjk0NmVhMDEzOTFlMjA4OWIwNGY2In0%3D;
karnafully_travel_inc_session=eyJpdiI6IkE0V1RJTVhEVEY1SnluR3VvZ3dSQVE9PSIsInZhbHVlIjoiOUlycm56TEl1eU
hVSmxjcTRPL1ZoVmdza0JaSVBTN2N2RXBSb3V2b2UwYnVuOEprWmZ6N1EzdUJ2b29LNUNQbUdtakV4SEcxL25KdG9MTmZuMjE1SE
h4aWdLUDRDOFZGVVhvenhHTDNRQW9JY2VteWlSQWFiNFNKOTVGVnlheVQiLCJtYWMiOiI2NzU4NzIxZWNkODJjYWZkZGI0NWMxZj
JlMWY4ZjA2YjFiN2NhZjYyZTdmNjk5ZTJmZDE2MmY1MDI2ZDc5NWI2In0%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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

References

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

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

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

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://karnafullytravel.ssbmultiservices.com/

Paths without CSP header:

- https://karnafullytravel.ssbmultiservices.com/
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/all.css
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/css/toastr.min.css
- https://karnafullytravel.ssbmultiservices.com/about-us
- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package
- https://karnafullytravel.ssbmultiservices.com/upload/brand-slide/
- https://karnafullytravel.ssbmultiservices.com/blog
- https://karnafullytravel.ssbmultiservices.com/booking
- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://karnafullytravel.ssbmultiservices.com/contact-us
- https://karnafullytravel.ssbmultiservices.com/hajj-package

- https://karnafullytravel.ssbmultiservices.com/hot-deals
- https://karnafullytravel.ssbmultiservices.com/photo-gallery
- https://karnafullytravel.ssbmultiservices.com/services
- https://karnafullytravel.ssbmultiservices.com/term-of-use
- https://karnafullytravel.ssbmultiservices.com/tourist-attraction
- https://karnafullytravel.ssbmultiservices.com/umrah-package
- https://karnafullytravel.ssbmultiservices.com/where-to-sleep
- https://karnafullytravel.ssbmultiservices.com/index.php
- https://karnafullytravel.ssbmultiservices.com/index.php/single-package/4-star-hajj-package

Request

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

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://karnafullytravel.ssbmultiservices.com/

Emails found:

- https://karnafullytravel.ssbmultiservices.com/
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/about-us
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/about-us
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/search
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/search
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/blog
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/blog
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/booking
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/booking
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now
  msalim@karnafullytravel.com

- https://karnafullytravel.ssbmultiservices.com/contact-us
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/contact-us
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/hajj-package
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/hajj-package
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/hot-deals
  karnafullytravel@yahoo.com
- https://karnafullytravel.ssbmultiservices.com/hot-deals
  msalim@karnafullytravel.com
- https://karnafullytravel.ssbmultiservices.com/photo-gallery
  karnafullytravel@yahoo.com

Request

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

File uploads

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

https://karnafullytravel.ssbmultiservices.com/

Pages with file upload forms:

- https://karnafullytravel.ssbmultiservices.com/booking

  ```
  Form name: <empty>
  Form action: https://karnafullytravel.ssbmultiservices.com/booking/message
  Form method: POST
  Form file input: document[] [file]
  ```

- https://karnafullytravel.ssbmultiservices.com/index.php/booking

  ```
  Form name: <empty>
  Form action:
  https://karnafullytravel.ssbmultiservices.com/index.php/booking/message
  Form method: POST
  Form file input: document[] [file]
  ```

Request

```
GET /booking HTTP/1.1
Referer: https://karnafullytravel.ssbmultiservices.com/
Cookie: XSRF-
TOKEN=eyJpdiI6InNtZ3V0RzhnQktYY3ZPSkpiazBqalE9PSIsInZhbHVlIjoiUkpWSUViMFQvUHJLYUtHWVpHOHdlMlpaZW8rRm
tkbUY3b1UxMmM5YmRyekVUS2hEVVg2akI1YmVRa1dOdmJmcUpOelhpQzVNMmZLZ2NPU2tONzNKdnorNm1yRkp1V0ZEQzdRM3VhNC
t3UExOUDhMWnFxNGYvWUtqbjFoVm1RWWEiLCJtYWMiOiIyOGY1YmM1ZjlmZjM2MGVkN2JhYTQ3Y2Q2MjE5N2JlZGViYjgyYWVmMT
lmMDc2MmM5NDg2YmEzNDVlOTBkNjRkIn0%3D;
karnafully_travel_inc_session=eyJpdiI6IktFMkxHVTB3amJKWVZrY25XNTVBNmc9PSIsInZhbHVlIjoiSFpESGxaR0Y3Zl
plU3p6RFNEbEFLYmR2SmhzWGw0Z09ucXgzMUt6Z256WmljUTZHaStXdjlnRUh5RUVVeVdNM2VmUDRVMXVPTW9TSnNPSEdxTjJYa3
JKTVd2bTNFMUZmNE5uOW5sZ1R4c094M3Z5UHpzaXJBQXVXbkhNaTF3MmkiLCJtYWMiOiJhNzZlYWE2ZjM2YTJiNDU1MDg4MTBhN2
RjMjlmN2I3MmE4NjU3NjVmNjI2ZTMxZTQ1ZmVkNjc4MWJmYjg0YTE1In0%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: karnafullytravel.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

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://karnafullytravel.ssbmultiservices.com/

URLs where HSTS configuration is not according to best practices:

- https://karnafullytravel.ssbmultiservices.com/ - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/about-us - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/search - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/blog - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/booking - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/contact-us - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/hajj-package - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/hot-deals - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/photo-gallery - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/services - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/term-of-use - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/tourist-attraction - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/umrah-package - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/where-to-sleep - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/index.php - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/index.php/single-package/4-star-hajj-package - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/index.php/single-travels/book-domestic-air-ticket-now - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/login - max-age is less that 1 year (31536000);
- https://karnafullytravel.ssbmultiservices.com/password/reset - max-age is less that 1 year (31536000);

Request

```
GET / HTTP/1.1
Referer: https://karnafullytravel.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: karnafullytravel.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://karnafullytravel.ssbmultiservices.com/ Confidence: 95%

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

Request

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

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

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

Locations without Permissions-Policy header:

- https://karnafullytravel.ssbmultiservices.com/
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/all.css
- https://karnafullytravel.ssbmultiservices.com/assets/toastr/css/toastr.min.css
- https://karnafullytravel.ssbmultiservices.com/about-us
- https://karnafullytravel.ssbmultiservices.com/single-package/4-star-hajj-package
- https://karnafullytravel.ssbmultiservices.com/search
- https://karnafullytravel.ssbmultiservices.com/upload/brand-slide/
- https://karnafullytravel.ssbmultiservices.com/blog
- https://karnafullytravel.ssbmultiservices.com/booking
- https://karnafullytravel.ssbmultiservices.com/single-travels/book-domestic-air-ticket-now
- https://karnafullytravel.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://karnafullytravel.ssbmultiservices.com/contact-us
- https://karnafullytravel.ssbmultiservices.com/hajj-package
- https://karnafullytravel.ssbmultiservices.com/hot-deals
- https://karnafullytravel.ssbmultiservices.com/photo-gallery
- https://karnafullytravel.ssbmultiservices.com/services
- https://karnafullytravel.ssbmultiservices.com/term-of-use
- https://karnafullytravel.ssbmultiservices.com/tourist-attraction
- https://karnafullytravel.ssbmultiservices.com/umrah-package
- https://karnafullytravel.ssbmultiservices.com/where-to-sleep
- https://karnafullytravel.ssbmultiservices.com/index.php

Request

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

Pages where SRI is not implemented:

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

- https://karnafullytravel.ssbmultiservices.com/
  Script SRC: **https://unpkg.com/sweetalert/dist/sweetalert.min.js**

- https://karnafullytravel.ssbmultiservices.com/
  Script SRC: **https://cdn.jsdelivr.net/jquery.marquee/1.3.1/jquery.marquee.min.js**

- https://karnafullytravel.ssbmultiservices.com/
  Script SRC: **https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit**

Request

```
GET / HTTP/1.1
Referer: https://karnafullytravel.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: karnafullytravel.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://karnafullytravel.ssbmultiservices.com
  - #fragments
    - umrah_10
    - umrah_11
    - umrah_12
    - umrah_4
    - umrah_8
    - umrah_9
  - Inputs
    - GET iv, value, mac
  - assets
    - Inputs
      - GET iv, value, mac
    - front
      - Inputs
        - GET iv, value, mac
      - css
        - preloader.css
        - style.css
      - fonts
        - fontawesome
          - css
            - all.css
      - grid-gallery
        - GridHorizontal.js
        - imagesloaded.pkgd.min.js
        - jquery.scripttop.min.css
        - lightbox.css
        - lightbox.js
      - image
        - Inputs

GET iv, value, mac

- js
  - main.js
  - sweet-alert.min.js
- owl-carousel
  - owl.carousel.min.css
  - owl.carousel.min.js
  - owl.theme.default.min.css
- slick-slider
  - slick.main.css
  - slick.min.js
  - slick.theme.min.css

- image
  - Inputs
    - GET iv, value, mac
- toastr
  - Inputs
    - GET iv, value, mac
  - css
    - toastr.min.css
  - js
    - toastr.min.js
- website
  - Inputs
    - GET iv, value, mac
  - css
    - style.css

- booking
  - Inputs
    - GET iv, value, mac
  - message
    - Inputs
      - GET iv, value, mac

POST iv, value, mac

POST _token, adults, adults_count, child, child_count, date_of_birth, departure_airport, departure_date, destination_airport, document[], email, fname, gender, infants, infants_count, lname, mname, other_inform, other_member_name, phone, return_date, ticket_type

- cgi-sys
  - Inputs
    - GET iv, value, mac
- contact-us
  - Inputs
    - GET iv, value, mac
  - message
    - Inputs
      - GET iv, value, mac
      - POST iv, value, mac
      - POST _token, email, message, name, phone
- index.php
  - Inputs
    - GET iv, value, mac
  - booking
    - Inputs
      - GET iv, value, mac
    - message
      - Inputs
        - GET iv, value, mac
        - POST iv, value, mac
        - POST _token, adults, adults_count, child, child_count, date_of_birth, departure_airport, departure_date, destination_airport, document[], email, fname, gender, infants, infants_count, lname, mname, other_inform, other_member_name, phone, return_date, ticket_type
  - contact-us
    - Inputs
      - GET iv, value, mac
    - message
      - Inputs
        - GET iv, value, mac
        - POST iv, value, mac

POST _token, email, message, name, phone

single-blog

Inputs

GET iv, value, mac

2050-sale-iurope-muslim-jnsngkhza-hbe-20-stangs

Inputs

GET iv, value, mac

adrs-smaj-grte-islamer-vuumika

Inputs

GET iv, value, mac

akhirat-obiswaseeder-ontr-stzbimukh

Inputs

GET iv, value, mac

ibadter-pasapasi-sttkajer-tagid-dey-islam

Inputs

GET iv, value, mac

islame-nareer-smman-mrzada-oo-odhikar

Inputs

GET iv, value, mac

manusher-suswasthz-allahr-neyamt

Inputs

GET iv, value, mac

mithza-blar-prinam

Inputs

GET iv, value, mac

namaje-mnozog-anar-7ti-upay

Inputs

GET iv, value, mac

pbitr-korane-brnit-fingoar-printer-rhsz

Inputs

GET iv, value, mac

roja-kbuler-jnz-za-krte-hbe

Inputs

GET iv, value, mac

ze-kaje-amader-saflz

Inputs

GET iv, value, mac

single-package

Inputs

GET iv, value, mac

4-star-hajj-package

Inputs

GET iv, value, mac

5-star-hajj-package

Inputs

GET iv, value, mac

5-star-umrah-package

Inputs

GET iv, value, mac

regular-hajj-package

Inputs

GET iv, value, mac

regular-umrah-package

Inputs

GET iv, value, mac

special-umrah-package

Inputs

GET iv, value, mac

single-tourist-attraction

Inputs

GET iv, value, mac

al-baqi

Inputs

GET iv, value, mac

al-wahaba-crater

Inputs

GET iv, value, mac

battle-of-badr

Inputs

GET iv, value, mac

battle-of-uhud

Inputs

GET iv, value, mac

hajar-al-aswad-the-black-stone-hajarai-aswad

Inputs

GET iv, value, mac

hira-cave

Inputs

GET iv, value, mac

jabal-al-nour-prophet-mohammad-received-the-first-verses-of-holy-quran

Inputs

GET iv, value, mac

jabal-magnet

Inputs

GET iv, value, mac

jabal-uhud-baqee

Inputs

GET iv, value, mac

jamrah

Inputs

GET iv, value, mac

madain-saleh

Inputs

GET iv, value, mac

masjid-al-haram

Inputs

GET iv, value, mac

masjid-al-qiblatayn

Inputs

GET iv, value, mac

- mecca-gate
  - Inputs
    - GET iv, value, mac
- mina-the-tent-city
  - Inputs
    - GET iv, value, mac
- mount-arafat
  - Inputs
    - GET iv, value, mac
- muzdalifah
  - Inputs
    - GET iv, value, mac
- prophets-mosque-and-rawdah
  - Inputs
    - GET iv, value, mac
- quba-mosque
  - Inputs
    - GET iv, value, mac
- safa-marwa-hills
  - Inputs
    - GET iv, value, mac
- taif
  - Inputs
    - GET iv, value, mac
- thour-mountain
  - Inputs
    - GET iv, value, mac
- zamzam-well
  - Inputs
    - GET iv, value, mac

- single-travels
  - Inputs

- GET iv, value, mac
- book-domestic-air-ticket-now
  - Inputs
    - GET iv, value, mac
- book-hajj-umrah-ticket-now
  - Inputs
    - GET iv, value, mac
- book-international-air-ticket-now
  - Inputs
    - GET iv, value, mac
- about-us
  - Inputs
    - GET iv, value, mac
- blog
  - Inputs
    - GET iv, value, mac
    - GET page
- booking
  - Inputs
    - GET iv, value, mac
- contact-us
  - Inputs
    - GET iv, value, mac
- hajj-package
  - Inputs
    - GET iv, value, mac
- hot-deals
  - Inputs
    - GET iv, value, mac
- photo-gallery
  - Inputs
    - GET iv, value, mac
- search

- Inputs
  - POST iv, value, mac
  - POST _token, search
  - GET iv, value, mac
  - GET page
- services
  - Inputs
    - GET iv, value, mac
- single-blog
  - Inputs
    - GET iv, value, mac
- single-package
  - Inputs
    - GET iv, value, mac
- single-tourist-attraction
  - Inputs
    - GET iv, value, mac
- single-travels
  - Inputs
    - GET iv, value, mac
- term-of-use
  - Inputs
    - GET iv, value, mac
- tourist-attraction
  - Inputs
    - GET iv, value, mac
    - GET page
- umrah-package
  - Inputs
    - GET iv, value, mac
- where-to-sleep
  - Inputs
    - GET iv, value, mac

- mailman
  - Inputs
    - GET iv, value, mac
  - archives
    - Inputs
      - GET iv, value, mac
- password
  - Inputs
    - GET iv, value, mac
  - email
    - Inputs
      - POST iv, value, mac
      - POST _token, email
      - POST _token, email
      - GET iv, value, mac
  - reset
    - #fragments
      - umrah_8
    - Inputs
      - GET iv, value, mac
- single-blog
  - Inputs
    - GET iv, value, mac
  - 2050-sale-iurope-muslim-jnsngkhza-hbe-20-stangs
    - Inputs
      - GET iv, value, mac
  - adrs-smaj-grte-islamer-vuumika
    - Inputs
      - GET iv, value, mac
  - akhirat-obiswaseeder-ontr-stzbimukh
    - Inputs
      - GET iv, value, mac
  - ibadter-pasapasi-sttkajer-tagid-dey-islam
    - Inputs

GET iv, value, mac

islame-nareer-smman-mrzada-oo-odhikar

Inputs

GET iv, value, mac

manusher-suswasthz-allahr-neyamt

Inputs

GET iv, value, mac

mithza-blar-prinam

Inputs

GET iv, value, mac

namaje-mnozog-anar-7ti-upay

Inputs

GET iv, value, mac

pbitr-korane-brnit-fingoar-printer-rhsz

Inputs

GET iv, value, mac

roja-kbuler-jnz-za-krte-hbe

Inputs

GET iv, value, mac

ze-kaje-amader-saflz

Inputs

GET iv, value, mac

single-package

Inputs

GET iv, value, mac

4-star-hajj-package

Inputs

GET iv, value, mac

5-star-hajj-package

Inputs

GET iv, value, mac

5-star-umrah-package

Inputs

GET iv, value, mac

- regular-hajj-package
  - Inputs
    - GET iv, value, mac
- regular-umrah-package
  - Inputs
    - GET iv, value, mac
- special-umrah-package
  - Inputs
    - GET iv, value, mac

- single-tourist-attraction
  - Inputs
    - GET iv, value, mac
  - al-baqi
    - Inputs
      - GET iv, value, mac
  - al-wahaba-crater
    - Inputs
      - GET iv, value, mac
  - battle-of-badr
    - Inputs
      - GET iv, value, mac
  - battle-of-uhud
    - Inputs
      - GET iv, value, mac
  - hajar-al-aswad-the-black-stone-hajarai-aswad
    - Inputs
      - GET iv, value, mac
  - hira-cave
    - Inputs
      - GET iv, value, mac
  - jabal-al-nour-prophet-mohammad-received-the-first-verses-of-holy-quran
    - Inputs

GET iv, value, mac

jabal-magnet

Inputs

GET iv, value, mac

jabal-uhud-baqee

Inputs

GET iv, value, mac

jamrah

Inputs

GET iv, value, mac

madain-saleh

Inputs

GET iv, value, mac

masjid-al-haram

Inputs

GET iv, value, mac

masjid-al-qiblatayn

Inputs

GET iv, value, mac

mecca-gate

Inputs

GET iv, value, mac

mina-the-tent-city

Inputs

GET iv, value, mac

mount-arafat

Inputs

GET iv, value, mac

muzdalifah

Inputs

GET iv, value, mac

prophets-mosque-and-rawdah

Inputs

GET iv, value, mac

quba-mosque

Inputs

GET iv, value, mac

safa-marwa-hills

Inputs

GET iv, value, mac

taif

Inputs

GET iv, value, mac

thour-mountain

Inputs

GET iv, value, mac

zamzam-well

Inputs

GET iv, value, mac

single-travels

Inputs

GET iv, value, mac

book-domestic-air-ticket-now

#fragments

umrah_8

Inputs

GET iv, value, mac

book-hajj-umrah-ticket-now

Inputs

GET iv, value, mac

book-international-air-ticket-now

Inputs

GET iv, value, mac

upload

Inputs

GET iv, value, mac

- about-us
  - Inputs
    - GET iv, value, mac
- brand-slide
  - Inputs
    - GET iv, value, mac
- documents
  - Inputs
    - GET iv, value, mac
  - img_1636177671_61861707055d4.HEIC
    - Inputs
      - GET iv, value, mac
  - img_1707580090_65c79aba53450.txt
    - Inputs
      - GET iv, value, mac
  - img_1707580090_65c79aba53734.txt
    - Inputs
      - GET iv, value, mac
  - img_1707580090_65c79aba537aa.txt
    - Inputs
      - GET iv, value, mac
  - img_1707580104_65c79ac8a807c.txt
    - Inputs
      - GET iv, value, mac
  - img_1707580138_65c79aea8fae5.'
    - Inputs
      - GET iv, value, mac
  - img_1707580140_65c79aec0f62d.
    - Inputs
      - GET iv, value, mac
  - img_1707580201_65c79b29b52d3.txt
    - Inputs
      - GET iv, value, mac
  - img_1707580233_65c79b491dbb1.

Inputs

GET iv, value, mac

img_1707580275_65c79b73b12b0.txt

Inputs

GET iv, value, mac

img_1707580304_65c79b9067fd4.

Inputs

GET iv, value, mac

img_1707580349_65c79bbdcaf01.txt

Inputs

GET iv, value, mac

img_1707580379_65c79bdb28e11.

Inputs

GET iv, value, mac

img_1707580423_65c79c07da069.txt

Inputs

GET iv, value, mac

img_1707580446_65c79c1e79bbc.

Inputs

GET iv, value, mac

hajj-umrah

Inputs

GET iv, value, mac

hot-deal

Inputs

GET iv, value, mac

logo

Inputs

GET iv, value, mac

photo-gallery

Inputs

GET iv, value, mac

posts

- Inputs
  - GET iv, value, mac
- slider
  - Inputs
    - GET iv, value, mac
- tourist_attractions
  - Inputs
    - GET iv, value, mac
- travel
  - Inputs
    - GET iv, value, mac
- where-to-sleep
  - Inputs
    - GET iv, value, mac
- about-us
  - Inputs
    - GET iv, value, mac
- blog
  - Inputs
    - GET iv, value, mac
    - GET page
- booking
  - Inputs
    - GET iv, value, mac
- contact-us
  - Inputs
    - GET iv, value, mac
- hajj-package
  - Inputs
    - GET iv, value, mac
- hot-deals
  - Inputs
    - GET iv, value, mac

- index.php
  - Inputs
    - GET iv, value, mac
- login
  - Inputs
    - GET iv, value, mac
    - POST _token, email, password
    - POST iv, value, mac
    - POST _token, email, password, remember
- password
  - Inputs
    - GET iv, value, mac
- photo-gallery
  - Inputs
    - GET iv, value, mac
- search
  - Inputs
    - POST iv, value, mac
    - POST _token, search
    - POST _token, search
    - GET page
    - GET iv, value, mac
- services
  - Inputs
    - GET iv, value, mac
- single-blog
  - Inputs
    - GET iv, value, mac
- single-package
  - Inputs
    - GET iv, value, mac
- single-tourist-attraction
  - Inputs
    - GET iv, value, mac

- single-travels
  - Inputs
    - GET iv, value, mac
- term-of-use
  - Inputs
    - GET iv, value, mac
- tourist-attraction
  - Inputs
    - GET iv, value, mac
    - GET page
- umrah-package