



## **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 Scan Type

Start Time Scan Duration

Requests

Average Response Time

Maximum Response Time

Application Build

### $\underline{sharift ax service.ssb multiservices.com}$

Full Scan

Jan 9, 2024, 3:21:29 PM GMT+8

49 minutes

175527

33ms

19697ms

v23.7.230728157







Medium



Low

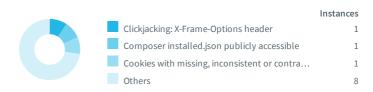


Informational

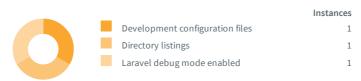
Severity	Vulnerabilities	Instances
High	0	0
Medium	3	3
! Low	10	11
<ul><li>Informational</li></ul>	8	9
Total	21	23

### Low Severity





### **Medium Severity**



# **Impacts**

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

## **Development configuration files**

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

Development configuration files:

• https://shariftaxservice.ssbmultiservices.com/project/docker-compose.yml

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

#### Request

GET /project/docker-compose.yml HTTP/1.1

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

 $TO KEN=eyJpdi16InZ4dmZoSXZmaVdhemZ0cGo5ZURCUEE9PSIsInZhbHVlIjoibzRvU203clQrZVhUbUlvajBwb1Q4SERCLzlJcG0zWjczdzZKM1RZSjFlQU0reGYrRzFaZlBtY0NEck1lYVVUcnhBT\\VIVRmZBUlR4WkU0UjZTUElvcFhTRUU2WlE4RU1Gc2huSnIxRE4vKzJ3N3E5UnRLT3lPV25BVDJiVmh0TVcilCJtYWMi0iJk0DFmYWRkNjc4MzYzMDFmYmZkNjY0NjM3M2I2Y2IzNzliZGFmYWFhZmY1\\YjFk0DA0MmY5NjkzYWZlZWEyYzVkIiwidGFnIjoiIn0%3D;$ 

sharif\_tax\_service\_session=eyJpdi16ImlsvVhoTlhlTWJpZURzTmZrY1dvZEE9PSIsInZhbHVlljoid2JUWUM2SFNTcWVBZKRmWXBwRmV5ZnZTWVdRZGwwRGpBTGhqU25SNmlqWVYxaTZEd2RO
elg2K29lUi9SWkM1cXc2dnd2ZGZGblhDNnU5akZTTlRpNGozZTZwU2xLMXppUWxNeVI0MktVSk5jZzd1MktmUXpvUXJGa0ZaQmhnNS8iLCJtYWMi0iJhN2IxNmQ0MWE1M2MwZmExYzMzNmEyZTZiYzQ
xZTNjM2U3NjU4ZGQ4NmM2ZTA4OTczNzljN2ZiNDg2ZTNkMmFmIiwidGFnIjoiIn0%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

 ${\tt Host: sharift axservice.ssb multiservices.com}$ 

Connection: Keep-alive

### Recommendation

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

## **Directory listings**

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

Verified

Folders with directory listing enabled:

- https://shariftaxservice.ssbmultiservices.com/assets/
- https://shariftaxservice.ssbmultiservices.com/assets/front/
- $\bullet \quad \text{https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/}$
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/css/
- https://shariftaxservice.ssbmultiservices.com/assets/front/css/
- https://shariftaxservice.ssbmultiservices.com/upload/
- https://shariftaxservice.ssbmultiservices.com/upload/client-review/
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- $\bullet \ \ https://shariftaxservice.ssbmultiservices.com/upload/header-footer/$
- https://shariftaxservice.ssbmultiservices.com/project/

- https://shariftaxservice.ssbmultiservices.com/project/vendor/
- https://shariftaxservice.ssbmultiservices.com/project/vendor/asm89/
- https://shariftaxservice.ssbmultiservices.com/upload/real-state/
- https://shariftaxservice.ssbmultiservices.com/project/vendor/asm89/stack-cors/
- https://shariftaxservice.ssbmultiservices.com/upload/service-photo/
- https://shariftaxservice.ssbmultiservices.com/assets/front/image/
- https://shariftaxservice.ssbmultiservices.com/assets/front/image/recognized-by/
- https://shariftaxservice.ssbmultiservices.com/upload/slider-image/
- https://shariftaxservice.ssbmultiservices.com/upload/post-image/
- https://shariftaxservice.ssbmultiservices.com/assets/front/js/

GET /assets/ HTTP/1.1

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TOKEN=evJpdiI6Inl4U1BHRXZvUFN1RHhoem5HMmU3OXc9PSIsInZhbHVlIioib05DTWtZMHN1SDk5Ykt0TU00a0F6am9vTGlUcW50SiYrT2taVnFiRi9wTXJwa1k5SXR1cE5BdHdlYTFEViV40Vdme EJad1hlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUlWV28iLCJtYWMi0iIyM2I5ZTFiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNm MjQ1NjQz0GM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D;

 $sharif\_tax\_service\_session=eyJpdi16Im5j0GtaTVM120xibVpyZjUyY2kwU1E9PSIsInZhbHVlljoiZjd6dlJ5TzdlK2FvNDZpeCszV2c5enVJ0VBlNG02bUtham5pbjhxYmFUbVJUM0xqRngv$ kZTNmYjYxYzBkZGI4YjczMTE4NGNmNTc0NDY0NzA4MzhlYjA4IiwidGFnIjoiIn0%3D

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, application/xml; q=0.9, applicat$ 

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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

#### Recommendation

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

#### References

### CWE-548: Exposure of Information Through Directory Listing

https://cwe.mitre.org/data/definitions/548.html

# Laravel debug mode enabled

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

### Request

PUT /index.php HTTP/1.1

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TO KEN = eyJpdi16In14U1BHRXZyUFN1RHhoem5HMmU3QXc9PSIsInZhbHVlIjoib05DTWtZMHN1SDk5Ykt0TUQ0a0F6am9yTGlucW5QSjYrT2taVnFjRi9wTXJwa1k5SXR1cE5BdHdlYTFEVjV40VdmeEJad1hlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUlWV28iLCJtYWMi0iIyM2I5ZTFiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNm MjQ1NjQzOGM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D;

RXR6TTZiOFdLdVJMend5Y0tJOUVaNC9iL3dvMlBOb3hRS1hRaDZuSlhvOS83NzMreGlmM054bGdHY2xXO2hCOTFFNEhXNWZkTXcwaGUiLCJtYWMi0iI3MTYxMDcxNWNlNzRhODJkOW05ZWRlZmM0MiF kZTNmYjYxYzBkZGI4YjczMTE4NGNmNTc0NDY0NzA4MzhlYjA4IiwidGFnIjoiIn0%3D

Content-Length: 0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate, br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36

Host: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

### Recommendation

#### References

#### **Error Handling**

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

# Clickjacking: X-Frame-Options header

Clickjacking (User Interface 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://shariftaxservice.ssbmultiservices.com/

Paths without secure XFO header:

- https://shariftaxservice.ssbmultiservices.com/
- https://shariftaxservice.ssbmultiservices.com/real-estate
- https://shariftaxservice.ssbmultiservices.com/upload/client-review/
- https://shariftaxservice.ssbmultiservices.com/about-us
- https://shariftaxservice.ssbmultiservices.com/blogs
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b
- https://shariftaxservice.ssbmultiservices.com/consultation
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://shariftaxservice.ssbmultiservices.com/contact-us
- https://shariftaxservice.ssbmultiservices.com/driving-school
- $\bullet \ \ https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea$
- https://shariftaxservice.ssbmultiservices.com/immigration
- https://shariftaxservice.ssbmultiservices.com/irs-publications
- https://shariftaxservice.ssbmultiservices.com/privacy-policy
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/real-state-home$
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/record-retention-guide$
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/tax-accounting$
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/tax-form$
- https://shariftaxservice.ssbmultiservices.com/tax-rates

- https://shariftaxservice.ssbmultiservices.com/terms-of-use
- https://shariftaxservice.ssbmultiservices.com/video-gallery

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

#### Recommendation

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

### References

#### The X-Frame-Options response header

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

#### Clickjacking

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

#### **OWASP Clickjacking**

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\_Defense\_Cheat\_Sheet.html

#### Frame Buster Buster

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

## Composer installed.json publicly accessible

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

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

### **Impact**

 $in stalled. js on\ discloses\ sensitive\ information.\ This\ information\ can\ be\ used\ to\ launch\ further\ attacks.$ 

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

### Request

GET /project/vendor/composer/installed.json HTTP/1.1

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TO KEN=eyJpdi16ImU5VDFaRyt0ekJzSHh3a0t6RTRoUWc9PSIsInZhbHVlIjoiM0dxK1NocGYxZTdudFl2dDuxMFJteVQ1dHl5S3JIM2VjNzFFeFpodWYvdEpTcDIrekQvRUo1QUR2K1NBWWxthXdQWFovUlVrcWVwdlFvQk9KN2ttN3gwZW9INVBQTXZiWGtvV2dSc2h4dFJYR2wleCtXV0ZzT0dzNk1vL2J5VVUiLCJtYWMi0iIxZmIwMzU0ZmUzMzRhYTUx0GRkNTM3ZWRmNjg1ZWNlYTY0ZmUz0DY0ZjM4NmM2OTk2Y2U5ZDFjZjRjM2Y0ZjQyIiwidGFnIjoiIn0%3D;

sharif\_tax\_service\_session=eyJpdi16ImsvL2c2YlVoRzNIYWdKUWJ3YmVVN3c9PSIsInZhbHVlIjoiMVFKSGJtRU9lb29uTTQrTHJXaWNMdjh1S0ZEdUZRTnhVZUtKQnVoQVZoUmU2UVo5VUpa anZ5TFNYeHQydWNHZXBXQ3RwUGtuVHM2cnVqYXR3YUgwQWpleFNHTzF5WVZUZENmenpSdTdZbTNLTWNvS2VtYlBTTTJL0HNxZjBwdXEiLCJtYWMi0iIxN2Y40TYyM2I0MGI2YmQ0YzMyNjhmZTZiNTg vM2I4MTkxMTk0YiM1NDRhNDhiZm01NzkxM2M3NDI0YW0vMDc1IiwidGFnIioiIn0%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

 $Host: \ sharift ax service.ssb multiservices.com$ 

Connection: Keep-alive

### Recommendation

Restrict access to vendors directory

#### Composer Basic usage

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

# Cookies with missing, inconsistent or contradictory properties

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

Verified

List of cookies with missing, inconsistent or contradictory properties:

• https://shariftaxservice.ssbmultiservices.com/

Cookie was set with:

Set-Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/

Cookie was set with:

Set-Cookie: PHPSESSID=4ea74df679607da4b5e81285b6a3e70a; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/\_ignition

Cookie was set with:

Set-Cookie: PHPSESSID=3973fdlea57fcf62f51d07a403871a46; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/about-us

Cookie was set with:

Set-Cookie: PHPSESSID=95fca0d2b59924fe6b47120a1e6d232e; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/contact-us

Cookie was set with:

Set-Cookie: PHPSESSID=aa9fd3d9775722331a63ca0d1de17640; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/blog

Cookie was set with:

Set-Cookie: PHPSESSID=2e73a2f3ad63bb0b4dd19a6d0c0cec30; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/blogs

Cookie was set with:

Set-Cookie: PHPSESSID=ae6b6f707e718c60b5973a549dcd8377; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/cgi-sys/

Cookie was set with:

Set-Cookie: PHPSESSID=43a1b9a19f139aa804073b553b36fb8a; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/consultation

Cookie was set with:

Set-Cookie: PHPSESSID=aefcf163e1f67a68e2ee0718f743cca0; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/driving-school

Cookie was set with:

Set-Cookie: PHPSESSID=50b2ab58cb83c3a259931c60547cdea5; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/tax-form

Cookie was set with:

Set-Cookie: PHPSESSID=65b82cf76le2alb63lcd6842b2d977cd; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/immigration

Cookie was set with:

Set-Cookie: PHPSESSID=9fb01901dd65c1lee21b2b6be6cf48c4; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/where-refund

Cookie was set with:

Set-Cookie: PHPSESSID=126a1a3e3ce2c74953fd00f09b5eb61f; 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".

 $\bullet \quad https://shariftaxservice.ssbmultiservices.com/index.php$ 

Cookie was set with:

Set-Cookie: PHPSESSID=1c6a5763c08730b2573b1d5dc42efdc9; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/irs-publications

Cookie was set with:

Set-Cookie: PHPSESSID=83343f23bc27650851fa914295f10832; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/mailman/

Cookie was set with:

Set-Cookie: PHPSESSID=113f15bfe334452b1fe6d096ae7dc6ca; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/privacy-policy

Cookie was set with:

Set-Cookie: PHPSESSID=f97b6530f5b8d19cd308359b5a948aed; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/real-estate

Cookie was set with:

Set-Cookie: PHPSESSID=ade08cfe06280dla854ab8ade9ebaa4c; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/real-state-home

Cookie was set with:

Set-Cookie: PHPSESSID=8b2bc25ae273bbf0bd3ab43lle1b408d; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore

recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

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

Cookie was set with:

Set-Cookie: PHPSESSID=1a51401bf2f96cab7082a3a790eb613d; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

• https://shariftaxservice.ssbmultiservices.com/tax-rates

Cookie was set with:

Set-Cookie: PHPSESSID=31acd1595e94ac0c912e35ba40458a90; 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://shariftaxservice.ssbmultiservices.com/

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, application/xml; q=0.9, application/xml; q=0.9, application/xml; q=0.9, application/xml; q=0.9, application/xml; q=0.8, application/xml; q=0.9, application/xml; q=0$ 

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: shariftaxservice.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://shariftaxservice.ssbmultiservices.com/

Verified

Cookies without HttpOnly flag set:

https://shariftaxservice.ssbmultiservices.com/

Set-Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; path=/

https://shariftaxservice.ssbmultiservices.com/

Set-Cookie: XSRF-

TOKEN=eyJpdi16Inl4U1BHRXZyUFN1RHhoem5HMmU3QXc9PSIsInZhbHVlIjoib05DTWtZMHN1SDk5Ykt0TUQ0a0F6am9yTGlucW5QSjYrT2taVnFjRi9wTXJwa1k5 SXR1cE5BdHdlYTFEVjV40VdmeEJad1hlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUlWV28iLCJtYWMi0iIyM2I5ZT FiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNmMjQ1NjQz0GM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:21:31 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/real-estate

Set-Cookie: XSRF-

TOKEN=eyJpdi16IktmWU1Bd3FQUzd3SHh1RG8xQ3FMQ0E9PSIsInZhbHVlIjoidTUzbUZJWGdveHRzM1pKVE03SThHUG10Ym80MVRRWlM3bXZNd1JoTWU4Nml0UGJ1 cFVzYyt5MWgyM0pvQVJHQzM2QWNUYkUvbUVGTGNRTm0rUGNlZjQvbE5rcnhWTS9iTmE1RWhwYi9mTEE4N1VQK05NMWZha3Q5cTNEL29JRjgiLCJtYWMi0iJlNTNkZW EyMjZmZGQ0ZTRm0WUxNzBiNzRmZGRhMjc10WYwZGRjYTQwZmFhNjVmNGJmMTczNzIzMWM30WU4MWQ2IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:28 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/about-us

Set-Cookie: XSRF-

TOKEN=eyJpdi16InRreDUvd3FYR0o2Qmhhd29NWHVGNkE9PSIsInZhbHVlIjoiT1pJUEJhM1RoUFRjdkF1bktSbko5VytrUFo40HA5U1F5Z25mMDRzSFF4cVUwUHpU WjhTbFdwVWlmWmtZajlZNWZ0bGh2eWRXN01wYXJHeWNuM2JLY3A3NktBdW9tUktzYm9RMnA00HVmWWN0L0ptaHYrT3lsa2E3Q3hYcGRBSVkiLCJtYWMi0iJhYzU4MT k50GM4ZDE40TZmYzUxYWM4MjVkMTg1MDI3NjI3M2JlZmNlYWQwM2Vj0DZjNDJiMzI10Tc10DZmMzExIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:43 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/blogs

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjZBOUp6VlFlL3V2RWRtMDlKTUl2Rmc9PSIsInZhbHVlIjoiQjZoYVlRTmR3TTdxSEJCRlowVjM3aTdrOStNcm15am85aGhG0FZOaFNQbi9HbmJ3
TmF5bFV3eHBGeEFMbXlUdkJERTFKNjZNUWUvUjFZa2VjR3MydDFoK0JWZUlSSGRjVTFldit00DR0MHRWZzVJa1JVVTlTSE5jem9USEVlVzYiLCJtYWMi0iISYTE0Mj
U0NzBjMmZlNzNmMDg40GM1NDg50GEyMjgyNDk4Mzc5MjM2NTlkMDg3ZTJlZDc20WQx0TRmYTNiNWIyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:23:46 GMT; Max-Age=7200; path=/; samesite=lax

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

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjRkR2VFTUFNdmFxQnBtcVI5bjIwT1E9PSIsInZhbHVlIjoiUC9IRFpT0HdnenlXM2RXQnlyU002UGxiZGE3YUZ1WUdnVXpyRzc5ZVgvSTR0TTBy MllyY25CeHpaTTZIMFlqWDVITkx0WWFsb09QUmRsempGdyttdU1Ya2tMQmpDTGpGM3d0and2ZHRkYXAvQW5sdmZGbU4vNm5jNEZGSWpBcjEiLCJtYWMi0iI5M2Qx0T U3NTFhMzg1Mjk5NTExOWQxZGQ10GMwYTVlMzBiZGU4NDRhZWViMTUx0DJj0TE2ZWNmNjkyMTc5YjY0IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:55 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/consultation

Set-Cookie: XSRF-

TOKEN=eyJpdi16IktBTG5oRXVTUmVJSUJVUUtsZEJleWc9PSIsInZhbHVlIjoiQW5zbGVXekRFVWZhenczUTBBWTZkMlYvZU5I0HIxVEVa0TJqNmZWWHBnWjRjSnhPdUpTNSt5SzQxU2htRDRFMUUvenhJUnNiMVhWc0EyZXBGQVJqM3lSazJyYnVhdTh0bTdNVjV4elpBUUY3TEZhT215ZUFEUThodVBHUVQ5dWwilCJtYWMi0iI3N2QyND

g1MmNkZjJiYThlZDlmNTI5YWE2NWJmZTIyZDg5NjI3MTE1ZWY0NDE0ZmE4NGJhZGM0ZGZlZGI0ZDYzIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:56 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/contact-us

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImlKUm04MlZhRmhEUFhwYWJ0dDI1YWc9PSIsInZhbHVlIjoibGhoV200Z3IzclM3L2Z5TTBGR0VLRlcvbk1LMzI2Z3o1cWtlUmFuQlhMcm8xYmdQ V1ZwWXBxRm93eUxWTHU3RE02WGRpVERiamxiS2pWNlo5QjBWV3d5RWZQMTg5ZEVxOS9DZWs2c2ppd25iY25nT3NXVG5ZVDdXVXNFUzQ3QnoiLCJtYWMi0iI4Nzc1MjlNWUxODhmMGU0YWIzODQxMDk0ZDg4MDkxZTNjYmFlNGU0NWE2OGVlMzJlZDg2MmM0NDg3YWI5ZTNiIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/driving-school

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImZrRGlabGVoOHl3WDdyS0ZLZUV3QVE9PSIsInZhbHVlIjoi0EIySDE4dzVSVWs3bTB4TXFxU3BHaXlhd01vTnJyaTlNWGF4bzgrdHJCa3YzVFZJ ZUhFdEI5Mm1HS1BZYUpaMjZMQjd5WjdzcWloS2t4YXVhQk1DNXBCdlk3MXBwcVE2ckZTQTBjSGl0cU55Mlh2SHlZNmFrSXNxWWtY0VdMUFgiLCJtYWMi0iI2ZmFmN2 RkZWU2M2ZkMTg1YjhmZWU4MmY2NmY1Njk4N2E20DQ10Tky0WY1ZmVlMzlhMjA5NmQ4NzUwNDBkYTc4IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; samesite=lax

 $\bullet \quad https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea$ 

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImtEUXdoQ2NSaHlDTW4rd05mTlU5UUE9PSIsInZhbHVlIjoicFFNRWhEQlg5TXAvOTkxazZ0RDN1bFpIcVFu0VhBL0dzQUh0TGhsZ3dlemw3dVpt eW1PZlpVQk9jdTVpYWVI0Glj0VpFaG52V3R0WkorYmZuSkxUTElZblZ4Umkva24wWTV3UFdnWWd3VTVlbTM5di8vQi80aUlocFVrc2ZJa04iLCJtYWMi0iI1M2FmMT Q5Mjg3YWM1Nzg5NWM0YWQ2YTkwZjU5NGM4OTU5M2JkNzY2ZWQ1MTczNTI3ZGM0MDUxYzUwY2I2MDZjIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:18 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/immigration

Set-Cookie: XSRF-

TOKEN=eyJpdi161lBFcUhYeVo5YmRPZTNBZFhGNnkwV3c9PSIsInZhbHVlIjoiRUtRUys5L2FUbUxJazVwU3VHS0c2bWNxM3hIcGlXTWNMZHp5bTFHSm5Jc2Z0b29z Sk43Z3c30FNHbHpLT1V3d3lKRm51eXpIWWdnYXBrZ0JldGVkbEJEM2l1Zk8xU3JteFB2VzFubnVGaEEzYytZdUx6dkZBbkIxbElEaHEwaTUiLCJtYWMi0iIxNGE5N2 VmZTEzZWMwNGZkNzRlMWJmZjU2MWQ1MDk2MzFjZWYyNTRiZTZhZTBiYjFhNWNhMjRiZjM1MmRjNzkzIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:20 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/irs-publications

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjRUQ1ArMVMzZWxIVE1STVVTcUtvdWc9PSIsInZhbHVlIjoiQ3BJNGpKRmdLUjQ5Ti9hb1pZMDR6Y2FqclVucHl6YlZ5RmUwR3gyRHJSTVVGVXcz
TW5ITmpDRUdkdS9xbk1lLytjR0sr0UZWZHFqUkJ5WjNTb09URUV0YzB2YVJqZ2tiSGU2b2lVTmR0M2tpSzNhaGg5Sysy0TMxd3ZVSEZPckIiLCJtYWMi0iI0MTIyYT
BiNDlhYWZjZGM00DgxNWFiZTk2NGM0Yzc0NjYwZTEwNzE3NTA0MzFkZjdkMmJkNWIzOThkNTRiZDliIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:24:21 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/privacy-policy

Set-Cookie: XSRF-

TOKEN=eyJpdi16IkpXMGVRNUJUSmhaYXdhUWJPak0rVVE9PSIsInZhbHVlIjoiNXZIREIxdnc3K2JocmJvdTRnQ1ZPaHl2ZnhrM01jN0FjMzg0ai9BTnh0dTd0Ulds VDdRdWw4YnJNajZMLzllQlRRcEkvdFRsbWdwVS9CZTJXazhuYjF4MHlUNVFTUk9zUEt3QXFGMHFSM3lmRm0zMWd5ZkJLMFFPd1JlRnh1bU8iLCJtYWMi0iI3YjJjND Nm0ThhNzE2NDI30Dk5ZDU3YTlhYmRkZTYw0Dc3YTdmYzg2NTM4MmJiNzZiN2JmMzA4ZjE0MjUyZmZlIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:21 GMT; Max-Age=7200; path=/; samesite=lax

 $\bullet \quad https://shariftaxservice.ssbmultiservices.com/real-state-home$ 

Set-Cookie: XSRF-

TOKEN=eyJpdi16InBDYWlPR01tR0FMNUJ6eW94TEhMVUE9PSIsInZhbHVlIjoiNDRSdlczK0N3TkJLSmREcWZRcTRuMjVkYWY1aXlmdkoyV1JYUm5CaU14cm9teWhveVRyWUR6K3R0RlJieWIvTnZmeDFsSjJUaURzeTUyVERNN0JoeVBTalhJRlcvNDczMVVBRFozcTVLeHdSYVNzNDF0NlFIdGoyK2FJR1ZISnoiLCJtYWMi0iI30TZhNT

hlNTJhNmFlyzA0ZTU2MjMzNDg30TU2YmM4NjM3ZWI0MjUyYWViNjVhZGRmNTY5NWYzZDJlMjM5ZGRhIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:21 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/record-retention-guide

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImNqS1F3VVVNNU9TVHlOMklvSWpyWWc9PSIsInZhbHVlIjoiTnhSQzFnOVZ4VVZsaXZ3c09IQ1JYa0pTQ01MN0NLWVR6dFYrY295cTB0bE41M240 Q0tmN0lnWE5lWjR2M3FDZUdERVFheStqbnlZNnVsRWJiMExZek5iTlBnYnZrWncrMFpVSHlkMW5XazZ0ZVBlRm5mMWFFZ2QyMzZrMmthWlUiLCJtYWMi0iI2OTVjMm UzNTY0YWNlMmY3ZjMyMWM4NmEyN2JjMjRlNTk5M2UyNzAxN2MyNWRiYzVlMDgwYTUxNzk3ZTUyYjRiIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:21 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/tax-accounting

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjJpZVN3eXBGM25VWU9MYWhnd2YxUXc9PSIsInZhbHVlIjoi0HJjM0J1U1F0My8yeTBTY2VsYW5iR3JXVUsvVm5Xa2ZxVER0b0w2c3F0WndPSnJC NW56S0VWL0owQ1U4dTJEZmdta3o4RW1CN1ZBd09TTFRFTHlJNHJ6RUlCNDRNMnN5anhhUGNZTHRTNWJzT0M4eGorV3N2TjdmeWVld21tdXUiLCJtYWMi0iI2Y2JjMjYwZTgzNjViNDhhMTA3Mjk4NTgwYzFmZWNj0DY40WQwNjZlMzdjY2RiZmQzZDdlZjNiZjE1YzhhOTcyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:21 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/contact-us

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImZQUGV0Y2tkNGVwem03UTRsZmZwRXc9PSIsInZhbHVlIjoiMWJnaTIyL0ZnRjR4YzBrbi9rMVNtUEwwaWltTDR5MEtHRUlNczZMVlQvVUJaeDky
0W14Y3lMY1prT3JtQ1FJV005eXF1ZmYwdGJKZUF4VTQ5b3QyTFFUNnN1emFTaEdyRGRjU3ppL3ZTRDVFdHdXSzZFMnRobSs5VDJrdE9KN3UiLCJtYWMi0iIwY2ZiMj
QxNTc1Nzll0DkzMDAxY2RjYTdm0TU00WNkNDBlMzVjM2Y2MDc4MjRkMTBlZTkxYjEyMGM0Mjk4MmQyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:24:27 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/tax-form

Set-Cookie: XSRF-

TOKEN=eyJpdi16Ii9iR04xUkdwRllPa0o3T3RLTG1LQnc9PSIsInZhbHVlIjoiakFSSWVmY0wyalJZV2J4cWFhQXZ6SEk0Z3h1UjhjbWZN0DhIMGkrdWdwV3RPNTU4
YzZhVnZHVFJidkVpVnlKRmZpN1JvVmcyVEZmdWphNmhTVzhXcHExUy9aV25MWEQ3RzlLd2FkU000ck9wYTlLQnFRbDNCdExWbElTTXB1Q2oiLCJtYWMi0iIzMTQ2Zj
NmNThkMTg0YTBkMzMyZTg4MmEzMjdmZTgxMDJjM2FlNzJkMWRl0Tk5Nzg5Y2RjYTQ2YjFmMTY50TcxIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:24:27 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/tax-rates

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjhQUklINXl2MHNLZFozb1NSV29NZFE9PSIsInZhbHVlIjoiVkhXeEFlY3VmeGNMdGl0eEdjc0JiTEFyYjM2OURxQT03MmFZcHRTV3AyalgzR3U2 SEdmWEFnZTlyL0hCVklsSjgrbXJVRjhHN25HNW94YStib2MxZ2IwbXNLTWlsUU9FVWxTZ09sTlhlVy92YzVVdkJha0F4d3BzMHNCODVBYmoiLCJtYWMi0iIIZTk4Mm M4Y2YzOWQyM2RhYTE5MjI0NjgyMTlhY2Iw0TVkN2Q0Yzg4MWNhODVkMDZiYmJhMjc5MzQxMTA0ZTcyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:27 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/terms-of-use

Set-Cookie: XSRF-

TOKEN=eyJpdi161k5jblFQZkJOTWc1dkQvUWZ3NFczN1E9PSIsInZhbHVlIjoiN2xBS2dkbkxtZjNtZ21zWG4zMFRueGR3UDRHclBUYTJ2SThsWjVIa3BlTXNiZ1BK
T0lqTkZvOTJvY3JIWDlUNDNQbnNUcElSZjJCaVpKZVp3d1gxYjZCNkYrUmJ3TDZaN1ZSekNwSXFhQVdxVmJyNElEeEhkVmlmTkl3UGMrRXAiLCJtYWMi0iJlZjE2Yj
gyMDRhMDc4Mzk1YTA4OGQxOGNhNmY3ZjA1NmYxYWM0YTMyNzI10Dk2ZGVhMmEwMTFjZjk2MWFlN2ZjIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:24:27 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/video-gallery

Set-Cookie: XSRF-

 E5MDg4MmRiMTdlZjAyZmQzM2IzNzYlZDVlMTNiODlhYjJhNjc5ZjkyZTUyMjhiM2JkYTNkNDYzM2ZiIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:28 GMT; Max-Age=7200; path=/; samesite=lax

#### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.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://shariftaxservice.ssbmultiservices.com/

Verified

Cookies without Secure flag set:

• https://shariftaxservice.ssbmultiservices.com/

Set-Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; path=/

• https://shariftaxservice.ssbmultiservices.com/

Set-Cookie: XSRF-

TOKEN=eyJpdi16Inl4U1BHRXZyUFN1RHhoem5HMmU3QXc9PSIsInZhbHVlIjoib05DTWtZMHN1SDk5Ykt0TUQ0a0F6am9yTGlUcW5QSjYrT2taVnFjRi9wTXJwa1k5 SXR1cE5BdHdlYTFEVjV40VdmeEJadlhlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUUWV28iLCJtYWMi0iIyM2I5ZT FiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNmMjQ1NjQz0GM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:21:31 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/

### Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16Im5j0GtaTVM1Z0xibVpyZjUyY2kwU1E9PSIsInZhbHVlIjoiZjd6dlJ5TzdlK2FvNDZpeCszV2c5enVJ0VBlNG02bUt ham5pbjhxYmFUbVJUM0xqRngvRXR6TTZi0FdLdVJMend5Y0tJQUVaNC9iL3dyMlBQb3hRS1hRaDZuSlhy0S83NzMreGlmM054bGdHY2xXQ2hC0TFFNEhXNWZkTXcwaGUiLCJtYWM10iI3MTYxMDcxNWNlNzRh0DJk0WQ5ZWRlZmM0MjFkZTNmYjYxYzBkZGI4YjczMTE4NGNmNTc0NDY0NzA4MzhlYjA4IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:21:31 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/real-estate

Set-Cookie: XSRF-

TOKEN=eyJpdi161ktmWU1Bd3FQUzd3SHh1RG8xQ3FMQ0E9PSIsInZhbHVlIjoidTUzbUZJWGdveHRzM1pKVE03SThHUG10Ym80MVRRWlM3bXZNd1JoTWU4Nml0UGJ1 cFVzYyt5MWgyM0pvQVJHQzM2QWNUYkUvbUVGTGNRTm0rUGNlZjQvbE5rcnhWTS9iTmE1RWhwYi9mTEE4N1VQK05NMWZha3Q5cTNEL29JRjgiLCJtYWMi0iJlNTNkZW EyMjZmZGQ0ZTRm0WUxNzBiNzRmZGRhMjc10WYwZGRjYTQwZmFhNjVmNGJmMTczNzIzMWM30WU4MWQ2IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:28 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/real-estate

#### Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16Imhu0XlaZXNjRGhTWFZ6aXRoM0VHc1E9PSIsInZhbHVlIjoiVHpRTXRFTDhZWnBYa0g3Qy9SaHJQSjM5VjYvdnAxdnp Qc1NsQW55bnZVdW5nbU5VS3ZaeWJxQlF1UmVuQlIxYUFLVEx2cjVRTEdsVXlCTmZJazF4TjNtVzRJa3NvdkczR3RHR2FWZFR3MlJoRTh2N2RMVjFxaTRFeHpiWTV60 EEiLCJtYWMi0iJhMzJkZDQ5NzI1Nzg00TkyMWJkMWVlZDM3YTNhMDUxNzEyMTc4Yjk5MjBkNWNiZWNh0DZlNjBiYTY3ZTAx0TU4IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:28 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/about-us

Set-Cookie: XSRF-

TOKEN=eyJpdi16InRreDUvd3FYR0o2Qmhhd29NWHVGNkE9PSIsInZhbHVlIjoiT1pJUEJhMlRoUFRjdkF1bktSbko5VytrUFo40HA5U1F5Z25mMDRzSFF4cVUwUHpU WjhTbFdwVWlmWmtZajlZNWZ0bGh2eWRXN01wYXJHeWNuM2JLY3A3NktBdW9tUktzYm9RMnA00HVmWWN0L0ptaHYrT3lsa2E3Q3hYcGRBSVkiLCJtYWMi0iJhYzU4MT k50GM4ZDE40TZmYzUxYWM4MjVkMTg1MDI3NjI3M2JlZmNlYWQwM2Vj0DZjNDJiMzI10Tc10DZmMzExIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:43 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/about-us

#### Set-Cookie:

sharif\_tax\_service\_session=eyJpdi161lJxMzVjU0ZKMjIvbGtjT045UEJLd3c9PSIsInZhbHVlIjoiY0VCRkRiMHJsWVdJMnExeTlsWm10d2140DF0YnlKNmE 0ZWNKR00xQUI3WjEyQ01wN09HWXEyM25DWjc2ZHplbkd5MlNvQzVkK3BaZXJ0NHF6SC9Ca3lzV2JmbllZTVhP0ExoYXZ3WFhjQnBHNHRCWUsyTjVKU1EzdGluWHFlV EsiLCJtYWMi0iJlYTNmZGRhYTY0ZGMwNzhmZjg1YmMw0GNhZDJmZjcyM2RlMGU50DRkZDQyMzA5YzM10TYyYTcyYzgwMDU1ZmJlIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:43 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/blogs

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjZBOUp6VlFlL3V2RWRtMDlKTUl2Rmc9PSIsInZhbHVlIjoiQjZoYVlRTmR3TTdxSEJCRlowVjM3aTdrOStNcm15am85aGhG0FZOaFNQbi9HbmJ3
TmF5bFV3eHBGeEFMbXlUdkJERTFKNjZNUWUvUjFZa2VjR3MydDFoK0JWZUlSSGRjVTFldit00DR0MHRWZzVJa1JVVTlTSE5jem9USEVlVzYiLCJtYWMi0iI5YTE0Mj
U0NzBjMmZlNzNmMDg40GM1NDg50GEyMjgyNDk4Mzc5MjM2NTlkMDg3ZTJlZDc20WQx0TRmYTNiNWIyIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024
09:23:46 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/blogs

### Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16InZ2NGpQVlVld3BKMGpnU3plQUhwSmc9PSIsInZhbHVlIjoiUEJkY0pxaGNLWmMxUlIralRIUlhGak12eVN4OUtFQjV sVHhSUFhjNGNLY0JDQjY5aDVlRnBkbjl2aEJlb2w4d0lPTDNjWC9Q0GlqRC9qQkhQ0E0yUENZU0NQdkU0TC9LdEZKcWM1Skt3WDR4WWJacnJFT0xpOWNTYnZ5eDB6R XoiLCJtYWMi0iI4ZTU0MjBl0GUwY2VmZWVjNGE4ZDIxNzdkZTVlNWEzYzIxNzgyOTM2ZGE2OTIxODY5ZDE2OGIyZWEzMDhmYzFlIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:46 GMT; Max-Age=7200; path=/; httponly; samesite=lax

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

Set-Cookie: XSRF-

TOKEN=eyJpdi16IjRkR2VFTUFNdmFxQnBtcVI5bjIwT1E9PSIsInZhbHVlIjoiUC9IRFpT0HdnenlXM2RXQnlyU002UGxiZGE3YUZ1WUdnVXpyRzc5ZVgvSTR0TTBy MllyY25CeHpaTTZIMFlqWDVITkx0WWFsb09QUmRsempGdyttdU1Ya2tMQmpDTGpGM3d0and2ZHRkYXAvQW5sdmZGbU4vNm5jNEZGSWpBcjEiLCJtYWMi0iI5M2Qx0T U3NTFhMzg1Mjk5NTEx0WQxZGQ10GMwYTVlMzBiZGU4NDRhZWViMTUx0DJj0TE2ZWNmNjkyMTc5YjY0IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:55 GMT; Max-Age=7200; path=/; samesite=lax

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

### Set-Cookie:

sharif\_tax\_service\_session=eyJpdi161lVqblAxbHBQa2RrVTd0VkprRjdlWHc9PSIsInZhbHVlIjoiWHZMbUt0aU80amE3dTRnVFBJRzFScms1SXdlQWdDOGd hdXdDTnk4bWhveGRDd0U1anJEYlByY1BXUUVvUHpJVmRzcHFIREJobXVUVVo0Vm1LSEdMK3VrUWFhM2J4cXZX0EJuREZmQ0d5RE1kMnBuTzlkdk5yc2NETmJI0DZ1d FkilCJtYWMi0iJmMDQzYTI1NzhmM2YxNjdmZjNi0DY10GRhNmFiNDEwZjE5YTM4MjE1MDFhYjc0ZGRiMDgyZDE5ZTFkZDYxNGZmIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:55 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/consultation

Set-Cookie: XSRF-

TOKEN=eyJpdi16IktBTG5oRXVTUmVJSUJVUUtsZEJleWc9PSIsInZhbHVlIjoiQW5zbGVXekRFVWZhenczUTBBWTZkMlYvZU5I0HIxVEVa0TJqNmZWWHBnWjRjSnhPdUpTNSt5SzQxU2htRDRFMUUvenhJUnNiMVhWc0EyZXBGQVJqM3lSazJyYnVhdTh0bTdNVjV4elpBUUY3TEZhT215ZUFEUThodVBHUVQ5dWwiLCJtYWMi0iI3N2QyNDg1MmNkZjJiYThlZDlmNTI5YWE2NWJmZTIyZDg5NjI3MTE1ZWY0NDE0ZmE4NGJhZGM0ZGZlZGI0ZDYzIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:56 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/consultation

Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16ImhSM0pzMVZnNlNscmxxMDdnNUtjbWc9PSIsInZhbHVlIjoidjFjSFJEdjVZTlRNRU8rcGhxWUI3bEV6czRWa0VIZGR Wc0FWenFVK21LbXpwYm9zTHJETFFjQXZBcEpy0VBjYy9oekNvMmx3RTAyWVFMSlUzR3Y5c3RMVm10bDhxdHlPZXhvZnBnWjMzdnZHcXRraFVCVVpKYnNpVFE4QkZKV DciLCJtYWMi0iI3NmQ0NTc30WY1ZTI00DU1MmQ3MTJmZmY2YTVmZjgxMjY5YWVkZWFmMzE1YWExMTJjYjg4MWU1NGM0ZGY4NGQ5IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:23:56 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/contact-us

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImlKUm04MlZhRmhEUFhwYWJ0dDI1YWc9PSIsInZhbHVlIjoibGhoV200Z3IzclM3L2Z5TTBGR0VLRlcvbk1LMzI2Z3o1cWtlUmFuQlhMcm8xYmdQ V1ZwWXBxRm93eUxWTHU3RE02WGRpVERiamxiS2pWNlo5QjBWV3d5RWZQMTg5ZEVx0S9DZWs2c2ppd25iY25nT3NXVG5ZVDdXVXNFUzQ3QnoiLCJtYWMi0iI4Nzc1MjlNWUx0DhmMGU0YWIzODQxMDk0ZDg4MDkxZTNjYmFlNGU0NWE20GVlMzJlZDg2MmM0NDg3YWI5ZTNiIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/contact-us

Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16IitiZUJodDZQenhxVkx0L0dOWkJt0Xc9PSIsInZhbHVlIjoiMGtCN0JlSkxPV0VQQ3BTU2x2UGxVMmMxR0FNQW1lZ0F zMTVxK21MRXF2Z2o00HZ3Ui9pUVZnUTB2ZVlHVDE3ZGgwMDBFTW5rdGJ5cDFtakQwWklqSklSckVVejVaejVhNWJZTFV1UVRYVytpUVFINnhvNFp1ZmFnMWpuT084Z TMiLCJtYWMi0iJi0WM0ZDBhYzZiMGMzYzE2NGEyNDY5Nzk5NjUwZGFmMDFhMGEwZjRiZTFlMmY30DMyNzBjYTE00WE2YjU4YWQxIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/driving-school

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImZrRGlabGVoOHl3WDdyS0ZLZUV3QVE9PSIsInZhbHVlIjoi0EIySDE4dzVSVWs3bTB4TXFxU3BHaXlhd01vTnJyaTlNWGF4bzgrdHJCa3YzVFZJ ZUhFdEI5Mm1HS1BZYUpaMjZMQjd5WjdzcW1oS2t4YXVhQk1DNXBCdlk3MXBwcVE2ckZTQTBjSGl0cU55Mlh2SHlZNmFrSXNxWWtY0VdMUFgiLCJtYWMi0i12ZmFmN2 RkZWU2M2ZkMTg1YjhmZWU4MmY2NmY1Njk4N2E20DQ10Tky0WY1ZmVlMzlhMjA5NmQ4NzUwNDBkYTc4IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; samesite=lax

 $\bullet \quad https://shariftaxservice.ssbmultiservices.com/driving-school$ 

Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16IndramZoaGpOTnFuYzUyWkFLVS85RVE9PSIsInZhbHVlIjoiWGdYWDVEQldaTVZ4dUoyRGNIejNleVNkcUlLOWpzWm0 0am8vQ3ArdEhlZDV6eE5zdzFSNjFBNHg3bkdxcnBsR0EwUkNwSUdOenl3aEszcEpWRnZENER4TVRaL253dyt6c3NZVmJCaUlRSzNsYlNaaEZORXNxM2F0WGF6dmRL0 WcilCJtYWMi0iJlZWRkNjNmYjMxZTdmZmE2ZGIzYmIyYzZjYTA1NDFmZTYxMDU2Njc4ZmU5ZGEzODNh0GU4YTBiZjQxZWJlY2NmIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:09 GMT; Max-Age=7200; path=/; httponly; samesite=lax

 $\bullet \ \ https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea$ 

Set-Cookie: XSRF-

TOKEN=eyJpdi16ImtEUXdoQ2NSaHlDTW4rd05mTlU5UUE9PSIsInZhbHVlIjoicFFNRWhEQlg5TXAvOTkxazZ0RDN1bFpIcVFu0VhBL0dzQUh0TGhsZ3dlemw3dVpt eW1PZlpVQk9jdTVpYWVI0Glj0VpFaG52V3R0WkorYmZuSkxUTElZblZ4Umkva24wWTV3UFdnWWd3VTVlbTM5di8vQi80aUlocFVrc2ZJa04iLCJtYWMi0iI1M2FmMT Q5Mjg3YWM1Nzg5NWM0YWQ2YTkwZjU5NGM4OTU5M2JkNzY2ZWQ1MTczNTI3ZGM0MDUxYzUwY2I2MDZjIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:18 GMT; Max-Age=7200; path=/; samesite=lax

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

Set-Cookie:

sharif\_tax\_service\_session=eyJpdi16IlhoWGFMUGpvTmNEcTQ0a0lsVkE3MlE9PSIsInZhbHVlIjoidHMrcml1aEpabTZleVV0Vkg4NXBFQjIxcjlCei9ScFR lSmRQazM3QnhLdU4xYnZWN1V2ZVFzYU5mSy96L0p4UU0vblNWVFJxS1Q2OUhtd0crQ2ZjNk04SjFUbzNEOXVKbVVUNEFiTmY2dEdNN0Uvc3d3M2JIaVVYUGh0QjFhU FgiLCJtYWMi0iJhZjNiMmU4ZmMyYzViZmQ0MjY2ZDYwZTM5Y2I3Nzc4MWQxZTI1YzU40TU5NjFlYTQyZDdmYmJkYTk40GZjZTU5IiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:18 GMT; Max-Aqe=7200; path=/; httponly; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/immigration

Set-Cookie: XSRF-

TOKEN=eyJpdi161lBFcUhYeVo5YmRPZTNBZFhGNnkwV3c9PSIsInZhbHVlIjoiRUtRUys5L2FUbUxJazVwU3VHS0c2bWNxM3hIcGlXTWNMZHp5bTFHSm5Jc2Z0b29z Sk43Z3c30FNHbHpLT1V3d3lKRm51eXpIWWdnYXBrZ0JldGVkbEJEM2l1Zk8xU3JteFB2VzFubnVGaEEzYytZdUx6dkZBbkIxbElEaHEwaTUiLCJtYWMi0iIxNGE5N2 VmZTEzZWMwNGZkNzRlMWJmZjU2MWQ1MDk2MzFjZWYyNTRiZTZhZTBiYjFhNWNhMjRiZjM1MmRjNzkzIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:20 GMT; Max-Age=7200; path=/; samesite=lax

• https://shariftaxservice.ssbmultiservices.com/immigration

Set-Cookie:

sharif\_tax\_service\_session=eyJpdi161k5tbWpXR2Zs0DNxaUwyR3d4Um4ra1E9PSIsInZhbHVlIjoicWhsZlB0WnpGSFBVaGdxbVFzbStwU2RMc2Y1SmFoZ2t qQUs3Zk9TZFpCT0g0TW9nNkQzTW1MVldIK0ZRdXg4a0t1TEJ2cmFpVlFSYW5vWVp0R3VVbldsY1NXcjZ3SWVv0GhEbHl4eFRISEk4VVRlbE9qN1IzbDRpVVhPRTNDY zQilCJtYWMi0iJjYWM0ZjY4YTkxN2U3YWMxMjU0ZGRjNGQ0MWE3MTcxMjUxNDI30GVhNjAlZTE4MGM0NDY0MDJjN2UzNzFkNTJiIiwidGFnIjoiIn0%3D; expires=Tue, 09-Jan-2024 09:24:20 GMT; Max-Age=7200; path=/; httponly; samesite=lax

#### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.ssbmultiservices.com/

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, */*; q=0$ 

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

 ${\tt Host: sharift axservice.ssb multiservices.com}$ 

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://shariftaxservice.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://shariftaxservice.ssbmultiservices.com/
- https://shariftaxservice.ssbmultiservices.com/real-estate
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/upload/client-review/$
- https://shariftaxservice.ssbmultiservices.com/about-us
- https://shariftaxservice.ssbmultiservices.com/blogs
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b
- https://shariftaxservice.ssbmultiservices.com/consultation
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/contact-us$

- https://shariftaxservice.ssbmultiservices.com/driving-school
- https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea
- https://shariftaxservice.ssbmultiservices.com/immigration
- https://shariftaxservice.ssbmultiservices.com/irs-publications
- https://shariftaxservice.ssbmultiservices.com/privacy-policy
- https://shariftaxservice.ssbmultiservices.com/real-state-home
- https://shariftaxservice.ssbmultiservices.com/record-retention-guide
- https://shariftaxservice.ssbmultiservices.com/tax-accounting
- https://shariftaxservice.ssbmultiservices.com/tax-form
- https://shariftaxservice.ssbmultiservices.com/tax-rates
- https://shariftaxservice.ssbmultiservices.com/terms-of-use
- https://shariftaxservice.ssbmultiservices.com/video-gallery

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.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://shariftaxservice.ssbmultiservices.com/

Verified

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

### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

### $\underline{https://shariftaxservice.ssbmultiservices.com/contact-us}$

Verifie

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

GET /contact-us HTTP/1.1

Referer: https://shariftaxservice.ssbmultiservices.com/ Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TOKEN=eyJpdi161jZB0Up6VlFlL3V2RWRtMDlKTUl2Rmc9PSIsInZhbHVlIjoi0jZoYVlRTmR3TTdxSEJCRlowVjM3aTdrOStNcm15am85aGhG0FZ0aFNQbi9HbmJ3TmF5bFV3eHBGeEFMbXlUdkJER
TFKNjZNUWUvUjFZa2VjR3MydDFoK0JWZUlSSGRjVTF1dit00DR0MHRWZzVJa1JVVTlTSE5jem9USEVlVzYiLCJtYWMi0iISYTE0MjU0NzBjMmZlNzNmMDg40GM1NDg50GEyMjgyNDk4Mzc5MjM2NTlk
MDa3ZTJ1ZDc20W0x0TRmYTNiNWTvIiwidGFnIioiIn0%3D:

 $sharif\_tax\_service\_session=eyJpdi16InZ2NGpQVlVld3BKMGpnU3plQUhwSmc9PSIsInZhbHVlIjoiUEJkY0pxaGNLWmMxUlIralRIUlhGak12eVN40UtFQjVsVHhSUFhjNGNLY0JDQjY5aDVl RnBkbjl2aEJlb2w4d0lPTDNjWC9Q0GlqRC9qQkhQ0E0yUENZU0NQdkU0TC9LdEZKcWM1Skt3WDR4WWJacnJFT0xpOWNTYnZ5eDB6RXoiLCJtYWMi0iI4ZTU0MjBl0GUwY2VmZWVjNGE4ZDIxNzdkZTV lNWEzYzIxNzgy0TM2ZGE2OTIx0DY5ZDE2OGIyZWEzMDhmYzFlliwidGFnIjoiIn0%3D$ 

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

The following issues were detected:

• The tag img references the resource http://shariftaxservice.com/upload/gallery-image/img\_1621849573\_60ab75e52c98b.jpg

### Request

 ${\tt GET\ /blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea\ HTTP/1.1}$ 

Referer: https://shariftaxservice.ssbmultiservices.com/blogs

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TO KEN=eyJpdi16IllalJTY2QwdmvJVU43UERZSjBseGc9PSIsInZhbHVlIjoiWk5renIzSXJlRFpueHI3d1ZDa0VWN1FaYlF50EcwWVVUTUlxTlFYZ2c1TjZWUkJHQkN5bmVpUER2K2Q4dHNRYnVEbWhWRE1qZllSVng5UmdPNUVUNlMvdzl6UTNST2g0dDlrNzNDVEcyZmtQZEtE0Fo0a0NMMk5UYzRyVUVDKzQilCJtYWMi0iJj0WNjMDljZTAxN2E1NzZmZDYyM2UxYjQwNjYwYTQxY2U20WIzZDhjNTAzNjBmZjVkNjQlMzE2YjcwZDMxNmQzIiwidGFnIjoiIn0%3D;

sharif\_tax\_service\_session=eyJpdi161i80VFlPeWtJZUE3K1E5RWwvQmJDRFE9PSIsInZhbHVlljoiTWNlY0ZNb2xYKzloN3UrMFBiUzBFU0g5M01aWXgxdy9pZ01zb2VCSUJqdHlSRjA2ZURC
RXZvY3lTdWZyNnJuZ2Yxa1R6YXF0MW8xL3pDUnljT25pQi9KQm9uYmhIVy9JZk84RUVMTkNBRWh0SUFFZEhlWGhmTjlTZDE2L2F0azEiLCJtYWMi0iJi0TRiMzMxZGM10GJkZjhiYjZlM2JhYWVhMjQ
xZDdhM2ZmZihlM200N2U2MiM0NWZiMWFiZTM3M2M0NmM30TViIiwidGFnIioiIn0%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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

#### Recommendation

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

#### References

#### **MDN: Mixed Content**

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed\_content

### What is mixed content?

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

#### Fixing mixed content

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

### Possible sensitive directories

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

Possible sensitive directories:

- https://shariftaxservice.ssbmultiservices.com/upload
- https://shariftaxservice.ssbmultiservices.com/database

### Request

GET /upload/ HTTP/1.1

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

 $TOKEN=eyJpdiIGInl4U1BHRXZyUFN1RHhoem5HMmU3QXc9PSIsInZhbHVlIjoib05DTWtZMHN1SDk5Ykt0TUQ0a0F6am9yTGlUcW5QSjYrT2taVnFjRi9wTXJwa1k5SXR1cE5BdHdlYTFEVjV40Vdme\\ EJad1hlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUlWV28iLCJtYWMi0iIyM2I5ZTFiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNm\\ MjQ1NjQz0GM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D;$ 

 $sharif\_tax\_service\_session=eyJpdiIGIm5j0GtaTVM1Z0xibVpyZjUyY2kwU1E9PSIsInZhbHVlIjoiZjd6dlJ5TzdlK2FvNDZpeCszV2c5enVJ0VBlNG02bUtham5pbjhxYmFUbVJUM0xqRngv RXR6TTZi0FdLdVJMend5Y0tJQUVaNC9iL3dyMlBQb3hRS1hRaDZuSlhy0S83NzMreGlmM054bGdHY2xXQ2hC0TFFNEhXNWZkTXcwaGUiLCJtYWMi0iI3MTYxMDcxNWNlnzRh0DJk0WQ5ZWRlZmM0MjF kZTNmYjYxYzBkZGI4YjczMTE4NGNmNTc0NDY0NzA4MzhlYjA4IiwidGFnIjoiIn0%3D$ 

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8$ 

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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

### Recommendation

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

### References

### Web Server Security and Database Server Security

https://www.acunetix.com/websitesecurity/webserver-security/

### Possible sensitive files

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

### **Impact**

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

### https://shariftaxservice.ssbmultiservices.com/

Possible sensitive files:

• https://shariftaxservice.ssbmultiservices.com/web.config

#### Request

GET /web.config HTTP/1.1
Accept: aktdrlmi/nxhz

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52: XSRF-

 $TO KEN=eyJpdiIGInl4U1BHRXZyUFN1RHhoem5HMmU3QXc9PSIsInZhbHVlIjoib05DTWtZMHN1SDk5Ykt0TUQ0a0F6am9yTGlUcW5QSjYrT2taVnFjRi9wTXJwa1k5SXR1cE5BdHdlYTFEVjV40Vdme\\ EJad1hlZ1VKeUtENUJ3Z1FSMTdiNTBCbE1CTkFJS0ZBN2Q5czNnQndNVnkrZ2pkLy9YU2JXQ0pwWUlWV28iLCJtYWMi0iIyM2I5ZTFiYWMxZWU0MDRlMmUyNzA0MzU2NjM0YTgxY2VjNzVhNGEyMWNm\\ MjQ1NjQz0GM5MzJhZDUzYjdmMDIyIiwidGFnIjoiIn0%3D;$ 

 $sharif\_tax\_service\_session=eyJpdiIGIm5j0GtaTVM1Z0xibVpyZjUyY2kwU1E9PSIsInZhbHVlIjoiZjd6dlJ5TzdlK2FvNDZpeCszV2c5enVJ0VBlNG02bUtham5pbjhxYmFUbVJUM0xqRngv RXR6TTZi0FdLdVJMend5Y0tJQUVaNC9iL3dyMlBQb3hRS1hRaDZuSlhy0S83NzMreGlmM054bGdHY2xXQ2hC0TFFNEhXNWZkTXcwaGUiLCJtYWMi0iI3MTYxMDcxNWNlnzRh0DJk0WQ5ZWRlZmM0MjF kZTNmYjYxYzBkZGI4YjczMTE4NGNmNTc0NDY0NzA4MzhlYjA4IiwidGFnIjoiIn0%3D$ 

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: shariftaxservice.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://shariftaxservice.ssbmultiservices.com/

Paths without CSP header:

- https://shariftaxservice.ssbmultiservices.com/
- https://shariftaxservice.ssbmultiservices.com/real-estate
- https://shariftaxservice.ssbmultiservices.com/upload/client-review/
- https://shariftaxservice.ssbmultiservices.com/about-us
- https://shariftaxservice.ssbmultiservices.com/blogs
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b
- https://shariftaxservice.ssbmultiservices.com/consultation
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://shariftaxservice.ssbmultiservices.com/contact-us
- https://shariftaxservice.ssbmultiservices.com/driving-school
- $\bullet \ \ https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea$
- https://shariftaxservice.ssbmultiservices.com/immigration
- https://shariftaxservice.ssbmultiservices.com/irs-publications
- https://shariftaxservice.ssbmultiservices.com/privacy-policy
- https://shariftaxservice.ssbmultiservices.com/real-state-home
- $\bullet \quad https://shariftaxservice.ssbmultiservices.com/record-retention-guide$
- https://shariftaxservice.ssbmultiservices.com/tax-accounting
- https://shariftaxservice.ssbmultiservices.com/tax-form
- https://shariftaxservice.ssbmultiservices.com/tax-rates
- https://shariftaxservice.ssbmultiservices.com/terms-of-use
- https://shariftaxservice.ssbmultiservices.com/video-gallery

### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.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

## 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://shariftaxservice.ssbmultiservices.com/

Verified

Pages where the content-type header is not specified:

- https://shariftaxservice.ssbmultiservices.com/web.config
- https://shariftaxservice.ssbmultiservices.com/project/vendor/asm89/stack-cors/LICENSE
- https://shariftaxservice.ssbmultiservices.com/project/docker-compose.yml

#### Request

GET /web.config HTTP/1.1

Referer: https://shariftaxservice.ssbmultiservices.com/ Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

TOKEN=eyJpdi16ImU5VDFaRyt0ekJzSHh3a0t6RTRoUWc9PSIsInZhbHVlIjoiM0dxK1NocGYxZTdudFl2dDuxMFJteVQ1dHl5S3JIM2VjNzFFeFpodWYvdEpTcDIrekQvRUo1QUR2K1NBWWxtNXdQW FovUlVrcWVwdlFvQk9KN2ttN3gwZW9INVBQTXZiWGtvV2dSc2h4dFJYR2wleCtXV0ZzT0dzNk1vL2J5VVUiLCJtYWMi0iIxZmIwMzU0ZmUzMzRhYTUxOGRkNTM3ZWRmNjg1ZWNlYTY0ZmUz0DY0ZjM4 NmM2OTk2Y2U5ZDFjZjRjM2Y0ZjQyIiwidGFnIjoiIn0%3D;

sharif\_tax\_service\_session=eyJpdi16ImsvL2c2YlVoRzNIYWdKUWJ3YmVVN3c9PSIsInZhbHVlIjoiMVFKSGJtRU9lb29uTTQrTHJXaWNMdjh1S0ZEdUZRTnhVZUtKQnVoQVZoUmU2UVo5VUpa anZ5TFNYeHQydWNHZXBXQ3RwUGtuVHM2cnVqYXR3YUgwQWpleFNHTzF5WVZUZENmenpSdTdZbTNLTWNvS2VtYlBTTTJL0HNxZjBwdXEiLCJtYWMi0iIxN2Y40TYyM2I0MGI2YmQ0YzMyNjhmZTZiNTg yM2I4MTkxMTk0YjM1NDRhNDhiZmQ1NzkxM2M3NDI0YWQyMDc1IiwidGFnIjoiIn0%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

 ${\tt Host: sharift axservice.ssb multiservices.com}$ 

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://shariftaxservice.ssbmultiservices.com/

Emails found:

- https://shariftaxservice.ssbmultiservices.com/ sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/ shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/real-estate sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/real-estate shariftaxservice@gmail.com

- https://shariftaxservice.ssbmultiservices.com/about-us sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/about-us shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/blogs sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/blogs shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/consultation sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/consultation shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/contact-us sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/contact-us shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/driving-school sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/driving-school shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/immigration sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/immigration shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/irs-publications sqalam718@gmail.com
- https://shariftaxservice.ssbmultiservices.com/irs-publications shariftaxservice@gmail.com
- https://shariftaxservice.ssbmultiservices.com/privacy-policy sqalam718@gmail.com

GET / HTTP/1.1

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, */*; q=0$ 

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

 $Host: \ sharift ax service.ssb {\tt multiservices.com}$ 

Connection: Keep-alive

### Recommendation

Check references for details on how to solve this problem.

### References

### Anti-spam techniques

https://en.wikipedia.org/wiki/Anti-spam\_techniques

# **Outdated JavaScript libraries**

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

### **Impact**

Consult References for more information.

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

- ¡Query 3.5.1
  - o URL: https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js
  - o 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://shariftaxservice.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: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

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

- bootstrap.js 4.5.2
  - o URL: https://shariftaxservice.ssbmultiservices.com/
  - o Detection method: The library's name and version were determined based on its dynamic behavior.
  - o References:
    - https://github.com/twbs/bootstrap/releases

#### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.ssbmultiservices.com/

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, */*; q=0$ 

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: shariftaxservice.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://shariftaxservice.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://shariftaxservice.ssbmultiservices.com/
- https://shariftaxservice.ssbmultiservices.com/real-estate
- https://shariftaxservice.ssbmultiservices.com/upload/client-review/
- https://shariftaxservice.ssbmultiservices.com/about-us
- https://shariftaxservice.ssbmultiservices.com/blogs
- https://shariftaxservice.ssbmultiservices.com/real-estate/luxury-villa-for-sale618958be90e4b
- https://shariftaxservice.ssbmultiservices.com/consultation
- https://shariftaxservice.ssbmultiservices.com/assets/front/fonts/fontawesome/webfonts/
- https://shariftaxservice.ssbmultiservices.com/contact-us
- https://shariftaxservice.ssbmultiservices.com/driving-school
- $\bullet \ \ https://shariftaxservice.ssbmultiservices.com/blog/answers-to-five-common-questions-about-2020-stimulus-payments-4u8ea$

- https://shariftaxservice.ssbmultiservices.com/immigration
- https://shariftaxservice.ssbmultiservices.com/irs-publications
- https://shariftaxservice.ssbmultiservices.com/privacy-policy
- https://shariftaxservice.ssbmultiservices.com/real-state-home
- https://shariftaxservice.ssbmultiservices.com/record-retention-guide
- https://shariftaxservice.ssbmultiservices.com/tax-accounting
- https://shariftaxservice.ssbmultiservices.com/tax-form
- https://shariftaxservice.ssbmultiservices.com/tax-rates
- https://shariftaxservice.ssbmultiservices.com/terms-of-use
- https://shariftaxservice.ssbmultiservices.com/video-gallery

GET / HTTP/1.1

Referer: https://shariftaxservice.ssbmultiservices.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate,br

 $User-Agent: Mozilla/5.0 \; (Windows \; NT \; 10.0; \; Win64; \; x64) \; AppleWebKit/537.36 \; (KHTML, \; like \; Gecko) \; Chrome/114.0.0.0 \; Safari/537.36 \; (Windows \; NT \; 10.0; \; Win64; \; x64) \; AppleWebKit/537.36 \; (KHTML, \; like \; Gecko) \; Chrome/114.0.0.0 \; Safari/537.36 \; (Windows \; NT \; 10.0; \; Win64; \; x64) \; AppleWebKit/537.36 \; (Win74.0.0.0) \; Win64; \; x64) \; AppleWebKit/537.36 \; (Win74.0.0.0.0) \; Win64; \; x64) \; Win64;$ 

Host: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

#### References

#### Permissions-Policy / Feature-Policy (MDN)

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

#### Permissions Policy (W3C)

https://www.w3.org/TR/permissions-policy-1/

## Possible server path disclosure (Unix)

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

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

### **Impact**

Possible sensitive information disclosure.

### https://shariftaxservice.ssbmultiservices.com/

Pages with paths being disclosed:

- https://shariftaxservice.ssbmultiservices.com/tax-form /home/ssbmul5/shariftaxservice.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php
- https://shariftaxservice.ssbmultiservices.com/where-refund /home/ssbmul5/shariftaxservice.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php
- /home/ssbmul5/shariftaxservice.ssbmultiservices.com/project/vendor/laravel/framework/src/llluminate/Routing/AbstractRouteCollection.php

   https://shariftaxservice.ssbmultiservices.com/index.php/tax-form
- /home/ssbmul5/sharift ax service. ssbmultiservices. com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php
- https://shariftaxservice.ssbmultiservices.com/index.php/where-refund /home/ssbmul5/shariftaxservice.ssbmultiservices.com/project/vendor/laravel/framework/src/Illuminate/Routing/AbstractRouteCollection.php

### Request

POST /tax-form HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Referer: https://shariftaxservice.ssbmultiservices.com/tax-form

Cookie: PHPSESSID=8928f7cd40dcd95f5c867fbe74ab4f52; XSRF-

 $TOKEN=eyJpdiI6IldRV3luaDUyZmo0blY3WmRyN1NhUGc9PSIsInZhbHVlljoiN241VUdnRzNFcDcrT0dsb1RkUFZVZ2ZIbHJaQ0M0Q3hxcnFkTmlaVll0UlFnRnZtaDVEYkNuaG5WaHpLRmYvdE45V\\ 2phaG1JNW91Z69JZitmaDd1VXlEQkNWUUdERWhHZzA1dHd4WlU2aytaeEdJNlF0ZVg2V1QyY0l5cmdwY0wilCJtYWMi0iI5N2M2NWVkNjIy0TQyMmYyZmNl0GJiYTM4NwMwNDk4MzgwZDk5Njg2MmEz\\ MjdlNGZiYzE2MmVjN2EyZTY2MDlmIiwidGFnIjoiIn0%3D;$ 

sharif\_tax\_service\_session=eyJpdi16Ilo3VXN5Tkovb0pGUVZVSmxNY3hEUUE9PSIsInZhbHVlIjoiYTl0QW5oZEJ1Y2VkTEllMFNXMlZmSlQzUWRWZU1HZkpB0UpT0E5BalQzYlFVZ1d4Vm80 bmJBSlBYZTI4SmUxT0hITGgwZ1pYL3NMaml4aTlBTEVUMEduMjN4S2JaZjdDalVvWExCZHdPYy95elQyK1FScVRyVmREZEtkSU95NmYiLCJtYWMi0iJlZWNjYzIyYjI0YTkzZmQ0ZjMzNWIxYzFjMzg 2ZjM1YjA2YTg10WRhMWY5ZTFmMTkxYWUxY2Q5YTRlMzBlYTdiIiwidGFnIjoiIn0%3D

Content-Length: 41

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8$ 

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36

Host: shariftaxservice.ssbmultiservices.com

Connection: Keep-alive

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

#### Recommendation

Prevent this information from being displayed to the user.

#### References

#### Full Path Disclosure

https://www.owasp.org/index.php/Full\_Path\_Disclosure

## Reverse proxy detected

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

#### **Impact**

No impact is associated with this vulnerability.

### https://shariftaxservice.ssbmultiservices.com/

Detected reverse proxy: Apache httpd

#### Request

GET / HTTP/1.1

Max-Forwards: 0

 $Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8, application/xml; q=0.9, application/xml; q=0$ 

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

 $Host: \ sharift ax service.ssb multiservices.com$ 

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://shariftaxservice.ssbmultiservices.com/

Pages where SRI is not implemented:

- https://shariftaxservice.ssbmultiservices.com/
   Script SRC: https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js
- https://shariftaxservice.ssbmultiservices.com/
   Script SRC: https://cdnjs.cloudflare.com/ajax/libs/lightgallery/1.9.0/js/lightgallery-all.min.js
- https://shariftaxservice.ssbmultiservices.com/
   Script SRC: https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js

### Request

GET / HTTP/1.1

Referer: https://shariftaxservice.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: shariftaxservice.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>

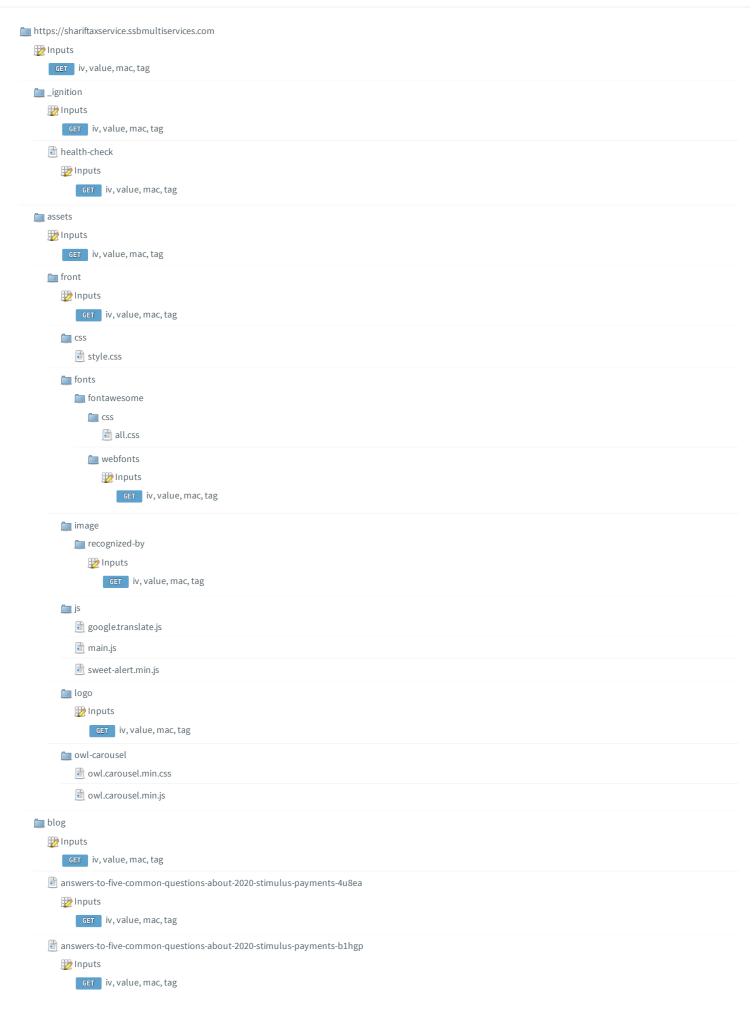
#### References

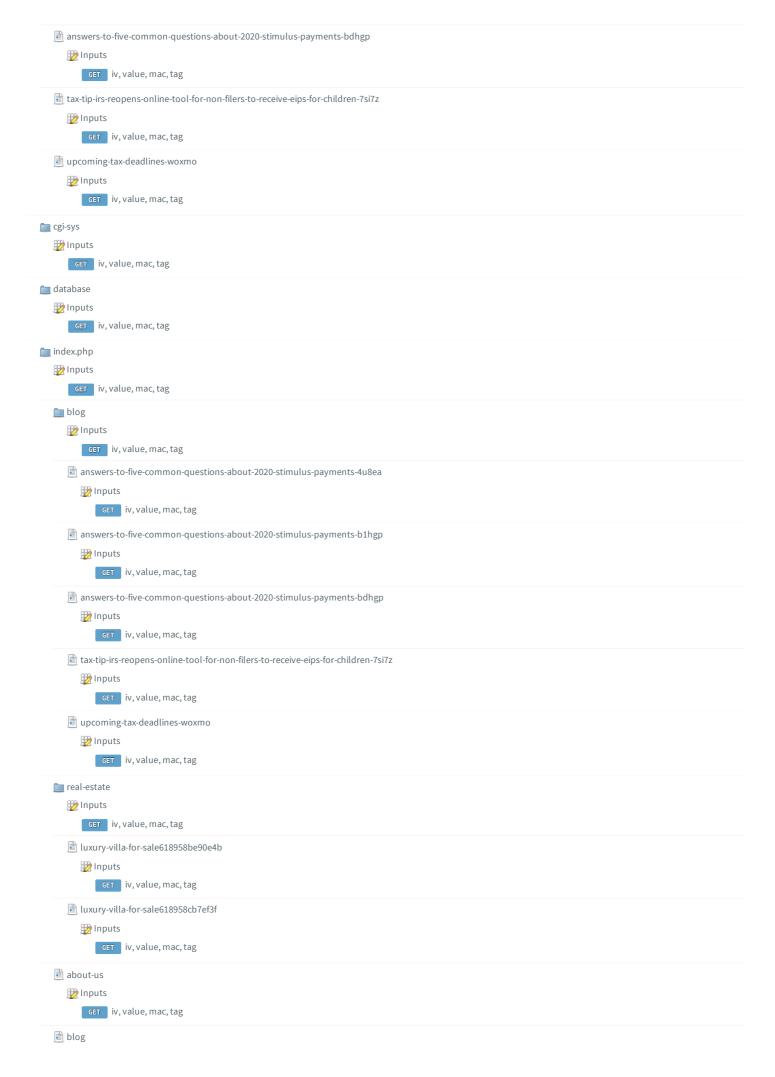
### Subresource Integrity

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource\_Integrity

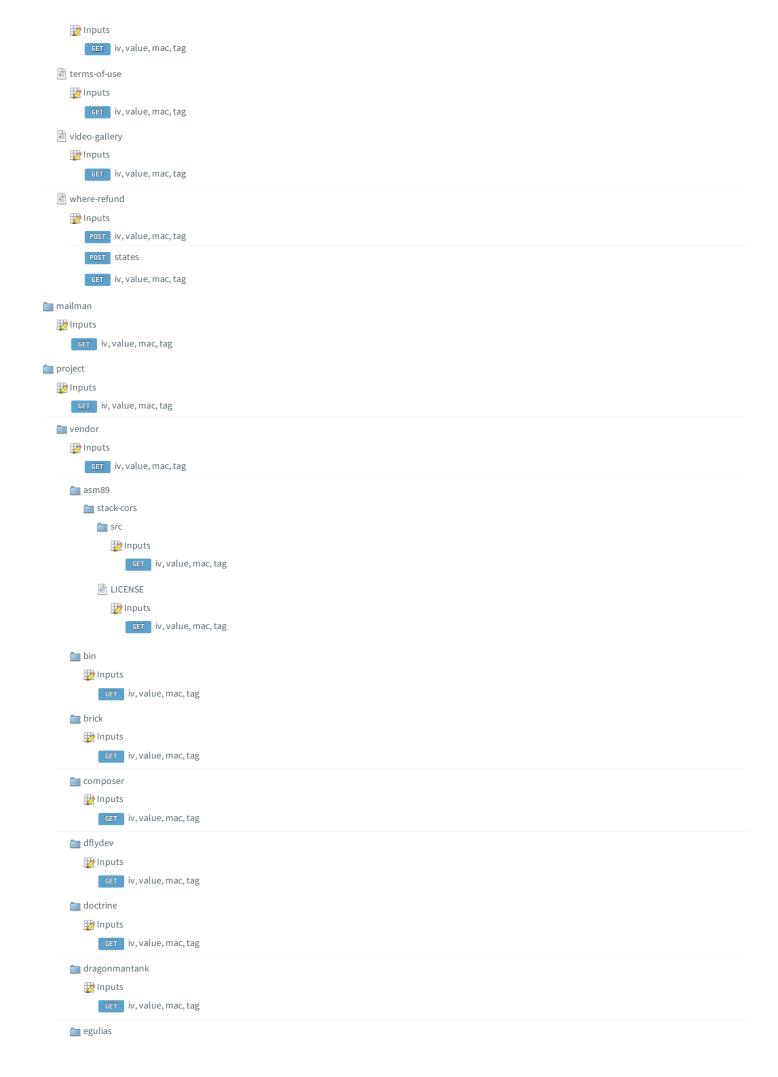
### **SRI Hash Generator**

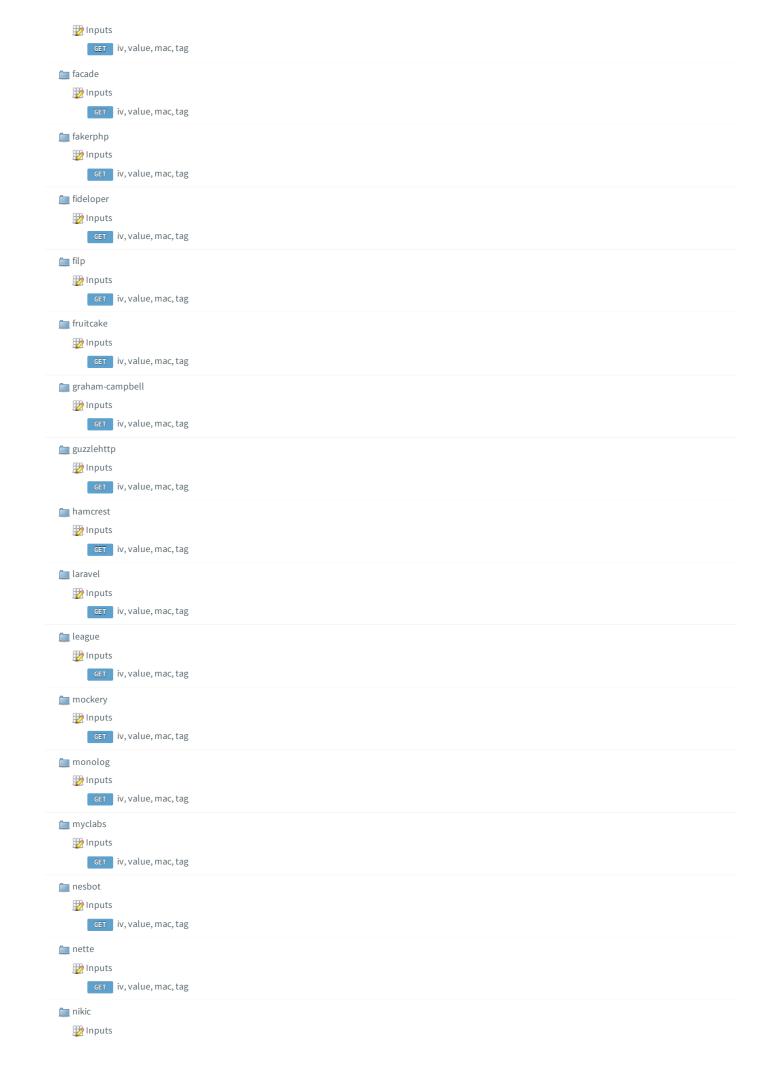
https://www.srihash.org/





	Inputs  GET iv, value, mac, tag
	blogs    Diputs   Dip
	consultation    Disputs   Consultation   Consultati
	contact-us    Inputs     Post iv, value, mac, tag     Post _token, email, message, name, phone, submit
	driving-school    Inputs
	immigration    Inputs   GET   iv, value, mac, tag
	irs-publications    irs-publications
	irs-withholding-calculator    inputs   iv, value, mac, tag   iv, v
	privacy-policy    privacy-policy   priva
	real-estate    Inputs   Inputs
	real-state-home    Inputs   In
	record-retention-guide    Inputs   Inpu
	tax-accounting    Inputs   Inp
	tax-appointment-checklist  Inputs  Inputs  iv, value, mac, tag
<u> </u>	tax-form    post iv, value, mac, tag    post states
	tax-rates





```
GET iv, value, mac, tag
nunomaduro
  mputs [mail]
     GET iv, value, mac, tag
i opis
  Inputs
     GET iv, value, mac, tag
paypal
  mputs [mail]
     GET iv, value, mac, tag
phar-io
  mputs [mail]
     GET iv, value, mac, tag
phpdocumentor
  Inputs
     GET iv, value, mac, tag
phpoption
  Inputs
     GET iv, value, mac, tag
phpspec
  Inputs
     GET iv, value, mac, tag
phpunit
  Inputs
     GET iv, value, mac, tag
iii psr
  Inputs
     GET iv, value, mac, tag
psy
  Inputs
     GET iv, value, mac, tag
ralouphie
  Inputs
     GET iv, value, mac, tag
i ramsey
  Inputs
     GET iv, value, mac, tag
sebastian
  Inputs
     GET iv, value, mac, tag
i swiftmailer
  Inputs
     GET iv, value, mac, tag
symfony
  Inputs
     GET iv, value, mac, tag
theseer
  Inputs
     GET iv, value, mac, tag
```

```
📺 tijsverkoyen
        Inputs
           GET iv, value, mac, tag
     vlucas
        Inputs
           GET iv, value, mac, tag
     📺 voku
        Inputs
           GET iv, value, mac, tag
     webmozart
        Inputs
           GET iv, value, mac, tag
     autoload.php
        Inputs
           GET iv, value, mac, tag
  docker-compose.yml
     Inputs
        GET iv, value, mac, tag
i real-estate
  Inputs
      GET iv, value, mac, tag
  luxury-villa-for-sale618958be90e4b
     Inputs
        GET iv, value, mac, tag
  luxury-villa-for-sale618958cb7ef3f
     Inputs
        GET iv, value, mac, tag
i upload
  Inputs
      GET iv, value, mac, tag
  client-review
     Inputs
        GET iv, value, mac, tag
  in header-footer
     Inputs
        GET iv, value, mac, tag
  post-image
     Inputs
        GET iv, value, mac, tag
  im real-state
     Inputs
        GET iv, value, mac, tag
  i realstate-post-image
     Inputs
        GET iv, value, mac, tag
  service-photo
     Inputs
        GET iv, value, mac, tag
  i slider-image
```

