

## 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	<a href="http://fillippartners.ssbmultiservices.com">fillippartners.ssbmultiservices.com</a>
Scan Type	Full Scan
Start Time	Jan 13, 2024, 8:32:34 PM GMT+8
Scan Duration	3 minutes
Requests	19102
Average Response Time	29ms
Maximum Response Time	1591ms
Application Build	v23.7.230728157



High



Medium



Low

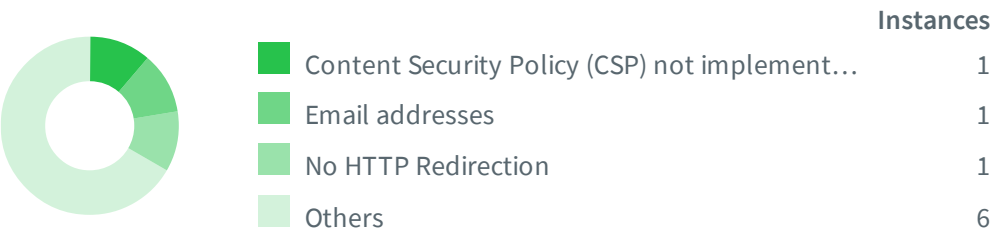


Informational

Severity	Vulnerabilities	Instances
High	0	0
Medium	2	2
Low	4	4
Informational	7	9
Total	13	15

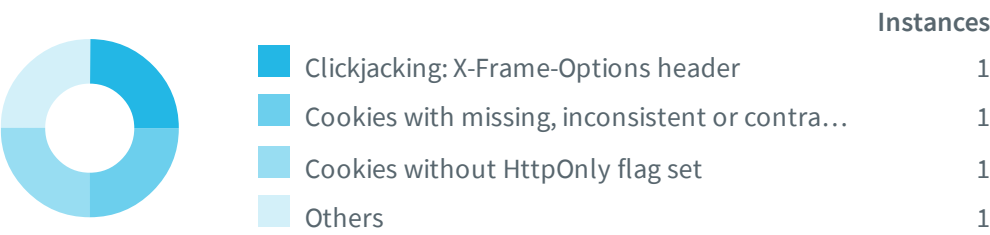
## Informational

---



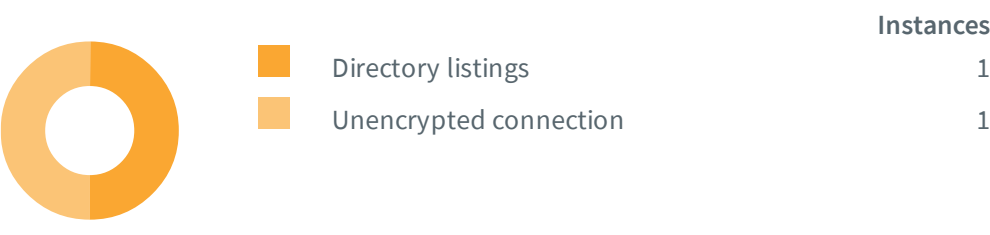
## Low Severity

---
















## Medium Severity

---



# Impacts

SEVERITY	IMPACT	
 Medium	<b>1</b>	<b>Directory listings</b>
 Medium	<b>1</b>	<b>Unencrypted connection</b>
 Low	<b>1</b>	<b>Clickjacking: X-Frame-Options header</b>
 Low	<b>1</b>	<b>Cookies with missing, inconsistent or contradictory properties</b>
 Low	<b>1</b>	<b>Cookies without HttpOnly flag set</b>
 Low	<b>1</b>	<b>Insecure Inline Frame (iframe)</b>
 Informational	<b>1</b>	<b>Content Security Policy (CSP) not implemented</b>
 Informational	<b>1</b>	<b>Email addresses</b>
 Informational	<b>1</b>	<b>No HTTP Redirection</b>
 Informational	<b>3</b>	<b>Outdated JavaScript libraries</b>
 Informational	<b>1</b>	<b>Permissions-Policy header not implemented</b>
 Informational	<b>1</b>	<b>Reverse proxy detected</b>
 Informational	<b>1</b>	<b>Subresource Integrity (SRI) not implemented</b>

# 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.

<http://fillippartners.ssbmultiservices.com/>

Verified

Folders with directory listing enabled:

- <http://fillippartners.ssbmultiservices.com/assets/>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/css/>
- <http://fillippartners.ssbmultiservices.com/assets/css/>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/webfonts/>
- <http://fillippartners.ssbmultiservices.com/assets/js/>
- <http://fillippartners.ssbmultiservices.com/assets/owl-carousel/>
- <http://fillippartners.ssbmultiservices.com/assets/slick-slider/>
- <http://fillippartners.ssbmultiservices.com/assets/image/>
- <http://fillippartners.ssbmultiservices.com/assets/logo/>
- <http://fillippartners.ssbmultiservices.com/assets/icon/>
- <http://fillippartners.ssbmultiservices.com/assets/svg/>

## Request

---

```
GET /assets/ 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: fillippartners.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)

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

## Unencrypted connection

---

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

### Impact

---

Possible information disclosure.

<http://fillippartners.ssbmultiservices.com/>

Verified

### Request

---

```
GET / HTTP/1.1
Referer: http://fillippartners.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: fillippartners.ssbmultiservices.com
Connection: Keep-alive
```

### Recommendation

---

The site should send and receive data over a secure (HTTPS) connection.

## 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.

### <http://fillippartners.ssbmultiservices.com/>

Paths without secure XFO header:

- <http://fillippartners.ssbmultiservices.com/>
- <http://fillippartners.ssbmultiservices.com/about-us.php>
- <http://fillippartners.ssbmultiservices.com/advisors.php>
- <http://fillippartners.ssbmultiservices.com/contact-us.php>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/webfonts/>
- <http://fillippartners.ssbmultiservices.com/disclaimer.php>
- <http://fillippartners.ssbmultiservices.com/investment-service.php>
- <http://fillippartners.ssbmultiservices.com/investment-team.php>
- <http://fillippartners.ssbmultiservices.com/legal-service.php>
- <http://fillippartners.ssbmultiservices.com/legal-team.php>
- <http://fillippartners.ssbmultiservices.com/our-firm.php>
- <http://fillippartners.ssbmultiservices.com/publications.php>
- <http://fillippartners.ssbmultiservices.com/index.php>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/css/>
- <http://fillippartners.ssbmultiservices.com/assets/image/>
- <http://fillippartners.ssbmultiservices.com/assets/logo/>

- <http://fillippartners.ssbmultiservices.com/assets/css/>
- <http://fillippartners.ssbmultiservices.com/assets/owl-carousel/>
- <http://fillippartners.ssbmultiservices.com/assets/>
- <http://fillippartners.ssbmultiservices.com/assets/js/>
- <http://fillippartners.ssbmultiservices.com/assets/slick-slider/>

## Request

---

GET / HTTP/1.1  
Referer: <http://fillippartners.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: fillippartners.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)

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

### [Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

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

### [OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

[https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\\_Defense\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

### [Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

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

# Cookies with missing, inconsistent or contradictory properties

---



At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, or 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.

<http://fillippartners.ssbmultiservices.com/> Verified

List of cookies with missing, inconsistent or contradictory properties:

- <http://fillippartners.ssbmultiservices.com/contact-us.php>

Cookie was set with:

Set-Cookie: PHPSESSID=9bbac2caaf1ded0674497f1c0c4723ef; 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 /contact-us.php HTTP/1.1
Referer: http://fillippartners.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: fillippartners.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.

<http://fillippartners.ssbmultiservices.com/>

Verified

Cookies without HttpOnly flag set:

- <http://fillippartners.ssbmultiservices.com/contact-us.php>

Set-Cookie: PHPSESSID=9bbac2caaf1ded0674497f1c0c4723ef; path=/

### Request

---

GET /contact-us.php HTTP/1.1

Referer: http://fillippartners.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: fillippartners.ssbmultiservices.com

Connection: Keep-alive

## Recommendation

---

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

# 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.

<http://fillippartners.ssbmultiservices.com/contact-us.php> Verified

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

## Request

---

```
GET /contact-us.php HTTP/1.1
Referer: http://fillippartners.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: fillippartners.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)

<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)

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

# 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.

### <http://fillippartners.ssbmultiservices.com/>

Paths without CSP header:

- <http://fillippartners.ssbmultiservices.com/>
- <http://fillippartners.ssbmultiservices.com/about-us.php>
- <http://fillippartners.ssbmultiservices.com/advisors.php>
- <http://fillippartners.ssbmultiservices.com/contact-us.php>

- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/webfonts/>
- <http://fillippartners.ssbmultiservices.com/disclaimer.php>
- <http://fillippartners.ssbmultiservices.com/investment-service.php>
- <http://fillippartners.ssbmultiservices.com/investment-team.php>
- <http://fillippartners.ssbmultiservices.com/legal-service.php>
- <http://fillippartners.ssbmultiservices.com/legal-team.php>
- <http://fillippartners.ssbmultiservices.com/our-firm.php>
- <http://fillippartners.ssbmultiservices.com/publications.php>
- <http://fillippartners.ssbmultiservices.com/index.php>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/css/>
- <http://fillippartners.ssbmultiservices.com/assets/image/>
- <http://fillippartners.ssbmultiservices.com/assets/logo/>
- <http://fillippartners.ssbmultiservices.com/assets/css/>
- <http://fillippartners.ssbmultiservices.com/assets/owl-carousel/>
- <http://fillippartners.ssbmultiservices.com/assets/>
- <http://fillippartners.ssbmultiservices.com/assets/js/>
- <http://fillippartners.ssbmultiservices.com/assets/slick-slider/>

## Request

---

```
GET / HTTP/1.1
Referer: http://fillippartners.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: fillippartners.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)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/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.

**<http://fillippartners.ssbmultiservices.com/>**

Emails found:

- <http://fillippartners.ssbmultiservices.com/advisors.php>  
**nanameki@vbest.jp**
- <http://fillippartners.ssbmultiservices.com/advisors.php>  
**nanameki@fillippartners.com**
- <http://fillippartners.ssbmultiservices.com/investment-team.php>  
**nafees@fillippartners.com**
- <http://fillippartners.ssbmultiservices.com/investment-team.php>  
**salim@fillippartners.com**
- <http://fillippartners.ssbmultiservices.com/investment-team.php>  
**fayaad@fillippartners.com**
- <http://fillippartners.ssbmultiservices.com/investment-team.php>  
**adnan@fillippartners.com**

- <http://fillippartners.ssbmultiservices.com/legal-team.php>  
[monirul@fillippartners.com](mailto:monirul@fillippartners.com)
- <http://fillippartners.ssbmultiservices.com/legal-team.php>  
[zeeshan@fillippartners.com](mailto:zeeshan@fillippartners.com)

## Request

---

GET /advisors.php HTTP/1.1  
Referer: <http://fillippartners.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: fillippartners.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](https://en.wikipedia.org/wiki/Anti-spam_techniques)

# No HTTP Redirection

---

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

## Impact

---

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

<http://fillippartners.ssbmultiservices.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

## Recommendation

---

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

## References

---

### HTTP Redirections

[https://infosec.mozilla.org/guidelines/web\\_security#http-redirections](https://infosec.mozilla.org/guidelines/web_security#http-redirections)

# 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.

<http://fillippartners.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: <http://fillippartners.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: fillippartners.ssbmultiservices.com



<http://fillippartners.ssbmultiservices.com/>

Confidence: 95%

- **bootstrap.js 4.5.2**
  - URL: <http://fillippartners.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: <http://fillippartners.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: fillippartners.ssbmultiservices.com  
Connection: Keep-alive

<http://fillippartners.ssbmultiservices.com/>

Confidence: 95%

- **slick 1.5.9**
  - URL: <http://fillippartners.ssbmultiservices.com/assets/slick-slider/slick.min.js>
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - <https://github.com/kenwheeler/slick/tags>

## Request

GET /assets/slick-slider/slick.min.js HTTP/1.1  
Referer: <http://fillippartners.ssbmultiservices.com/>  
Cookie: PHPSESSID=e73e5f8eabb238e79d6bb56a6c335e63  
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: fillippartners.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

---

### <http://fillippartners.ssbmultiservices.com/>

Locations without Permissions-Policy header:

- <http://fillippartners.ssbmultiservices.com/>
- <http://fillippartners.ssbmultiservices.com/about-us.php>
- <http://fillippartners.ssbmultiservices.com/advisors.php>
- <http://fillippartners.ssbmultiservices.com/contact-us.php>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/webfonts/>
- <http://fillippartners.ssbmultiservices.com/disclaimer.php>
- <http://fillippartners.ssbmultiservices.com/investment-service.php>
- <http://fillippartners.ssbmultiservices.com/investment-team.php>
- <http://fillippartners.ssbmultiservices.com/legal-service.php>
- <http://fillippartners.ssbmultiservices.com/legal-team.php>
- <http://fillippartners.ssbmultiservices.com/our-firm.php>
- <http://fillippartners.ssbmultiservices.com/publications.php>
- <http://fillippartners.ssbmultiservices.com/index.php>
- <http://fillippartners.ssbmultiservices.com/assets/fonts/fontawesome/css/>
- <http://fillippartners.ssbmultiservices.com/assets/image/>
- <http://fillippartners.ssbmultiservices.com/assets/logo/>
- <http://fillippartners.ssbmultiservices.com/mailman/>
- <http://fillippartners.ssbmultiservices.com/assets/css/>
- <http://fillippartners.ssbmultiservices.com/assets/owl-carousel/>
- <http://fillippartners.ssbmultiservices.com/assets/>
- <http://fillippartners.ssbmultiservices.com/assets/js/>

## Request

---

GET / HTTP/1.1

Referer: <http://fillippartners.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: fillippartners.ssbmultiservices.com

## References

---

[Permissions-Policy / Feature-Policy \(MDN\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)

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

[Permissions Policy \(W3C\)](https://www.w3.org/TR/permissions-policy-1/)

<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.

**<http://fillippartners.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: fillippartners.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.

### <http://fillippartners.ssbmultiservices.com/>

Pages where SRI is not implemented:

- <http://fillippartners.ssbmultiservices.com/>  
Script SRC: <https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js>
- <http://fillippartners.ssbmultiservices.com/>  
Script SRC: <https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit>

## Request

---

```
GET / HTTP/1.1
Referer: http://fillippartners.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: fillippartners.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)

[https://developer.mozilla.org/en-US/docs/Web/Security/Subresource\\_Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

### [SRI Hash Generator](https://www.srihash.org/)

<https://www.srihash.org/>

## Coverage

---

 <http://fillippartners.ssbmultiservices.com>

 assets


 css

 style.css

 fonts

 fontawesome

 css

 all.css

 all.min.css

 webfonts

 icon

 image

 js

 main.js

 sweet-alert.min.js

 logo

 owl-carousel

 owl.carousel.min.css

 owl.carousel.min.js

 slick-slider

 slick.main.css

 slick.min.js

 slick.theme.min.css

 svg

 cgi-sys

 mailman

 archives

 about-us.php

 advisors.php

 contact-us.php


 disclaimer.php

 index.php

 investment-service.php

 investment-team.php

 legal-service.php

 legal-team.php

 our-firm.php

 publications.php

 send-message.php

 Inputs

**POST** name, phone, email, subject, message

**POST** email, message, name, phone, subject, submit