netsparker

10/2/2023 7:21:38 PM (UTC+05:30)

Detailed Scan Report

https://main--taupe-shortbread-314b46.netlify.app/

Scan Time	: 10/2/2023 7:12:05 PM (UTC+05:30)
Scan Duration	: 00:00:06:14
Total Requests	: 6,914
Average Speed	: 18.4r/s

Risk Level:
LOW

10
IDENTIFIED

2
CONFIRMED

0
CRITICAL

0
HIGH

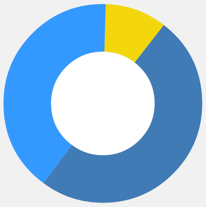
0
MEDIUM

1
LOW

5
BEST PRACTICE

4
INFORMATION

Identified Vulnerabilities



🟥	Critical	0
🟥	High	0
🟧	Medium	0
🟨	Low	1
🟦	Best Practice	5
🟦	Information	4
	TOTAL	**10**

Confirmed Vulnerabilities

🟥	Critical	0
🟥	High	0
🟧	Medium	0
🟨	Low	0
🟦	Best Practice	0
🟦	Information	2
	TOTAL	**2**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
⚑	Missing X-Frame-Options Header	GET	https://main--taupe-shortbread-314b46.netlify.app/	
❗	Content Security Policy (CSP) Not Implemented	GET	https://main--taupe-shortbread-314b46.netlify.app/	
❗	Expect-CT Not Enabled	GET	https://main--taupe-shortbread-314b46.netlify.app/	
❗	Missing X-XSS-Protection Header	GET	https://main--taupe-shortbread-314b46.netlify.app/	
❗	Referrer-Policy Not Implemented	GET	https://main--taupe-shortbread-314b46.netlify.app/static/css/	
❗	Subresource Integrity (SRI) Not Implemented	GET	https://main--taupe-shortbread-314b46.netlify.app/static/css/	
ℹ	CDN Detected (Netlify)	GET	https://main--taupe-shortbread-314b46.netlify.app/	
ℹ	Email Address Disclosure	GET	https://main--taupe-shortbread-314b46.netlify.app/static/js/main.c1d7921f.js	
✓ ℹ	File Upload Functionality Detected	GET	https://main--taupe-shortbread-314b46.netlify.app/	
✓ ℹ	Robots.txt Detected	GET	https://main--taupe-shortbread-314b46.netlify.app/robots.txt	

1. Missing X-Frame-Options Header

LOW | 1

Netsparker detected a missing `X-Frame-Options`header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options`HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame`or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

1.1. https://main--taupe-shortbread-314b46.netlify.app/

Certainty

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id: 01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.p
ng"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" conten
t="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="man
ifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/ma
in.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><nosc
ript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY`It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN`It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *`URL`*It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	693
CAPEC	103
ISO27001	A.14.2.5

2. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe in the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly ends with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
  - child-src
  - connect-src
  - font-src
  - img-src
  - manifest-src
  - media-src
  - object-src
  - script-src
  - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Vulnerabilities

2.1. https://main--taupe-shortbread-314b46.netlify.app/

Certainty

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id: 01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.p
ng"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" conten
t="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="man
ifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/ma
in.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><nosc
ript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

3. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

3.1. https://main--taupe-shortbread-314b46.netlify.app/

Certainty

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id: 01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.p
ng"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" conten
t="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="man
ifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/ma
in.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><nosc
ript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

4. Missing X-XSS-Protection Header

BEST PRACTICE ❗ 1

Netsparker detected a missing `X-XSS-Protection`header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

4.1. https://main--taupe-shortbread-314b46.netlify.app/

Certainty

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id: 01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.png"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="manifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/main.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

-
  ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION

SANS Top 25	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5

5. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

5.1. https://main--taupe-shortbread-314b46.netlify.app/static/css/

Certainty

Request

```
GET /static/css/ HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 243.6815 **Total Bytes Received :** 3471 **Body Length :** 3082 **Is Compressed :** No

```
HTTP/1.1 404 Not Found
Server: Netlify
Content-Length: 1450
Vary: Accept-Encoding
X-Nf-Request-Id: 01HBRA29GPMTHG3YN6W2S6E34B
Age: 68052
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Etag: 1689333542-ssl-df
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 02 Oct 2023 13:43:27 GMT
Cache-Control: public,max-age=0,must-revalidate

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<title>Page Not Found</title>
<link href='https://fonts.googleapis.com/css?family=Roboto:400,700&subset=latin,latin-ext' rel='stylesheet' type='text/css'>
<style>
body {
font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, Helvetica, Arial, sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol";
background: rgb(52, 56, 60);
color: white;
overflow: hidden;
margin: 0;
padding: 0;
}

h1 {
margin: 0;
font-size: 22px;
line-height: 24px;
}

.main {
position: relative;
display: flex;
flex-direction: column;
align-items: center;
justify-content: center;
height: 100vh;
width: 100vw;
}

.card {
position: relative;
display: flex;
flex-direction: column;
width: 75%;
max-width: 364px;
padding: 24px;
background: white;
color: rgb(14, 30, 37);
border-radius: 8px;
box-shadow: 0 2px 4px 0 rgba(14, 30, 37, .16);
}

a {
margin: 0;
font-weight: 600;
line-height: 24px;
color: #054861;
}

a svg {
position: relative;
top: 2px;
}

a:hover,
a:focus {
text-decoration: none;
}

a:hover svg path{
fill: #007067;
}

p:last-of-type {
margin-bottom: 0;
}

</style>
</head>
<body>
<div class="main">
<div class=
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-
origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	200
ISO27001	A.14.2.5

6. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

6.1. https://main--taupe-shortbread-314b46.netlify.app/static/css/

Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Roboto:400,700&subset=latin,latin-ext

Certainty

Request

```
GET /static/css/ HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 243.6815 **Total Bytes Received :** 3471 **Body Length :** 3082 **Is Compressed :** No

```
HTTP/1.1 404 Not Found
Server: Netlify
Content-Length: 1450
Vary: Accept-Encoding
X-Nf-Request-Id: 01HBRA29GPMTHG3YN6W2S6E34B
Age: 68052
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Etag: 1689333542-ssl-df
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Mon, 02 Oct 2023 13:43:27 GMT
Cache-Control: public,max
…
html>
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">

<title>Page Not Found</title>
<link href='https://fonts.googleapis.com/css?family=Roboto:400,700&subset=latin,latin-ext' rel='stylesheet' type='text/css'>
<style>
body {
font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, Helvetica, Arial, sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol";
backgrou
…
```

Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity

- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

7. CDN Detected (Netlify)

INFORMATION ⓘ | 1

Netsparker detected that your website uses Netlify. Netlify is a Content Delivery Network product which is responsible for caching your website to speed it up.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

7.1. https://main--taupe-shortbread-314b46.netlify.app/

Certainty

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id:01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.p
ng"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" conten
t="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="man
ifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/ma
in.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><nosc
ript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

External References

- Netlify Official Website

CLASSIFICATION

SANS Top 25	200
CAPEC	224
WASC	45
ISO27001	A.18.1.3

8. Email Address Disclosure

INFORMATION ⓘ | 1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

8.1. https://main--taupe-shortbread-314b46.netlify.app/static/js/main.c1d7921f.js

Email Address(es)

- chupurnov@gmail.com

Certainty

Request

```
GET /static/js/main.c1d7921f.js HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://main--taupe-shortbread-314b46.netlify.app/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1434.954 **Total Bytes Received :** 2217877 **Body Length :** 2217430 **Is Compressed :** No

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Netlify
Vary: Accept-Encoding
X-Nf-Request-Id: 01HBRA29K4Z982J63J58BSZJQV
Age: 68016
Accept-Ranges: bytes
Etag: "25985edaaf4135aa4d77cf7feb1fdd8a-ssl-df"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: application/javascript; charset=UTF-8
Content-Encoding:
Date: Mon, 02 Oct 2023 13:43:27 GMT
Cache-Control: public,max-age=0,
…
sertInto:void 0};n(6)(r,o),r.locals&&(e.exports=r.locals)},function(e,t,n){(t=n(5)(!1)).push([e.i,'/*!
\n * jodit - Jodit is awesome and usefully wysiwyg editor with filebrowser\n * Author: Chupurnov <chupu
rnov@gmail.com> (https://xdsoft.net/)\n * Version: v3.19.3\n * Url: https://xdsoft.net/jodit/\n * Licen
se(s): MIT\n */\n\t.jodit-wysiwyg{outline:0}.jodit-wysiwyg ::-moz-selection, .jodit-wysiwyg::-moz-selec
tion{bac
…
```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- [Wikipedia - Email Spam](https://en.wikipedia.org/wiki/Email_spam)

CLASSIFICATION

SANS Top 25	200
CAPEC	118
WASC	13
OWASP Proactive Controls	C7
ISO27001	A.9.4.1

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

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

9. File Upload Functionality Detected

INFORMATION ⓘ | 1   CONFIRMED | 1

Netsparker detected file upload functionality, which allows users to upload files to the web server.

Upload forms are generally dangerous, unless they are coded with a great deal of care. If there is any other vulnerability identified regarding this resource, Netsparker will report it as a separate issue.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

9.1. https://main--taupe-shortbread-314b46.netlify.app/

CONFIRMED

Input Name

- fileType

Form target action

- https://main--taupe-shortbread-314b46.netlify.app/products

Request

```
GET / HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 374.929 **Total Bytes Received** : 993 **Body Length** : 612 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 612
X-Nf-Request-Id: 01HBR9ZZQK574C5MF893APYYXH
Age: 69249
Accept-Ranges: bytes
Etag: "61eb810e6d5a6bc66e66af1509d6a757-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/html; charset=UTF-8
Date: Mon, 02 Oct 2023 13:42:11 GMT
Cache-Control: public,max-age=0,must-revalidate

<!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="shortcut icon" href="./favicon.p
ng"><meta name="viewport" content="width=device-width,initial-scale=1"/><meta name="theme-color" conten
t="#000000"/><meta name="description" content="Web site created using create-react-app"/><link rel="man
ifest" href="/manifest.json"/><title>Coloration Colombo</title><script defer="defer" src="/static/js/ma
in.c1d7921f.js"></script><link href="/static/css/main.b230abf7.css" rel="stylesheet"></head><body><nosc
ript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

CLASSIFICATION

OWASP Proactive Controls	C4
ISO27001	A.8.1.1

10. Robots.txt Detected

INFORMATION ⓘ 1 CONFIRMED 1

Netsparker detected a `Robots.txt`file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

10.1. https://main--taupe-shortbread-314b46.netlify.app/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- Disallow:

Request

```
GET /robots.txt HTTP/1.1
Host: main--taupe-shortbread-314b46.netlify.app
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 77.4449 **Total Bytes Received :** 448 **Body Length :** 67 **Is Compressed :** No

```
HTTP/1.1 200 OK
Server: Netlify
Content-Length: 67
X-Nf-Request-Id: 01HBRA2B9Q3N5SRBE2Y0F5YMMH
Age: 68019
Accept-Ranges: bytes
Etag: "f2aabe7591e806d63f2cb3bf38b8b8d8-ssl"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-Type: text/plain; charset=UTF-8
Date: Mon, 02 Oct 2023 13:43:29 GMT
Cache-Control: public,max-age=0,must-revalidate

# https://www.robotstxt.org/robotstxt.html
User-agent:*
Disallow:
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.
`Robots.txt`is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag`can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag`you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag`resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf`or an `.htaccess`file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

External References

- What Content Is Not Crawled? - Google
- How Search organizes information
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Content Security Policy,
Content-Type Sniffing,
Cookie,

Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,
Mixed Content,
Open Redirection,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,
Web Cache Deception,
WebDAV,
Windows Short Filename,
XML External Entity,

<table>
<tr><td></td><td></td><td>XML External Entity (Out of Band)</td></tr>
<tr><td><b>URL Rewrite Mode</b></td><td>:</td><td>Heuristic</td></tr>
<tr><td><b>Detected URL Rewrite Rule(s)</b></td><td>:</td><td>None</td></tr>
<tr><td><b>Excluded URL Patterns</b></td><td>:</td><td>(log|sign)\-?(out|off)
exit
endsession
gtm\.js
WebResource\.axd
ScriptResource\.axd</td></tr>
<tr><td><b>Authentication</b></td><td>:</td><td>None</td></tr>
<tr><td><b>Scheduled</b></td><td>:</td><td>No</td></tr>
<tr><td><b>Additional Website(s)</b></td><td>:</td><td>https://www.main--taupe-shortbread-314b46.netlify.app/</td></tr>
</table>

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com