detectify

VULNERABILITY REPORT

cloudfield.be

Scan Started

2021-12-06T19:01:01+00:00

Scan Finished

2021-12-06T21:39:57+00:00

Your findings

Your scan was completed with the following findings discovered.

High	Medium	Low	Information
1	3	2	14

Listed below are your most recent findings, with the most severe listed first. To improve your threat score, prioritise these top issues.

Severity	Issue Type	Times found
HIGH	Request Smuggling	1
MEDIUM	Cookie is not set to be HttpOnly	1
MEDIUM	X-Frame-Options / Missing Header (Cross-Origin Pixel Stealing)	2
LOW	Cookie lack Secure flag	2
INFORMATION	Fingerprinted Software	1
INFORMATION	Deprecated Security Header / X-XSS-Protection	1
INFORMATION	Remote Administration Portal	1
INFORMATION	Content-Security-Policy / Missing Header	5
INFORMATION	HTML Comments	2
INFORMATION	Discovered Host	1
INFORMATION	Crawled URL's	1
INFORMATION	Lacking DMARC Policy	1
INFORMATION	Service Providers	1

1 Request Smuggling

Summary

What does this mean?

Request smuggling vulnerabilities are often critical in nature, allowing an attacker to bypass security controls, gain unauthorized access to sensitive data, and directly compromise other application users.

What can happen?

HTTP request smuggling is a technique for interfering with the way a web site processes sequences of HTTP requests that are received from one or more users.

Found at	CVSS Score
1.1 https://cloudfield.be/	6.8

1.1 Request Smuggling

Summary

Found at

https://cloudfield.be/

CVSS Score

6.8

Request URL

https://cloudfield.be/

Command

python3 smuggler.py -m 'badwrap' -u 'https://cloudfield.be/'

References

PORTSWIGGER - HTTP Request Smuggling	https://portswigger.net/web-security/request-smuggling
PORTSWIGGER - HTTP Desync Attacks: Request Smuggling Reborn	https://portswigger.net/research/http-desync-attacks-request-smuggling-reborn
GITHUB - smuggler.py	https://github.com/gwen001/pentest-tools/blob/master/smuggler.py
MISC - Help you understand HTTP Smuggling in one article	https://blog.zeddyu.info/2019/12/08/HTTP-Smuggling-en/
MISC - HTTP Request Smuggling – 5 Practical Tips	https://honoki.net/2020/02/18/http-request-smuggling-5-practical-tips/

Method: CL:TE1|badwrap
Status: 405
Time: 9797ms

```
POST / HTTP/1.1
 Transfer-Encoding: chunked
Host: cloudfield.be
User-Agent: Mozilla/5.0 (compatible; Detectify)
+https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a
Accept: */*
Accept-Language: en-US,en;q=0.5
```

Content-Type: application/x-www-form-urlencoded
Connection: close
Cookie: XSRF-TOKEN=eyJpdiI6IjBGSHpteEhRQkFSOUVwR1lhU3Y5Qmc9PSIsInZhbHVlIjoid0VYdCtCa1QwS3dIODJFUlhmNjFZOWdpVERHZjBYVTAvUjlIZGs4MDNPd3RsbldyYU9VSk14SjdhVHRYZHgwejdwWU9XcHNOM2RKUlh0Wm94MGNyNUx4TDQvR3VBcnduNnBza1Y5Sk9tKzhSam5UNXBabjFiT3M1d1hzSU0vdmEiLCJtYWMiOiIzNTVjOWRlODkxMTNiYjc1MDYxOGU0ZGIyMjJmNTFkYjMwODI3NGMxYTVhOGQwODY0YTYxNjQ4ODRiOGEwMzg5IiwidGFnIjoiIn0%3D; binary_beasts_session=eyJpdiI6Im5yZkNHMk11bTFTSlpuUytXeUtoUUE9PSIsInZhbHVlIjoiVU1aZmluYnQrSjREU2h6STZQcFRpL0xUZWE4YjZqME9OWVYvV0tlNExXRzhMQVp4N3lTU1kwVURCOFkwMENrcVd3czZRaUdJbUJCZ2MrTEY5SDhlZUZyOUhwa0tyQVJEeWN6TStBRkdKTUNjSHM0MTl5bEpQazRpbnh6YkJnai8iLCJtYWMiOiJkMmUzYTY0MmYzOTU0OWI0NjliMTY5NGI0ZTFkOTgxMTYzMzZjOWVkYzcyODhjOTJlMzcyYzUxZjZkMjRjMzZkIiwidGFnIjoiIn0%3D
Content-Length: 5
Foo: bar

1
Z
Q

2 Cookie is not set to be HttpOnly

Summary

What does this mean?

If an attacker discovers an XSS he may use it to steal cookies which haven't got the HttpOnly-flag.

What can happen?

One or more cookies lack the HttpOnly flag.

Read more at [https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies|our knowledge base].

Found at		CVSS Score
2.1	cloudfield.be	4.3

2.1 Cookie is not set to be HttpOnly

Summary

Found at

cloudfield.be

CVSS Score

4.3

Vulnerable Cookie

XSRF-TOKEN

Cookie

Name	XSRF-TOKEN
Value	eyJpdiI6IktrMDVLY0pOU1pqSGNwYzFWZ0dFdUE9PSIsInZhbHVlIjoiSWdCOUNlZ3NnSHRiM1l5dTBjWWZGUC9Jc05kZHVZb3hycVh1UzVHVElwcm1LZ0M0bEczVktRVWFQV3RvU0Rhdkk2MXVEYldER0tvTE9SWmhBSXFKR3I1c0ZZNzE1RUkyak9rWHpoUUJJNWhFL1pXY0lUQkI1V3RyU2ZWaXU5V1ciLCJtYWMiOiI0OTQxMzFmNzZlMGQ3NmQwNjg3YWNiYmY4OWIyNGEyMDNiNmI4ZGEzOTNiNDJhMjMwYmU3ZWUzYzEzZWUzMWY4IiwidGFnIjoiIn0%3D
Domain	cloudfield.be
Path	/
Secure	No
HttpOnly	No
Expires	2021-12-06T21:21:16.000Z

References

DETECTIFY - Detectify Support Center - Missing HttpOnly flag on cookies	https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

3 X-Frame-Options / Missing Header (Cross-Origin Pixel Stealing)

Summary

What does this mean?

With a carefully crafted combination of stylesheets and iframes, an attacker can read pixels from cross-origin iframes using an OCR-style technique to obtain potentially sensitive data from the website.

What can happen?

Cross-Origin Pixel Stealing is a technique where an attacker abuse an iframe and CSS to be able to read each pixel inside of the iframe to determine the text.

Found at		CVSS Score
3.1	https://cloudfield.be/js/app.js	4.3
3.2	https://cloudfield.be/css/app.css	4.3

3.1 X-Frame-Options / Missing Header (Cross-Origin Pixel Stealing)

Summary

Found at

https://cloudfield.be/js/app.js

CVSS Score

4.3

Request URL

https://cloudfield.be/js/app.js

Missing Response Header

X-Frame-Options = SAMEORIGIN

Missing Response Header

Content-Security-Policy = frame-ancestors 'none'

Request Headers

GET /js/app.js HTTP/1.1

Referer	
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

content-length	726588
content-type	application/javascript; charset=utf-8
date	Mon, 06 Dec 2021 20:08:04 GMT
last-modified	Mon, 15 Nov 2021 19:50:59 GMT
server	nginx/1.20.0
accept-ranges	bytes
etag	"6192ba23-b163c"

References

STACKEXCHANGE - Security Headers for a web API	https://security.stackexchange.com/questions/147554/security-headers-for-a-web-api#answer-147559:~:text=Yet%2C%20as%20there%20are%20advanced%20attacks,want%20to%20leave%20that%20header%20there.
MISC - Bad timing: New HTML5 trickery lets hackers silently spy on browsers	https://www.theregister.com/2013/08/05/html5_timing_attacks/
MISC - Pixel Perfect Timing Attacks with HTML5 [PDF]	https://paper.bobylive.com/Meeting_Papers/BlackHat/USA-2013/US-13-Stone-Pixel-Perfect-Timing-Attacks-with-HTML5-WP.pdf
BLACKHAT - Pixel Perfect Timing Attacks with HTML5	https://www.youtube.com/watch?v=KcOQfYlyIqw
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

If other legitimate websites have frames going to cloudfield.be, then use an "ALLOW-FROM"-directive instead of a "SAMEORIGIN"-directive.

3.2 X-Frame-Options / Missing Header (Cross-Origin Pixel Stealing)

Summary

Found at

https://cloudfield.be/css/app.css

CVSS Score

4.3

Request URL

https://cloudfield.be/css/app.css

Missing Response Header

X-Frame-Options = SAMEORIGIN

Missing Response Header

Content-Security-Policy = frame-ancestors 'none'

Request Headers

GET /css/app.css HTTP/1.1

Referer	
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

last-modified	Mon, 15 Nov 2021 19:50:59 GMT
server	nginx/1.20.0
accept-ranges	bytes
etag	"6192ba23-ac7a"
content-length	44154
content-type	text/css
date	Mon, 06 Dec 2021 20:08:04 GMT

References

STACKEXCHANGE - Security Headers for a web API	https://security.stackexchange.com/questions/147554/security-headers-for-a-web-api#answer-147559:~:text=Yet%2C%20as%20there%20are%20advanced%20attacks,want%20to%20leave%20that%20header%20there.
MISC - Bad timing: New HTML5 trickery lets hackers silently spy on browsers	https://www.theregister.com/2013/08/05/html5_timing_attacks/
MISC - Pixel Perfect Timing Attacks with HTML5 [PDF]	https://paper.bobylive.com/Meeting_Papers/BlackHat/USA-2013/US-13-Stone-Pixel-Perfect-Timing-Attacks-with-HTML5-WP.pdf
BLACKHAT - Pixel Perfect Timing Attacks with HTML5	https://www.youtube.com/watch?v=KcOQfYlyIqw
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

If other legitimate websites have frames going to cloudfield.be, then use an "ALLOW-FROM"-directive instead of a "SAMEORIGIN"-directive.

4 Cookie lack Secure flag

Summary

What does this mean?

On successful exploitation of session cookies, the attacker will be able to set the cookies in his own browser and gain the same privileges as the attacked user. The impact for none-session based cookies varies between systems.

What can happen?

The cookie(s) lack the Secure-flag attribute. An attacker can force the cookie(s) to be sent over plain text HTTP, and can therefor intercept the content.

Read more [https://support.detectify.com/support/solutions/articles/48001048982-cookie-lack-secure-flag|here].

Found at		CVSS Score
4.1	cloudfield.be	2.7
4.2	cloudfield.be	2.7

4.1 Cookie lack Secure flag

Summary

Found at

cloudfield.be

CVSS Score

2.7

Vulnerable Cookie

XSRF-TOKEN

Cookie

Name	XSRF-TOKEN
Value	eyJpdiI6IktrMDVLY0pOU1pqSGNwYzFWZ0dFdUE9PSIsInZhbHVlIjoiSWdCOUNlZ3NnSHRiM1l5dTBjWWZGUC9Jc05kZHVZb3hycVh1UzVHVElwcm1LZ0M0bEczVktRVWFQV3RvU0Rhdkk2MXVEYldER0tvTE9SWmhBSXFKR3I1c0ZZNzE1RUkyak9rWHpoUUJJNWhFL1pXY0lUQkI1V3RyU2ZWaXU5V1ciLCJtYWMiOiI0OTQxMzFmNzZlMGQ3NmQwNjg3YWNiYmY4OWIyNGEyMDNiNmI4ZGEzOTNiNDJhMjMwYmU3ZWUzYzEzZWUzMWY4IiwidGFnIjoiIn0%3D
Domain	cloudfield.be
Path	/
Secure	No
HttpOnly	No
Expires	2021-12-06T21:21:16.000Z

References

OWASP - Secure Cookie Attribute	https://owasp.org/www-community/controls/SecureCookieAttribute
PORTSWIGGER - SSL cookie without secure flag set	https://portswigger.net/KnowledgeBase/issues/Details/00500200_SSLcookiewithoutsecureflagset
MISC - Securing Cookies with HttpOnly and secure Flags	http://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/

4.2 Cookie lack Secure flag

Summary

Found at

cloudfield.be

CVSS Score

2.7

Vulnerable Cookie

binary_beasts_session

Cookie

Name	binary_beasts_session
Value	eyJpdiI6IjQwekhuK1hFSXFjU1c4WkVENWlkNkE9PSIsInZhbHVlIjoiZlVTVkRzUDkxMXNRelZDdTRhbVUzWjd3UzEzMzQ1ajN3TG41Vm9FZEJxUmVRZktzb0VOblBmRkg2dGJ5VXU0OWRESDFxWm9LWXdOeDlaS2E2b2ZKVDNQWWxlNGdTTkVSU2lnSVd3RE5haWt3cHZzdW41SytTOExPUWpuWk9pQVoiLCJtYWMiOiJjNjA0YTYzYjQ5NWJlMGNjZWRlZGQzYmMxMzRiYjE4ZjhjZGRiODBkYTY2N2QzMTMxZDNhZDU4YjhiYjcxNGU4IiwidGFnIjoiIn0%3D
Domain	cloudfield.be
Path	/
Secure	No
HttpOnly	Yes
Expires	2021-12-06T21:21:16.000Z

References

OWASP - Secure Cookie Attribute	https://owasp.org/www-community/controls/SecureCookieAttribute
PORTSWIGGER - SSL cookie without secure flag set	https://portswigger.net/KnowledgeBase/issues/Details/00500200_SSLcookiewithoutsecureflagset
MISC - Securing Cookies with HttpOnly and secure Flags	http://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/

5 Fingerprinted Software

Summary

What does this mean?

Invalid fingerprints may cause a audit to take longer, and the lack of fingerprints may cause Detectify to miss running specific tests.

What can happen?

When Detectify audits an application, it collects various fingerprints that indicate what software is running. These fingerprints then allow Detectify to run specific tests when the time is right.

Please make sure Detectify provide accurate data for these fingerprints, by sending us a message in the feedback form on the finding details page.

Found at		CVSS Score
5.1	cloudfield.be	0

5.1 Fingerprinted Software

Summary

Found at

cloudfield.be

CVSS Score

0

References

DETECTIFY - An intelligent way to look for vulnerabilities	https://blog.detectify.com/2016/01/28/an-intelligent-way-to-look-for-vulnerabilities/
DETECTIFY - What's under the hood	https://detectify.com/technology

Vendor: amazon
Software: elb
Confidence: 100

Vendor: amazon
Software: waf
Confidence: 100

Software: php
Version: 8.0.8
Confidence: 100

6 Deprecated Security Header

Summary

What does this mean?

It may be possible to do some client side attacks that was assumed to be mitigated.

What can happen?

We found a security header that is no longer maintained (or supported) by most modern browsers. This may cause you to believe a certain attack vector is mitigated, while it offer no real protection in practice.

Found at		CVSS Score
6.1	https://cloudfield.be/	0

6.1 Deprecated Security Header / X-XSS-Protection

Summary

Found at

https://cloudfield.be/

CVSS Score

0

Request URL

https://cloudfield.be/

Request Headers

GET / HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a
Host	cloudfield.be
Cookie	XSRF-TOKEN=eyJpdiI6InFoTUNsaUJ4S2I0cWFXalJKWXJheGc9PSIsInZhbHVlIjoiMjNMczUxR2o4eWR2SWEzZDVBbkFaWllmVU1ibFBOcDlMYWhBWDlDdmYrNkVrZGxGVjRFcWlPQTBxOG1JeE5DUEs4dkRNR3FyN1Z0VjI5MVFQMUoxR1N5RXgzK1Y2V0wxMUlwOHEzOUJ6a1BZUU5YbmFiM1lxYit5OHRLZTBSSXgiLCJtYWMiOiJiZjM2ODc3NTg4OTc1ZmI5ZTIxY2U3MjRhZTRlNjRmOTEwZTVkNzU1MThhZDU2Njk4MTZkMWEwM2M5Y2JjMTU1IiwidGFnIjoiIn0%3D; binary_beasts_session=eyJpdiI6IlYyRzg3aW5QTE5rUXA2S1Y3cE05ZWc9PSIsInZhbHVlIjoia3FaN3NiWERuU0t2V0FRcHRVVngvL2lPVkpzRTBNNzJUOXJtVGRHcCtGTTlPeEY5aTNSL0k3RkFjNmlreHc5d2VTS0tSY01ZMmx5elhkMnB5R2lmdVg1dmp2MlB3ZEd3eDFpRkcxOWpQcXJKWk5wYU02RlF0Q0U4Nm9EUHJoWVkiLCJtYWMiOiI3MWE5Nzg4NDI5MTYwMDk2ZjdiNmRkYTRmNmIwMTdjZjExZWQ1YTAyN2RkOTJjYmEyNDM0OTdlODdlYWMxZDQwIiwidGFnIjoiIn0%3D
Cache-Control	no-store, no-cache
Pragma	no-cache
Accept-Encoding	gzip, deflate

Response Headers

HTTP/1.1 302 Found

Transfer-Encoding	chunked

Connection	keep-alive
Permissions-Policy	accelerometer=(self), ambient-light-sensor=(self), autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self), display-capture=(self), document-domain=*, encrypted-media=(self), execution-while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*, publickey-credentials-get=(self), screen-wake-lock=(self), sync-xhr=*, usb=(self), web-share=(self), xr-spatial-tracking=(self)
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload
X-Content-Type-Options	nosniff
X-Download-Options	noopen
X-Frame-Options	sameorigin
X-Permitted-Cross-Domain-Policies	none
X-XSS-Protection	1; mode=block
Referrer-Policy	no-referrer
Cache-Control	no-cache, private
Content-Type	text/html; charset=UTF-8
Date	Mon, 06 Dec 2021 20:22:17 GMT
Location	https://cloudfield.be/login
Set-Cookie	XSRF-TOKEN=eyJpdiI6IjgvZUo4NnZ6UERid0dQSlBYZmlOYWc9PSIsInZhbHVlIjoicEpyQUdhTVVyR3BmQW51WE1QOEQ2dXlGZGt2QytyN2o5RnVwOGdPQlJSMHlWaGM0NzZBd3RSZ1BCaVhvU0NEdnhDdGlkQ0c2YWFPZ1JNV05JWlNRcys3OGNPQnU3SkRBQVVRblVaR1MxZ3MxZnplazZkN2pDM1V0Vnkva053NGEiLCJtYWMiOiJkZDY1YTY1YTg3OGVkNTlkM2U2ZGNhYmI0ZWNkZjAxY2MxNTIxNzI2MWNjMGMzZjc2MTg2Yzc5Y2JjMTVjZjgzIiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 22:22:17 GMT; Max-Age=7200; path=/; samesite=lax,binary_beasts_session=eyJpdiI6IlVLSjAzR1dZK2NwL3J2cmpUcFhpZWc9PSIsInZhbHVlIjoiL3J6bCtXRDNFMDdNVHZPczNhUVpEN3hxOGI1ZHZpZGZrS3Y2SGc2ZytrUkRETWdNay9EMkZ2amxVdVlVVTZ3dVBRdWRkUDR2LytoL3JLY3hiM0EvdEQ5bit0UGNsY1gvUVlPMFZPRkVaSTczRG9sek40ek5zTzIrVlZtV1l2OU8iLCJtYWMiOiIyYjcyN2Y1NDg1YzI5M2UxZmIzZTFmNWNmNmVmZjkyZmQwM2NjY2UxNTk5M2U1YjgzOTRkNzgzOWE0NGI2ODUwIiwidGFnIjoiIn0%3D; expires=Mon, 06-Dec-2021 22:22:17 GMT; Max-Age=7200; path=/; httponly; samesite=lax
Server	nginx/1.20.0
X-Powered-By	PHP/8.0.8

References

OWASP - X-XSS-Protection	https://owasp.org/www-project-secure-headers/#x-xss-protection

DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

The X-XSS-Protection header has been deprecated by modern browsers and its use can introduce additional security issues on the client side. As such, it is recommended to set the header as X-XSS-Protection: 0 in order to disable the XSS Auditor, and not allow it to take the default behavior of the browser handling the response. Please use Content-Security-Policy instead.

7 Remote Administration Portal

Summary

What can happen?

A remote administration interface has been found.

Read more about the issue
[https://support.detectify.com/support/solutions/articles/48001048975-remote-administration-portal|here].

Found at		CVSS Score
7.1	https://cloudfield.be/login	0

7.1 Remote Administration Portal

Summary

Found at

https://cloudfield.be/login

CVSS Score

0

Request URL

https://cloudfield.be/login

Request Headers

GET /login HTTP/1.1

Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

x-content-type-options	nosniff
x-download-options	noopen
x-frame-options	sameorigin
x-xss-protection	1; mode=block
content-type	text/html; charset=UTF-8
server	nginx/1.20.0
permissions-policy	accelerometer=(self), ambient-light-sensor=(self), autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self), display-capture=(self), document-domain=*, encrypted-media=(self), execution-while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*, publickey-credentials-get=(self), screen-wake-lock=(self), sync-xhr=*, usb=(self), web-share=(self), xr-spatial-tracking=(self)
strict-transport-security	max-age=31536000; includeSubDomains; preload
referrer-policy	no-referrer
date	Mon, 06 Dec 2021 20:11:31 GMT

x-powered-by	PHP/8.0.8
cache-control	no-cache, private
x-permitted-cross-domain-policies	none

References

DETECTIFY - Detectify Support Center - Remote Administration Portal	https://support.detectify.com/support/solutions/articles/48001048975-remote-administration-portal

8 Invalid Header Value

Summary

What does this mean?

Browsers may interpret this in different ways, and may open up for undefined behaviors.

What can happen?

The header contain an undefined policy.

Found at		CVSS Score
8.1	https://cloudfield.be/register	0
8.2	https://cloudfield.be/forgot-password	0
8.3	https://cloudfield.be/login	0
8.4	https://cloudfield.be/js/app.js	0
8.5	https://cloudfield.be/css/app.css	0

8.1 Content-Security-Policy / Missing Header

Summary

Found at

https://cloudfield.be/register

CVSS Score

0

Request URL

https://cloudfield.be/register

Missing Response Header

Content-Security-Policy-Report-Only = 'your-policy-goes-here-to-check-that-it-works'

Missing Response Header

Content-Security-Policy = 'your-policy-goes-here-when-you-want-to-enforce-it'

Request Headers

GET /register HTTP/1.1

Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

content-type	text/html; charset=UTF-8
server	nginx/1.20.0
strict-transport-security	max-age=31536000; includeSubDomains; preload
x-content-type-options	nosniff
x-download-options	noopen
x-permitted-cross-domain-policies	none
x-xss-protection	1; mode=block
referrer-policy	no-referrer
date	Mon, 06 Dec 2021 20:09:25 GMT
x-powered-by	PHP/8.0.8

cache-control	no-cache, private
permissions-policy	accelerometer=(self), ambient-light-sensor=(self), autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self), display-capture=(self), document-domain=*, encrypted-media=(self), execution-while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*, publickey-credentials-get=(self), screen-wake-lock=(self), sync-xhr=*, usb=(self), web-share=(self), xr-spatial-tracking=(self)
x-frame-options	sameorigin

References

MISC - Content Security Policy Reference	https://content-security-policy.com/
OWASP - Content Security Policy Cheat Sheet	https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
GOOGLE - Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
MOZILLA - Content Security Policy	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
WIKIPEDIA - Content Security Policy	https://en.wikipedia.org/wiki/Content_Security_Policy
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security. Before setting a CSP policy it can help to first set a CSP-report-only policy to detect any issues first.

8.2 Content-Security-Policy / Missing Header

Summary

Found at

https://cloudfield.be/forgot-password

CVSS Score

0

Request URL

https://cloudfield.be/forgot-password

Missing Response Header

Content-Security-Policy-Report-Only = 'your-policy-goes-here-to-check-that-it-works'

Missing Response Header

Content-Security-Policy = 'your-policy-goes-here-when-you-want-to-enforce-it'

Request Headers

GET /forgot-password HTTP/1.1

Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

server	nginx/1.20.0
permissions-policy	accelerometer=(self), ambient-light-sensor=(self), autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self), display-capture=(self), document-domain=*, encrypted-media=(self), execution-while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*, publickey-credentials-get=(self), screen-wake-lock=(self), sync-xhr=*, usb=(self), web-share=(self), xr-spatial-tracking=(self)
strict-transport-security	max-age=31536000; includeSubDomains; preload
x-content-type-options	nosniff

x-permitted-cross-domain-policies	none
x-xss-protection	1; mode=block
referrer-policy	no-referrer
content-type	text/html; charset=UTF-8
x-powered-by	PHP/8.0.8
cache-control	no-cache, private
x-download-options	noopen
x-frame-options	sameorigin
date	Mon, 06 Dec 2021 20:09:55 GMT

References

MISC - Content Security Policy Reference	https://content-security-policy.com/
OWASP - Content Security Policy Cheat Sheet	https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
GOOGLE - Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
MOZILLA - Content Security Policy	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
WIKIPEDIA - Content Security Policy	https://en.wikipedia.org/wiki/Content_Security_Policy
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security. Before setting a CSP policy it can help to first set a CSP-report-only policy to detect any issues first.

8.3 Content-Security-Policy / Missing Header

Summary

Found at

https://cloudfield.be/login

CVSS Score

0

Request URL

https://cloudfield.be/login

Missing Response Header

Content-Security-Policy-Report-Only = 'your-policy-goes-here-to-check-that-it-works'

Missing Response Header

Content-Security-Policy = 'your-policy-goes-here-when-you-want-to-enforce-it'

Request Headers

GET /login HTTP/1.1

Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

x-content-type-options	nosniff
x-download-options	noopen
x-frame-options	sameorigin
x-xss-protection	1; mode=block
content-type	text/html; charset=UTF-8
server	nginx/1.20.0

permissions-policy	accelerometer=(self), ambient-light-sensor=(self), autoplay=(self), battery=(self), camera=(self), cross-origin-isolated=(self), display-capture=(self), document-domain=*, encrypted-media=(self), execution-while-not-rendered=*, execution-while-out-of-viewport=*, fullscreen=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), midi=(self), navigation-override=(self), payment=(self), picture-in-picture=*, publickey-credentials-get=(self), screen-wake-lock=(self), sync-xhr=*, usb=(self), web-share=(self), xr-spatial-tracking=(self)
strict-transport-security	max-age=31536000; includeSubDomains; preload
referrer-policy	no-referrer
date	Mon, 06 Dec 2021 20:11:31 GMT
x-powered-by	PHP/8.0.8
cache-control	no-cache, private
x-permitted-cross-domain-policies	none

References

MISC - Content Security Policy Reference	https://content-security-policy.com/
OWASP - Content Security Policy Cheat Sheet	https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
GOOGLE - Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
MOZILLA - Content Security Policy	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
WIKIPEDIA - Content Security Policy	https://en.wikipedia.org/wiki/Content_Security_Policy
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security. Before setting a CSP policy it can help to first set a CSP-report-only policy to detect any issues first.

8.4 Content-Security-Policy / Missing Header

Summary

Found at

https://cloudfield.be/js/app.js

CVSS Score

0

Request URL

https://cloudfield.be/js/app.js

Missing Response Header

Content-Security-Policy-Report-Only = 'your-policy-goes-here-to-check-that-it-works'

Missing Response Header

Content-Security-Policy = 'your-policy-goes-here-when-you-want-to-enforce-it'

Request Headers

GET /js/app.js HTTP/1.1

Referer	
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

content-length	726588
content-type	application/javascript; charset=utf-8
date	Mon, 06 Dec 2021 20:08:04 GMT
last-modified	Mon, 15 Nov 2021 19:50:59 GMT
server	nginx/1.20.0
accept-ranges	bytes
etag	"6192ba23-b163c"

References

MISC - Content Security Policy Reference https://content-security-policy.com/

OWASP - Content Security Policy Cheat Sheet	https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
GOOGLE - Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
MOZILLA - Content Security Policy	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
WIKIPEDIA - Content Security Policy	https://en.wikipedia.org/wiki/Content_Security_Policy
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security. Before setting a CSP policy it can help to first set a CSP-report-only policy to detect any issues first.

8.5 Content-Security-Policy / Missing Header

Summary

Found at

https://cloudfield.be/css/app.css

CVSS Score

0

Request URL

https://cloudfield.be/css/app.css

Missing Response Header

Content-Security-Policy-Report-Only = 'your-policy-goes-here-to-check-that-it-works'

Missing Response Header

Content-Security-Policy = 'your-policy-goes-here-when-you-want-to-enforce-it'

Request Headers

GET /css/app.css HTTP/1.1

Referer	
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/ad480570137996a4678887929762a0d6d3d0f39a

Response Headers

HTTP/1.1 200

last-modified	Mon, 15 Nov 2021 19:50:59 GMT
server	nginx/1.20.0
accept-ranges	bytes
etag	"6192ba23-ac7a"
content-length	44154
content-type	text/css
date	Mon, 06 Dec 2021 20:08:04 GMT

References

MISC - Content Security Policy Reference https://content-security-policy.com/

OWASP - Content Security Policy Cheat Sheet	https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
GOOGLE - Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
MOZILLA - Content Security Policy	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
WIKIPEDIA - Content Security Policy	https://en.wikipedia.org/wiki/Content_Security_Policy
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a cross-site Scripting (XSS) attack, then the CSP can mitigate the flaw. By not implementing CSP you will be missing out on this layer of security. Before setting a CSP policy it can help to first set a CSP-report-only policy to detect any issues first.

9 HTML Comments

Summary

What does this mean?

The snippets of code within comments will remain inactive until you remove the comment brackets. The comments might also contain sensitive information not meant for the public.

What can happen?

HTML comments, used to store temporary code written by the developers, are visible to the public. Read more at our [https://support.detectify.com/support/solutions/articles/48001048959-html-comments|knowledge base].

Found at		CVSS Score
9.1	https://cloudfield.be/login	0
9.2	https://cloudfield.be/js/app.js	0

9.1 HTML Comments

Summary

Found at

https://cloudfield.be/login

CVSS Score

0

Request URL

https://cloudfield.be/login

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

9.2 HTML Comments

Summary

Found at

https://cloudfield.be/js/app.js

CVSS Score

0

Request URL

https://cloudfield.be/js/app.js

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

10 Discovered Host(s)

Summary

What can happen?

Detectify has found the following hosts. This is in no way a vulnerability, but should be considered an indicator for what has been covered.

Read more [https://support.detectify.com/support/solutions/articles/48001048970-discovered-endpoint|here].

Found at		CVSS Score
10.1	cloudfield.be	0

10.1 Discovered Host

Summary

Found at

cloudfield.be

CVSS Score

0

Detectify found and tried to access 1 domain, and have analyzed it for security flaws.

cloudfield.be:
> 3.248.105.58
80/tcp http open
443/tcp https open
443/tcp http open
81/tcp closed
444/tcp closed
2181/tcp closed
2375/tcp closed
2376/tcp closed
3000/tcp closed
3001/tcp closed
3128/tcp closed
3790/tcp closed
4443/tcp closed
4444/tcp closed
4567/tcp closed
4848/tcp closed
5432/tcp closed
5858/tcp closed
5984/tcp closed
5985/tcp closed
5986/tcp closed
6443/tcp closed
7001/tcp closed
7077/tcp closed
8000/tcp closed

8001/tcp closed
8009/tcp closed
8047/tcp closed
8069/tcp closed
8080/tcp closed
8081/tcp closed
8083/tcp closed
8088/tcp closed
8089/tcp closed
8100/tcp closed
8181/tcp closed
8443/tcp closed
8444/tcp closed
8500/tcp closed
8880/tcp closed
8888/tcp closed
9000/tcp closed
9001/tcp closed
9002/tcp closed
9080/tcp closed
9090/tcp closed
9418/tcp closed
9443/tcp closed
11211/tcp closed
16686/tcp closed
50000/tcp closed
50013/tcp closed
50014/tcp closed

> 52.214.34.61
80/tcp http open
443/tcp https open
443/tcp http open
81/tcp closed
444/tcp closed
2181/tcp closed
2375/tcp closed
2376/tcp closed
3000/tcp closed
3001/tcp closed
3128/tcp closed
3790/tcp closed
4443/tcp closed

4444/tcp closed
4567/tcp closed
4848/tcp closed
5432/tcp closed
5858/tcp closed
5984/tcp closed
5985/tcp closed
5986/tcp closed
6443/tcp closed
7001/tcp closed
7077/tcp closed
8000/tcp closed
8001/tcp closed
8009/tcp closed
8047/tcp closed
8069/tcp closed
8080/tcp closed
8081/tcp closed
8083/tcp closed
8088/tcp closed
8089/tcp closed
8100/tcp closed
8181/tcp closed
8443/tcp closed
8444/tcp closed
8500/tcp closed
8880/tcp closed
8888/tcp closed
9000/tcp closed
9001/tcp closed
9002/tcp closed
9080/tcp closed
9090/tcp closed
9418/tcp closed
9443/tcp closed
11211/tcp closed
16686/tcp closed
50000/tcp closed
50013/tcp closed
50014/tcp closed

11 Crawled URL's

Summary

What does this mean?

A scan might take too long due to representative content on the application. Vulnerabilities may also be missed if Detectify lack coverage in some area of the application. If you suspect Detectify can perform better, then take a look at the associated CSV.

What can happen?

This finding is generated for debugging purposes. A link is associated with this finding containing a CSV file with all crawled URL's.

Found at	CVSS Score
11.1 cloudfield.be	0

11.1 Crawled URL's

Summary

Found at

cloudfield.be

CVSS Score

0

References

DETECTIFY - Download Crawled URL's CSV	https://s3-eu-west-1.amazonaws.com/dtfy.crawl/dca4dc9678a39877bc0397cada945a23/ad480570137996a4678887929762a0d6d3d0f39a/91b82511-c0dd-4b0e-a86a-3af907eee7d2/cloudfield.be-20211206 2011-crawl.csv

Detectify tried to access 12 URL's, 8 of these were identified as unique during crawling and went through further testing.

12 Lacking DMARC Policy

Summary

What does this mean?

An attacker will be able to spoof emails originating from any subdomain having either an A, AAAA or MX record. In most clients, this is possible regardless of whether SPF policies are in place.

What can happen?

The domain lacks a DMARC policy.

Read more in [https://support.detectify.com/support/solutions/articles/48001048963-missing-insufficient-dmarc-record|our knowledge base].

Found at	CVSS Score
12.1 _dmarc.cloudfield.be	0

12.1 Lacking DMARC Policy

Summary

Found at

_dmarc.cloudfield.be

CVSS Score

0

Command

nslookup.exe -type=TXT _dmarc.cloudfield.be

References

DETECTIFY - Detectify Support Center - Missing/insufficient DMARC record	https://support.detectify.com/support/solutions/articles/48001048963-missing-insufficient-dmarc-record
DETECTIFY - Misconfigured email servers open the door to spoofed emails from top domains	https://blog.detectify.com/2016/06/20/misconfigured-email-servers-open-the-door-to-spoofed-emails-from-top-domains/
DETECTIFY - How to identify a phishing email	https://blog.detectify.com/2016/10/20/how-to-identify-a-phishing-email/
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

Consider adding a DMARC policy on _dmarc.cloudfield.be and set the directive "p" to "reject".

13 Service Providers

Summary

What does this mean?

Anyone can retrieve this data. It's only here to serve as an indicator of what vendors have access to.

What can happen?

The listed providers are authorized to host different parts of your infrastructure.

Read more [https://support.detectify.com/support/solutions/articles/48001048980-service-providers|here].

Found at		CVSS Score
13.1	cloudfield.be	0

13.1 Service Providers

Summary

Found at

cloudfield.be

CVSS Score

0

References

DETECTIFY - Detectify Support Center - Service Providers	https://support.detectify.com/support/solutions/articles/48001048980-service-providers

Amazon AWS

Amazon AWS