



10/13/2020 12:59:07 AM (UTC-08:00)

Detailed Scan Report

<https://heybuddy.cf/>

Scan Time : 10/13/2020 12:13:27 AM (UTC-08:00)
Scan Duration : 00:00:45:39
Total Requests : 13,759
Average Speed : 5.0r/s

Risk Level:
MEDIUM

15
IDENTIFIED

5
CONFIRMED

0
CRITICAL

0
HIGH

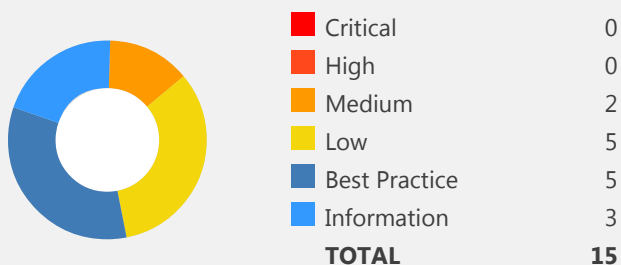
2
MEDIUM

5
LOW

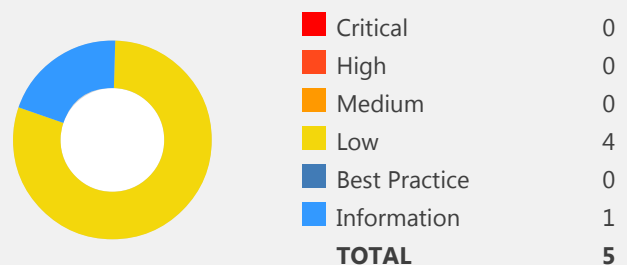
5
BEST PRACTICE

3
INFORMATION































Identified Vulnerabilities



Confirmed Vulnerabilities



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
 	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://heybuddy.cf/	
 	SSL/TLS Not Implemented	GET	https://heybuddy.cf/	
 	[Possible] Cross-site Request Forgery	GET	https://heybuddy.cf/	
 	Cookie Not Marked as HttpOnly	GET	https://heybuddy.cf/	
 	Cookie Not Marked as Secure	GET	https://heybuddy.cf/	
 	Insecure Frame (External)	GET	https://heybuddy.cf/	
 	Internal Server Error	POST	https://heybuddy.cf/cdn-cgi/challenge-platform/h/g/generate/ov1/0.5590507158990875:1602571552:fef027055796fa7bc60a72f9f87e96cdde38ba4732e77c1d52f43aec8a90faf9/5e17422bbd3a3329/fe6564ab979041d	
 	Content Security Policy (CSP) Not Implemented	GET	https://heybuddy.cf/	
 	Expect-CT Not Enabled	GET	https://heybuddy.cf/cdn-cgi/styles/cf.errors.css	
 	Missing X-XSS-Protection Header	GET	https://heybuddy.cf/	
 	Referrer-Policy Not Implemented	GET	https://heybuddy.cf/	
 	SameSite Cookie Not Implemented	GET	https://heybuddy.cf/	
 	Expect-CT in Report Only Mode	GET	https://heybuddy.cf/	
 	Web Application Firewall Detected	GET	https://heybuddy.cf/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED
 	Forbidden Resource	GET	https://heybuddy.cf/	

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM



1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, <http://example.com/some/page/> will be modified to <https://example.com/some/page/> before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

1.1. <https://heybuddy.cf/>

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 2094.0462 Total Bytes Received : 13088 Body Length : 12157 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e174358bce33328-CDG

cf-request-id: 05c2686b7300003328b118d200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573260"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=dc7cb98938cc194c4435978043222b3d21602573259; expires=Thu, 12-Nov-20 07:14:19 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:14:19 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # Further Configuration goes here
    [...]
</VirtualHost>
```

External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)



CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	523
CAPEC	217
WASC	4
ISO27001	A.14.1.2

2. SSL/TLS Not Implemented

MEDIUM  1

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

2.1. <https://heybuddy.cf/>

Certainty



Request			
[NETSPARKER] SSL Connection			
Response			
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No			
[NETSPARKER] SSL Connection			

Remedy

We suggest that you implement SSL/TLS properly, for example by using [the Certbot tool](#) provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	311
CAPEC	217
WASC	4
HIPAA	164.306
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

3. [Possible] Cross-site Request Forgery

LOW



1

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

3.1. <https://heybuddy.cf/>

Form Action(s)

- /?__cf_chl_captcha_tk__=ceea7d82a0008dd289eaf92446b9a430e9cb2d97-1602573211-0-AZtMuvukB3BhpeWkoDuyb6oFMKUewxdXsnu-KxNJLWcOPQPwyO82F1JIU7cdg5qohK57ttfXKQcj_HyOaYbDKwm05Rh5YDAEGvFDpVxi18Fd7ZRxAu6LhnhJo1j9OIGAmioZmPSb4Vi5Y29Gw266M2XUFRGE2ikCLZTwDiaJLGy8kXbo1lQHd0jAIXJCSyXqJ5Ym-GalFRTb4_B_1AY-HMLI-XaP5ddSovJwFghi4Es2-QrWC-ngxENZbFLrxSN6MBb5_3N8f5rMoPFuNp-I0y3cBHeQbFILJ03q4_Rfg1YkYnbIIgiUNsi_RRFCVBj7UpC7xOHZlefV7dEMUKoTOwUfqVG4RZQ9Ln-iyAK8WQ-tBvR99GOBS6hb4EpUaHFKAMv_me1OLB7S9Wd0gJKobPEsL6QLHNkfa17Hpg4TGUqXJwuVs8VwoAMPsfWcnK87bTAv-GytYHD-Tb-4DABueb3klki0w

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
 - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();  
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

a. individual request

```
$.ajax({  
  url: 'foo/bar',  
  headers: { 'x-my-custom-header': 'some value' }  
});
```

b. every request

```
$.ajaxSetup({  
  headers: { 'x-my-custom-header': 'some value' }  
});  
OR  
$.ajaxSetup({  
  beforeSend: function(xhr) {  
    xhr.setRequestHeader('x-my-custom-header', 'some value');  
  }  
});
```

External References

- [OWASP Cross-Site Request Forgery \(CSRF\)](#)

Remedy References

- [OWASP Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](#)



CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
SANS Top 25	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ISO27001	A.14.2.5

4. Cookie Not Marked as HttpOnly

LOW



1

CONFIRMED



1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

4.1. <https://heybuddy.cf/>

CONFIRMED

Identified Cookie(s)

- cf_chl_1
- cf_chl_prog
- cf_chl_rc_i

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```


Actions to Take


- 1. See the remedy for solution.
- 2. Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as [XSS Tunnel](#) to bypass HTTPOnly protection.

External References

- [Netsparker - Security Cookies - HTTPOnly Flag](#)
- [OWASP HTTPOnly Cookies](#)
- [MSDN - ASP.NET HTTPOnly Cookies](#)

 CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
CAPEC	107
WASC	15
ISO27001	A.14.2.5

5. Cookie Not Marked as Secure

LOW



1

CONFIRMED



1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

5.1. <https://heybuddy.cf/>

CONFIRMED

Identified Cookie(s)

- cf_chl_1
- cf_chl_prog
- cf_chl_rc_i

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- [Netsparker - Security Cookies - Secure Flag](#)
 - [.NET Cookie.Secure Property](#)
 - [How to Create Totally Secure Cookies](#)
-



CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	614
CAPEC	102
WASC	15
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

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

6. Insecure Frame (External)

LOW



1

CONFIRMED



1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- allow-same-origin will not treat it as a unique origin.
- allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- allow-forms will allow form submissions from inside the iframe.
- allow-popups will allow popups.
- allow-scripts will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

6.1. https://heybuddy.cf/

CONFIRMED

Frame Source(s)

- https://assets.hcaptcha.com/captcha/v1/0d0e5c3/static/hcaptcha-checkbox.html?id=0bvboq5oys4&host=heybuddy.cf&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptch8bfa-4fc9-8ee5-9c91c6276dff
- https://assets.hcaptcha.com/captcha/v1/0d0e5c3/static/hcaptcha-challenge.html?id=0bvboq5oys4&host=heybuddy.cf&sentry=true&reportapi=https%3A%2F%2Faccounts.hcaptcha.com&recaptch8bfa-4fc9-8ee5-9c91c6276dff

Parsing Source

- DOM Parser

Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of seamlessattribute and allow-top-navigation, allow-popupsand allow-scriptsin sandbox attribute.

External References

- [HTML5 Security Cheat Sheet](#)

Remedy References

- [How to Safeguard your Site with HTML5 Sandbox](#)
- [Play safely in sandboxed IFrames](#)



CLASSIFICATION

OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

7. Internal Server Error

LOW



1

CONFIRMED



1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

7.1. <https://heybuddy.cf/cdn-cgi/challenge-platform/h/g/generate/ov1/0.5590507158990875:1602571552:fef027055796fa7bc60a72f9f87e96cdde38ba4732e77c1d52f43aec8a90faf9/5e17422bbd3a3329/fe6564ab979041d>

CONFIRMED

Method	Parameter	Value
POST	v_5e17422bbd3a3329	expr 268409241 - 27791;

Request

POST /cdn-cgi/challenge-platform/h/g/generate/ov1/0.5590507158990875:1602571552:fef027055796fa7bc60a72f9f87e96cdd38ba4732e77c1d52f43aec8a90faf9/5e17422bbd3a3329/fe6564ab979041d HTTP/1.1

Host: heybuddy.cf

Accept: */*

Accept-Encoding: gzip, deflate

Accept-Language: en-us,en;q=0.5

Cache-Control: no-cache

CF-Challenge: fe6564ab979041d

Content-Length: 44

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

Cookie: cf_chl_seq_fe6564ab979041d=5a5272058afc58e; __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; PHPSESSID=d62f875a79f9461f8eee37c381318c1a; access=1; ad-con=%7B%26quot%3Bdate%26quot%3B%3A%26quot%3B2020-10-13%26quot%3B%2C%26quot%3Bads%26quot%3B%3A%5B%5D%7D; mode=day; src=1; _us=1602660165; cf_chl_cc_LxWScetPgMvD=wZVmhrkmQe; cf_chl_prog=e; cf_chl_rc_i=150

Origin: https://heybuddy.cf

Referer: https://heybuddy.cf/

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

v_5e17422bbd3a3329=expr+268409241+--+27791%3b

Response

Response Time (ms) : 7858.1541 Total Bytes Received : 577 Body Length : 8 Is Compressed : No

HTTP/1.1 500 Internal Server Error

cf-request-id: 05c280aa5d000006c1ce1d2200000001

NEL: {"report_to":"cf-nel","max_age":604800}

CF-RAY: 5e176a23ccaa06c1-LHR

Server: cloudflare

Connection: keep-alive

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=21&lkg-time=1602574849"}],"group":"cf-nel","max_age":604800}

Content-Length: 8

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Content-Type: text/plain; charset=UTF-8

Date: Tue, 13 Oct 2020 07:40:48 GMT

Vary: Accept-Encoding

Invalid.

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.



CLASSIFICATION

SANS Top 25	550
WASC	13
ISO27001	A.14.1.2

8. 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

8.1. <https://heybuddy.cf/>

Certainty

Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```


Actions to Take

- Enable CSP on your website by sending the Content-Security-Policyin 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-Policyin 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

9. 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 misissued certificates to be used.

Vulnerabilities

9.1. <https://heybuddy.cf/cdn-cgi/styles/cf.errors.css>

Certainty



Request

```
GET /cdn-cgi/styles/cf.errors.css HTTP/1.1
Host: heybuddy.cf
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
Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; cf_chl_rc_i=9; cf_chl_prog=a16
Referer: https://heybuddy.cf/
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) : 1999.2952 Total Bytes Received : 24154 Body Length : 23688 Is Compressed : No

```
HTTP/1.1 200 OK
cf-request-id: 05c268605c0000048f9420f200000001
Server: cloudflare
CF-RAY: 5e174346fc30048f-CDG
Expires: Tue, 13 Oct 2020 09:14:16 GMT
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Last-Modified: Mon, 12 Oct 2020 17:39:39 GMT
Vary: Accept-Encoding
Content-Type: text/css
Transfer-Encoding: chunked
Content-Encoding:
Date: Tue, 13 Oct 2020 07:14:16 GMT
ETag: W/"5f8494db-5c88"
Cache-Control: max-age=7200
Cache-Control: public
```

```
#cf-wrapper a,#cf-wrapper abbr,#cf-wrapper article,#cf-wrapper aside,#cf-wrapper b,#cf-wrapper big,#cf-
wrapper blockquote,#cf-wrapper body,#cf-wrapper canvas,#cf-wrapper caption,#cf-wrapper center,#cf-wrapp
er cite,#cf-wrapper code,#cf-wrapper dd,#cf-wrapper del,#cf-wrapper details,#cf-wrapper dfn,#cf-wrapper
div,#cf-wrapper dl,#cf-wrapper dt,#cf-wrapper em,#cf-wrapper embed,#cf-wrapper fieldset,#cf-wrapper fi
gcaption,#cf-wrapper figure,#cf-wrapper footer,#cf-wrapper form,#cf-wrapper h1,#cf-wrapper h2,#cf-wrapp
er h3,#cf-wrapper h4,#cf-wrapper h5,#cf-wrapper h6,#cf-wrapper header,#cf-wrapper hgroup,#cf-wrapper ht
ml,#cf-wrapper i,#cf-wrapper iframe,#cf-wrapper img,#cf-wrapper label,#cf-wrapper legend,#cf-wrapper l
i,#cf-wrapper mark,#cf-wrapper menu,#cf-wrapper nav,#cf-wrapper object,#cf-wrapper ol,#cf-wrapper outpu
t,#cf-wrapper p,#cf-wrapper pre,#cf-wrapper s,#cf-wrapper samp,#cf-wrapper section,#cf-wrapper small,#c
f-wrapper span,#cf-wrapper strike,#cf-wrapper strong,#cf-wrapper sub,#cf-wrapper summary,#cf-wrapper su
p,#cf-wrapper table,#cf-wrapper tbody,#cf-wrapper td,#cf-wrapper tfoot,#cf-wrapper th,#cf-wrapper thea
d,#cf-wrapper tr,#cf-wrapper tt,#cf-wrapper u,#cf-wrapper ul{margin:0;padding:0;border:0;font:inherit;f
ont-size:100%;text-decoration:none;vertical-align:baseline}#cf-wrapper a img{border:none}#cf-wrapper ar
ticle,#cf-wrapper aside,#cf-wrapper details,#cf-wrapper figcaption,#cf-wrapper figure,#cf-wrapper foote
r,#cf-wrapper header,#cf-wrapper hgroup,#cf-wrapper menu,#cf-wrapper nav,#cf-wrapper section,#
...
```

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 enforce mode. 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

10. Missing X-XSS-Protection Header

BEST PRACTICE

💡

1

Netsparker detected a missing X-XSS-Protectionheader 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

10.1. <https://heybuddy.cf/>

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

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

11. 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

11.1. <https://heybuddy.cf/>

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

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	<u>A6</u>
OWASP 2017	<u>A3</u>
SANS Top 25	<u>200</u>
ISO27001	<u>A.14.2.5</u>

12. SameSite Cookie Not Implemented

BEST PRACTICE



1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

12.1. <https://heybuddy.cf/>

Identified Cookie(s)

- cf_chl_1
- cf_chl_prog
- cf_chl_rc_i

Cookie Source

- JavaScript

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```

Remedy

The server can set a same-site cookie by adding the SameSite=...attribute to the Set-Cookieheader. There are three possible values for the SameSiteattribute:

- Lax:In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with SameSite=Nonemust also specify the Secureattribute to transfer them via a secure context. Setting a SameSite=Nonecookie without the Secureattribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- [Security Cookies - SameSite Attribute - Netsparker](#)
- [Using the Same-Site Cookies Attribute to Prevent CSRF Attacks](#)
- [Same-site Cookies](#)
- [Preventing CSRF with the same-site cookie attribute](#)
- [SameSite cookies explained](#)
- [Get Ready for New SameSite=None; Secure Cookie Settings](#)



CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

13. Expect-CT in Report Only Mode

INFORMATION ⓘ

1

Netsparker identified that Expect-CT is in **report only mode**. The optional **enforced** directive controls whether the browser should drop the connection when the policy is violated.

Impact

When Expect-CT policy is deployed in **report only mode** and the user agent does not receive a valid Certificate Transparency Log, rather than dropping the connection it will simply send a report to the specified endpoint which is set with **report-uri** directive.

Vulnerabilities

13.1. <https://heybuddy.cf/>

Certainty



Request

```
GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT

Content-Encoding:

```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

```
<!--[if gte IE 10]><!-->
```

```
<
```

```
...
```



Remedy

Use enforce flag in definition of Expect-CT.

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

External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)
- [Expect-CT Header](#)

 CLASSIFICATION	
OWASP Proactive Controls	C9
ISO27001	A.14.1.2

14. Forbidden Resource

INFORMATION



1

CONFIRMED



1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

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

Vulnerabilities

14.1. <https://heybuddy.cf/>

CONFIRMED

Request

GET / HTTP/1.1
Host: heybuddy.cf
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) : 1399.9188 Total Bytes Received : 13129 Body Length : 12198 Is Compressed : No

HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

CF-RAY: 5e17422bbd3a3329-CDG

cf-request-id: 05c267af5600003329de348200000001

Transfer-Encoding: chunked

Server: cloudflare

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573211"}],"group":"cf-nel","max_age":604800}

CF-Chl-Bypass: 1

Connection: close

Expires: Thu, 01 Jan 1970 00:00:01 GMT

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Set-Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; expires=Thu, 12-Nov-20 07:13:31 GMT; path=/; domain=.heybuddy.cf; HttpOnly; SameSite=Lax; Secure

Content-Type: text/html; charset=UTF-8

NEL: {"report_to":"cf-nel","max_age":604800}

Date: Tue, 13 Oct 2020 07:13:31 GMT HTTP/1.1 403 Forbidden

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

...



CLASSIFICATION

OWASP Proactive Controls

[C8](#)

ISO27001

[A.8.1.1](#)

15. Web Application Firewall Detected

INFORMATION ⓘ

1

Netsparker detected that the target website is using a Web Application Firewall (WAF).

Impact

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

Vulnerabilities

15.1. https://heybuddy.cf/%3Cscript%3Ealert(0)%3C/script%3E

Method	Parameter	Value
GET	URI-BASED	<script>alert(0)</script>

WAF Name

- Cloudflare

Certainty



Request

GET /%3Cscript%3Ealert(0)%3C/script%3E HTTP/1.1
Host: heybuddy.cf
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
Cookie: __cfduid=d24f5fe1adf7901d3df9a127e65c2de201602573211; cf_chl_rc_i=9; cf_chl_prog=a16
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) : 490.364 Total Bytes Received : 12936 Body Length : 12169 Is Compressed : No

```
HTTP/1.1 403 Forbidden
cf-request-id: 05c2685be90000edffd01fd200000001
Expires: Thu, 01 Jan 1970 00:00:01 GMT
CF-RAY: 5e17433fdc31edff-CDG
CF-Chl-Bypass: 1
Connection: close
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report?lkg-colo=19&lkg-time=1602573256"}],"group":"cf-nel","max_age":604800}
Server: cloudflare
NEL: {"report_to":"cf-nel","max_age":604800}
X-Frame-Options: SAMEORIGIN
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Tue, 13 Oct 2020 07:14:15 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Vary: Accept-Encoding

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Attention Required! | Cloudflare</title>
<meta name="captcha-bypass" id="captcha-bypass" />
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>

<!--[if gte IE 10]><!-->
<script>
if (!navigator.cookieEnabled) {
window.addEventListener('DOMContentLoaded', function () {
var cookieEl = document.getElementById('cookie-alert')
...

```



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,
XML External Entity (Out of Band)

URL Rewrite Mode	: Heuristic
-------------------------	-------------

Detected URL Rewrite Rule(s)	: None
-------------------------------------	--------

Excluded URL Patterns	: (log sign)\-?(out off) exit endsession gtm\.js WebResource\.axd ScriptResource\.axd
------------------------------	--

Authentication	: None
-----------------------	--------

Scheduled	: No
------------------	------

Additional Website(s)	: None
------------------------------	--------
