netsparker

19.08.2022 21:45:02 (UTC+03:00)

Detailed Scan Report

https://www.ecder.net/

Scan Time	: 19.08.2022 20:35:31 (UTC+03:00)
Scan Duration	: 00:00:08:43
Total Requests	: 459
Average Speed	: 0,9r/s

Risk Level:
MEDIUM

14
IDENTIFIED

4
CONFIRMED

0
CRITICAL

0
HIGH

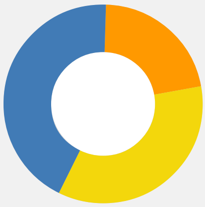
3
MEDIUM

5
LOW

6
BEST PRACTICE

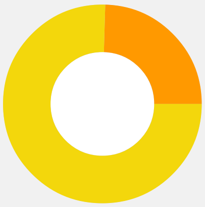
0
INFORMATION

Identified Vulnerabilities



🟥	Critical	0
🟧	High	0
🟧	Medium	3
🟨	Low	5
🟦	Best Practice	6
🟦	Information	0
	TOTAL	**14**

Confirmed Vulnerabilities



🟥	Critical	0
🟧	High	0
🟧	Medium	1
🟨	Low	3
🟦	Best Practice	0
🟦	Information	0
	TOTAL	**4**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
👤 🚩	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.ecder.net/	
👤 🚩	Out-of-date Version (jQuery)	GET	https://www.ecder.net/.well-known/	
👤 🚩	Weak Ciphers Enabled	GET	https://www.ecder.net/	
👤 🚩	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.ecder.net/	
👤 🚩	Missing X-Frame-Options Header	GET	https://www.ecder.net/	
👤 🚩	Cookie Not Marked as HttpOnly	GET	https://www.ecder.net/.well-known/	
👤 🚩	Cookie Not Marked as Secure	GET	https://www.ecder.net/video/arkaplan.mp4	
👤 🚩	Insecure Frame (External)	GET	https://www.ecder.net/.well-known/	
👤 ❗	Content Security Policy (CSP) Not Implemented	GET	https://www.ecder.net/	
👤 ❗	Expect-CT Not Enabled	GET	https://www.ecder.net/	
👤 ❗	Missing X-XSS-Protection Header	GET	https://www.ecder.net/	
👤 ❗	Referrer-Policy Not Implemented	GET	https://www.ecder.net/	
👤 ❗	SameSite Cookie Not Implemented	GET	https://www.ecder.net/.well-known/	
👤 ❗	Subresource Integrity (SRI) Not Implemented	GET	https://www.ecder.net/	

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://www.ecder.net/

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 362,8949 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:54 GMT; Domain=www.ecder.net; Path=/; Htt
pOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:54 GMT
cf-edge-cache: no-cache
Content-Type: text/html
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:54 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Captcha</title>
<link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css"
integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7"
crossorigin="anonymous">
<link href="data:image/x-icon;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAAQEAYAAABPYyMiAAAABmJLR0T///////8JWP
fcAAAACXBIWXMAAABIAAAASABGyWs+AAAAF0lEQVRIx2NgGAWjYBSMglEwCkbBSAcACBAAAeaR9cIAAAAASUVORK5CYII="
rel="icon" type="image/x-icon"/>
<link href="https://fonts.googleapis.com/css?family=Noto+Sans"
rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

<script src="https://www.google.com/recaptcha/api.js?hl=en"
async defer>
</script>


<style>
html, body {
height: 100%;
}

.wraper {
padding-bottom: 56px;
position: relative;
min-height: 100%;
}
.invisible_mode .wraper {
display: none;
```

```
}

.header {
height: 63px;
background-color: white;
}

.middle {
height: 186px;
background-color: rgba(55, 171, 99, 0.75);
}

.bottom {
background-color: #f2f2f
…
```

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. Out-of-date Version (jQuery)

MEDIUM 1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Affected Versions

1.8.0 to 2.2.4

External References

- CVE-2015-9251

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing &lt;option&gt; elements from untrusted sources - even after sanitizing it - to one of jQuery&#39;s DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

- CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery&#39;s DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

External References

- CVE-2020-11022

JQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions

1.0 to 3.3.1

External References

- CVE-2019-11358

Vulnerabilities

2.1. https://www.ecder.net/.well-known/

Identified Version

- 1.12.4

Latest Version

- 1.12.4 (in this branch)

Vulnerability Database

- Result is based on 04/27/2020 15:00:00 vulnerability database content.

Certainty

Request

```
GET /.well-known/ HTTP/1.1
Host: www.ecder.net
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: cl-bypass-cache=yes
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) : 350,7602 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:54 GMT; Domain=www.ecder.net; Path=/; Htt
pOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:54 GMT
cf-edge-cache: no-cache
Content-Type: text/html
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:54 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-ag
…

rel="icon" type="image/x-icon"/>
<link href="https://fonts.googleapis.com/css?family=Noto+Sans"
rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

<script src="https://www.google.com/recaptcha/api.js?hl=en"
async defer>

…
Please, restart captcha server after your changes.
service imunify360-captcha restart
service imunify360-captchaserver-nginx restart

Example:
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
Add your custom css from customize/static/ folder
<link type="text/css" rel="stylesheet" href="static/my.css">
-->
</head>
<body class="invisible_mode">
<div class="wraper">

<!--
You can
…
```

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

- Downloading jQuery

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
SANS Top 25	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

3. Weak Ciphers Enabled

MEDIUM | **1**   **CONFIRMED** | **1**

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

3.1. https://www.ecder.net/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0x00BA)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (0x00C0)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1   **Total Bytes Received** : 27   **Body Length** : 0   **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

   ```
   ssl.honor-cipher-order = "enable"
   ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
   ```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

   ```
   SCHANNEL\Ciphers\DES 56/56
   SCHANNEL\Ciphers\RC4 64/128
   SCHANNEL\Ciphers\RC4 40/128
   SCHANNEL\Ciphers\RC2 56/128
   SCHANNEL\Ciphers\RC2 40/128
   SCHANNEL\Ciphers\NULL
   SCHANNEL\Hashes\MD5
   ```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6,8 (Medium)
Temporal	6,8 (Medium)
Environmental	6,8 (Medium)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	6,8 (Medium)
Temporal	6,8 (Medium)
Environmental	6,8 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

4. [Possible] Phishing by Navigating Browser Tabs

LOW ⚑ 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

4.1. https://www.ecder.net/

External Links

- https://www.discord.gg/ANgyUYMWrn

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received :** 8357 **Body Length :** 7916 **Is Compressed :** No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary:
…
ody>
<tr>
<td>
Lorem
<br />
233
</td>
</tr>
</tbody>
</table>
<div class="sosyal-link">
<a href="https://www.discord.gg/ANgyUYMWrn" target="_blank" >discord.gg/ANgyUYMWrn</a>
</div>
</div>
</div>
</td>

</tr>
</table>
<br /><br /><br /><br /><br /><br /><br/> <br/> <br/>
</main>


<main>
<h2>Referanslarım</
…
```

Remedy

- Add `rel=noopener`to the linksto prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener*property in Chrome and Opera browsers.

- For older browsers and in Firefox, you can add `rel=noreferrer`which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target="_blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

5. 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

5.1. https://www.ecder.net/.well-known/

CONFIRMED

Identified Cookie(s)

- locale

Cookie Source

- JavaScript

Request

```
GET /.well-known/ HTTP/1.1
Host: www.ecder.net
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: cl-bypass-cache=yes
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) : 350,7602 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:54 GMT; Domain=www.ecder.net; Path=/; Htt
pOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:54 GMT
cf-edge-cache: no-cache
Content-Type: text/html
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:54 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Captcha</title>
<link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css"
integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7"
crossorigin="anonymous">
<link href="data:image/x-icon;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAAQEAYAAABPYyMiAAAABmJLR0T///////8JWP
fcAAAACXBIWXMAAABIAAAASABGyWs+AAAAF0lEQVRIx2NgGAWjYBSMglEwCkbBSAcACBAAAeaR9cIAAAAASUVORK5CYII="
rel="icon" type="image/x-icon"/>
<link href="https://fonts.googleapis.com/css?family=Noto+Sans"
rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

<script src="https://www.google.com/recaptcha/api.js?hl=en"
async defer>
</script>


<style>
html, body {
height: 100%;
}

.wraper {
padding-bottom: 56px;
position: relative;
min-height: 100%;
}
.invisible_mode .wraper {
display: none;
```

```
}

.header {
height: 63px;
background-color: white;
}

.middle {
height: 186px;
background-color: rgba(55, 171, 99, 0.75);
}

.bottom {
background-color: #f2f2f
…
```

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 Tunnelto 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

6. 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

6.1. https://www.ecder.net/video/arkaplan.mp4

CONFIRMED

Identified Cookie(s)

- cl-bypass-cache

Cookie Source

- HTTP Header

Request

```
GET /video/arkaplan.mp4 HTTP/1.1
Host: www.ecder.net
Accept: */*
Accept-Encoding: identity;q=1, *;q=0,gzip, deflate
Accept-Language: en-us,en;q=0.5,en-US,en;q=0.9
Cache-Control: no-cache
chrome-proxy: frfr
Referer: https://www.ecder.net/
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) : 593,7346 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:34 GMT; Domain=www.ecder.net; Path=/; HttpOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:34 GMT
cf-edge-cache: no-cache
Content-Type: video/mp4
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:34 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-agHTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:34 GMT; Domain=www.ecder.net; Path=/; HttpOnly; SameSite=Lax

Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:34 GMT
cf-edge-cache: no-cache
Content-Type: video/mp4
Transf
…
```

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

7. 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

7.1. https://www.ecder.net/.well-known/

CONFIRMED

Frame Name(s)

- a-j52u7edkkh9

Sandbox Value(s)

- allow-forms allow-popups allow-same-origin allow-scripts allow-top-navigation allow-modals allow-popups-to-escape-sandbox

Parsing Source

- DOM Parser

Request

```
GET /.well-known/ HTTP/1.1
Host: www.ecder.net
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: cl-bypass-cache=yes
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) : 350,7602 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:54 GMT; Domain=www.ecder.net; Path=/; Htt
pOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:54 GMT
cf-edge-cache: no-cache
Content-Type: text/html
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:54 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Captcha</title>
<link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css"
integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7"
crossorigin="anonymous">
<link href="data:image/x-icon;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAAQEAYAAABPYyMiAAAABmJLR0T///////8JWP
fcAAAACXBIWXMAAABIAAAASABGyWs+AAAAF0lEQVRIx2NgGAWjYBSMglEwCkbBSAcACBAAAeaR9cIAAAAASUVORK5CYII="
rel="icon" type="image/x-icon"/>
<link href="https://fonts.googleapis.com/css?family=Noto+Sans"
rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

<script src="https://www.google.com/recaptcha/api.js?hl=en"
async defer>
</script>


<style>
html, body {
height: 100%;
}

.wraper {
padding-bottom: 56px;
position: relative;
min-height: 100%;
}
.invisible_mode .wraper {
display: none;
```

```
}

.header {
height: 63px;
background-color: white;
}

.middle {
height: 186px;
background-color: rgba(55, 171, 99, 0.75);
}

.bottom {
background-color: #f2f2f
…
```

Remedy

- Apply sandboxing in inline frame

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

- For untrusted content, avoid the usage of `seamless`attribute and `allow-top-navigation`, `allow-popups`and `allow-scripts`in 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

8. Missing X-Frame-Options Header

LOW ⚑ 1

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

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

Impact

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

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

Vulnerabilities

8.1. https://www.ecder.net/

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received** : 8357 **Body Length** : 7916 **Is Compressed** : No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="tr">
<head>
<link rel="icon" href="img/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="styleshee
t">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop playsinline muted></video>
<div class="description">
<h1>
Selam, Ben
<span>Berat Kadir Ecder</span>
</h1>
</div>
</header>





<main>
<h2>Hakkımda</h2>
<table class="hakkimda-tablo">
<tbody>
<tr>
<td>
<h4>Adım Kadir Berat Ecder. 3 Aralık 1998 Erzincan Merkez'de doğdum. Babamın adı Hüseyin, annemin adı N
```

```
urten dir. Bende dahil olmak üzere 3 kardeşiz. İlk, orta ve lise öğrenimimi Erzincan'da tamamladım. 14
 yaşımda tiyatroya olan ilgimi eğitim alarak ilerlettim. Lise olarak İpekyolu Mesleki ve Teknik Anadolu
 Lisesi Bilişim Teknolojileri bölümünü okudum ve 21 Eylül 2018 tarihinde mezun oldum. Mezun olduktan so
nra birkaç sitede editörlük yaptım askerliğimi tamamlamak için editörlüğü ara vermek zorunda kaldım. Ed
irne’nin Keşan ilçesinde 6 ay askerlik yaptım ve askerden döndüğümde bir e ticaret sitesinde web editör
 olarak işe başladım. </h4>
</td>
<td>
<img src="img/Ecder.j
…
```

Remedy

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

External References

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

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

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

9. 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

9.1. https://www.ecder.net/

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received :** 8357 **Body Length :** 7916 **Is Compressed :** No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="tr">
<head>
<link rel="icon" href="img/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="styleshee
t">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop playsinline muted></video>
<div class="description">
<h1>
Selam, Ben
<span>Berat Kadir Ecder</span>
</h1>
</div>
</header>






<main>
<h2>Hakkımda</h2>
<table class="hakkimda-tablo">
<tbody>
<tr>
<td>
<h4>Adım Kadir Berat Ecder. 3 Aralık 1998 Erzincan Merkez'de doğdum. Babamın adı Hüseyin, annemin adı N
```

```
urten dir. Bende dahil olmak üzere 3 kardeşiz. İlk, orta ve lise öğrenimimi Erzincan'da tamamladım. 14
 yaşımda tiyatroya olan ilgimi eğitim alarak ilerlettim. Lise olarak İpekyolu Mesleki ve Teknik Anadolu
 Lisesi Bilişim Teknolojileri bölümünü okudum ve 21 Eylül 2018 tarihinde mezun oldum. Mezun olduktan so
nra birkaç sitede editörlük yaptım askerliğimi tamamlamak için editörlüğü ara vermek zorunda kaldım. Ed
irne’nin Keşan ilçesinde 6 ay askerlik yaptım ve askerden döndüğümde bir e ticaret sitesinde web editör
 olarak işe başladım. </h4>
</td>
<td>
<img src="img/Ecder.j
…
```

Actions to Take

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

Remedy

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

External References

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

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

10. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

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

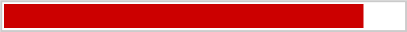
Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve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

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

Vulnerabilities

10.1. https://www.ecder.net/

Certainty



Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received** : 8357 **Body Length** : 7916 **Is Compressed** : No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="tr">
<head>
<link rel="icon" href="img/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="styleshee
t">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop playsinline muted></video>
<div class="description">
<h1>
Selam, Ben
<span>Berat Kadir Ecder</span>
</h1>
</div>
</header>





<main>
<h2>Hakkımda</h2>
<table class="hakkimda-tablo">
<tbody>
<tr>
<td>
<h4>Adım Kadir Berat Ecder. 3 Aralık 1998 Erzincan Merkez'de doğdum. Babamın adı Hüseyin, annemin adı N
```

```
urten dir. Bende dahil olmak üzere 3 kardeşiz. İlk, orta ve lise öğrenimimi Erzincan'da tamamladım. 14
 yaşımda tiyatroya olan ilgimi eğitim alarak ilerlettim. Lise olarak İpekyolu Mesleki ve Teknik Anadolu
 Lisesi Bilişim Teknolojileri bölümünü okudum ve 21 Eylül 2018 tarihinde mezun oldum. Mezun olduktan so
nra birkaç sitede editörlük yaptım askerliğimi tamamlamak için editörlüğü ara vermek zorunda kaldım. Ed
irne'nin Keşan ilçesinde 6 ay askerlik yaptım ve askerden döndüğümde bir e ticaret sitesinde web editör
 olarak işe başladım. </h4>
</td>
<td>
<img src="img/Ecder.j
…
```

Remedy

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

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

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

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

External References

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

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

11. Missing X-XSS-Protection Header

BEST PRACTICE | 1

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

Impact

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

Vulnerabilities

11.1. https://www.ecder.net/

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received :** 8357 **Body Length :** 7916 **Is Compressed :** No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="tr">
<head>
<link rel="icon" href="img/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="styleshee
t">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop playsinline muted></video>
<div class="description">
<h1>
Selam, Ben
<span>Berat Kadir Ecder</span>
</h1>
</div>
</header>





<main>
<h2>Hakkımda</h2>
<table class="hakkimda-tablo">
<tbody>
<tr>
<td>
<h4>Adım Kadir Berat Ecder. 3 Aralık 1998 Erzincan Merkez'de doğdum. Babamın adı Hüseyin, annemin adı N
```

```
urten dir. Bende dahil olmak üzere 3 kardeşiz. İlk, orta ve lise öğrenimimi Erzincan'da tamamladım. 14
 yaşımda tiyatroya olan ilgimi eğitim alarak ilerlettim. Lise olarak İpekyolu Mesleki ve Teknik Anadolu
 Lisesi Bilişim Teknolojileri bölümünü okudum ve 21 Eylül 2018 tarihinde mezun oldum. Mezun olduktan so
nra birkaç sitede editörlük yaptım askerliğimi tamamlamak için editörlüğü ara vermek zorunda kaldım. Ed
irne’nin Keşan ilçesinde 6 ay askerlik yaptım ve askerden döndüğümde bir e ticaret sitesinde web editör
 olarak işe başladım. </h4>
</td>
<td>
<img src="img/Ecder.j
…
```

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

12. 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

12.1. https://www.ecder.net/

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received** : 8357 **Body Length** : 7916 **Is Compressed** : No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000,
 h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="tr">
<head>
<link rel="icon" href="img/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="styleshee
t">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop playsinline muted></video>
<div class="description">
<h1>
Selam, Ben
<span>Berat Kadir Ecder</span>
</h1>
</div>
</header>





<main>
<h2>Hakkımda</h2>
<table class="hakkimda-tablo">
<tbody>
<tr>
<td>
<h4>Adım Kadir Berat Ecder. 3 Aralık 1998 Erzincan Merkez'de doğdum. Babamın adı Hüseyin, annemin adı N
```

```
urten dir. Bende dahil olmak üzere 3 kardeşiz. İlk, orta ve lise öğrenimimi Erzincan'da tamamladım. 14
 yaşımda tiyatroya olan ilgimi eğitim alarak ilerlettim. Lise olarak İpekyolu Mesleki ve Teknik Anadolu
 Lisesi Bilişim Teknolojileri bölümünü okudum ve 21 Eylül 2018 tarihinde mezun oldum. Mezun olduktan so
nra birkaç sitede editörlük yaptım askerliğimi tamamlamak için editörlüğü ara vermek zorunda kaldım. Ed
irne’nin Keşan ilçesinde 6 ay askerlik yaptım ve askerden döndüğümde bir e ticaret sitesinde web editör
 olarak işe başladım. </h4>
</td>
<td>
<img src="img/Ecder.j
…
```

Actions to Take

In a response header:

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

In a META tag

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

In an element attribute

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

or

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

Remedy

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

External References

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

CLASSIFICATION

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

13. 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

13.1. https://www.ecder.net/.well-known/

Identified Cookie(s)

- locale

Cookie Source

- JavaScript

Certainty

Request

```
GET /.well-known/ HTTP/1.1
Host: www.ecder.net
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: cl-bypass-cache=yes
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) : 350,7602 **Total Bytes Received** : 21229 **Body Length** : 20726 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: cl-bypass-cache=yes; Expires=Fri, 19-Aug-22 18:35:54 GMT; Domain=www.ecder.net; Path=/; Htt
pOnly; SameSite=Lax
Server: imunify360-webshield/1.18
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Connection: close
Last-Modified: Friday, 19-Aug-2022 17:35:54 GMT
cf-edge-cache: no-cache
Content-Type: text/html
Transfer-Encoding: chunked
Date: Fri, 19 Aug 2022 17:35:54 GMT
Cache-Control: private, no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0, s-maxage=0

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Captcha</title>
<link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css"
integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7"
crossorigin="anonymous">
<link href="data:image/x-icon;base64,iVBORw0KGgoAAAANSUhEUgAAABAAAAAQEAYAAABPYyMiAAAABmJLR0T///////8JWP
fcAAAACXBIWXMAAABIAAAASABGyWs+AAAAF0lEQVRIx2NgGAWjYBSMglEwCkbBSAcACBAAAeaR9cIAAAAASUVORK5CYII="
rel="icon" type="image/x-icon"/>
<link href="https://fonts.googleapis.com/css?family=Noto+Sans"
rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>

<script src="https://www.google.com/recaptcha/api.js?hl=en"
async defer>
</script>


<style>
html, body {
height: 100%;
}

.wraper {
padding-bottom: 56px;
position: relative;
min-height: 100%;
}
.invisible_mode .wraper {
display: none;
```

```
}

.header {
height: 63px;
background-color: white;
}

.middle {
height: 186px;
background-color: rgba(55, 171, 99, 0.75);
}

.bottom {
background-color: #f2f2f
…
```

Remedy

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

- 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=None`must also specify the `Secure`attribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute 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

14. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

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

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

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

Vulnerabilities

14.1. https://www.ecder.net/

Identified Sub Resource(s)

- https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap

Certainty

Request

```
GET / HTTP/1.1
Host: www.ecder.net
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) : 406,2762 **Total Bytes Received :** 8357 **Body Length :** 7916 **Is Compressed :** No

```
HTTP/1.1 200 OK
Alt-Svc: quic=":443"; ma=2592000; v="39,43,46", h3-Q039=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-23=":443"; ma=2592000, h3-24=":443"; ma=2592000
Server: LiteSpeed
Connection: Keep-Alive
Content-Length: 2062
Last-Modified: Sat, 02 Jul 2022 20:13:32 GMT
Accept-Ranges: bytes
Content-Type: text/html
Content-Encoding:
Date: Fri, 19 Aug 2022 17:35:28 GMT
Vary:
…
/mini-logo.png">
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="preconnect" href="https://fonts.gstatic.com">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@300&display=swap" rel="stylesheet">
<link href="css/default.css" rel="stylesheet" type="text/css" lang="tr"></link>
<title>Ecder</title>
</head>
<body>
<header class="video-header">
<video src="video/arkaplan.mp4" autoplay loop
…
```

Remedy

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

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

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

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

SANS Top 25	16
WASC	15
ISO27001	A.14.2.5

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

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