HTML/SEO III IIII

- 🗆 🗆 🗆
- Owner Key IIII III API III III
- □ □ (<h1>~<h6>)
- aria-label
- lang Ⅲ
- label Ⅲ
- alt □
- Apache 🛮 🖽 🔠
 - ∘ [SECURITY] http header cookie
 - [Security] Content-Security-Policy
 - ∘ [SECURITY] Header [[[[[]]]]

<title> Ⅲ</td></tr><tr><td>• 50~600</td></tr><tr><td>· · · · · · · · · · · · · · · · · · ·</td></tr><tr><td></td></tr><tr><td>• 150~1600</td></tr><tr><td><meta name="robots"> □</td></tr><tr><td></td></tr><tr><td> index / noindex : </td></tr><tr><td><meta name="keywords"> □</td></tr><tr><td></td></tr></tbody></table></title>

• 5~10
<meta charset="utf-8"/> □
<meta name="viewport"/> □
 width=device-width:
<meta property="og:title"/> []
• og:

•
<meta http-equiv="X-UA-Compatible"/> □
Internet Explorer

Owner Key IIII III API III III

Opticalpos | Host | |

• Owner Key: Opticalpos DB .env .env (.env) (

• Main (Host): Opticalpos

• Guest: Eyemsg

	API □ □	□ DВ
Opticalpos	Eyemsg API	Opticalpos DB
Eyemsg	Opticalpos API	Opticalpos DB

Eyemsg Host |

• Owner Key: Eyemsg DB .env .env (

Main (Host): EyemsgGuest: Opticalpos

	ΑΡΙ 🖽 🖽	□ DB
Eyemsg	Opticalpos API	Eyemsg DB
Opticalpos	Eyemsg API	Eyemsg DB

□:

- Host
 ☐ DB ☐☐ Owner Key
 ☐ ☐☐
- Guest□ Owner Key□ □□ Host□ API□ □□
- API III III Host II DB III III

$\Pi \Pi (< h1> \sim < h6>)$

```
\square <h1> ~ <h6>)
• <h2> ~ <h6> | |
 <h1>| | | | | | | </h1>
 <h2>1</h2>
 <h3> 1.1</h3>
 <h2>1 2</h2>
   aria-label III III III
<input type="text" aria-label="Search">
3. | | | | | | | | | | |
aria-label 🛮 🔲 🔲 🔲 🖽 🖽 🖽 .
 <input type="text" aria-label="Phone number">
 <i class="icon-phone"></i>
```

aria-l	label	ПП	ПП	$\Pi\Pi$

1.

<label> aria-label

aria-label 🔲

aria-label Ⅲ Ⅲ Ⅱ Ⅱ

<label> aria-label

1.

aria-label Ⅲ
aria-label
1
<input/> [<label></label>
<input aria-label="Search" type="text"/>
2. ::: :: :: :: :: :: :: :: :: :: :: :: :
aria-label]] [[[[[[[]]]]] [[[]] [[]] [[]] [[]]
3
aria-label
<input aria-label="Phone number" type="text"/> <i class="icon-phone"></i>

lang 📗

		_
DNA		
iana		
	_	_

<html lang="ko-KR">

label III

• [:||| (<|abel>) [| (|abel>) [| (|abel>) || (|abel>)

label <u></u>
<label> </label>
<form> <label for="email">Email Address</label> <input id="email" name="email" type="email"/> </form>
label III III III III III
• []: < abel >]
label IIII IIII III III

alt [
-------	--

alt <u></u>	
alt [
	

- alt IIII IIII IIII IIII III
- [] alt [] alt [] alt="" [].
- _____alt ____alt _____alt ______,



[SECURITY] http header[] cookie

	Ш	Secure III	HttpOnly III
PHPSESSID	PHP [] []		
XSRF-TOKEN	CSRF III III III		
Laravel []:	Laravel [] []		

PHPSESSID[] Secure [[]] [[]

• php.ini 🔲 📗

session.cookie_secure = On

. PHP | | | | |

ini_set('session.cookie_secure', 1);

ini_set('session.cookie_httponly', 1); // HttpOnly
session_start();

• .htaccess ☐☐☐ ☐

php_value session.cookie_secure On php_value session.cookie_httponly On

[Security] Content-Security-Policy

Content-Security-Policy header is not set. It restricts resources the page can load and prevents XSS attacks.

seo III III III III III III III IIII.

44

Content-Security-Policy(CSP)<a>□?

- 1. XSS(||| ||| ||||)
 - □□□ □ JavaScript □□□ □□□□.
- 2. | | | | | | | |
 - □ □ (URL, CSS, □ □) □ □ □ □ □ □
- 3. Clickjacking
 - ☐ iframe ☐ ☐ ☐ ☐ ☐.

44

Content-Security-Policy | | | | |

- •



Apache III III CSP III
Apache[Content-Security-Policy .htaccess .httpd.conf , apache2.conf)
<pre><ifmodule mod_headers.c=""> Header set Content-Security-Policy "default-src 'self'; script-src 'self' https://www.googletagmanager.com https://d3js.org https://cdnjs.cloudflare.com https://cdn.jsdelivr.net 'unsafe-inline' 'unsafe-eval'; style-src 'self' https://fonts.googleapis.com https://cdn.jsdelivr.net 'unsafe-inline'; font-src 'self' https://fonts.gstatic.com https://cdn.jsdelivr.net data:; connect-src 'self' https://www.google-analytics.com; img-src 'self' data: https://cdn.jsdelivr.net;" </ifmodule></pre>
default-src 'self'
self
unsafe-inline
unsafe-eval
eval() [setTimeout(string) [] [] [] [].
data:

* [[[]] 500 server error [[]] [[]].

2. [[[]] [[]] [[]

- 1. app/Http/Middleware \square class \square \square \square .
- 2. [____] handle function[] [_____]. \$csp [_] [_] [_] [_] [_] [____].

```
public function handle(Request $request, Closure $next)
{
    $response = $next($request);

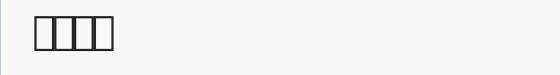
    $csp = "default-src 'self'; " .
    "script-src 'self' https://www.googletagmanager.com https://d3js.org https://cdnjs.cloudflare.com
https://cdn.jsdelivr.net 'unsafe-inline' 'unsafe-eval'; " .
    "style-src 'self' https://fonts.googleapis.com https://cdn.jsdelivr.net 'unsafe-inline'; " .
    "font-src 'self' https://fonts.gstatic.com https://cdn.jsdelivr.net data:; " .
    "connect-src 'self' https://www.google-analytics.com; " .
    "img-src 'self' data: https://cdn.jsdelivr.net;";

$response->headers->set('Content-Security-Policy', $csp);

return $response;
}
```

3. app/Http/Kernel.php [] [] [] [].

```
protected $middleware = [ \App\Http\Middleware\ContentSecurityPolicy::class, ];
```



- nonce [hash | CSP | III | III | IIII | IIIII | IIII | IIIII | IIII | IIIII | IIII | IIIII | IIII | IIII

Nonce ☐ ☐ (☐)

∏∏ nonce ∏∏∏∏∏.

- apache Ⅲ

Header set Content-Security-Policy "default-src 'self'; script-src 'self' https://www.googletagmanager.com https://d3js.org https://cdnjs.cloudflare.com 'nonce-abc123'; style-src 'self' https://fonts.googleapis.com https://cdn.jsdelivr.net 'unsafe-inline'; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://api.example.com; img-src 'self' data:;"

- script ⅢⅢ

<script nonce="abc123"> console.log('Inline script with nonce'); </script>

- Ⅲ Nonce Ⅲ

```
<?php
// php + javascript
$nonce = base64_encode(random_bytes(16));
header("Content-Security-Policy: script-src 'self' 'nonce-$nonce'");
?>
<script nonce="<?php echo $nonce; ?>">
console.log('This script uses a nonce');
</script>
```

```
<script>
// only javascript
// Generate a random nonce
const array = new Uint8Array(16);
```

```
window.crypto.getRandomValues(array);
const nonce = btoa(String.fromCharCode.apply(null, array));

// Set the Content-Security-Policy header
const meta = document.createElement('meta');
meta.setAttribute('http-equiv', 'Content-Security-Policy');
meta.setAttribute('content', `script-src 'self' 'nonce-${nonce}'`);
document.head.appendChild(meta);

// Dynamically create a script element with the nonce
const script = document.createElement('script');
script.setAttribute('nonce', nonce);
script.textContent = "console.log('This script uses a nonce')";
document.body.appendChild(script);
</script>
```

[SECURITY] Header [[[[]]

Header	OK	Notice	Warning	Critical Recommendation	
X-Frame-Option	s	0 0	77	0 X-Frame-Options header is not set.	
			It prev	ents clickjacking attacks when	
			set to	deny' or 'sameorigin.'	
X-Content-Type	-Opt	ions			
0	0	77	0	C-Content-Type-Options header is not set.	
			It stop	s MIME type sniffing and mitigates	
			conte	t type attacks.	
Referrer-Policy	0	0	77 0	Referrer-Policy header is not set.	
			It con	rols referrer header sharing and	
			enhar	ces privacy and security.	
Feature-Policy	0	0	77 0	Feature-Policy header is not set.	
			It allo	s enabling/disabling browser APIs	
			and fe	atures for security. Not important	
			if Perr	sissions-Policy is set.	
Permissions-Pol	icy	0 0	77	O Permissions-Policy header is not set.	
			It allo	s enabling/disabling browser APIs	
			and fe	atures for security.	
Server	0	0	77 0	Server header is set to known 'Apache.'	
			It is be	tter not to reveal used technologies.	
Set-Cookie	70	65	70 0	Set-Cookie header for 'PHPSESSID' does not	
			have '	SameSite' flag. Consider using	
			'Same	Site=Strict' or 'SameSite=Lax.'	
			Set-Co	okie header for 'XSRF-TOKEN' does not	
			have '	HttpOnly' flag. Attacker can steal	
			the co	okie using XSS. Consider using	

'HttpOnly' when cookie is not used by JavaScript.
"X-Frame-Options
X-Frame-Options III IIII II. X:
Apache
DENY: iframe . SAMEORIGIN:
"X-Content-Type-Options
X-Content-Type-Options III IIII II.
: Apache
Header always set X-Content-Type-Options "nosniff"

Referrer-Policy

□ :
Referrer-Policy
Apache [] [] [] []:
Header always set Referrer-Policy "no-referrer"
 no-referrer: [] [] []. strict-origin, strict-origin-when-cross-origin, same-origin [].
Feature-Policy / Permissions-Policy
: □:
• Feature-Policy Permissions-Policy
<u> </u>
Apache [] [] [] []:
Header always set Permissions-Policy "geolocation=(), camera=(), microphone=()"
 Permissions-Policy: [] [] [] [] []. [] geolocation, camera, microphone [].

Server

• Server III Apache IIII III III IIII.
Apache
ServerTokens Prod
ServerSignature Off
Header unset Server
 ServerTokens Prod:
"Set-Cookie
• SameSite [HttpOnly []].
Apache [] [] []:
Header always edit Set-Cookie ^(.*)\$ "\$1; SameSite=Strict; HttpOnly; Secure"
• SameSite=Strict:
HttpOnly: JavaScript□ □ □ □.
• Secure: HTTPS [[[[]] [[]] []].



X-Frame-Options □
Header always set X-Frame-Options "DENY"
X-Content-Type-Options □
Header always set X-Content-Type-Options "nosniff"
Referrer-Policy □
Header always set Referrer-Policy "no-referrer"
Permissions-Policy
Header always set Permissions-Policy "geolocation=(), camera=(), microphone=()"
Server III III
ServerTokens Prod
ServerSignature Off
Header unset Server
Set-Cookie [] [
Header always edit Set-Cookie ^(.*)\$ "\$1; SameSite=Strict; HttpOnly; Secure"