

[Security] Content-Security-Policy

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

seo 000 00 00 00000 0000 00 0000 000000.

“

Content-Security-Policy(CSP)?

CSP HTTP 00 00 0 000, 00000 0000 00 00000 0000 0 0000 00000 00 0000 0000.

00 00 000 00 00 0000 000 0 00000:

1. **XSS**(0000 0000 0000)
0000 00 JavaScript 00000 00 00000.
2. 0000 00 00
00 0000(URL, CSS, 00 0) 0000 00000.
3. **Clickjacking**
00 iframe 00 00 00000.

“

Content-Security-Policy 0000 00

CSP 0000 0000 00 0000 0000 0 00000:

- 00000000000000000000 00000
- 00000 00000 00000 00 00 00.
- HTTPS 000000 0000 0000 HTTP 00000 0000 0000.

🔒 🌐: Content-Security-Policy 🌐 🌐

Apache 🌐 🌐 CSP 🌐

Apache🌐Content-Security-Policy 🌐.htaccess 🌐httpd.conf, apache2.conf)🌐 🌐 🌐 🌐 🌐.

```
<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>
```

default-src 'self'

🌐 🌐 🌐 🌐 🌐 (🌐, 🌐, 🌐)🌐 🌐 🌐 🌐.

self

🌐 🌐 🌐 🌐 🌐 🌐.

unsafe-inline

🌐 🌐 🌐 (🌐 🌐 🌐).

unsafe-eval

eval() 🌐setTimeout(string) 🌐 🌐 🌐 🌐.

data:

🌐 URI🌐 🌐 🌐, 🌐 🌐 🌐 🌐.

* 500 server error가 발생함.

2. Content Security Policy (CSP)

1. app/Http/Middleware에 class를 생성함.
2. handle function을 생성함. \$csp 값을 설정함.

```
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.php에 등록함.

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



Content Security Policy

- `unsafe-inline` allows inline scripts, which is not recommended.
- `nonce` and `hash` are used to specify a unique key for the CSP. The key is generated and used to hash the content of the script.

Nonce (key)

The nonce is a unique key generated for each script.

- apache

```
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

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

- PHP Nonce

```
<?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>
```

Revision #2

Created 17 December 2024 02:17:17 by 

Updated 26 December 2024 06:14:10 by 