[Security] Content-Security-Policy

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

seo 진단시 위와 같은 진단내용이 잡힌다면 아래 내용들을 확인해주세요.

> ## **Content-Security-Policy(CSP)란?**

CSP는 HTTP 응답 헤더 중 하나로, 브라우저가 페이지에 어떤 리소스를 로드할 수 있는지 제어하는 보안 정책을 정의합니다.
이를 통해 아래와 같은 보안 위협을 방지할 수 있습니다:

1. **XSS(크로스 사이트 스크립팅)**
   공격자가 악성 JavaScript를 주입하는 것을 방지합니다.
2. 데이터 주입 공격
   악성 리소스(URL, CSS, 폰트 등)의 로드를 제한합니다.
3. **Clickjacking**
   악성 iframe 삽입 등을 방지합니다.

> ## **Content-Security-Policy**가 중요한 이유

CSP가 없으면 다음과 같은 문제가 발생할 수 있습니다:

- 외부에서 [illegible]를 주입하여 사
- 비인가된 리소스가 로드되어 정보 유출 가능.
- HTTPS 환경에서도 보안이 취약한 HTTP 리소스가 로드될 가능성.

□□ □□: 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 error□ □□□ □ □□□□.

2. □□□□□ □□□□ □□ (□□□ □□)

1. app/Http/Middleware□ □□□ class□ □□□□□.

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, ];
```

□□□

□□□ □□□□ □□

- [unsafe-inline]□ □□□ □ □□□, □□ □□□ □□□□ □□ □□□□.
- nonce [hash] □□ CSP□ □□□□ □□ □□□□□ □□□□□ □□□□ □□ □□□□.

Nonce□ □□ (□□)

□□ □□□ nonce □□□ □□ □□□□□□□.

- 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>
```

- □□ 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 □□□