[SECURITY] Header □□□□□

Header	OK	Notice	Warning	Critical	Recommendation
X-Frame-Options	0	0	77	0	X-Frame-Options header is not set. It prevents clickjacking attacks when set to 'deny' or 'sameorigin.'
X-Content-Type-Options	0	0	77	0	X-Content-Type-Options header is not set. It stops MIME type sniffing and mitigates content type attacks.
Referrer-Policy	0	0	77	0	Referrer-Policy header is not set. It controls referrer header sharing and enhances privacy and security.
Feature-Policy	0	0	77	0	Feature-Policy header is not set. It allows enabling/disabling browser APIs and features for security. Not important if Permissions-Policy is set.
Permissions-Policy	0	0	77	0	Permissions-Policy header is not set. It allows enabling/disabling browser APIs and features for security.
Server	0	0	77	0	Server header is set to known 'Apache.' It is better not to reveal used technologies.
Set-Cookie	70	65	70	0	Set-Cookie header for 'PHPSESSID' does not have 'SameSite' flag. Consider using 'SameSite=Strict' or 'SameSite=Lax.'
					Set-Cookie header for 'XSRF-TOKEN' does not have 'HttpOnly' flag. Attacker can steal the cookie using XSS. Consider using 'HttpOnly' when cookie is not used by JavaScript.

> “
> # X-Frame-Options

문제:

- X-Frame-Options 헤더가 설정되지 않음.

해결:

Apache 설정 파일에 다음을 추가:

```
Header always set X-Frame-Options "DENY"
```

- **DENY**: iframe 로딩을 완전히 차단.
- **SAMEORIGIN**: 같은 도메인에서만 iframe 로딩 허용.

> “
> # X-Content-Type-Options

문제:

- X-Content-Type-Options 헤더가 설정되지 않음.

해결:

Apache 설정 파일에 다음을 추가:

```
Header always set X-Content-Type-Options "nosniff"
```

- MIME 타입 스니핑 방지.

> # Referrer-Policy

문제:

- Referrer-Policy 헤더가 설정되지 않음.

해결:

Apache 설정 파일에 다음을 추가:

```
Header always set Referrer-Policy "no-referrer"
```

- **no-referrer**: 참조 헤더를 완전히 숨김.
- 다 `strict-origin`, `strict-origin-when-cross-origin`, `same-origin` 등.

> “
> # Feature-Policy / Permissions-Policy

문제:

- Feature-Policy 또는 Permissions-Policy 헤더가 설정되지 않음.

해결:

Apache 설정 파일에 다음을 추가:

```
Header always set Permissions-Policy "geolocation=(), camera=(), microphone=()"
```

- **Permissions-Policy**: 특정 브라우저 기능(API) 사용을 제한.
- 예: `geolocation`, `camera`, `microphone` 등.

Server

□□:

- Server □□□ Apache□ □□□□ □□ □□□ □□□.

□□:

Apache □□ □□□ □□□ □□:

```
ServerTokens Prod
ServerSignature Off
Header unset Server
```

- **ServerTokens Prod**: □□□□ □□□ □□.
- **ServerSignature Off**: □□ □□□□□ Apache □□ □□.
- **Header unset Server**: Server □□□ □□.

> “
Set-Cookie

□□:

- `SameSite` □ `HttpOnly` □□□□ □□.

□□:

Apache □□ □□□ □□□ □□:

```
Header always edit Set-Cookie ^(.*)$ "$1; SameSite=Strict; HttpOnly; Secure"
```

- **SameSite=Strict**: □□□ □□ □□□ □□□□ □□.
- **HttpOnly**: JavaScript□□ □□ □□□ □□.
- **Secure**: HTTPS □□□□□ □□□ □□.

>

전체 설정시

```
# X-Frame-Options 설정
Header always set X-Frame-Options "DENY"

# X-Content-Type-Options 설정
Header always set X-Content-Type-Options "nosniff"

# Referrer-Policy 설정
Header always set Referrer-Policy "no-referrer"

# Permissions-Policy 설정
Header always set Permissions-Policy "geolocation=(), camera=(), microphone=()"

# Server 정보 숨기기
ServerTokens Prod
ServerSignature Off
Header unset Server

# Set-Cookie 보안 설정
Header always edit Set-Cookie ^(.*)$ "$1; SameSite=Strict; HttpOnly; Secure"
```

Revision #1
Created 26 December 2024 06:14:16 by 유호경
Updated 26 December 2024 06:22:10 by 유호경