[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

□□:

- X-Frame-Options □□□ □□□□ □□.

□□:

Apache □□ □□□ □□□ □□:

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

- **DENY**: iframe □□□ □□□ □□.
- **SAMEORIGIN**: □□ □□□□□□ iframe □□ □□.

> “
>
> # X-Content-Type-Options

□□:

- X-Content-Type-Options □□□ □□□□ □□.

□□:

Apache □□ □□□ □□□ □□:

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

- MIME □□ □□□ □□.

>

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 □□□ □□□□ □□.

□□:

Apache □□ □□□ □□□ □□:

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

- **Permissions-Policy**: □□ □□□□ □□(API) □□□ □□.
- □: `geolocation`, `camera`, `microphone` □.

>

Server

문제:

- Server 헤더가 Apache로 설정되어 서버 정보가 노출됨.

해결:

Apache 설정 파일에 다음을 추가:

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

- **ServerTokens Prod**: 최소한의 정보만 노출.
- **ServerSignature Off**: 오류 페이지에서 Apache 정보 숨김.
- **Header unset Server**: Server 헤더를 제거.

Set-Cookie

문제:

- `SameSite` [`HttpOnly` 플래그가 없음.

해결:

Apache 설정 파일에 다음을 추가:

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

- **SameSite=Strict**: 쿠키를 외부 요청에 전송하지 않음.
- **HttpOnly**: JavaScript에서 쿠키 접근을 차단.
- **Secure**: HTTPS 요청에서만 쿠키를 전송.

□□ □□□

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

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

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