**PENGEMBANGAN WEB (TEORI)**

**LAPORAN EKSPERIMEN MENGENAI PROBLEM MENCEGAH SERANGAN CROSS-SITE SCRIPTING (XSS)**

**DENGAN PENYELESAIAN MENGGUNAKAN HEADER X-XSS NATIVE PHP**

*Laporan ini disusun untuk memenuhi tugas 1 mata kuliah Pengembangan Web (Teori)*



Disusun oleh kelompok B4:

**Asri Husnul Rosadi 221524035**

Faris Abulkhoir 221524040

Mahardika Pratama 221524044

Muhamad Fahri Yuwan 221524047

Najib Alimudin Fajri 221524053

Septyana Agustina 221524058

Sarah 221524059

Dosen Pengampu:

Joe Lian Min, M.Eng.

**JURUSAN TEKNIK KOMPUTER DAN INFORMATIKA**

**PROGRAM STUDI D4 TEKNIK INFORMATIKA**

**POLITEKNIK NEGERI BANDUNG**

**2024**

# **DAFTAR ISI**

[**DAFTAR ISI** i](#_Toc175484086)

[**A.** **IDENTIFIKASI PROBLEM** 1](#_Toc175484087)

[**B.** **DESKRIPSI PROBLEM** 1](#_Toc175484088)

[**C.** **METODOLOGI EKSPERIMEN** 1](#_Toc175484089)

[**D.** **PELAKSANAAN EKSPERIMEN** 1](#_Toc175484090)

[**E.** **ANALISIS HASIL EKSPERIMEN** 1](#_Toc175484091)

Link chatGPT : https://chatgpt.com/share/b4fefc0c-418d-45b2-b6a9-c921d60c14e2

# **IDENTIFIKASI PROBLEM**

Cross-Site Scripting (XSS) merupakan ancaman signifikan dalam keamanan web yang memungkinkan penyerang menyuntikkan skrip berbahaya ke dalam halaman web yang kemudian dijalankan di browser pengguna. Ini dapat mengakibatkan pencurian data dan perusakan sesi. Untuk menangkal XSS, berbagai teknik digunakan, salah satunya adalah header X-XSS-Protection.

# **DESKRIPSI PROBLEM**

Header X-XSS-Protection dirancang untuk memberikan perlindungan terhadap XSS dengan memberi instruksi kepada browser untuk memblokir konten yang dianggap berbahaya. Meskipun ini merupakan solusi yang populer di masa lalu, teknologi browser telah berkembang pesat. Header ini ternyata lebih efektif di browser lawas, sedangkan browser modern cenderung tidak mendukungnya atau mengabaikannya.

# **METODOLOGI EKSPERIMEN**

Eksperimen ini dilakukan dengan menerapkan Header X-XSS-Protection pada halaman web dan mengujinya menggunakan berbagai versi browser modern, termasuk yang terbaru. Tujuan utama adalah untuk mengevaluasi efektivitas header ini di browser yang saat ini digunakan secara luas.

# **PELAKSANAAN EKSPERIMEN**

Kami mengkonfigurasi server untuk menyertakan Header X-XSS-Protection dan melakukan pengujian di berbagai browser modern untuk melihat apakah header ini dapat mencegah serangan XSS. Hasil dari pengujian ini menunjukkan bahwa header tidak memberikan perlindungan yang diharapkan pada browser yang lebih baru

# **ANALISIS HASIL EKSPERIMEN**

Hasil eksperimen menunjukkan bahwa Header X-XSS-Protection tidak efektif dalam melindungi dari serangan XSS di browser modern, yang mengarah pada kesimpulan bahwa header ini lebih relevan untuk browser lawas. Sebaliknya, Content Security Policy (CSP) terbukti memberikan perlindungan yang lebih komprehensif dan luas pada browser modern. Validasi input/output juga tetap menjadi teknik yang penting dan efektif namun memerlukan penerapan yang konsisten.

Perbandingannya antara ketiga solusi ini :

**Header X-XSS-Protection**

* **Pro:** Mudah diimplementasikan, dapat efektif di browser lawas.
* **Kontra:** Tidak berfungsi di browser modern, solusi yang semakin usang.

**Content Security Policy (CSP)**

* **Pro:** Perlindungan yang komprehensif, dukungan luas pada browser modern.
* **Kontra:** Implementasi yang lebih kompleks, potensi gangguan pada fitur web jika tidak dikonfigurasi dengan benar.

**Validasi Input/Output Escaping**

* **Pro:** Teknik dasar yang sangat efektif dalam mencegah data berbahaya.
* **Kontra:** Memerlukan perhatian konstan dari pengembang untuk memastikan penerapan yang benar, masih mungkin ada celah jika tidak diterapkan dengan cermat.

# **KESIMPULAN**

Eksperimen yang dilakukan menunjukkan bahwa Header X-XSS-Protection, meskipun merupakan teknik yang dahulu populer untuk melindungi terhadap Cross-Site Scripting (XSS), kini tidak efektif pada browser modern. Header ini dirancang untuk browser lawas dan tidak memberikan perlindungan yang memadai pada teknologi web yang lebih baru.

Sebaliknya, Content Security Policy (CSP) dan teknik validasi input/output escaping terbukti menjadi solusi yang lebih efektif dan relevan untuk melindungi situs web dari XSS di era modern. CSP menawarkan perlindungan yang komprehensif dengan dukungan luas pada browser modern, sedangkan validasi input/output tetap menjadi teknik penting namun memerlukan implementasi yang hati-hati.

Dengan demikian, meskipun Header X-XSS-Protection memiliki nilai historis, pendekatan keamanan web yang lebih efektif saat ini melibatkan penggunaan CSP bersama dengan validasi input/output untuk memastikan perlindungan yang lebih baik dan menyeluruh terhadap ancaman XSS. Implementasi metode-metode ini secara bersamaan memberikan perlindungan yang lebih solid dan sesuai dengan standar keamanan web yang terbaru.