Open Journal Systems (OJS) merupakan platform manajemen jurnal ilmiah berbasis open source yang banyak digunakan oleh institusi pendidikan tinggi, lembaga penelitian, dan asosiasi profesi di seluruh dunia, termasuk di Indonesia. Melalui OJS, proses pengelolaan jurnal — mulai dari pengiriman naskah, proses review, hingga publikasi artikel — dapat dilakukan secara digital dan transparan. Selain itu, OJS dirancang agar hasil publikasi ilmiah dapat diindeks oleh berbagai mesin pencari akademik seperti **Google Scholar**, **Dimensions**, **Crossref**, dan **Garuda**, yang berperan penting dalam meningkatkan visibilitas dan reputasi jurnal.

Namun, dalam beberapa tahun terakhir, semakin banyak kasus **peretasan OJS (OJS hacking)** dengan modus penyisipan **konten perjudian online atau slot judi** ke dalam halaman jurnal ilmiah. Serangan ini biasanya memanfaatkan **kerentanan pada plugin, tema (template), atau versi OJS yang belum diperbarui**, sehingga memungkinkan penyerang menanamkan skrip HTML dan tautan (backlink) menuju situs judi online di dalam metadata, menu, atau footer situs jurnal. Akibatnya, situs jurnal tersebut terdeteksi oleh sistem Google sebagai situs spam atau berisi konten melanggar kebijakan, sehingga **dihapus atau diblokir dari hasil indeks Google Scholar**.

Kondisi ini berdampak serius bagi pengelola jurnal ilmiah. Hilangnya indeksasi Google Scholar tidak hanya menurunkan reputasi jurnal, tetapi juga mengurangi aksesibilitas artikel oleh peneliti lain di seluruh dunia. Selain itu, adanya konten ilegal di laman jurnal dapat menimbulkan **pelanggaran etika akademik dan reputasi institusi penerbit**, serta menghambat proses akreditasi jurnal di sistem nasional seperti **Arjuna dan SINTA**

Setelah terjadinya serangan yang menyebabkan penyisipan konten **slot judi online** pada situs OJS dan berdampak pada **hilangnya indeksasi Google Scholar**, tim pengelola jurnal segera melakukan serangkaian langkah pemulihan dan penguatan keamanan sistem. Langkah pertama yang dilakukan adalah penerapan **Web Application Firewall (WAF)** pada server untuk memfilter dan memblokir aktivitas berbahaya dari luar, termasuk percobaan injeksi skrip maupun akses tidak sah. Selain itu, sistem juga diamankan melalui integrasi dengan **Cloudflare** sebagai lapisan proteksi tambahan terhadap serangan DDoS, bot traffic, serta manipulasi DNS yang sering dimanfaatkan oleh pelaku penyusupan.

Langkah berikutnya adalah melakukan sinkronisasi dan validasi ulang dengan **Google Search Console**, guna menghapus URL berbahaya dari indeks Google dan memastikan struktur metadata jurnal kembali bersih dari tautan ilegal. Melalui Google Console pula dilakukan proses **reindexing** agar halaman OJS dapat kembali terdeteksi oleh Google Scholar secara normal. Tak hanya itu, tim juga memperbarui seluruh **plugin, tema, dan versi OJS** ke rilis terbaru untuk menutup celah keamanan yang sebelumnya dimanfaatkan oleh penyerang.

Namun, **hingga saat ini hasilnya belum sepenuhnya berhasil**; jurnal masih **belum terindeks kembali di Google Scholar** dan **terkadang tidak muncul di hasil pencarian Google umum (search engine visibility masih rendah)**. Hal ini kemungkinan besar disebabkan oleh reputasi domain yang sempat tercatat sebagai situs spam oleh algoritma Google akibat konten judi online yang sebelumnya tertanam.