**Assalamualaikum.**
Perkenalkan nama saya Jainal Abidin. Dan saya adalah seorang Bug Hunter.

Hari ini saya akan Sharing tentang XSS dan di kesempatan kali ini saya akan membahas dan menjelaskan tentang BUG XSS Reflected sesuai pengetahuan saya.

Sebelum masuk ke pembahasan BUG XSS Reflected, Saya akan memberikan pengertian tentang apa itu BUG XSS ?

Bug XSS atau (Cross Site Scripting) adalah celah keamanan di mana penyerang menyisipkan kode berbahaya, biasanya dalam bentuk script JavaScript, ke dalam situs web. Ada 3 jenis XSS Yaitu "Reflected XSS, Stored XSS, Dan DOM-based XSS" Namun saya hanya akan membahas jenis xss yang pertama yaitu Reflected XSS.

Dari pengertian di atas dapat kita simpulkan bahwa XSS adalah Bug yang terdapat pada website yang dapat membahayakan keamanan website.

Baiklah mungkin itu saja yang dapat saya jelaskan tentang XSS. Dan sekarang mari kita masuk ke pembahasan BUG XSS Reflected.

1.Pengertian BUG XSS REFLECTED

Reflected XSS (Cross-Site Scripting) adalah jenis serangan di mana penyerang menyisipkan kode jahat ke dalam respon HTTP yang dikirimkan oleh aplikasi web. Kode ini tidak disimpan di server, melainkan dieksekusi hanya saat pengguna mengklik tautan yang berisi script berbahaya. Serangan ini sering terjadi ketika aplikasi tidak memvalidasi atau menyaring input pengguna dengan benar.

2.Cara kerja Reflected XSS

Server memproses permintaan dan mengembalikan halaman yang berisi skrip jahat. Skrip ini kemudian dieksekusi di browser pengguna, yang dapat menyebabkan pencurian data, pengalihan ke situs lain. Ada 2 cara kerja xss reflected di antaranya yaitu, melalui "kolom pencarian" dan "parameter url" namun kali ini saya akan memberikan cara yang mudah saja yaitu dari kolom pencarian.

Contohnya seperti ini : Misalkan ada situs web yang memiliki column pencarian dan websete tersebut memiliki celah xss reflected kemudian di masukan sebuah script seperti ini <script>alert(1);</script> kemudian kita klik enter maka skript akan dieksekusi dan menampilkan jendela peringatan, menunjukkan bahwa skrip tersebut berhasil dijalankan.

Jika kalian masih belum mengerti cara kerja XSS Reflected saya akan memberikan tutorial cara kerja dari bug tersebut.

Pertama yang paling penting kita harus punya code/script untuk menjalankan XSS disini saya mengunakan code <script>alert(1);</script>
Setelah itu mari kita kunjungi website -http://testphp.vulnweb.com/
Jika sudah masuk maka kita akan melihat kolom pencarian di pojok kiri atas.


Setalah itu kita masukan code <script>alert(1);</script> ke dalam kolom pencarian. Kemudian klik enter maka akan muncul pop up seperti ini.


Jika sudah muncul pop up seperti itu maka kita berhasil melakukan XSS REFLECTED.

Bug tersebut sering kali di salah gunakan oleh seseorang karna dampak dari bug tersebut sangatlah berbahaya untuk keamanan website.

Apasaja sih dampak dari bug Reflected XSS ini. Ada beberapa dampak yang cukup berbahaya di antanya yaitu :

-Pencurian Data Sensitif mengambil informasi pribadi seperti cookie, token sesi, atau data login pengguna yang sedang aktif.

-Pengalihan Pengguna: Mengarahkan pengguna ke situs web berbahaya atau phishing yang dirancang untuk mencuri informasi lebih lanjut.

-Eksekusi Skrip Berbahaya: Menjalankan skrip yang dapat mengubah tampilan halaman atau mencuri data dari pengguna.

-Serangan Phishing: Membuat halaman palsu yang terlihat asli untuk menipu pengguna agar memasukkan informasi sensitif.

-Manipulasi Konten: Mengubah konten yang ditampilkan kepada pengguna, yang dapat merusak reputasi situs web atau menyesatkan pengguna.

Dari beberapa dampak tersebut dapat mengakibatkan kerugian yang signifikan baik bagi pengguna maupun pemilik situs web.

Lalu bagaimana cara mengatasi Bug xss reflected ini. Saya juga belum terlalu faham bagaimana cara mengatasinya jadi saya akan memberikan pendapat dari “Ai” Tentang bagaimana caranya mengatasi Bug tersebut.

Berikut cara mengatasinya :

Untuk mengatasi bug Reflected XSS pada kolom pencarian dan parameter URL, beberapa langkah pencegahan yang dapat diterapkan adalah:

Validasi dan Sanitasi Input: Pastikan semua input dari pengguna, termasuk parameter URL dan kolom pencarian, disaring untuk karakter berbahaya dan tag HTML.

Encoding Output: Gunakan encoding yang tepat saat menampilkan data yang diterima dari pengguna untuk mencegah eksekusi skrip berbahaya.

Penggunaan Library Keamanan: Manfaatkan library anti-XSS yang tersedia, seperti HTML Purifier atau OWASP Java Encoder, untuk melindungi aplikasi dari serangan ini.

Content Security Policy (CSP): Terapkan CSP untuk membatasi sumber skrip yang dapat dijalankan di halaman web, sehingga mengurangi risiko eksekusi skrip berbahaya.

Audit dan Penetration Testing: Lakukan audit keamanan secara berkala dan pengujian penetrasi untuk mengidentifikasi dan memperbaiki kerentanan XSS yang mungkin ada.

Mungkin itu saja yang dapat saya jelaskan tentang XSS Reflected jika ada kekurangan dalam pembahasan kali ini saya mohon maaf **wasalamualikum wr.wb.**