I spy… - LA CTF

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 1 preview

Tantangan web ini memberikan sebuah textbox yang sepertinya digunakan untuk menginputkan sebuah token.

Pertama aku ingin memasukkan token yang diberikan dan website menampilkan pesan  
A token in the HTML source code...

Jadi aku membuka HTML source codenya untuk melihat token selanjutnya

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 2 HTML\_Source\_Code

dan benar terdapat token di HTML Source Codenya, setelah itu aku inputkan ke textboxnya dan website menampilkan pesan

A token in the JavaScript console...

Jadi aku mengecek Javascript console dari website ini

Sebuah gambar berisi teks, cuplikan layar, Font, nomor

Konten yang dihasilkan AI mungkin salah.

Figure 3 Javascript\_Console

Dan benar terdapat token di javascript console, setelah itu aku inputkan ke websitenya dan website menampilkan pesan

A token in the stylesheet...

Jadi aku membuka source code website ini dan mengecek style.css untuk melihat token selanjutnya

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 4 stylesheet

Dan benar terdapat token di css website ini, setelah itu aku menginputkannya ke website dan menerima pesan

A token in javascript code...

Jadi aku membuka source code website ini dan mengecek thingy.js untuk melihat token selanjutnya

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 5 Javascript\_Code

Dan benar terdapat token di file javascriptnya, setelah itu di aku menginputkannya ke website dan menerima pesan

A token in a header...

Dari pesan yang didapat, token berdada di header, jadi aku mengecek header website ini lewat inspect browser ini

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 6 Headers

Di bagian response headers terdapat X-token yang berisi token untuk stage ini. Ketika ku masukkan ke website ini, tedapat pesan yang muncul

A token in a cookie...

Karena petunjuk mengatakan token berada di cookie, saya mengecek bagian request headers dan melihat bagian cookienya

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 7 Cookies

Dan ternyata terdapat token di cookienya, ketika saya masukkan ke website terdapat pesan

A token where the robots are forbidden from visiting...

Karena petunjuk menyebut the robots, saya mencoba untuk mengecek robots.txt

User-agent: \*

Disallow: /a-magical-token.txt

/robots.txt mengarahkan ke file /a-magical-token.txt , jadi saya mencoba untuk mengeceknya

Sebuah gambar berisi teks, cuplikan layar, Font

Konten yang dihasilkan AI mungkin salah.

Figure 8 a-magical-token

Ternyata di file itu terdapat token , setelah itu saya memasukkan token tersebut ke website dan mendapat pesan

A token where Google is told what pages to visit and index...

karena token menyebutkan Dimana google laman yang visit dan index, saya mengecek file /sitemap.xml

Sebuah gambar berisi teks, cuplikan layar, software, Software multimedia

Konten yang dihasilkan AI mungkin salah.

Figure 9 sitemap

Dan benar terdapat token di file ini, saya mencoba menginputkannya di website ini dan mendapat pesan

A token received when making a DELETE request to this page...

Karena petunjuk bilang membuat DELETE request, saya mencoba mengedit method GET menjadi method DELETE dengan burpsuite.

Sebuah gambar berisi teks, Font, cuplikan layar, nomor

Konten yang dihasilkan AI mungkin salah.

Figure 10 DELETE

Setelah diubah ke DELETE method, website mersepon dengan memberikan token. Setelah itu saya menginputkan ke website dan mendapatkan pesan

A token in a TXT record at i-spy.chall.lac.tf...

Dari petunjuk diatas saya memakai perintah Resolve-DnsName di poweshell untuk mengetahui tokennya

Resolve-DnsName -Type TXT i-spy.chall.lac.tf

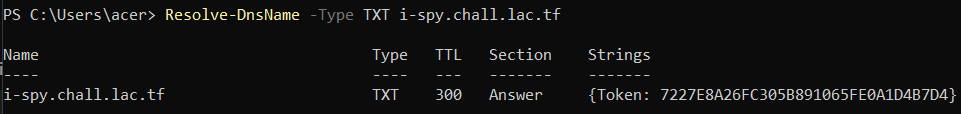


Figure 11 TXT

Setelah mendapat token saya mencoba menginputkannya ke website dan menampilkan

A Flag! lactf{1\_sp0773d\_z\_t0k3ns\_4v3rywh3r3}

Dan akhirnya kita menemukan flagnya

lactf{1\_sp0773d\_z\_t0k3ns\_4v3rywh3r3}