Laporan Hasil Scan Web Palio di Beberapa Tools

1.SiteGuading

Permasalahan: Versi Apache yang digunakan saat ini sudah tidak berfungsi dengan baik dan rentan terhadap serangan

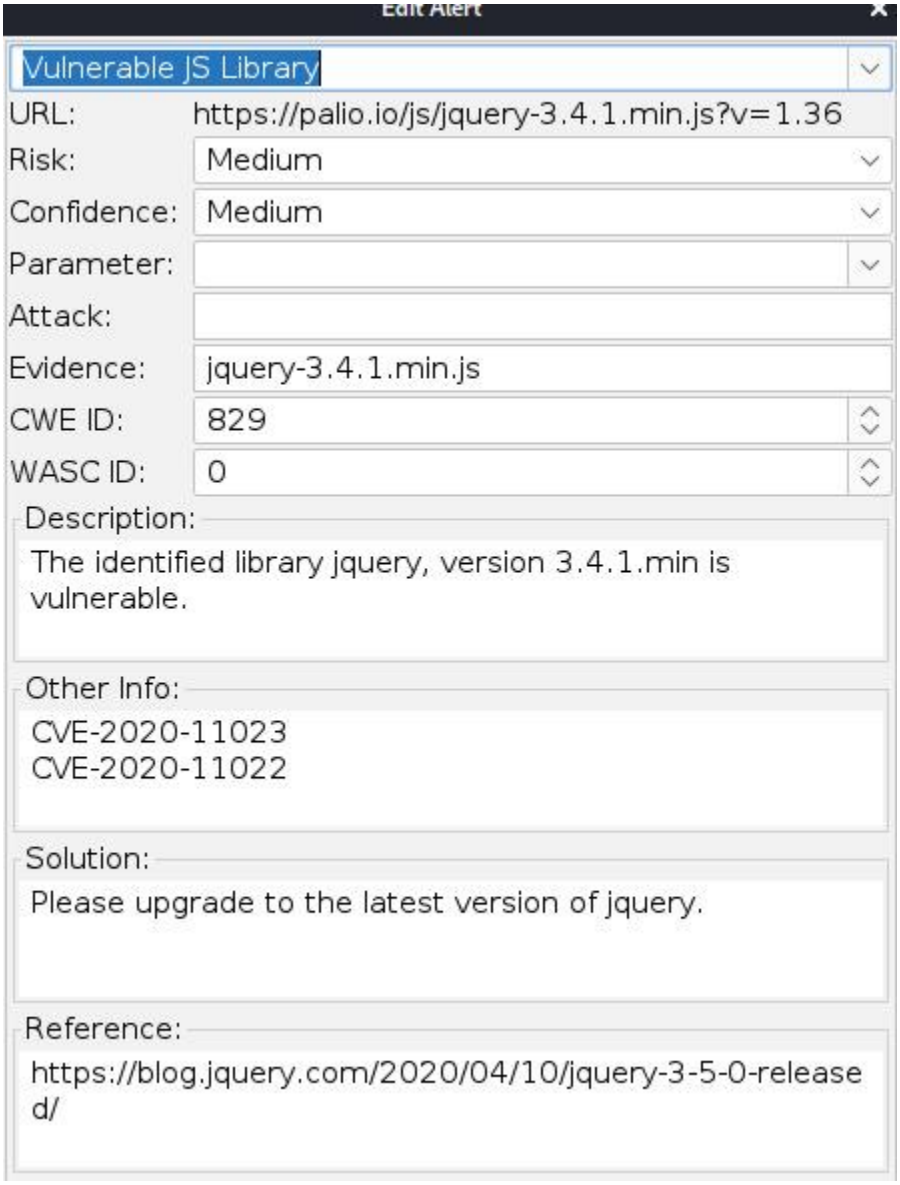
Solusi: Update Apache dari 2.4.6 ke versi Apache 2.4.44

2.Sucuri

Permasalahan: Versi Apache yang digunakan saat ini sudah tidak berfungsi dengan baik dan rentan terhadap serangan

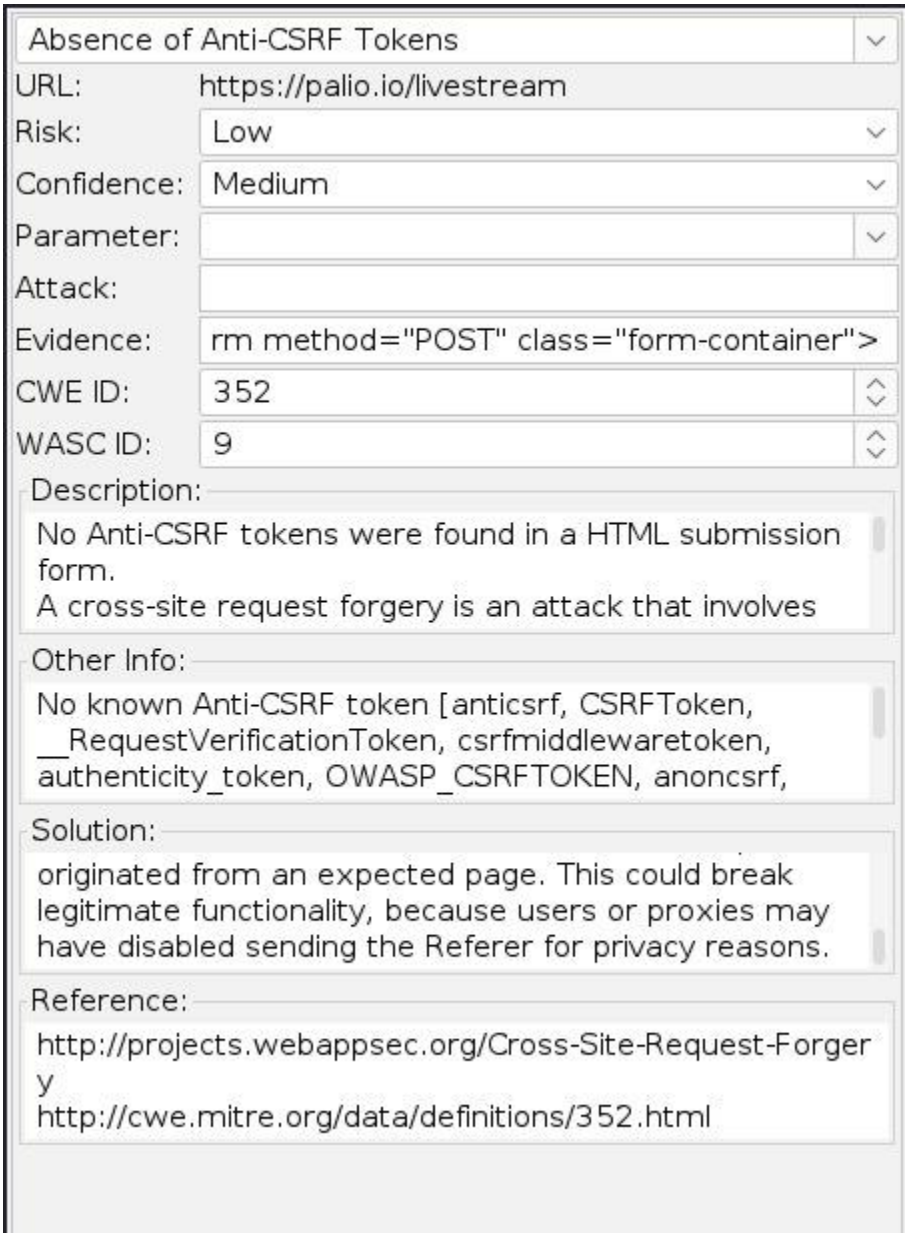
Solusi: Update Apache dari 2.4.6 ke versi Apache 2.4.44

3.OWASP ZAP



Permasalahan: Versi Jquery pada web palio sekarang rentan dikarenakan masih menggunakan versi Jquery 3.4.1

Solusi: Update versi Jquery 3.4.1 ke versi Jquery 3.5.0



Permasalahan: Tidak adanya script Anti-CRFS pada html form yang dapat memudahkan attacker memanipulasi permintaan palsu crossed

Solusi: Menambahkan tipe input menjadi hidden lalu membuat value dengan token

Contoh:

```
<input type="hidden" name="csrf" value="Fijd93djskDsdis9wijdSD938jISdj93jdISdj9s" />
```

4.Pentest-Tools

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Permasalahan: Versi software yang dipakai sudah lama

Solusi: Versi software harus di update ke versi terbaru

Missing HTTP security headers

HTTP Security Header	Header Role	Status
Strict-Transport-Security	Protects against man-in-the-middle attacks	Not set

Details

Risk description:
The HTTP Strict-Transport-Security header instructs the browser not to load the website via plain HTTP connection but always use HTTPS. Lack of this header exposes the application users to the risk of data theft or unauthorized modification in case the attacker implements a man-in-the-middle attack and intercepts the communication between the user and the server.

Recommendation:
We recommend setting the Strict-Transport-Security header.
More information about this issue:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Permasalahan : Disini tertulis SSL masih kurang aman

Solusi: ssl untuk di disable dan diganti dengan TLS 1.2 atau lebih. Dengan menambahkan perintah SSLProtocol +TLSv1.2 pada mod_ssl module

●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4.6

Permasalahan : Apache masih versi 2.4.6

Solusi: Update versi Apache ke versi terbaru

5.SSL Labs

Permasalahan : netsparker mendeteksi bahwa SSL tidak aman. Karena SSL v3 memiliki kekurangan yaitu penyerang dapat menyebabkan kegagalan koneksi dan dapat mengekploitasi kerentanan

Solusi : sebaiknya ssl3 untuk di disable dan diganti dengan TLS 1.2 atau lebih. Dengan menambahkan perintah SSLProtocol +TLSv1.2 pada mod_ssl module