

Laporan Hasil Scan Web Palio di Beberapa Tools

1.SiteGuading



 **Outdated**

Name: Apache

Version: 2.4.6

Safe Version: 2.4.44

Upgrade Text: Vulnerabilities on Apache 2.4 web server

Upgrade Url: http://httpd.apache.org/security/vulnerabilities_24.html

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



Outdated Software Detected

Apache under 2.4.44

[Vulnerabilities on Apache 2.4 web server](#)

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

✕

Edit Alert

Vulnerable JS Library

▼

URL:

https://palio.io/js/jquery-3.4.1.min.js?v=1.36

Risk:

Medium

▼

Confidence:

Medium

▼

Parameter:

▼

Attack:

Evidence:

jquery-3.4.1.min.js

CWE ID:

829

⬆
⬆

WASC ID:

0

⬆
⬆

Description:

The identified library jquery, version 3.4.1.min is vulnerable.

Other Info:

CVE-2020-11023
CVE-2020-11022

Solution:

Please upgrade to the latest version of jquery.

Reference:

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-release/>

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

Absence of Anti-CSRF Tokens		▼
URL:	https://palio.io/livestream	
Risk:	Low	▼
Confidence:	Medium	▼
Parameter:		▼
Attack:		
Evidence:	rm method="POST" class="form-container">	
CWE ID:	352	⬆⬇⬆
WASC ID:	9	⬆⬇⬆
Description:		
No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves		
Other Info:		
No known Anti-CSRF token [anticsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf,		
Solution:		
originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.		
Reference:		
http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html		

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="Fijd93djskDsd9wijdSD938jISdj93jdlSdj9s" />
```

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

Configuration		
	Protocols	
	TLS 1.3	No
	TLS 1.2	Yes*
	TLS 1.1	Yes
	TLS 1.0	Yes*
	SSL 3 ² INSECURE	Yes
	SSL 2	No
(2) This site requires support for virtual secure hosting (SNI), but SSL 2 and SSL 3 do not support this feature.		
(*) Experimental: Server negotiated using No-SNI		

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