

Date: Jun 22, 2024 (EST) **Ref:** STK/2024/M118G/MD

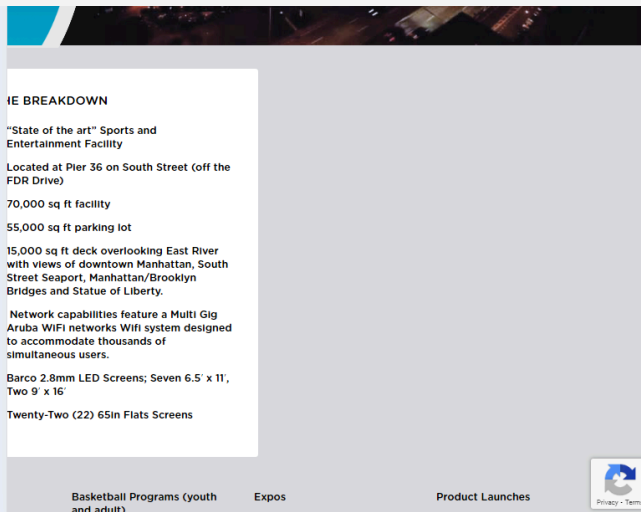
Website:

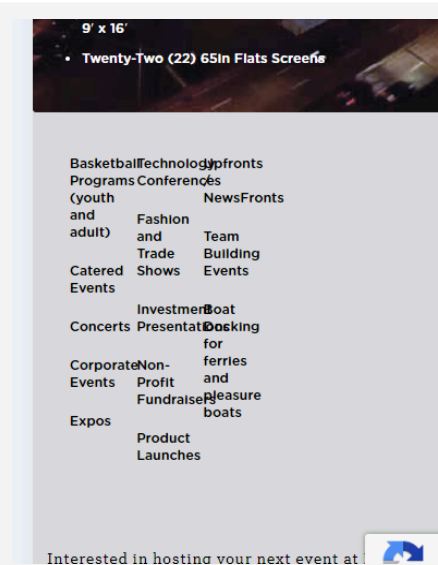
<https://pier36nyc.com>

Maintenance Type: Backup, Update, and Security Check

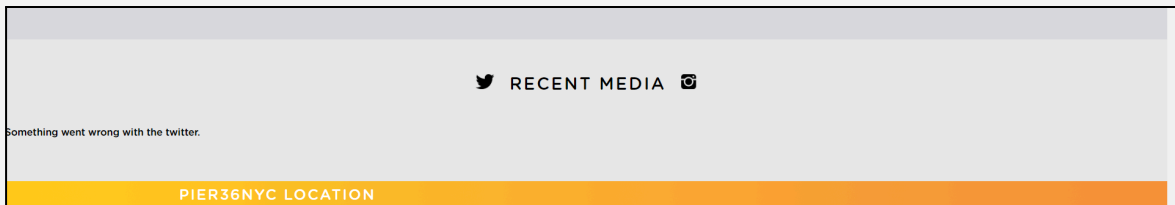
Pre-Maintenance Observations:

All the unique templates have been checked. We have found some structural misplacement of contents on the following page (page link: <https://pier36nyc.com/venue>) of your site in mobile view and tab view.

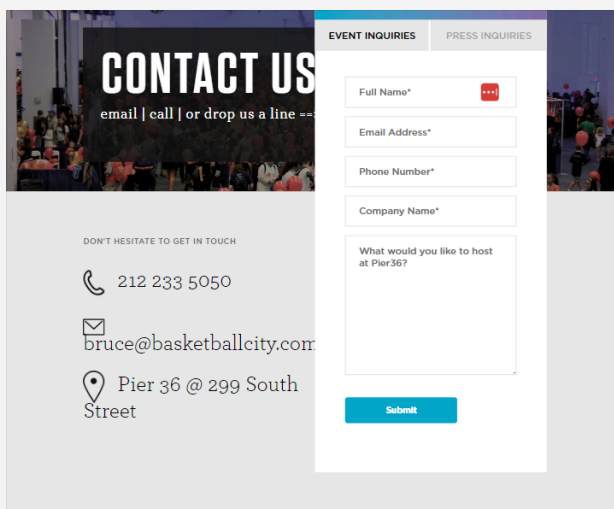




Some content is missing on the page (<https://pier36nyc.com/venue>) in the “RECENT MEDIA” section.



Contact details are hidden by “SEND A MESSAGE” form in tablet and mobile view.



SEND A MESSAGE

EVENT INQUIRIES | PRESS INQUIRIES

Full Name*

Email Address*

Phone Number*

Company Name*

What would you like to host at Pier36?

Submit

✉ bruce@basketballcity.com

📍 Pier 36 @ 299 South Street

The forms are working well.

Post-Maintenance Report:

Core Update:

WordPress update version 6.5.3 to 6.5.4

Update list:

#	Plugin / Theme Name	Previous Version	Updated Version
1.	Contact Form 7 Captcha	0.1.4	0.1.5

2.	SEO Optimized Images	2.1	2.1.1
3.	WP Migrate Lite	2.6.10	2.6.11
4.	WPS Hide Login	1.9.15.2	1.9.16.4
5.	Yoast SEO	22.7	22.9

Backup Details:

Database, Plugins, Themes, and Uploads

Individual Templates Checkup:

Following a thorough examination of all unique templates, we've discovered consistent structural misplacement of content on the page (page link: <https://pier36nyc.com/venue>) of your site across both mobile and tab views.

Additionally, we've observed that some content is missing in the "RECENT MEDIA" section of the page (<https://pier36nyc.com/venue>), as previously noted.

The contact details are obscured by the "SEND A MESSAGE" form in tablet and mobile view like before.

Special Features Checkup:

The forms are working well.

Security Checkup:

We have manually checked the files, and some security issues were found. We've detected a potentially malicious file at the following location: /home/pier36ny/public_html/wp-content/plugins/wpematico/app/lib/index.php. It seems to have been tampered with by an unauthorized party to carry out harmful actions. Should you recognize this file, you may ignore it or it's crucial to

address these issues seriously and consider whether fixing or permanently removing it is necessary.

The 'AccessPress Twitter Feed" and "Huge IT Image Gallery " plugins have been removed from wordpress. That means future updates may or may not be available in the near future for them. Sometimes old versions of plugins might appear to be a security threat to the entire site. So, it's worth taking these matters seriously and thinking about whether to replace or remove them permanently.

We couldn't upgrade the following plugins "Advanced Custom Fields", "Contact Form 7" and "Custom Post Type UI" because of the compatibility issue of their latest version and the php version of your server. The latest version of these plugins require php version 7.4 or higher. You need to upgrade your php version.

Please get in touch with us if you want to fix the issues through us.

Others:

N/A

Jahid

Maintenance Engineer

Khalid

Supervisor