The leak of Internal IP Addresses. IP Addresses:- 10.6.96.4 10.6.136.194 10.6.127.182

**Assessment:**

[add your assessment of the vulnerability]

**Steps To Reproduce:**

1. Open request page of (graphql2.trint.com) with "getUser" Operation name.
2. Remove "authorization: Bearer" line and error will raise.
3. You can see ("ip":"::ffff:10.6.127.182) and ("data":{"user":null}) in error. It is happening only on "getUser" operation name.

**Supporting Material/References:**

[list any additional material (e.g. screenshots, logs, etc.)]

* [attachment / reference] [ipleak1.JPG (F555596)](https://hackerone-us-west-2-production-attachments.s3.us-west-2.amazonaws.com/CitRdaUFJggPjYut3MrS2PXR?response-content-disposition=attachment%3B%20filename%3D%22ipleak1.JPG%22%3B%20filename%2A%3DUTF-8%27%27ipleak1.JPG&response-content-type=image%2Fjpeg&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIAQGK6FURQ4YGFVSHH%2F20211215%2Fus-west-2%2Fs3%2Faws4_request&X-Amz-Date=20211215T005504Z&X-Amz-Expires=3600&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEID%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLXdlc3QtMiJIMEYCIQDRHepACRwRxZj03gSteEiPMiWg2qh%2FUcuDjHLoAahGrwIhAMjTrDfbHBKiE994vrDd5UFzHKuO2kUunCGw%2BDUy66IzKvoDCGkQAhoMMDEzNjE5Mjc0ODQ5Igyi5B%2B3HPQQMzi%2BJrsq1wM4dG8w26sIZuikkpjaaYsUQYv2M0YaPI9%2BJuYRBozIRuHSzGE0wqvib4zRjvJWSOLAzDqeTfh5ZOQVbvhLZD7Q7QZrhYttWNQg5W1E8IuZcdYwc60rhuKkOP58UPoB%2BcljJJ6B9Nu6o8KYU7Hc5BIh5l7bf7A62HruGJZF8X0w5%2BYKHi5yxJjcPWTS5qwVtI2UodhB2F%2BgBvtDIte2pH7SjiR2GoFZNEMRcx6VkiKxn1fRiHPWnep8F0c%2Bhx%2FElLEjueERuQ5cupt34CC%2BM9HrJH%2BSAhP6Kwrm1ijU5aP5Eux6nEctNreXykfQqPSnCu3C8ucRhxkfF1rXSdkxkHWoLBmW0xi75jWeEnN0IUvCqIglKcBEof0I1G%2BJ%2FJEUT2%2F8KukD03KObYdeKlDYHpLPYLNs%2B8IVovzqMUHMfPn3lBbGgu4%2FWWb1x0e7fcY%2FdZOoYJIQd8KtDbzHI34EFO7thwQ06zzpZiJR%2Bq9%2FnAEZxGPwPPDB8dHhIKI3aHNlZhgg58T7d3NdUsFUdRko5pY%2BbKmnwmgR2PlwcxY90sS3Z4g%2F3fIVQ7gTzBVnwUVCdLuZqNRr%2Bb6NBVhllQMTAmW2%2BizYI06dvrfWU3tFwiz54U89uYomLbgwoOHkjQY6pAHnhwVv0VRfjmcP9kYScZ%2F3Z7Fi30Zq4vVkXPY1gRj0o%2FOYYm23Ah1YLI4ZGMOVBiudoSSoGE6GV9SNyC3nM2zcnc%2BBCbx0pB5hXW0iDqD786rWN%2FOEUTi61P1e4wlfn58nrFhp4GmTPE8ZC6VxwUkoYthYxXMGaVg8KNMXzftMHNa9OWZC7Pvuk2DVVRf7JkVQyFQFb3PL89yak8Uk6QilpANdYg%3D%3D&X-Amz-SignedHeaders=host&X-Amz-Signature=ac02bbc69a9b46f6a32eecad2c556672e3af34ec28ee47602fef99cd8eac4f02)

**Impact**

The leak of Internal IP Addresses will allow the attacker to get more information about the server.

192.168.10.111 – DNS Server

192.168.221.212 – DMZ App Server

192.168.20.1 – File Server A

192.168.30.1 – File Server B