ARAIZ NAQVI

INCIDENT REPORT

Infinity Travels

02ND OCTOBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

- Disclaimer
- Incident Summary
- Incident Details
- Impact assessment

2024-2025

ARAIZ NAQVI

DISCLAIMER

This incident report is a project-based simulation for the fictional organization *Infinity Travels*, as part of the "Fundamentals of Cybersecurity" course on Google's Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This incident report does not reflect any actual incidents or vulnerabilities affecting any real organization, including Infinity Travels.

Though based on practical analysis and protocols, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

ARAIZ NAQVI

INCIDENT SUMMARY

Time of Incident:	2024-10-05 00:16:00:000000 (05th October, 2024 12:16am)
Summary of Incident:	Clients at Infinity Travels are unable to access infinitytravels.com due to a DOS SYN attack causing servers to be on the brink of crash.
Location of Incident:	https://infinitytravels.com
Reported By:	Araiz Naqvi
Reported On:	2024-10-05 00:20:00:000000 (05th October, 2024 12:20am)

ARAIZ NAQVI

INCIDENT DETAILS

Type of Incident: DOS SYN Attack

Description: The user with IP Address *203.0.113.0* appears to be the likely threat actor, as they persistently sent multiple SYN requests, indicating deliberate malicious intent. This is not a DDoS attack, as it originates from a single IP. Initially, the server could handle requests from legitimate users, but as the attack's frequency escalated, it became overwhelmed and is now unable to process any requests, blocking real users from accessing the website.

2024-2025

ARAIZ NAQVI

IMPACT ASSESSMENT

Initial Response:

The first security measures put into place were to take down the servers and configure the firewall to block the threat actors IP Address. However, threat actor can change their IP Address and attack again.

Scope of Impact:

The attack severely impacted the server’s computational capacity due to the overwhelming volume of incoming requests, which also prevented legitimate customers from accessing the website.

As a result, all third-party clients relying on Infinity Travels' services would have experienced outages, leading to significant reputational damage and substantial financial losses.

(PTO)

Potential Future Risks:

After crashing the server, the threat actor can:

- Force a fallback to older software versions with known vulnerabilities that can still be exploited.
- Expose sensitive data, leaving it unprotected and easy for hackers to exploit.
- Compromise data integrity by injecting malicious code that could execute once the servers are restored.
- Hijack session cookies, allowing them to impersonate legitimate users.
- Exploit the chaos to implement social engineering tactics and manipulate employees or users.
- Gain insights into the system's defenses and recovery measures, identifying overlooked weaknesses.
- Install backdoors, enabling them to spy on communications and potentially regain access in the future.

Araiz Naqvi

Network Security Engineer

If you find this helpful, you'll love my content!

@araiz-naqvi

@araiznaqvi