Penetration Testing Report

Full Name: Muhammad Bokhtiar Uddin
Program: hackerone

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **www.kkr.com**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

1. Objective

The objective of the assessment was to uncover vulnerabilities in the www.kkr.com and provide a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

2. Scope

This section defines the scope and boundaries of the project.

Application Name	www.kkr.com

3. Summary

Outlined is a Black Box Application Security assessment for the www.kkr.com

High	Medium	Low
0	0	1

1. Non-Cloudflare IPs allowed to access origin servers

Reference	Risk Rating
Non-Cloudflare IPs allowed to access origin servers	**Low / Medium / High**

Tools Used

Burp Suite, Nmap, Subfinder, Httpx

Vulnerability Description

The "Non-Cloudflare IPs allowed to access origin servers" vulnerability occurs when server configurations allow direct access to the origin server by IP addresses not associated with Cloudflare, bypassing its protection. This vulnerability can lead to data exposure, DDoS attacks, and security breaches.

How It Was Discovered

Manual Analysis

Vulnerable URLs

https://199.168.174.14/

Consequences of not Fixing the Issue

Failing to fix the "Non-Cloudflare IPs allowed to access origin servers" vulnerability can have serious consequences for a website or online service. Here are some potential outcomes:

Data Breaches: Sensitive server data, including user credentials and financial information, can be vulnerable to unauthorized access, potentially leading to identity theft and other cybercrimes.

Server Compromise: Attackers can compromise server integrity by installing malware, manipulating data, or taking control, leading to service disruptions, data loss, and reputational damage.

DDoS Attack: Cloudflare's DDoS protection is bypassed, exposing the origin server to direct DDoS attacks, causing downtime and rendering the website or service inaccessible to legitimate users.

Loss of Customer Trust: Security breaches harm an organization's reputation and customer trust, potentially causing a decline in customer base and revenue.

Suggested Countermeasures

Implementing countermeasures can help mitigate the vulnerability of non-Cloudflare IPs accessing origin servers and enhance the security of the origin server.

IP Whitelisting: Configure the origin server to accept only incoming connections from specific Cloudflare IP addresses, ensuring only legitimate traffic through Cloudflare's network can access the server directly.

Firewall Rules: Implement firewall rules on the origin server to block all incoming traffic except from Cloudflare's IP ranges, providing additional protection against unauthorized access.

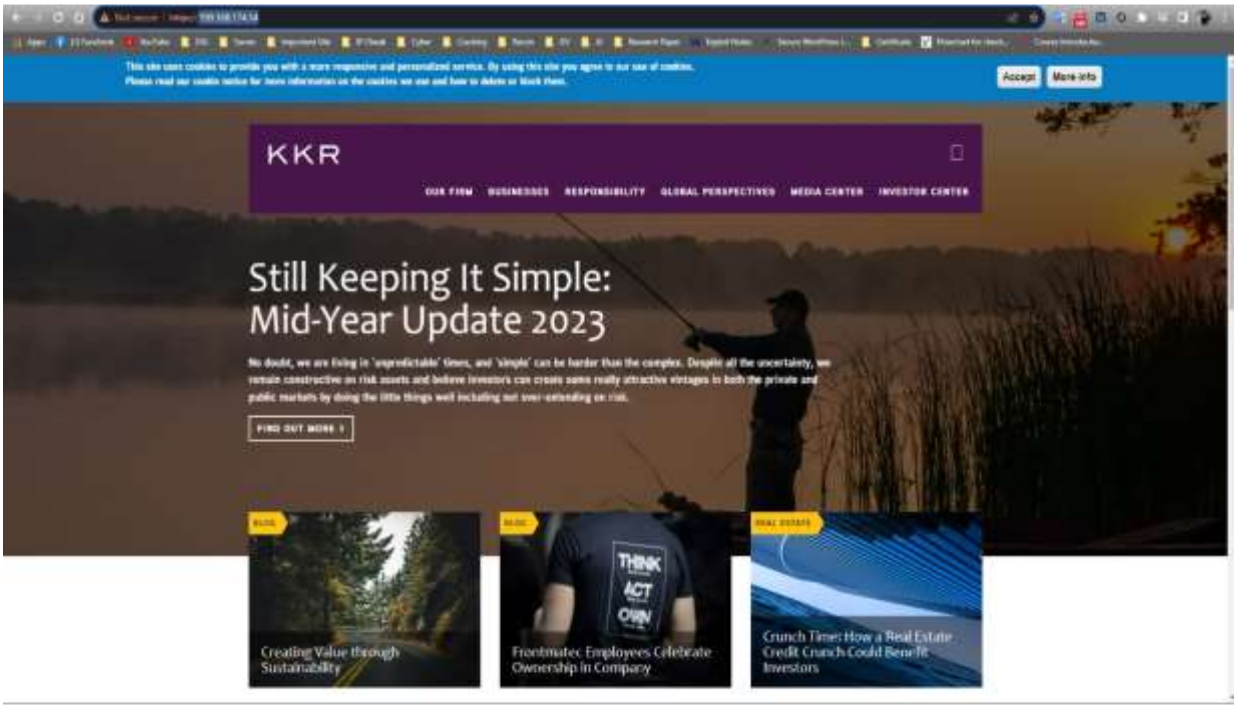
Cloudflare Access Policies: Cloudflare Access policies restrict access to the origin server based on user identity and permissions, adding an additional authentication layer for only authorized users.

Monitoring and Logging: Implement comprehensive logging and monitoring solutions to track access attempts, unusual activities, and potential security incidents, and set up alerts for suspicious behavior.

References

https://hackerone.com/reports/255978

Proof of Concept



This site uses cookies to provide you with a more responsive and personalized service. By using this site you agree to our use of cookies.
Please read our cookie notice for more information on the cookies we use and how to delete or block them.

Still Keeping It Simple:
Mid-Year Update 2023

No doubt, we are living in 'unpredictable' times, and 'simple' can be harder than the complex. Despite all the uncertainty, we remain constructive on risk assets and believe investors can create some really attractive vintages in both the private and public markets by doing the little things well including not over-extending on risk.

Creating Value through Sustainability

Frontmatec Employees Celebrate Ownership in Company

Crunch Time: How a Real Estate Credit Crunch Could Benefit Investors