

Forum:[Hack Forums](#)

Thread: [Gray hat - scam websites all hosted on CloudFlare or other enterprise hosts.](#)

PatientStudent - *October 3, 2024, 3:36 am*

Hey guys,

talking about web apps, unlike the machines on HackTheBox or whatever, in real world people hosting websites host them on secure enterprise servers.

For example - if we go through about 20 scam sites, they all are on CloudFlare, M 247, Powerhouse Inc. or whatever.

Getting through to these fraudulent websites means getting through the host's infrastructure.

Is this a known blocker for getting these websites down?

What's the point of nmaping the website's IP if it's CloudFlare's IP or whatever?

DramaKing - *October 3, 2024, 4:08 am*

(Oct 3, 2024 03:36 AM)PatientStudent Wrote: [\[CITE\]](#) Hey guys,

talking about web apps, unlike the machines on HackTheBox or whatever, in real world people hosting websites host them on secure enterprise servers.

For example - if we go through about 20 scam sites, they all are on CloudFlare, M 247, Powerhouse Inc. or whatever.

Getting through to these fraudulent websites means getting through the host's infrastructure.

Is this a known blocker for getting these websites down?

What's the point of nmaping the website's IP if it's CloudFlare's IP or whatever?

None. But will you exploit an open SMTP or POP3 port? These vulnerabilities are specific to web apps but beware of WAFs.

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Broken Access Control
- Security Misconfiguration
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection

Sensitive Data Exposure

XML External Entities (XXE)

Insecure Deserialization

Money- - *October 3, 2024, 7:15 am*

There's ways to bypass cloudflare. You need to obtain the Origin IP hosting behind cloudflare. They are several known methods and unique and private ones obviously. But yea.