Take Control of Your Web Applications Before Others

網站安全 – 先發制人、後發制於人

Agenda

1. What is happening in the Internet?
2. How do we tackle these threats?
3. Points to be noted in Vulnerability Scan
4. Some useful tools in Vulnerability Scan
5. Q&A

What is happening in the Internet?

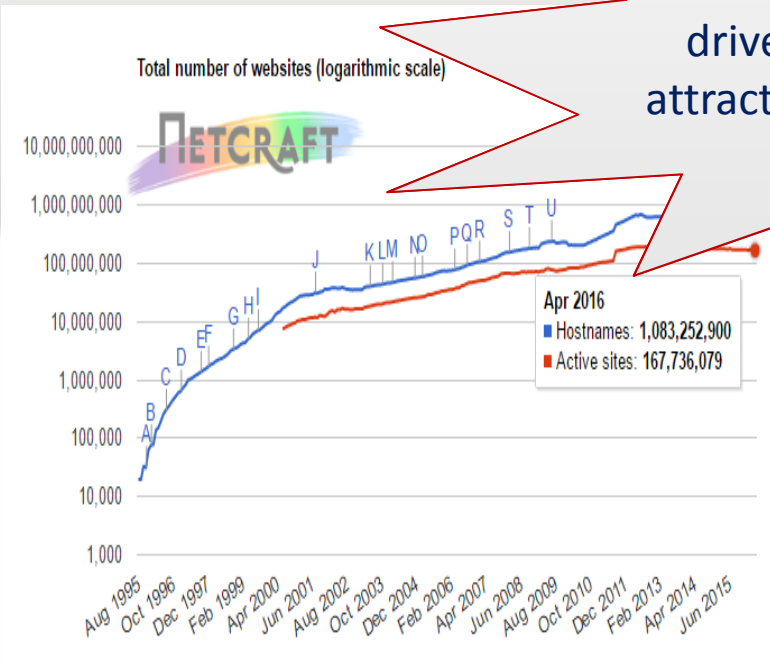
"As of Apr 2016, it is estimated that there 1,083,252,900 websites on the Internet today."

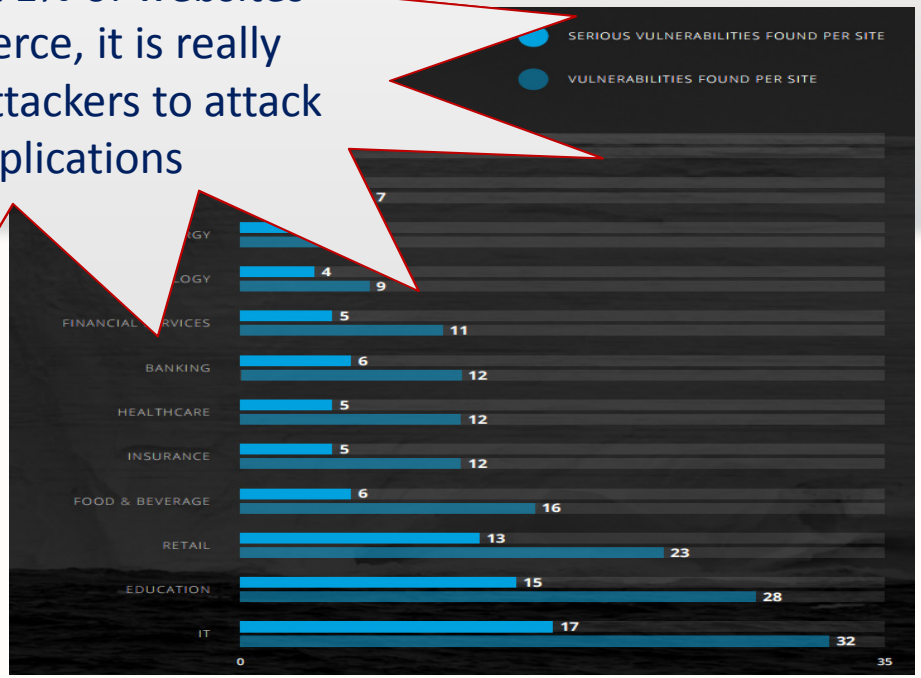
Netcraft Web

"Average vulnerabilities per site varies from 5 (in Manufacturing) to 32 (in IT)."

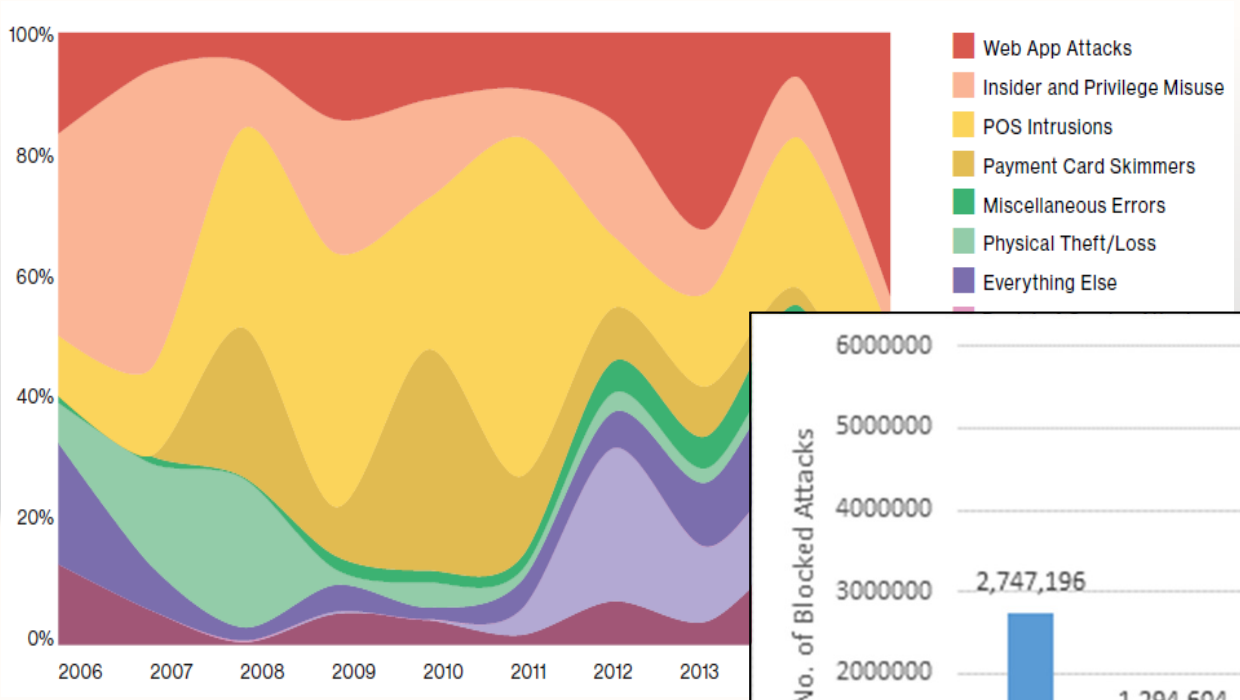
bsite Security Statistic Report, 2016

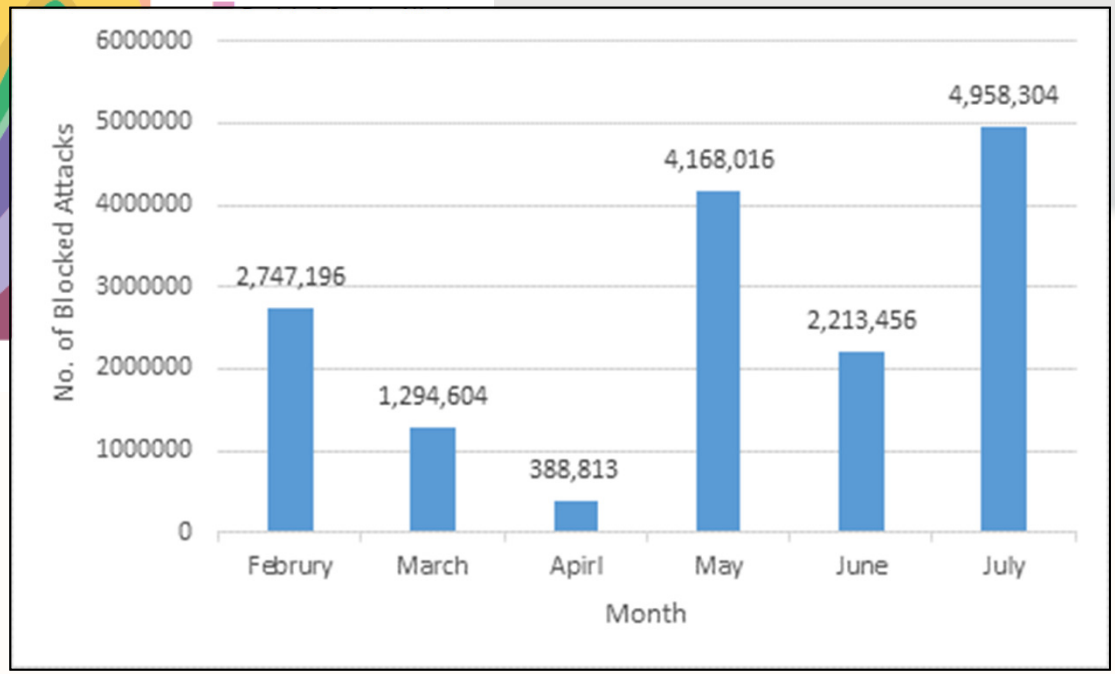
Assuming just 1% of websites drive commerce, it is really attractive to attackers to attack web applications



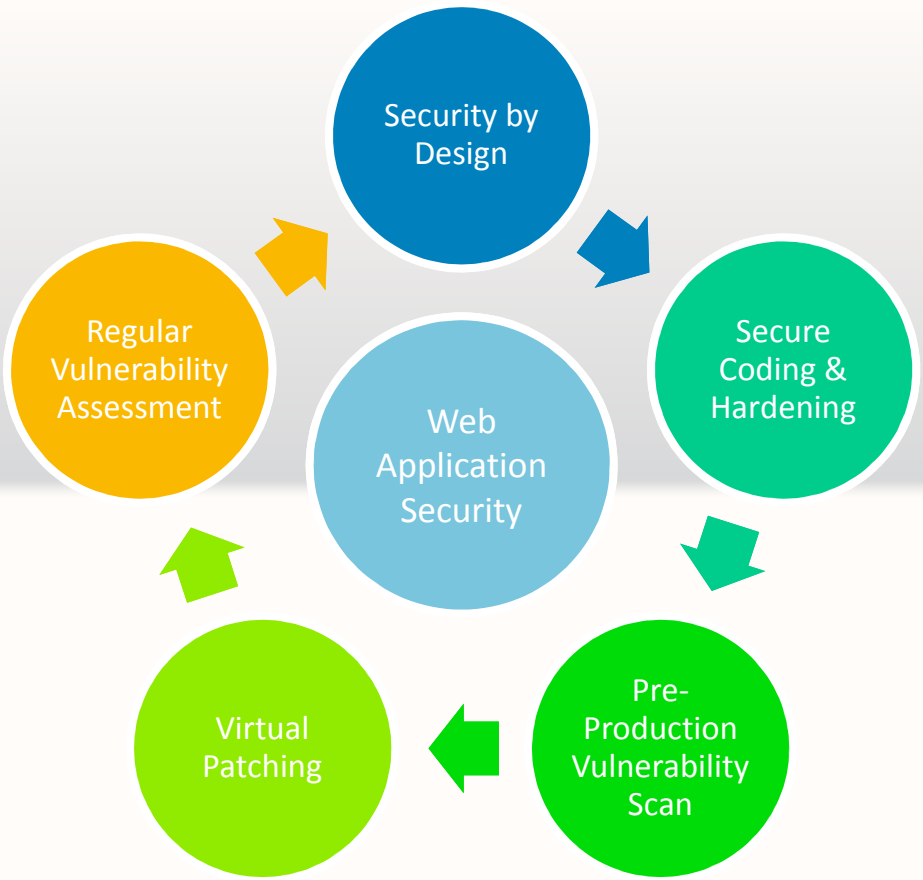


What is happening in the Internet?

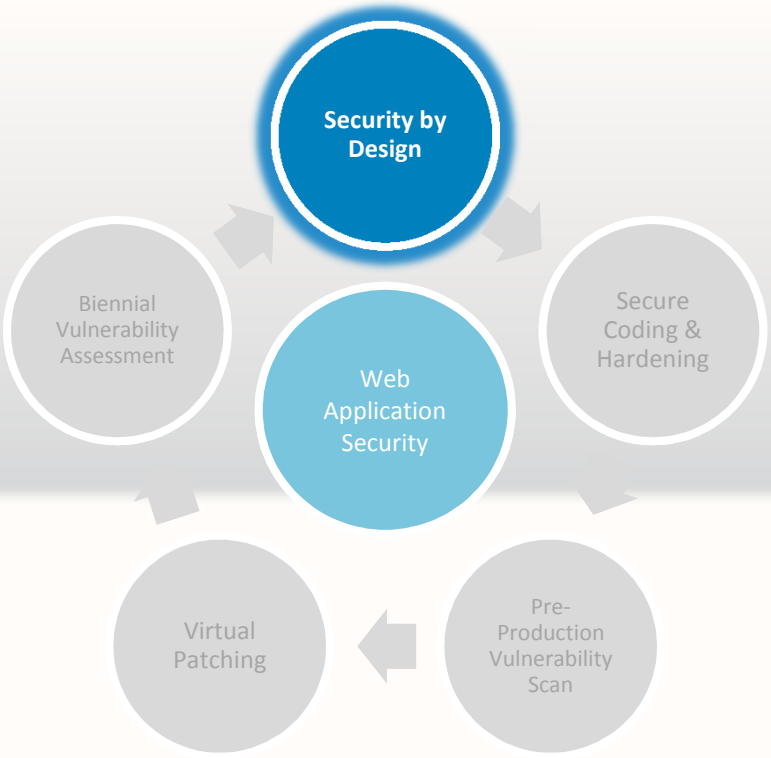


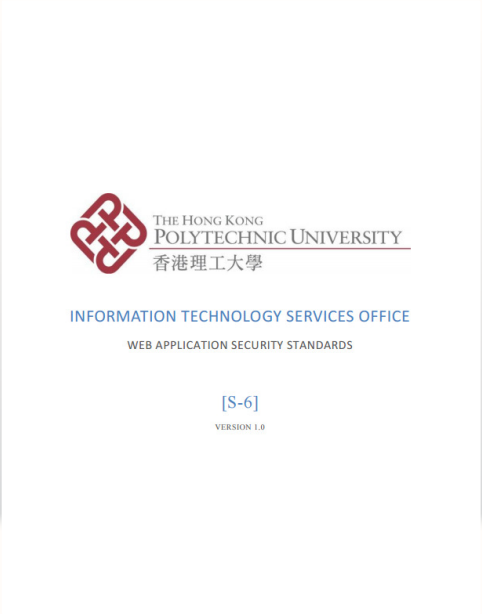


How do we tackle this threat?



Security by Design

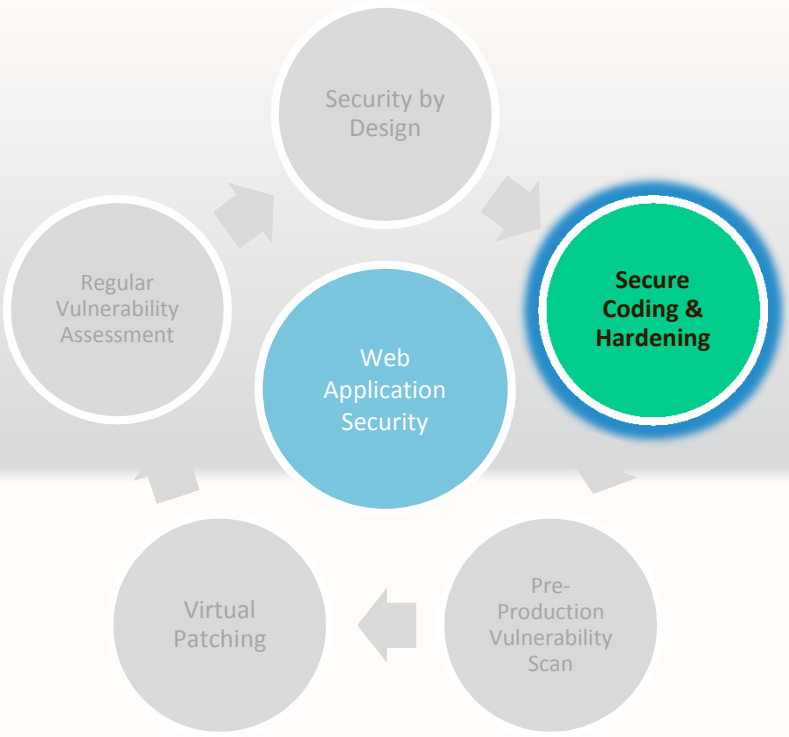




Security requirements on web application developments are developed for user departments' reference.

Sample tender specifications are provided for reference.

Secure Coding and Hardening




THE HONG KONG POLYTECHNIC UNIVERSITY 香港理工大學

Secure Coding Guidelines for Web Application & Mobile App Development

THE HONG KONG POLYTECHNIC UNIVERSITY 香港理工大學

Minimum Security Baseline

Microsoft IIS 8.5 Web Server

Version 1.0

THE HONG KONG POLYTECHNIC UNIVERSITY 香港理工大學

Minimum Security Baseline

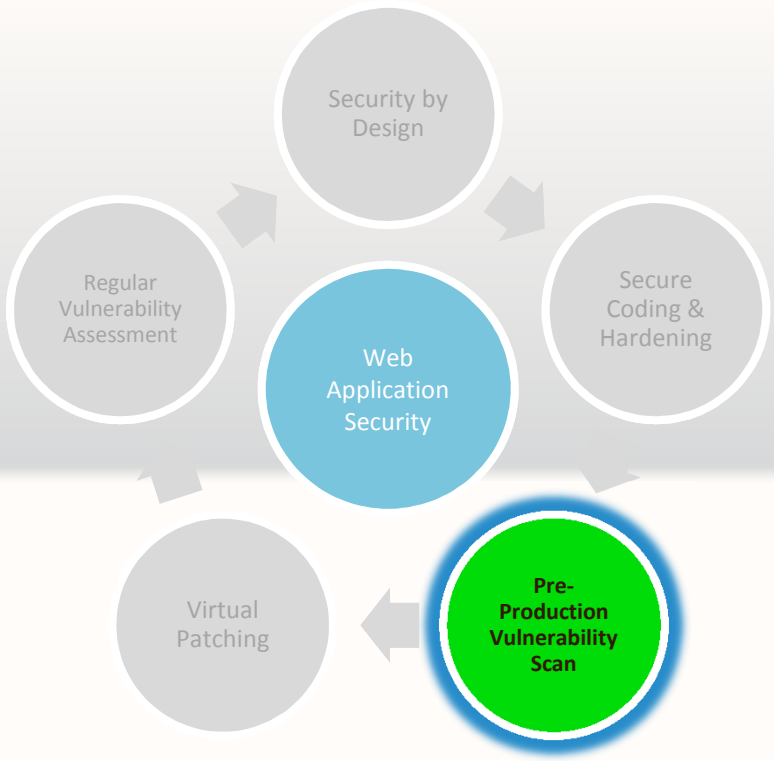
Apache HTTP Server 2.2

Version 1.1

Secure Coding Practices are provided to developers. Pseudo Codes are included.

Security Hardening Configuration Standards are developed for various web server platform.

Pre-Production Vulnerability Scan



Pre-Production Vulnerability Scan is the cornerstone of our web application security strategy

All web applications / websites need to pass through vulnerability scan before production

It is a credential / authenticated scan

Virtual Patching

- Application
- Web CMS
- Database
- System

- No input validation
- Insecure Output Handling

Virtual Patching

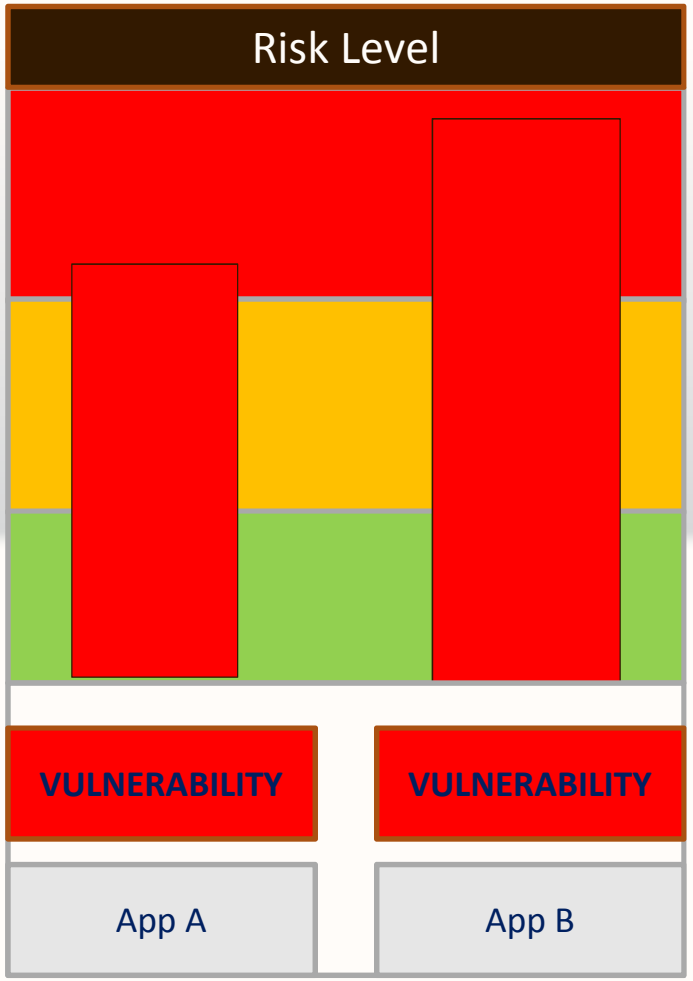
LAYERED DEFENCE

- INTERNET FW
- NETWORK IPS
- WAF
- ENDPOINT SECURITY

THREAT INTELLIGENCE

WEBINSPECT

NEXPOSE



Regular Vulnerability Assessment

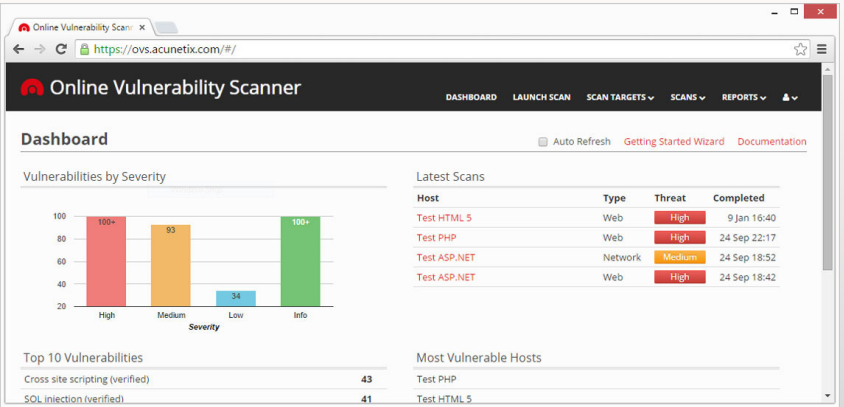
- Pre-Production Scan can only provide a snapshot. A regular vulnerability assessment is required in accordance with our security policy.
- Black Box Web Application Vulnerability Scanning from external IP addresses
  - Understand security state of an application from the outside looking in.
  - Will not exempt scanners' IP addresses on any security products like IPS / WAFs
  - No system / application credential is required

Points to be noted in Vulnerability Scan

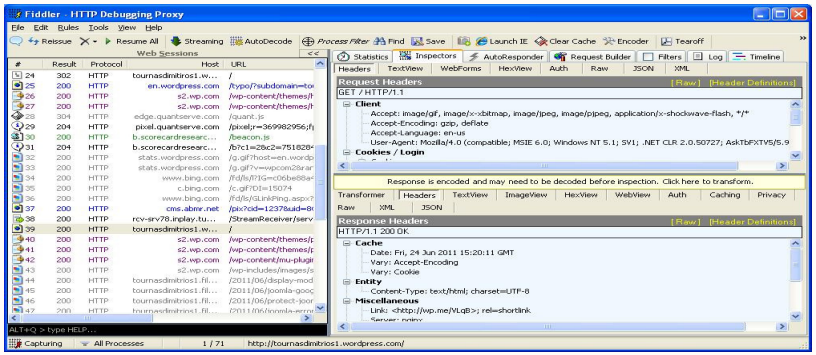
Some Useful Tools

Open Source Vulnerability Scan Tools

Free Online Scan



Free Tools Useful in Vulnerability Scan



Commercial Vulnerability Scanners

THANK YOU!

Your Logo