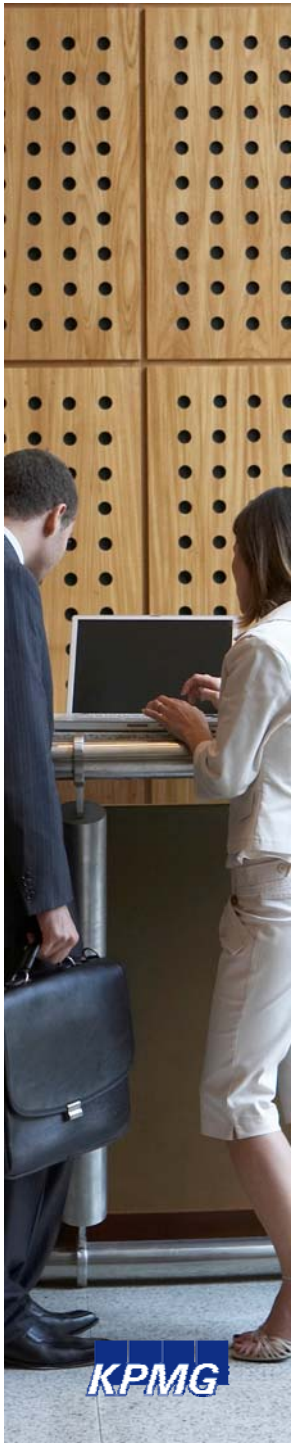
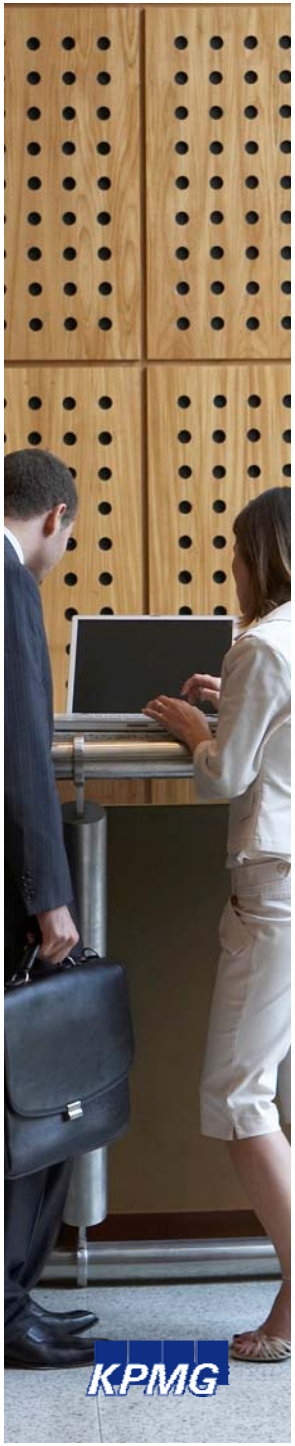

KPMG
IT ADVISORY
Google Hacking
ADVISORY
AUDIT ▪ TAX ▪ ADVISORY



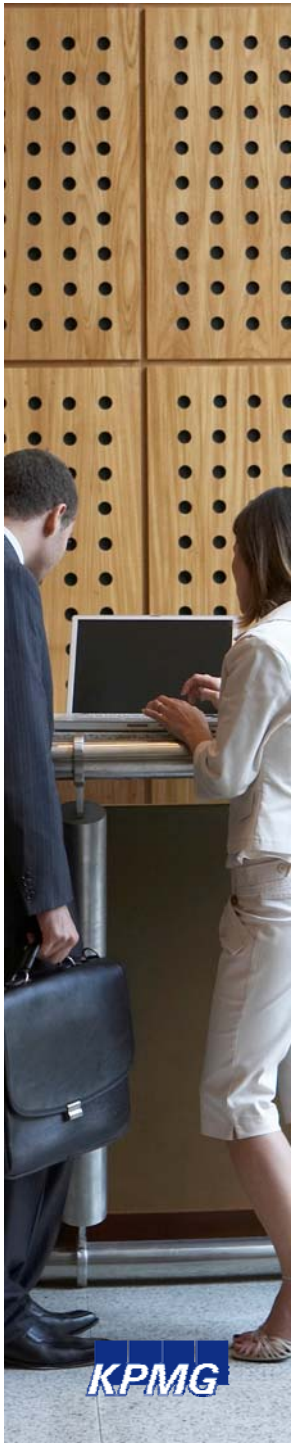
Google Hacking

- Introductie
- Wat is google hacking?
- Beperkingen
- Google Operators
- Informatievergaring & mapping
- Zoeken naar mogelijke targets
- Zoeken naar login portals en andere specifieke objecten
- Zoeken naar usernames & wachtwoorden
- Tegenmaatregelen



Introductie

- Wie ben ik?



Google Hacking, wat is het?

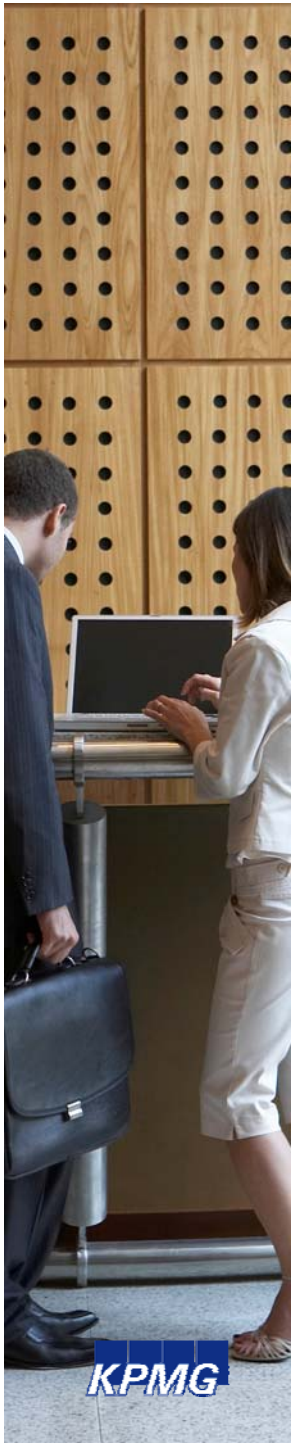
Wat is google hacking?

Web Hacking: Bepaal de site, zoek de zwakheid.
Google Hacking : Bepaal de zwakheid, zoek de site.

Maar voor security consultants ook:

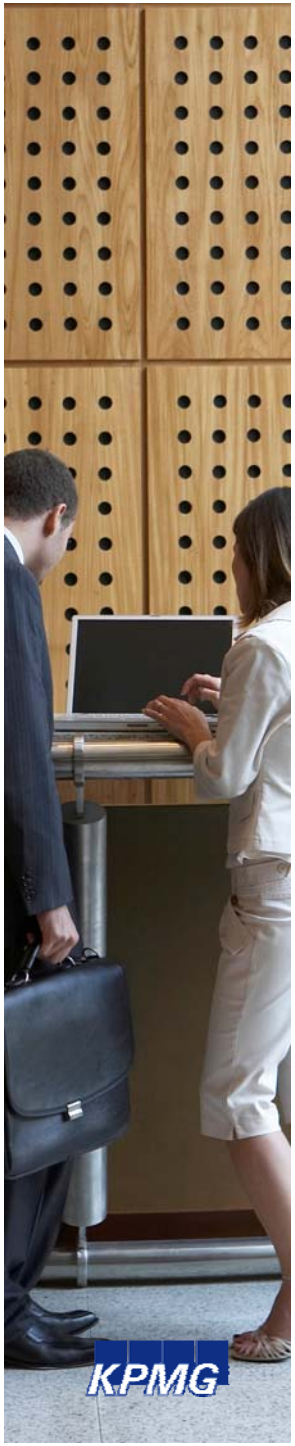
- Mapping
- Informatievergaring voor pentests
- Informatievergaring voor social engineering

Wees geen laaghangend fruit!



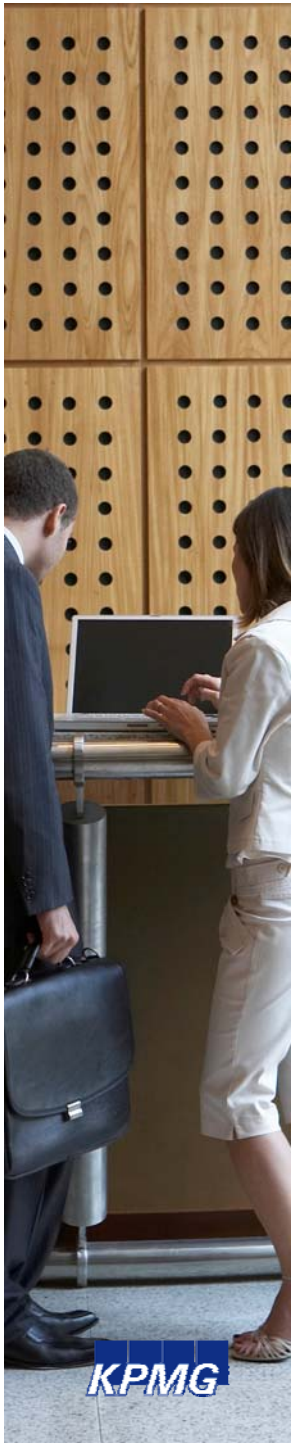
Google hacking, beperkingen

- Google indexeert veel, maar niet alles. Als google groeit, groeien ook de mogelijkheden om te googlehacken
- Te hacken content is statisch: google kan niet met dynamische content omgaan, het zijn snapshots
- Geen interactie met site



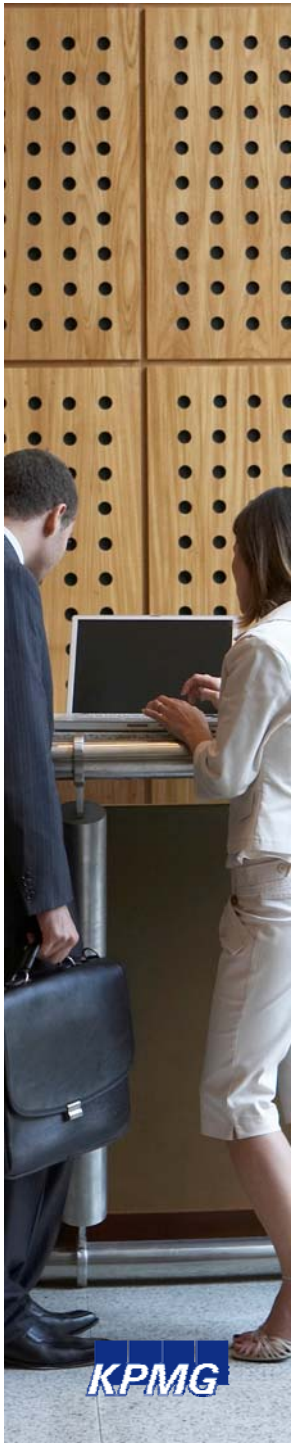
Google operators

- De normale interface
  - Web
  - Discussiegroepen (Usenet)
  - Afbeeldingen
  - Voorkeuren
  - …
- Google queries
  - Niet case sensitive
  - Wildcards
  - “Stemming”
  - Maximaal aantal termen
  - Boolean operators



Google operators - vervolg

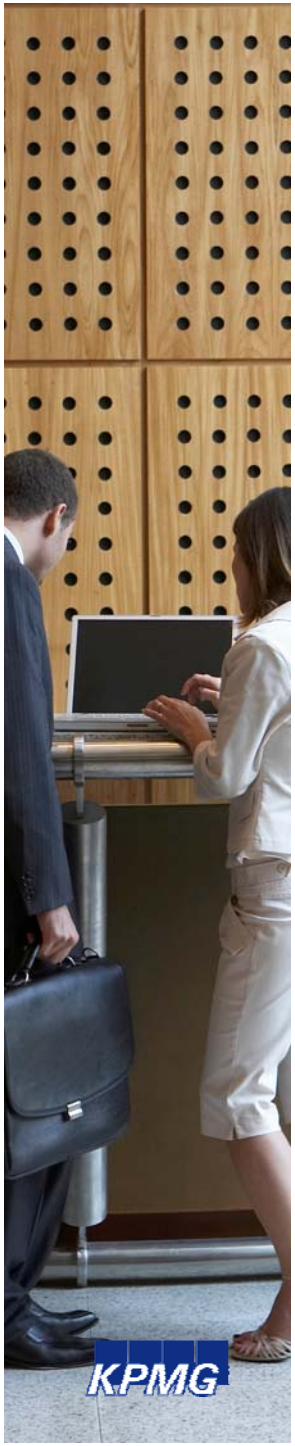
- Advanced operators
  - Intitle
  - Inurl
  - filetype
  - site
  - Link
  - Inanchor
  - Author
  - insubject
  - Phonebook
  - Cache
  - …



Informatievergaring & Mapping

- Sites vinden
  - Subdomains
  - Links
- Versie en andere informatie
  - Directory listings
  - Intranet
  - Helpdesk
  - Namen en emailadressen
- Specifieke bestanden vinden
  - Backup files
  - Configuratie files
  - Andere files
- Gebruik van online tools

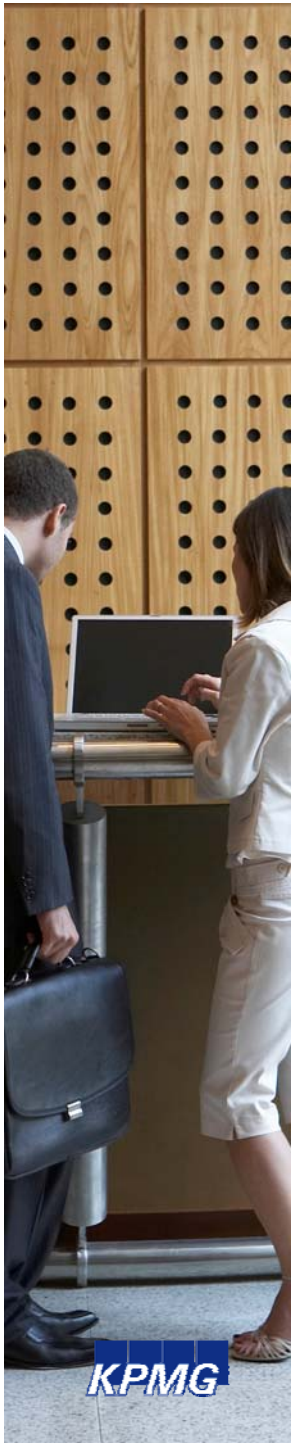
DEMO'S



Mogelijke targets

- “powered by”
- Directory listings
- Cgi scanning via Google
- Default pagina’s en voorbeeld programma’s
- Errors

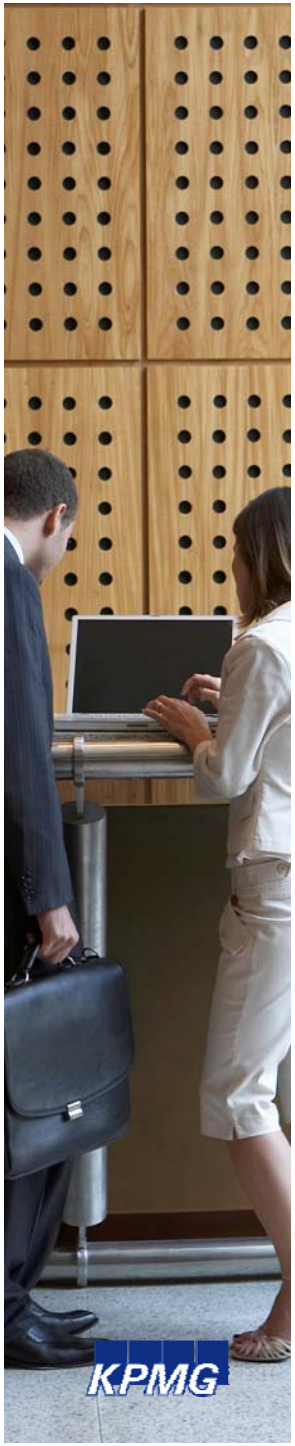
DEMO’S



Login portals en andere specifieke objecten

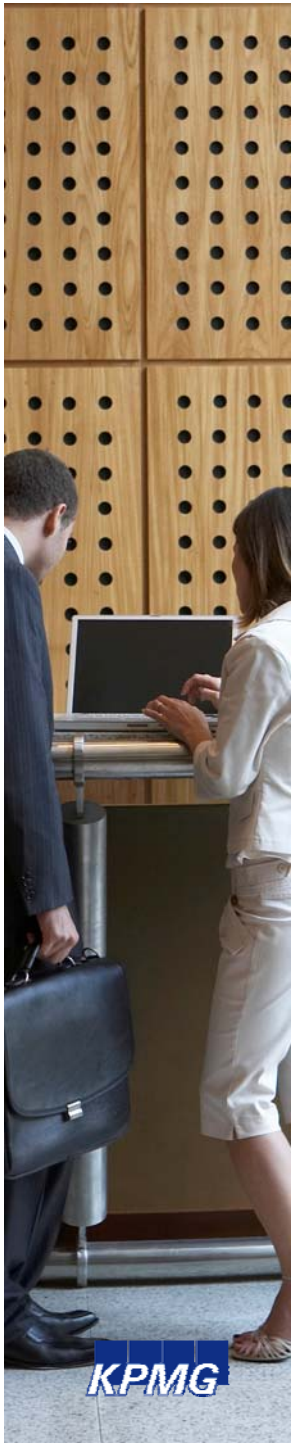
- Bekende URL’s
- Bekende titels
- Bekende tekst

DEMO’S



Usernames & Wachtwoorden

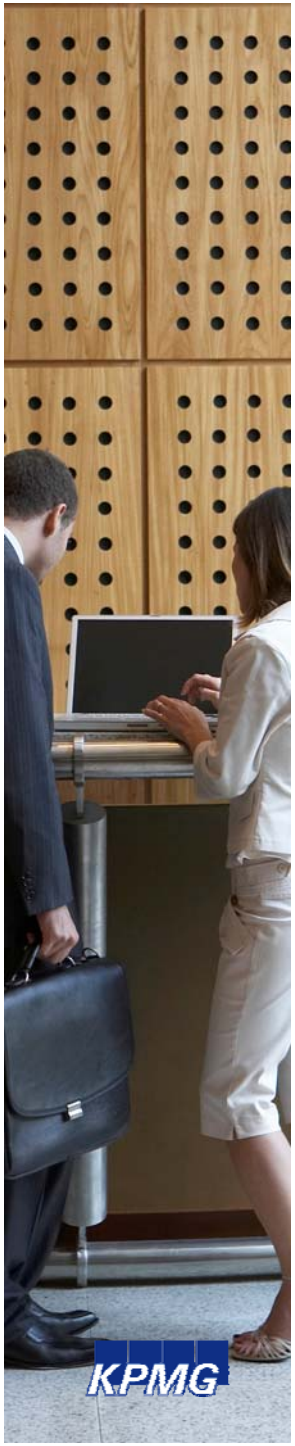
DEMO'S



Phishing voorbeeld

- Cross-site framing
  - Site zet content in frames
  - Content is extern
  - Frame source aan clientzijde bepaald

DEMO



Tegenmaatregelen

- User awareness
- Hardening
- Testing
- Wijziging versie informatie
- Stop robots volledig (nou ja…)

  User-Agent: *

  Disallow: /
- Stop robots gedeeltelijk (nou ja…)

  User-Agent: Googlebot

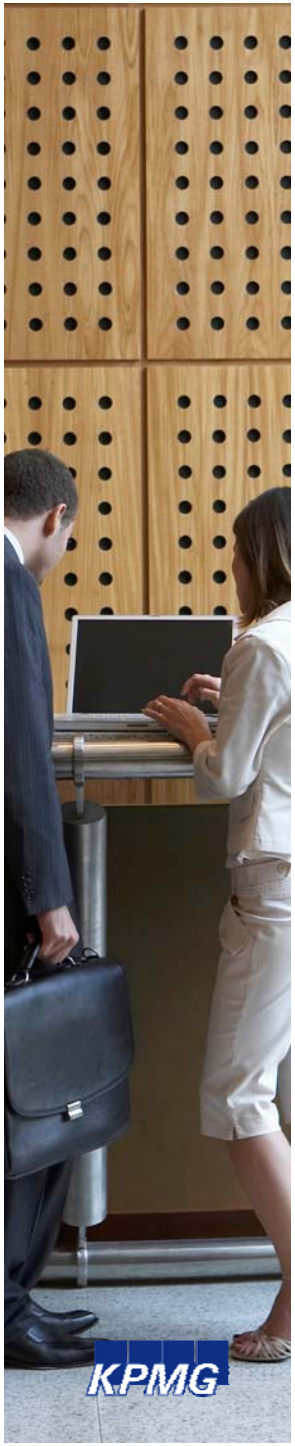
  Disallow: /*.PDF$
- Voorkom google caching / snippets

  <META NAME="ROBOTS" CONTENT="NOARCHIVE">

  <META NAME="ROBOTS" CONTENT="NOSNIPPET">
- Hulp van Google

  URL verwijdering

- Meer info: http://johnny.ihackstuff.com/ghdb.php | google hacking boek | Athena



Contactgegevens

Hans IJkel

KPMG

+31 (20) 656 8755

ijkel.hans@kpmg.nl