A Post-Mortem on Heartbleed – What Worked and What didn't

Jonathan Trull – CISO State of Colorado
Wolfgang Kandek – CTO Qualys

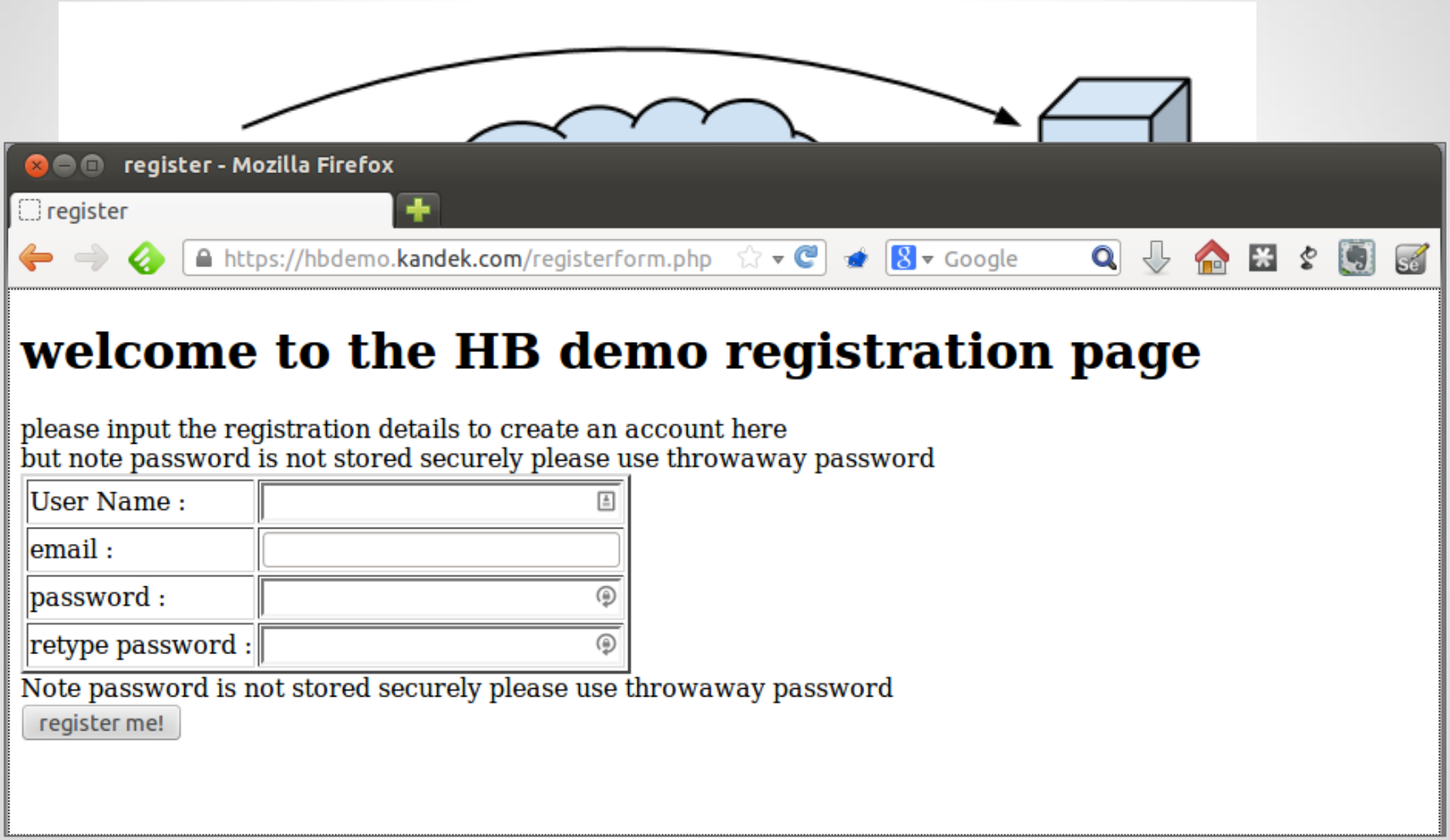
Agenda

- Technical background
- Timeline
- Testing
- Tools
- Volumes
- Stats
- Q&A

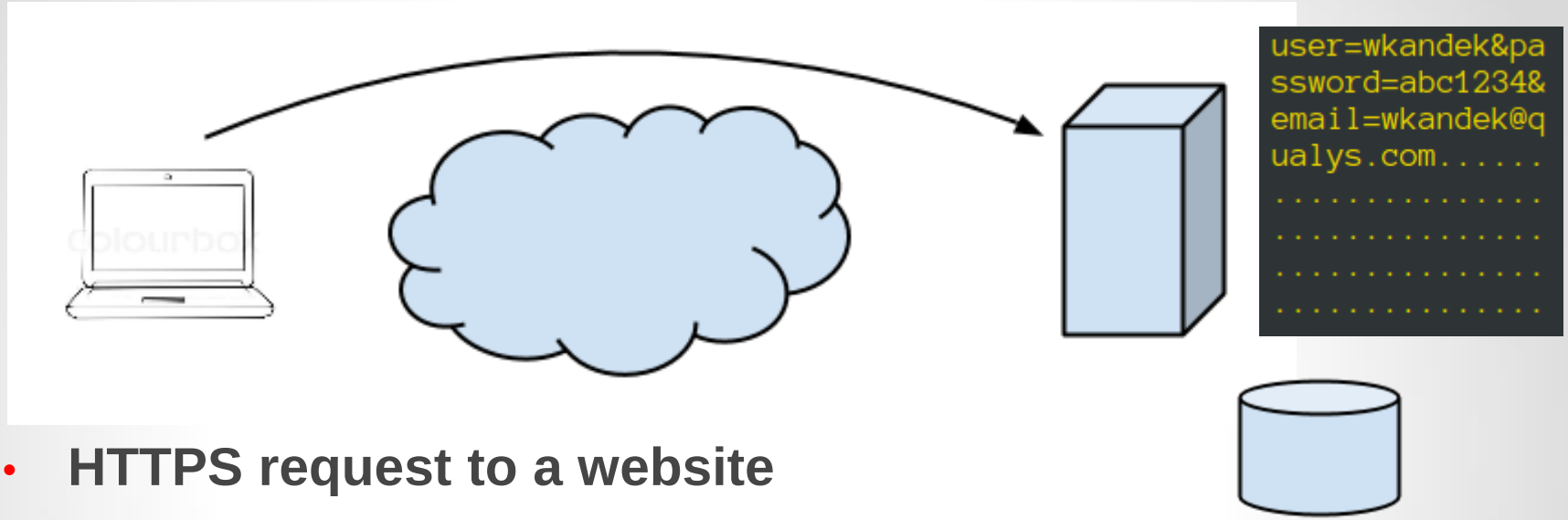
Heartbleed

- **Heartbleed is a vulnerability in the “heartbeat” extension of OpenSSL**
- **SSL (Secure Socket Layer) most visibly in use in secure web transactions**

SSL

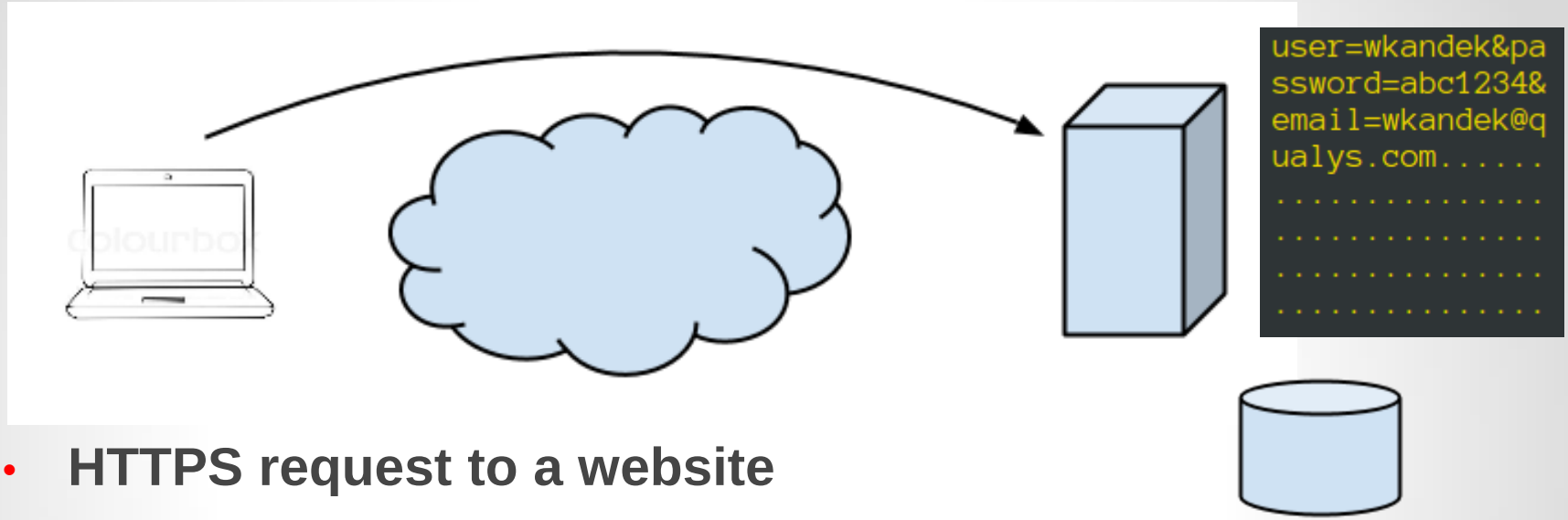

register - Mozilla Firefox
register
https://hbdemo.kandek.com/registerform.php
Google
welcome to the HB demo registration page
please input the registration details to create an account here
but note password is not stored securely please use throwaway password
User Name :
email :
password :
retype password :
Note password is not stored securely please use throwaway password
register me!

SSL



- **HTTPS request to a website**
  - https://hbdemo.kandek.com
  - Simple site with registration, login, sessions
  - Data: username, password, email
  - Ubuntu 12.04, Apache, OpenSSL, MySQL
  - Data gets written to database
  - But stays in memory as well

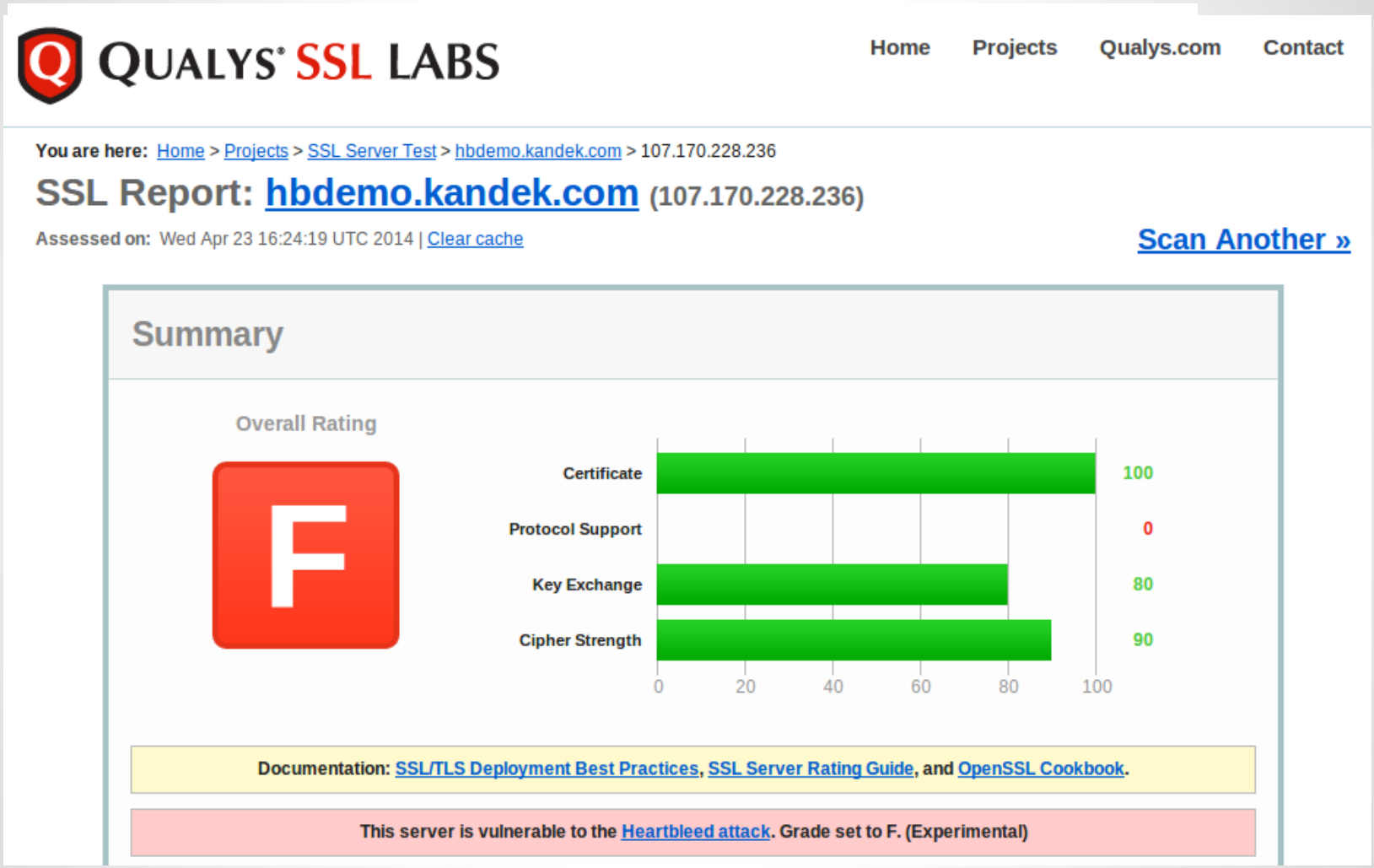
Website is vulnerable to Heartbleed!



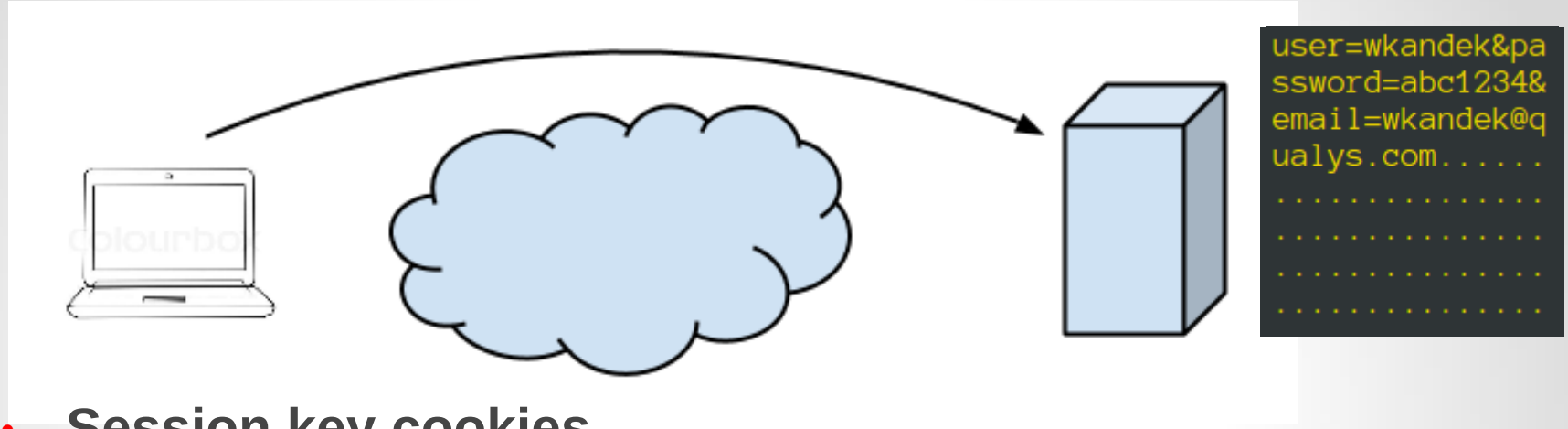
- **HTTPS request to a website**
  - https://hbdemo.kandek.com
  - Simple site with registration, login, sessions
  - Data: Username, password, email
  - Ubuntu 12.04, Apache, OpenSSL, MySQL
  - Data gets written to database
  - But stays in memory as well

SSL

Website is vulnerable to Heartbleed!

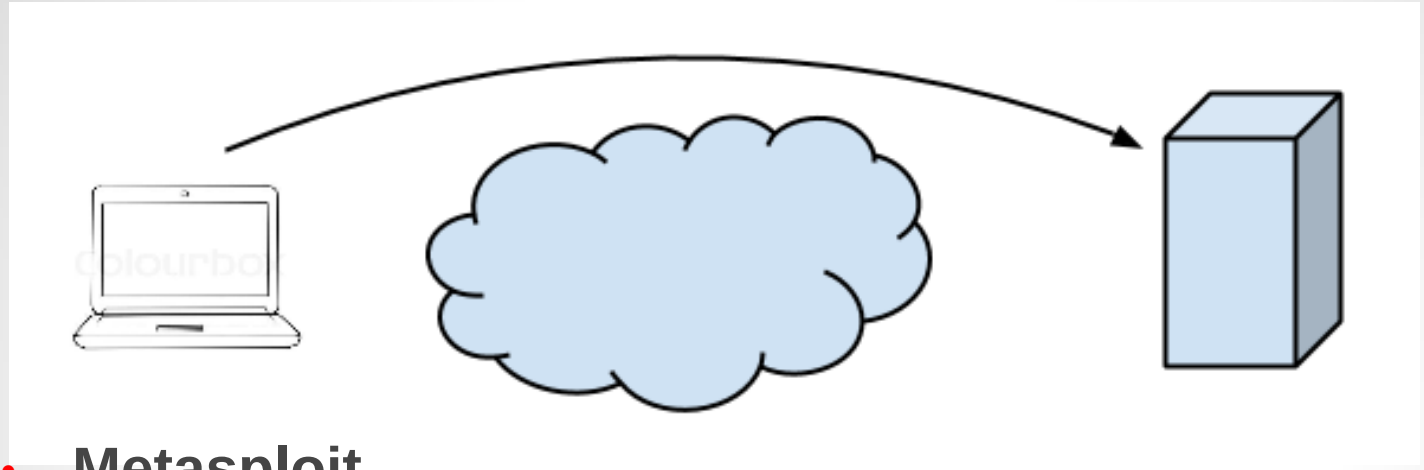


Heartbleed – What can leak



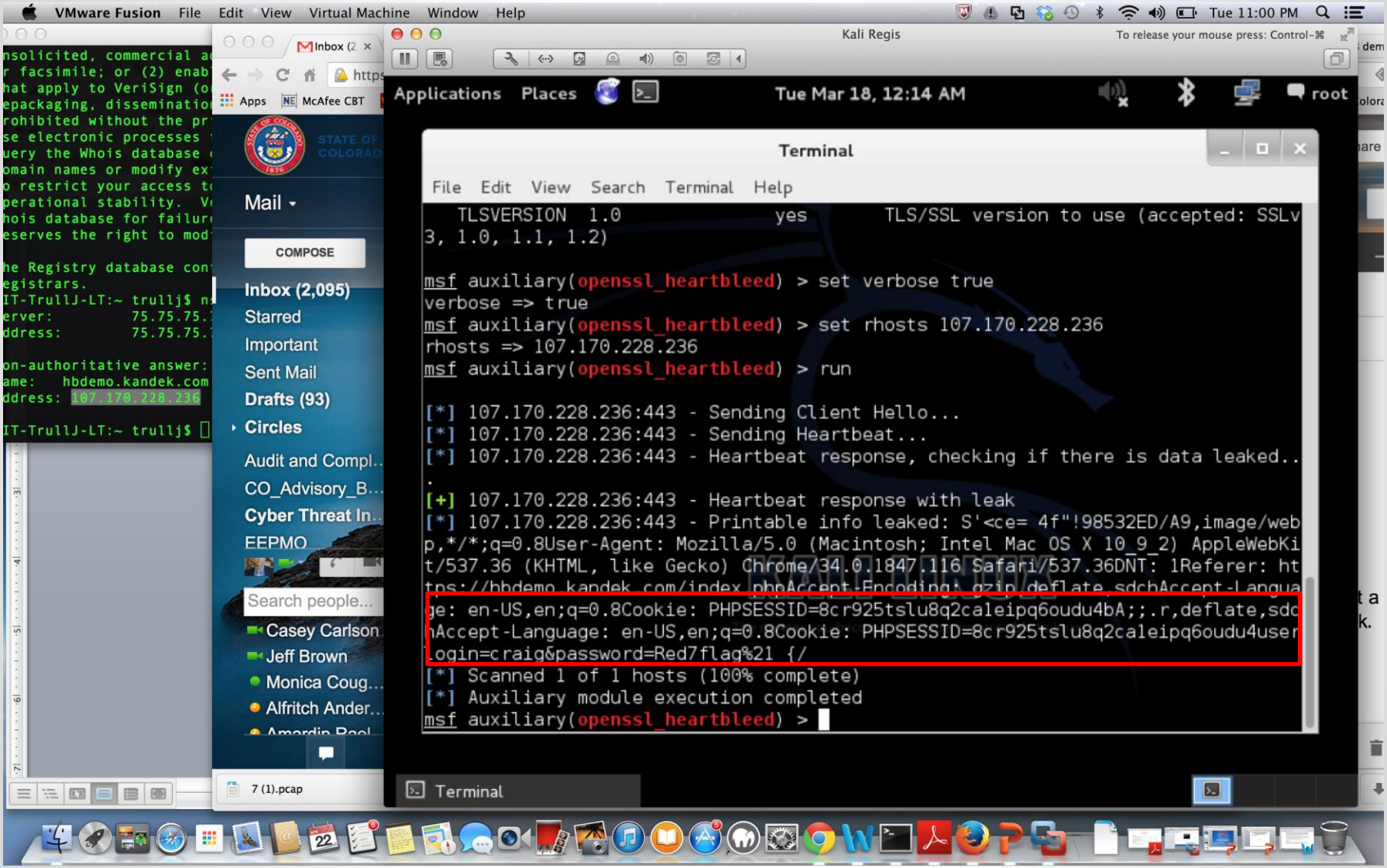
- **Session key cookies**
  - PHPSESSIONID = 0xFFA34E2DE7E1
- **Userdata, including passwords**
  - Wait - Shouldn't they be hashed?
  - Passwords are typically not hashed on client, but on server
- **Private key for certificate**
  - Allows for decryption of all traffic, future and past

Heartbleed – Leak demo

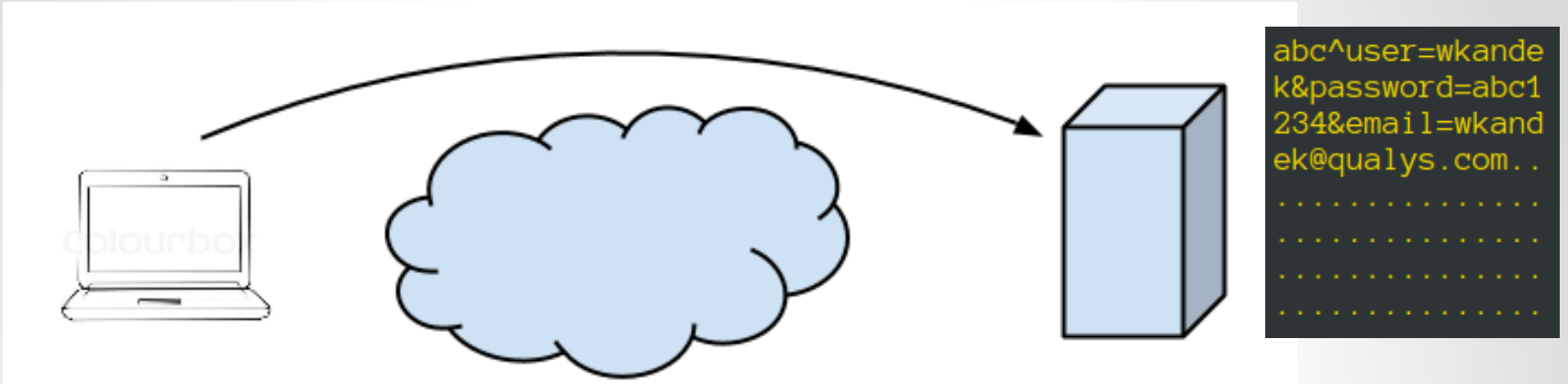


- **Metasploit**
  - About 1 week old
  - Eases Exploitation for sessions and passwords
- **Heartleech**
  - Autopwn: great for private keys

Heartbleed – Leak demo



Heartbleed - details



- **Heartbeat extension is enabled: good for performance as it keeps the session alive**
- **The Heartbeat extension has a programming flaw that allows us to receive more bytes than we sent:**
  - Regular: sent “abc”, length 3, received “abc”
  - Exploit: send “abc” length 64, received “abc” plus registration data
- **Size upto 64 KB, not logged, can be repeated freely**

Heartbleed – who is affected

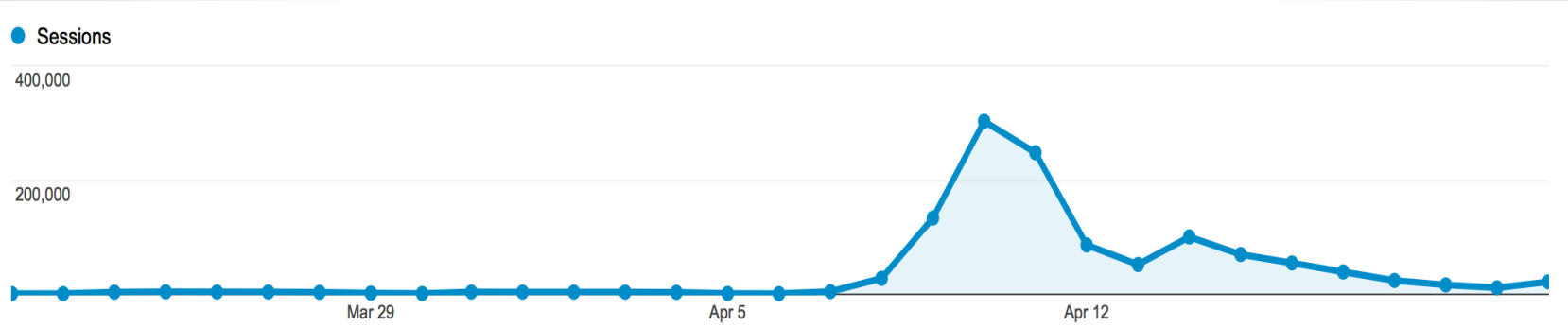
- **Vulnerability disclosed on April 7 – heartbleed.com**
  - Independently found by Google researcher Neel Mehta & Codenomicon team
- **Sites running Open SSL 1.0.1**
  - Version 1.01a-f starting from March 2012
  - Version1.0.1g from April 7 is patched
  - OpenSSL 1.0.0 is ok, so is 0.9.8
- **Other SSL implementations are not affected**
  - Microsoft IIS
  - Most SSL accelerators

Heartbleed – how to test

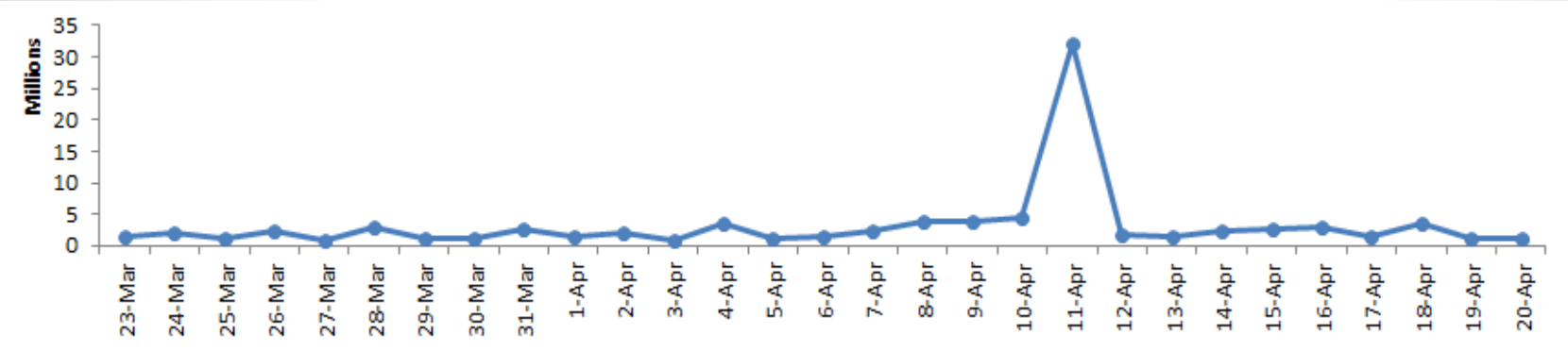
- **Internet facing: SSLLabs.com, filippo.io**
- **Scripts:**
  - nmap 6.46: --script=ssl-heartbleed ubudc.kandek.com
  - Metasploit: openssl_heartbleed scanner
  - heartleech: https://github.com/robertdavidgraham/heartleech
  - Cardiac Arrest: https://gist.github.com/ah8r/10632982
    - iLO problems
  - Others: http://www.hut3.net/blog/cns---networks-security/2014/04/14/bugs-in-heartbleed-detection-scripts-
- **Commercial Vulnerability Scanners**

Heartbleed – Test volumes

- **SSLLabs**



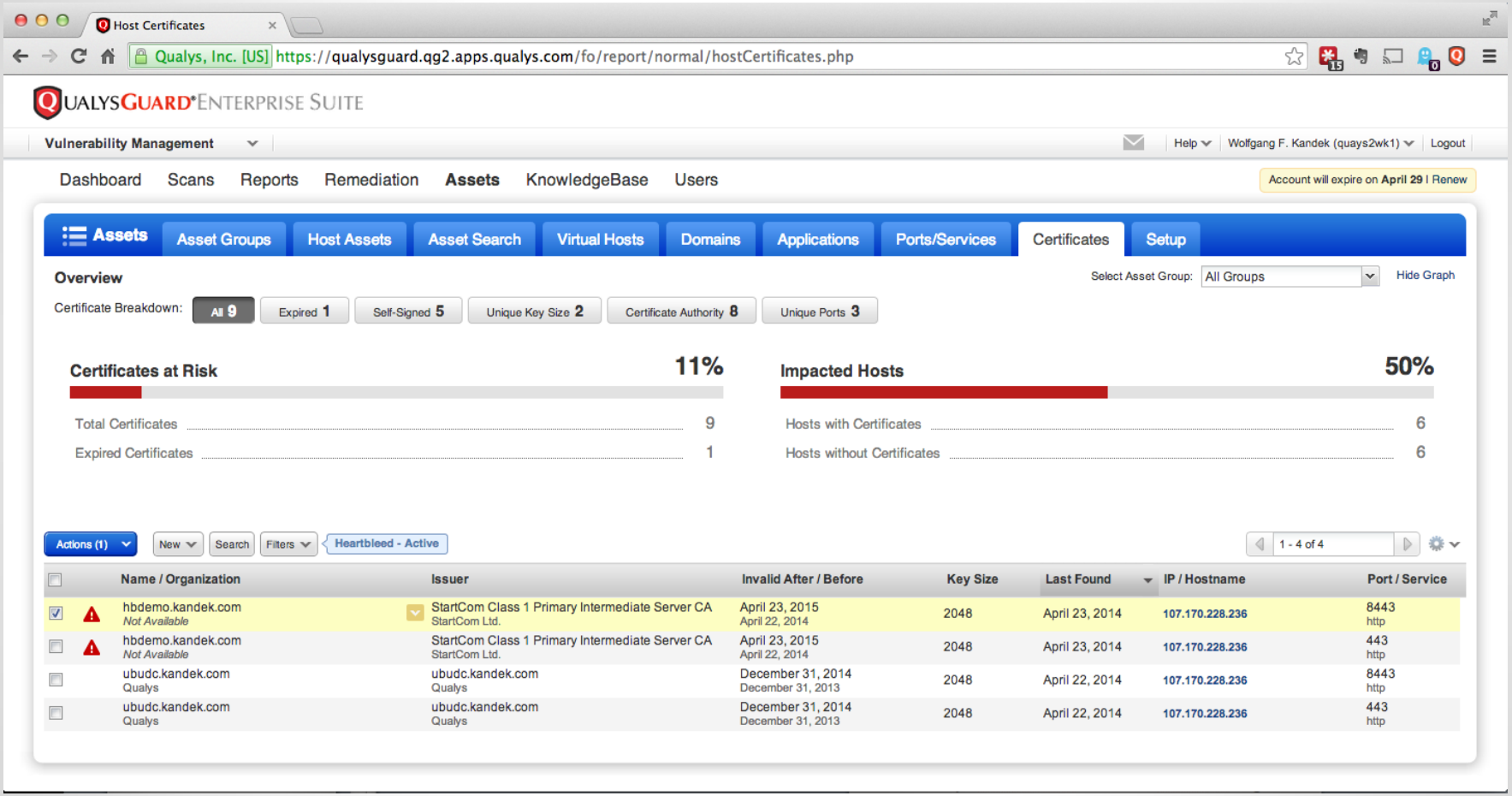
- **QualysGuard**



Heartbleed – Remediation

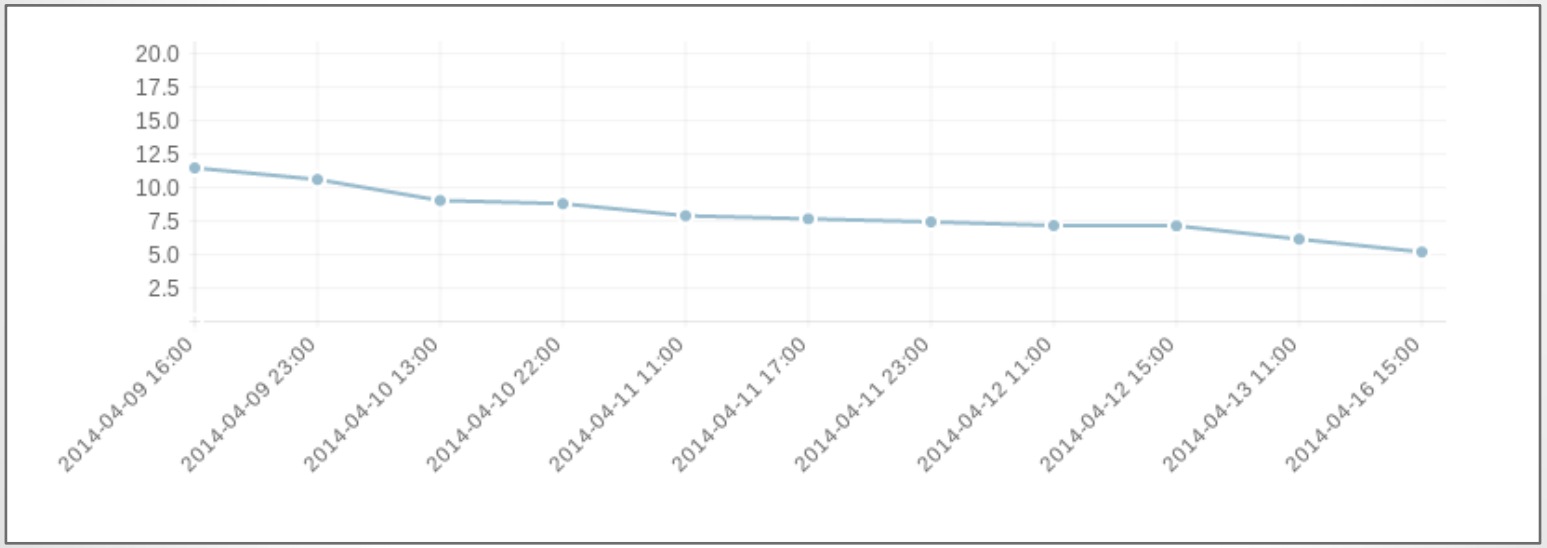
- **Find vulnerable servers**
  - Scan with your favorite tool
  - Also vendor and product alerts
- **Patch Servers**
  - Patches available for all Linux distros
  - Custom situations for other vendors
- **Renew Certificates**
  - Assume the private key was compromised
  - Your CA might offer free replacements
- **Inform your users for password changes**
  - Inform/Enforce

Heartbleed – Remediation



Heartbleed – Sites affected

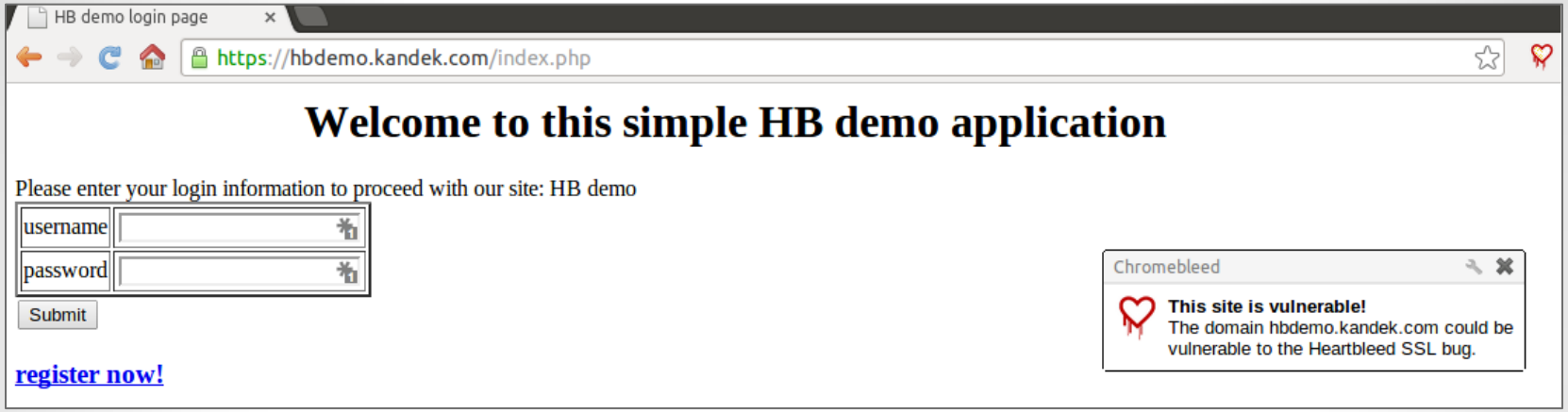
- **Yahoo, Imgur, Okcupid, Canadian IRS, Healthcare.gov?**
- **Cloudflare, Akamai**
- **Alexa 1 Million sites – percent vulnerable**



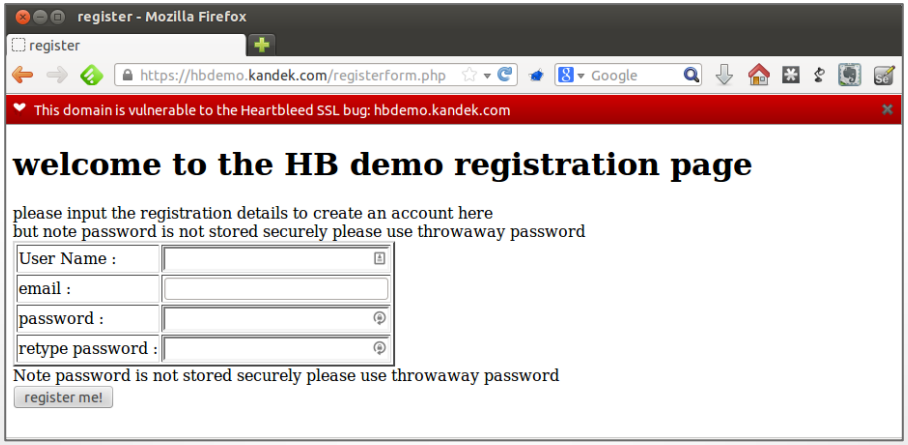
- **Check here: https://zmap.io/heartbleed/vulnerable.html**
- **Also: SSL Pulse https://www.trustworthyinternet.org/ssl-pulse/**

Heartbleed – More Tools

- **Chrome Browser Plugin – Chromebleed**

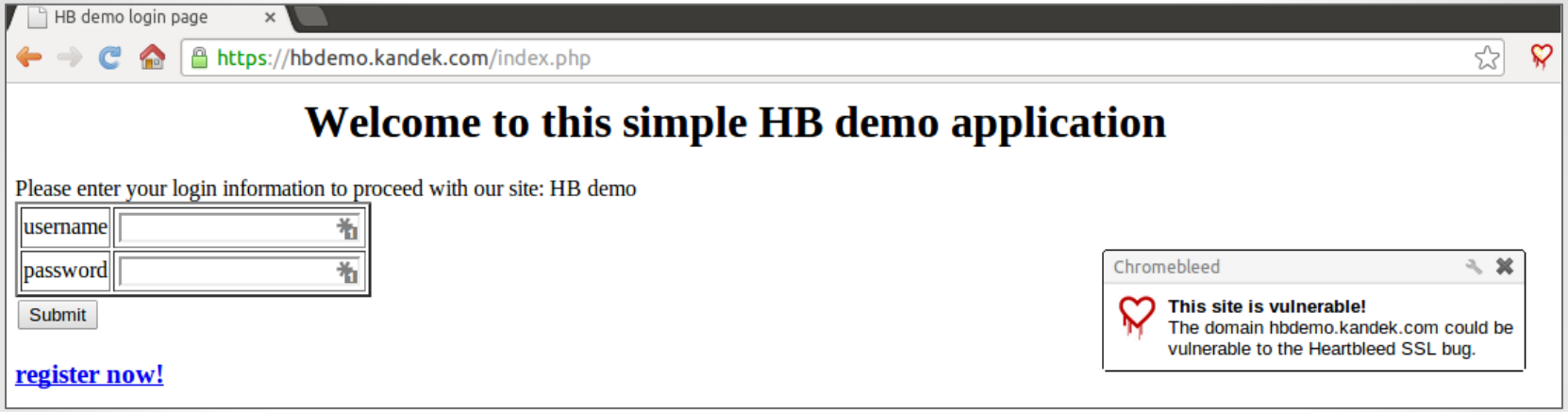


- **Firefox Browser Plugin**



Heartbleed – Demo Site

- **https://hbdemo.kandek.com**



- **Feel free to create an account and test**
- **There is a file on there with a secret message**
- **Email us the cleartext of the secret message**
  - First 3 get a Qualys sponsored prize
  - Same for best writeup of the exploit process with screenshots

Thank you

Questions?

jonathan.trull@state.co.us
wkandek@qualys.com

***Visit the Qualys community page at** https://community.qualys.com/docs/DOC-4767