



# Cloudy with a chance of 0-day


Jon Rose  
Trustwave  
[jrose@trustwave.com](mailto:jrose@trustwave.com)

**OWASP**


November 12, 2009

**The OWASP Foundation**

<http://www.owasp.org>

A close-up photograph of a person's hand holding a white rectangular card. The hand is positioned on the left side of the frame, with the thumb and index finger gripping the edges of the card. The card is held horizontally and contains four lines of black text. The background is a plain, light-colored surface.

Jon Rose  
Trustwave SpiderLabs  
Phoenix OWASP  
DC AppSec 09!


A close-up photograph of a person's hand holding a white rectangular card. The hand is positioned on the left side of the frame, with the thumb and index finger gripping the edges of the card. The card is held horizontally and contains three lines of black text. The background is a plain, light-colored surface.

Tom Leavey  
Trustwave SpiderLabs  
NYC

# Cloud Fluff

## Google App Engine

### Security risks




**“... dynamically scalable and often virtualized resources are provided as a service over the internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure”**

**Source: Wikipedia**



# Marketing Hype



# **Software** **as a Service**

# Platform as a Service





# Infrastructure as a Service

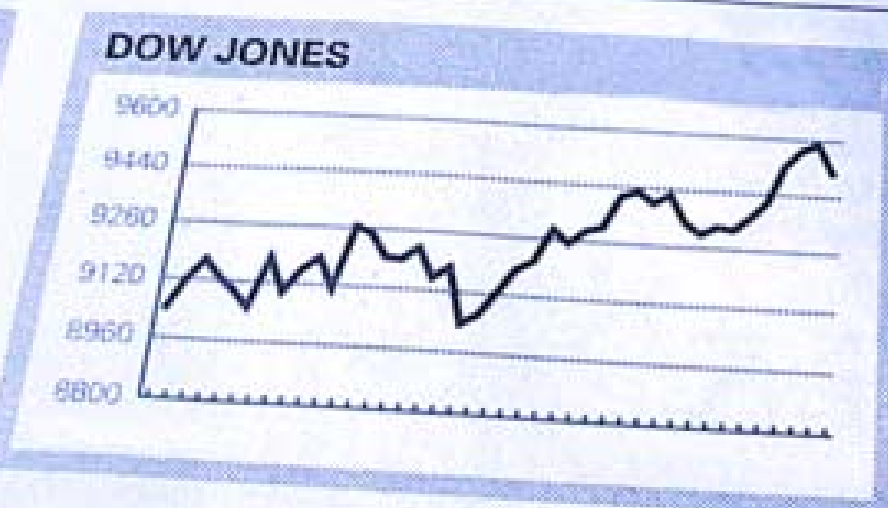




**Why the Cloud?**

ING linc euro100	58,30	59,75
ING linc dowjones	72,25	72,30
ING linc nvidia	65,00	65,00
ING linc eur at50	67,70	67,75
ING linc eur at50	43,10	43,10
ING linc eur tec	56,45	56,75
ING linc usa 500	42,20	42,35
ING north am f.	58,85	60,05
ING oblig. f	31,40	31,20
ING onr.aandf.	18,50	18,65
ING protec.mia-70	15,97	15,97
ING protec.mia-80	47,85	48,53
ING protec.mia-90	20,55	21,05
ING telecom serv.f.	22,85	22,85
ING utilities fd	24,60	24,70
ING verre doestf.	26,65	26,70
Intereff.jap.af.	28,60	28,40
Intereff.jap.w.	24,30	24,30
IS himal.f	13,20	13,02
Jap.conv.fund	1,69	1,63
Japan fund c	13,00	12,00
Labouch.glob.af	28,10	29,00
Labouch.obl.fd	3,45 A	3,45 A
Lanschat dutch ef.	24,10	23,50
Lanschat euro credt.	53,30	53,55
Lanschat eur.af.	26,80	26,89
Lanschat far.af.	48,99	49,00
Lanschat gl.bond f.	16,75	16,46
Lanschat gl.eqf.	27,40	26,60
Lanschat ict f.	58,20	58,20
Lanschat raged	31,89	31,68
	9,75	9,75
	156,30	157,90

Opt biotech fd		
Opt europe fd D		
Opt income fd C		
Opt mix fd E		
Opt techn. fd A		
Orange deeln fd		
Orange eur comp fd		
Orange eur mc f		
Orange eur prop fd		
Orange eur smc f		
Orange fund		
Orange eur.largecapf		
Orange largecapf		
Orange sense fd		
Orange wine fund	11,10	
Pacific r.c.f.	58,50	
Pan glob conv f.	34,26	
Postb.aandf	31,00	
Postb.aex click 00/05	48,00	
Postb.aex click 03/10	23,77	
Postb.amerika f.	34,15	
Postb.beleggf	17,90	
Postb.biotech f	34,01	
Postb.com tech f	14,30	
Postb.duurz.aandf	10,20	10,40
Postb.easy bluefd	17,00	17,20
Postb.eur.aandf	21,00	21,15
	18,40	18,35




Rob z	2,40	
Rob z	7,70	
Rob z	38,44	
Rob z	40,90	40,62
Rob z selfs.med.bio	12,12	11,92
Rob z selfs.property	65,25	64,55
Rob z selfs.soft&ser	9,25	9,50
Rob z selfs.telecom	26,15	26,50

**No infrastructure investment**

**Expand or shrink based on demand**





**Pay as  
you go**

# Scaling and load balancing





**It's the Next  
Big Thing**

# New Opportunities



- Nasdaq “Market Replay”
  - ▶ Amazon S3 & AIR frontend
- New York Times: 1851 – 1989
  - ▶ TIFF uploaded & PDF'd on Amazon S3



# Too expensive for traditional development process



# Potential Problems





**Vendor Lock-In**

# Multitenant Infrastructures



# **Evolving IT experiment vs. Enterprise-ready environments**





**Forensics**

# Compliance



# Third Party Data Processing





# Where are you in the "Cloud"?





# Compliance?

Sarbanes-Oxley

HIPAA



# Cloud (Mis)use

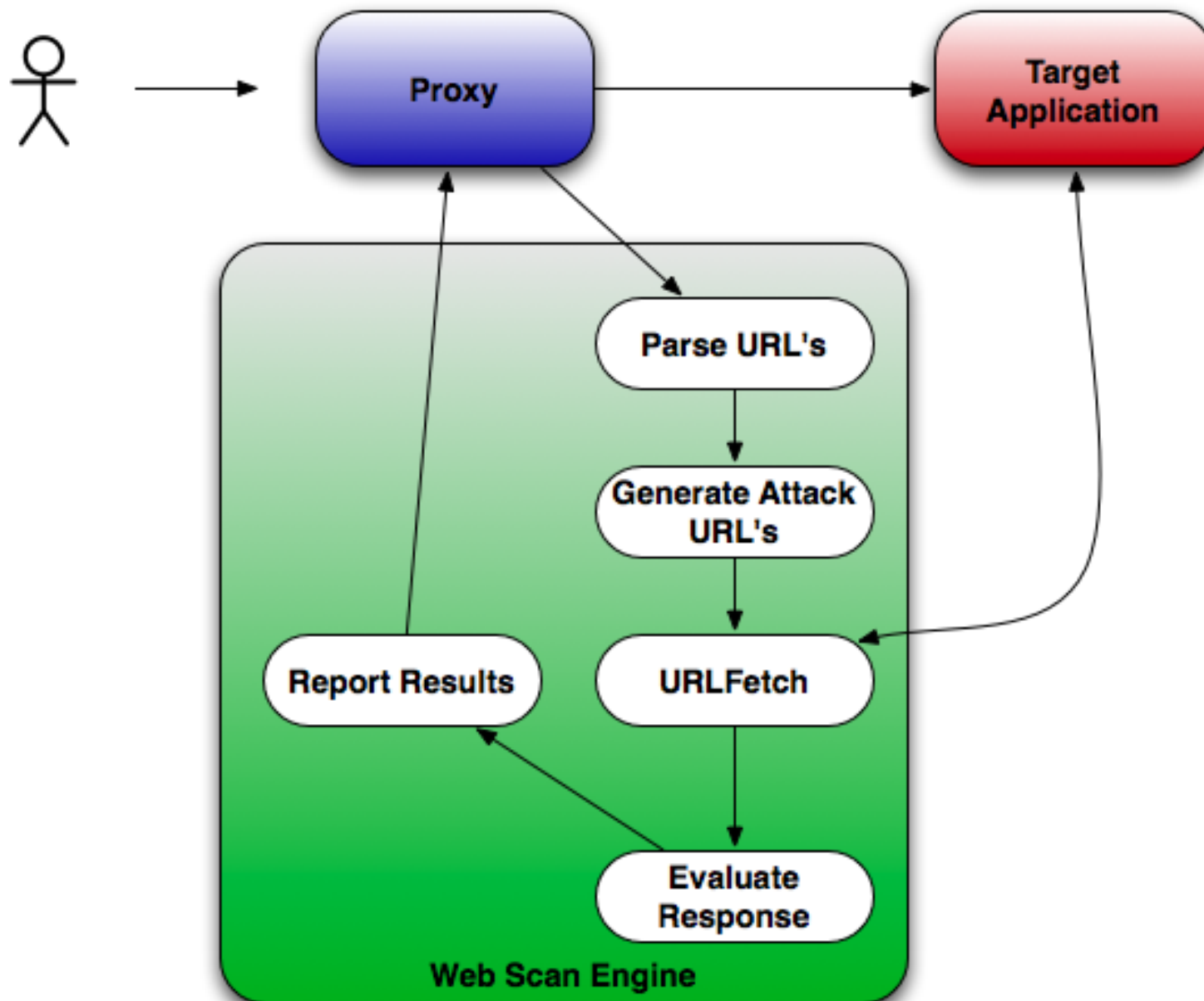


## ■ Sensepost

- ▶ Sifto
- ▶ Malicious vms
- ▶ BruteForce forgot password links

## ■ PGP zip password cracking

# Cloud Security Testing Service



# NSW Response Time Study

- 7 month study of Amazon EC2, Google AppEngine and Microsoft Azure
  - ▶ Scaled well to meet demand
  - ▶ Inconsistent performance results
    - Response times varied by a factor of 20
    - Effected by time of day
- No hard data
- Emailed Anna Liu...

# Cloud Providers



Google App Engine



at&t





# Google App Engine (GAE)



**Run your web apps on Google's infrastructure.**

Easy to build, easy to maintain, easy to scale.



# Google App Engine (GAE)

- Released April 2008
- Full application stack for developers
- Python/Java API into Google's infrastructure
- Currently free – Preview Release
- SDK provides local development environment

# Runtimes



- “webapp”  
Framework
- Version 2.5.2
- No C Extensions



- Servlets or JSP's
- Version 6

- White List

# Sandbox



- Limited access to OS
- Only access Internet through API's

**30 Seconds Max**

# Datastore

- Google DB: Bigtable
- Data objects AKA "Entities"
- Concurrency control
- Transactions



# API's

- Users API
- Email
- URL Fetch
- Memcache
- Image Manipulation

Google™



# Cron and Queues

## ■ Schedule Tasks

- ▶ Handled by the Cron service
- ▶ Invoke a URL at a given time

## ■ Task Queues

- ▶ Background task created while handling a request
- ▶ Experimental Feature
- ▶ “Web Hook”
- ▶ Only for Python

## ■ Same Limits/Quotas as HTTP request



# Quotas

Resource	Free Default Quota		Billing Enabled Quota	
	Daily Limit	Maximum Rate	Daily Limit	Maximum Rate
Requests	1,300,000 requests	7,400 requests/minute	43,000,000 requests	30,000 requests/minute
Outgoing Bandwidth ( <a href="#">billable</a> , includes HTTPS)	1 gigabyte	56 megabytes/minute	1 gigabyte free; 1,046 gigabytes maximum	740 megabytes/minute
Incoming Bandwidth ( <a href="#">billable</a> , includes HTTPS)	1 gigabyte	56 megabytes/minute	1 gigabyte free; 1,046 gigabytes maximum	740 megabytes/minute
CPU Time ( <a href="#">billable</a> )	6.5 CPU-hours	15 CPU-minutes/minute	6.5 CPU-hours free; 1,729 CPU-hours maximum	72 CPU-minutes/minute

Outgrowing the maximums? [Request an increase.](#)

# Billing Quotas

## Resource Allocations:

Resource	Budget	Unit Cost	Paid Quota	Free Quota	Total Daily Quota
CPU Time	n/a	\$0.10/CPU hour	n/a	6.50	6.50 CPU hours
Bandwidth Out	n/a	\$0.12/GByte	n/a	1.00	1.00 GBytes
Bandwidth In	n/a	\$0.10/GByte	n/a	1.00	1.00 GBytes
Stored Data	n/a	\$0.005/GByte-day	n/a	1.00	1.00 GBytes
Recipients Emailed	n/a	\$0.0001/Email	n/a	2,000.00	2,000.00 Emails
<b>Max Daily Budget:</b>	n/a				





**Account Signup requires **SMS** message to activate account**

# Terms of Service

- Only access Admin interface through API
- Cannot link multiple Apps into single App
- Pre-screen, review, flag, filter, modify, refuse or remove any or all Content from the Service
- Google has no responsibility or liability for the deletion or failure to store any Content and other communications maintained or transmitted

# App Engine Security Details



# Python Multiple Buffer Overflow Vulnerabilities

Bugtraq ID:	30491
Class:	Boundary Condition Error
CVE:	CVE-2008-2315 CVE-2008-2316 CVE-2008-3142 CVE-2008-3143 CVE-2008-3144
Remote:	Yes
Local:	No
Published:	Jul 31 2008 12:00AM
Updated:	Jul 27 2009 05:45PM
Credit:	David Remahl, Justin Ferguson, Google Security Team

# Python Multiple Buffer Overflow Vulnerabilities

Bugtraq ID: 30491

Class: Boundary Condition Error

CVE: CVE-2008-2315  
CVE-2008-2316  
CVE-2008-3142  
CVE-2008-3143  
CVE-2008-3144

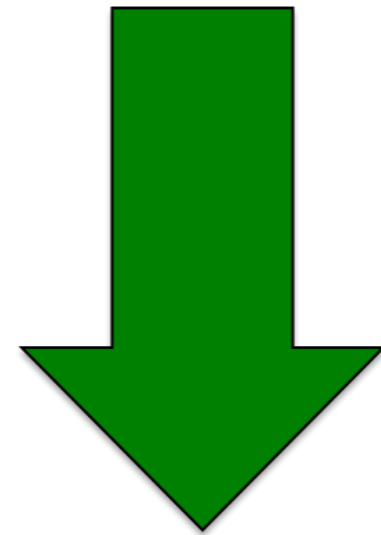
Remote: Yes

Local: No

Published: Jul 31 2008 12:00AM

Updated: Jul 27 2009 05:45PM

Credit: David Remahl, Justin Ferguson, Google Security Team



**“The team identified and fixed the underlying problem and service has now been restored.”**





# Cloud Risks





# Client-Server

Business Logic  
Data Validation

30 seconds



**SSL only on  
appspot.com  
subdomains**



# Availability & Crashes



Error

## Server Error

The service you requested is not available yet.

Please try again in 30 seconds.

---

# GAE System Status

	◀	▶	08/16/09	08/17/09	08/18/09	08/19/09	08/20/09	08/21/09	Yesterday	Today	Now
Serving											
Python	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	Normal
Java	✓	?	✓	✓	✓	✓	✓	✓	✓	✓	Normal
APIs											
Datastore	✓	✓	!	✓	!	✓	✓	✓	✓	✓	Normal
Images	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Normal
Mail	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Normal
Memcache	✓	✓	?	✓	✓	✓	✓	✓	✓	✓	Normal
Urlfetch	?	?	?	✓	✓	✓	✓	✓	✓	✓	Normal
Users	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Normal

The following symbols signify the most severe issue (if any) encountered during that day. Click a symbol in the table above to view a day's performance graphs.

✓ No issues or minor performance issues    ? Investigating    ! Service disruption    ? Unknown

# App Denial of Service

- The cloud expands based on demand
- Pricing is based on utilization
- Is this malicious? How can you tell?

GET <http://myapp.appspot.com> X 10

GET <http://myapp.appspot.com> X 1000000000000000

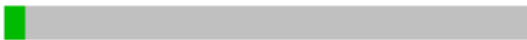
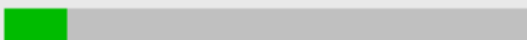



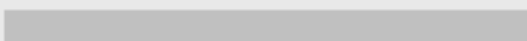

# App Denial of Service == \$\$\$

- Leverage application functionality to exceed quotas
  - ▶ Repeated URL fetch for large data
  - ▶ Forcing application to make multiple URL fetch requests
  - ▶ Invoking process intensive functions repeatedly
  
- DOS is way cooler when it costs people money

# Breaking Quotas

## Requests

Quotas are reset every 24 hours. Next reset: 10 hours

Resource	Daily Quota			Rate <span>?</span>
CPU Time		4%	0.26 of 6.50 CPU hours	Okay
Requests		12%	160585 of 1333328	Okay
Outgoing Bandwidth		11%	0.11 of 1.00 GBytes	Okay
Incoming Bandwidth		50%	0.50 of 1.00 GBytes	Okay
Secure Requests		0%	0 of 1333328	Okay
Secure Outgoing Bandwidth		0%	0.00 of 1.00 GBytes	Okay
Secure Incoming Bandwidth		0%	0.00 of 1.00 GBytes	Okay

# Java App - GaeFlood

08-11 01:58PM 02.294 / 405 129ms 21cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:51PM 08.446 / 405 95ms 20cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:50PM 06.882 / 405 90ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:50PM 02.023 / 405 83ms 19cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 56.065 / 405 84ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 51.968 / 405 104ms 19cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 35.375 / 405 100ms 15cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 32.586 / 405 160ms 18cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 12.240 / 405 85ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

250.2 - - [11/Aug/2009:13:49:12 -0700] "POST / HTTP/1.1" 405 124

08-11 01:49PM 11.751 / 405 135ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 04.197 / 405 100ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:49PM 03.299 / 405 102ms 20cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:48PM 39.659 / 405 83ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:48PM 31.785 / 405 120ms 16cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)

08-11 01:48PM 18.848 / 405 86ms 18cpu\_ms 0kb Java/1.5.0\_19,gzip(gfe)





# JS Malware - GaeDOS.js

POST / HTTP/1.1

Host: blue-dogz.appspot.com

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive

Referer: http://zusakita.appspot.com/news

Content-Type: application/x-www-form-urlencoded


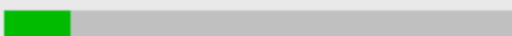




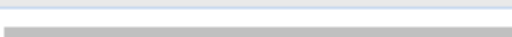
Content-Length: 16005

```
data=%5C%2CS%3Bj%279%23%7D%60uerl%60369tyJYaK7yT%2F7t%22I%3A5Q_i%3D%3Df_QZz_.C%24up%7B3H%5DaL%3D%5C%254Royj%3B_VCm%24kd%7%27I%2BY%22
5CyexUhZ%29o%7B%22%3C%2B%3DN%40%5BHg-CX%22R%5Bh%60o-%3AC%3Aum%7EI%3DYSR%60sFzpTc1%7EaxN7Nm%40%5B%3AYC%7D4O%21p%28wWt%23%5B%2B
22PQVsi%60e%7Du9F%7D%22q%3%FN%3AZ%27qTI%2CH%3BeE.rqd1%29pMXFO-8%3D%7C%21g5NgS%23%7DmH%3At%40%*3F%24%60oD%5C8_%3B%7Cd%2BKl6%2Br%
25d%29efF%7ERl%26%7C9Mhs%40IqQn-%5B.T5cxh%7EuGuaGZ%5DN%27evYt*8p%26.%3E%5BfQC9*sJmM%24sM%3B%7DYV2%27%7D7o%26%40u%5D%25v*05hM%22839
22Cbb7%23%29I%26aR74f%252y%2Cs%60IpA%2C2%3DOzPab%2C%7Cjx_S%22%21%29%7C%60%235%3DPl%246%3Du%242*n8C6vI*%2663j4R%28%5CuauR%5E%7D%5
3E%3BeU%2BwzEY%7B%3D%5C%25iOkU8ccf5Li%3FMh.%2C%7B%29%3ENp%25%7Cv%2FLNezxF%3EAwU%7E%2CYhA%3A%21hnE9D%23xlt%5EI%7C%3Fn%2B%5B%3AI*fz%3
3B4%60%60Tx%5DN%7Dd%3B%7Eu1%2FLmkYpL%25vi%3EjS4krL%5ETUS%2F-%3DJ4%3BeV%2F%5B%24IYdX5c%2982MxtDlPk%3FEX%21tMrQ6_Gljw%3Eoi*Ck%27R7NEBo9
7E6%29G9qk6sH1%5C0%222CZs%29ocBN%26MT%24%7Cs%5C%7CHq%60%3FumEI%7DF8%23%2F%5C%23mR%2Fv44x%26%24%2FVcQ%60i%3AxvGz5nP%7CCbl89%3Bp_
60XiN5__y%60-QhX%5E%26%3C%2F%2Fkhw%21GP0sMnP%5CLI%7BV%3Ek%3ADbLi6%22GAe9%5C%3E%28xNg%5D%3CwZa%2B%3FOhjHp%2B%7B%3Es%294%27pj%21%5
5C%23%22eajj%60%7D%7C%3Dz4%3B%7E%7B%28m%2C%28wt.5%28j%22glqg3JkIKX%2CPT.8y%5BuAy%23%5Ce4%60f%40b%26Q_%2C%5Di%7D%3F70%2F68n%29%22%5E
2FZS%3B%28%264Tj%24b-0z%3CI%5Bce%7CGGa%24%3D%3Do%26%28rb%23ZH%24U_mGPiD9%3BUT9%26%24UMAAx4%25%5Du-Lkp37-Flkp1%60DBNTF%28S%40Ywv%
5DaMEAzkC*RUrezK%7BBR%2CWcgsCM%26*N%2Fu%21%*27*FLID_R%29_%5D1%3DB%25%3BLU%3E%25X%2C54etMp%7D%2578%5E%3E%3Ey%7E9uhVv%29%3BvJ%2CwqW
26DQat3%2Fs%5BBRr%22K%7BZ%3F%3BF%21o%7D%27xquRDXZPzXsk%28uY1Wq%7DX9ngeK0%3EWun%3FWDU%5B%7Cq2c%7DZjjVQFH.m%21%21p0SZ%60%24%40RYw
jaj%5E%2422%2FK4*%7CzO%5Dk%3EWl%299x0%5Ddb%2BqVn5%7Dk%5D%28%3APTJ9%23-CFbU*87YFQ%28%23%3AgT%23%7DxWLN4v%60%2C%21%25%22%5Dv%3
5Dwtxkv%3Dpj1Qm9jrss%26%21%3D8%29ruwU%40Dvh14O%3CB%7Cz1b%22%3DP%22m5dj9C%3Fj*7O%21%26%25AjmBb%5Cz9Gu2Ql%279L%3EgQ%3FN%2C%26N4O
3C8%7DG2V.uGbk%3EBpu%25u4v7%40Nby1l6rcqM7%60Zg%3AS%7D%22vWeu.%2Bj.%2B%2C%22%21rKISq%266%2FIMWkm%3Av%21GoZ%266_%27%29-b%5EBg%60Oi%2
7Cs%7EqUiA%3C%7C_c%2F%23sb3%2CL%3Ap3%3Ej%2B%25WV%5DtYI%3Aae%5B-E8Gh%2CYvMkayRqI%25R%2BwsW1kQ2%7Ea%21E%27%23XApT4c0EiYa%2C7m%29P%
5C8nOh8%3F%3BR4W_VZnue%3Az%29%5DWKU%7D1_%24Z%27%3Cg%7EK_4KaV-HM%5Dm%7BJ%26jgl6T92H%28b6XC%29%7CgDO%5DwbLsN%218A%7BNyiGHC_b%2BZ
24g%29S%7C1%5B7INPhxVCgk%2FmQ2qb%7CfA%3BfBxSL6%3C%7D%5CLOI%2BejQuF%3C%27C%2701q%221p1%2CUAp%256%24Q%2BHEri%2FJ22%7BLD9bAI%5C%3BkjY
3ARnjvCePmFw4wEOg%3EC%5Dn%3A%7C%3B%24%40%5Cf%2F%29nH1DFuL8D%7B%40%23bhvAH44%3AHT%21%3BX*%3Ag*jj%2BBI9iIMMI%276%23YCW6QF%3ER%2BF%7
242bGH%3B5q%2Ban%27S4%60ZlUA%5DM%5B1J%7DEDrj%5DU%24Bhl%3D3mj%25_I%7D%3E8%29jgvXAgf%7C*yo4y%3CGI%7EM%5B%3C.%5D%25F%3BS%7D2z1%22T%2F
29L%3D9L%7EI%3Db%27A%285%21dmO%5C%5CMx_cV%2C8d%27%29QqUO4Sk%3ExX%7BgIgc%2BWKH%29RYB%60AhQwbAC7%40kDhW%3CtWxm%27xh%7C2kqP9%21
```

# Quota Denial of Service

## Requests

Quotas are reset every 24 hours. Next reset: 10 hours

Resource	Daily Quota			Rate <sup>?</sup>
CPU Time		4%	0.28 of 6.50 CPU hours	Okay
Requests		13%	171064 of 1333328	Okay
Outgoing Bandwidth		12%	0.12 of 1.00 GBytes	Okay
Incoming Bandwidth		100%	1.00 of 1.00 GBytes	Limited
Secure Requests		0%	0 of 1333328	Okay
Secure Outgoing Bandwidth		0%	0.00 of 1.00 GBytes	Okay
Secure Incoming Bandwidth		0%	0.00 of 1.00 GBytes	Limited

# Quota Denial of Service

Application Error

## Over Quota

This application is temporarily over its serving quota. Please try again later.

# Task Queues DOS

- App is still up, Queue functionality can no longer be used

```
File "/base/python_lib/versions/1/google/appengine/api/apiproxy_rpc.py", line 111,
      raise self.exception
OverQuotaError: The API call taskqueue.Add() required more quota than is available.
```

## Tasks Daily Quota

 100% 10000 of 10000



Queue Name	Maximum Rate	Bucket Size	Oldest Task	Tasks in Queue
default	5.00/s	5.0	2009/08/23 08:58:15 (0:06:11 ago)	2000+

# URLFetch Abuse

- Proxy attacks
- Delay investigations
- 10 seconds timeout



# App Versions

Version	Default	Live URI
<input type="radio"/> 1 (deployed 18:01:49 ago)	No	<a href="http://1.latest.zukakita.appspot.com">http://1.latest.zukakita.appspot.com</a> 
<input checked="" type="radio"/> 2 (deployed 0:00:15 ago)	Yes	<a href="http://2.latest.zukakita.appspot.com">http://2.latest.zukakita.appspot.com</a> 

- Apps with outdated versions exposed
  - ▶ 1.latest.app-id.appspot.com
  - ▶ 2.latest.app-id.appspot.com

# One Vuln to Own the All

- A single vulnerability in the Runtime would affect all apps
- HyperVM exploit (LXLabs)
  - ▶ 100,000 websites destroyed
  - ▶ Cheaper, non-backed up sites completely gone..
  - ▶ HyperVM boss commits suicide





# Code Security

```
package guestbook;

import java.io.IOException;
import java.util.Date;
import java.util.logging.Logger;
import javax.jdo.PersistenceManager;
import javax.servlet.http.*;
import com.google.appengine.api.users.User;
import com.google.appengine.api.users.UserService;
import com.google.appengine.api.users.UserServiceFactory;

import guestbook.Greeting;
import guestbook.PMF;

public class SignGuestbookServlet extends HttpServlet {
    private static final Logger log = Logger.getLogger(SignGuestboo

    public void doPost(HttpServletRequest req, HttpServletResponse
        throws IOException {
```



# It's just a web app...

- XSS
- Access Controls
- Response Splitting
- GQL injection
- Information Leakage
- Input validation
- Error handling

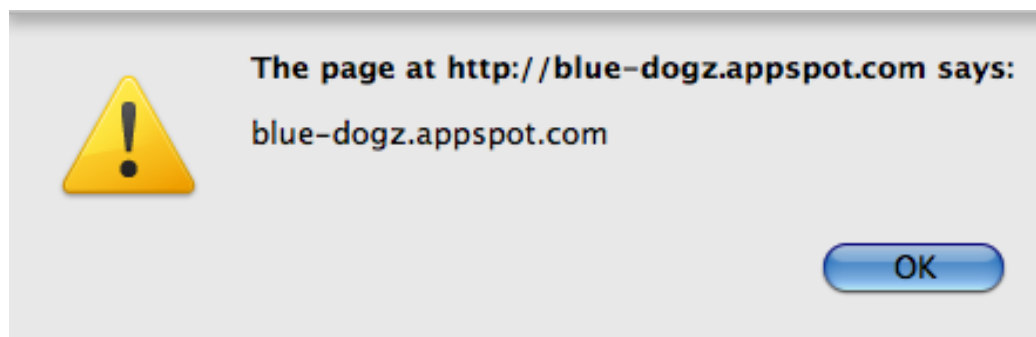


# XSS is still XSS

```
"><script>alert('xss')</script>
```

Sign Guestbook

```
self.response.out.write('<html><body>You wrote:<pre>')  
self.response.out.write(self.request.get('content'))  
self.response.out.write('</pre></body></html>')
```



- `cgi.escape()` required

# XSS impact on the cloud

- Code running in appspot.com domain
- Standard XSS exploits
  - ▶ Steal cookies
  - ▶ Deface pages
  - ▶ Serve exploits to vuln browsers
  - ▶ Portscan internal network
- No GoogValidateRequest?!?



# XSS Filters

## ■ IE 8 XSS Filter

- ▶ Detects JavaScript in URL and HTTP POST requests.
- ▶ Sanitizes the original request

If necessary, you can disable this feature by setting the HTTP response header:

```
X-XSS-Protection: 0
```

# Access Controls - Forceful Browsing

```
- url: /pages
  static_dir: pages
- url: /*
  script: notfound.py
```

GET /tmp HTTP/1.1  
Host: localhost:8083  
Content-Length: 2

Not Mapped

HTTP/1.0 200 Good to go  
Server: Development/1.0

GET /pages/ HTTP/1.1  
Host: localhost:8083  
Content-Length: 2

Mapped

HTTP/1.0 403  
Server: Development/1.0

GET /pages/asdasd HTTP/1.1  
Host: localhost:8083  
Content-Length: 2

Handler Misses

HTTP/1.0 404  
Server: Development/1.0

# Access Controls - Internal URL's

## ■ Task Queues & Scheduled Tasks

- ▶ Use app URL's to invoke action
- ▶ Opens the door for abuse by an attacker

```
class TaskQueue(webapp.RequestHandler):  
    def get(self):  
        for i in range(0, 1000):  
            taskqueue.add(url='/work/loader',  
                          params=dict(vars='From loader!'))  
        self.redirect("/")
```

# Access Controls - Datastore

- Data access controls still need to be enforced
  - ▶ Id=2
  - ▶ Id=4
  - ▶ Id=283
- Query Datastore through remote API (REST)
- Potential access to privileged info
- CSRF

# GQL Injection

- Google Example:
- `Greeting.gql("WHERE author = :author ORDER BY date DESC",  
author=users.get_current_user())`
- `greetings = db.GqlQuery("SELECT * FROM Greeting WHERE content = '" +  
self.request.get('searchstr') + "'")`



# GQL Injection

- Does not appear to be possible
- Further research required

```
(error_message, self.__symbols[self.__next_symbol]))  
BadQueryError: Parse Error: Expected no additional symbols at
```

# Fingerprinting GAE sites

```
PORT      STATE  SERVICE
80/tcp    open   http
113/tcp   closed auth
443/tcp   open   https
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Thu, 05 Nov 2009 16:50:32 GMT
Server: Google Frontend
X-XSS-Protection: 0
Transfer-Encoding: chunked
```

# Summary

## ■ Cloud Technologies

- ▶ Business's starting to experiment
- ▶ Varied definition, services, and providers
- ▶ Hottest buzzword of '09
- ▶ Potential Legal and compliance issues

## ■ GAE

- ▶ Provides infrastructure & platform
- ▶ Currently Preview release
- ▶ 30 second response limit
- ▶ Doesn't seem ready for Enterprise usage

# Questions





[jrose@trustwave.com](mailto:jrose@trustwave.com)