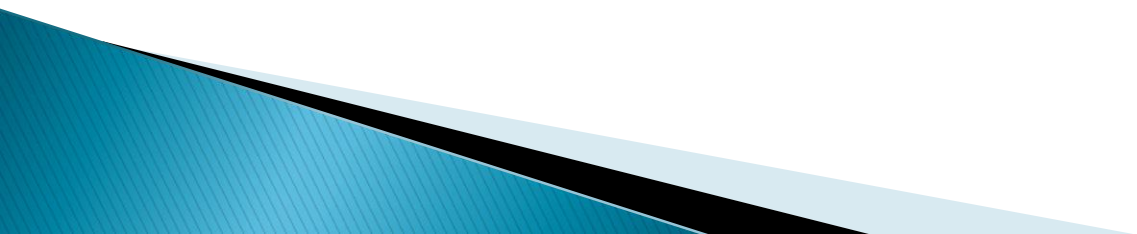
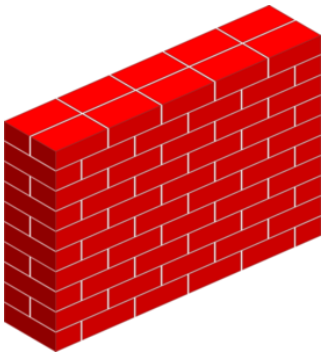
SECURITY TESTING In A Nutshell

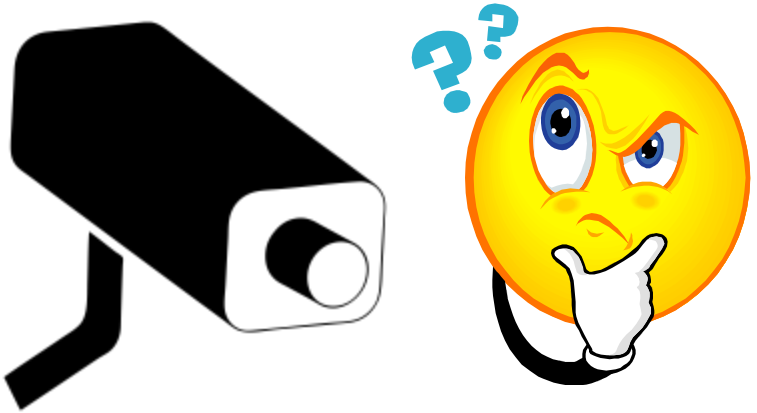
Simon Innes
Test Tools Coordinatior
Insurance Commission of WA



What is Security?

Examples of Security Measures





What is Security?

Applications of Security

Security in IT

Security in IT

- What are you trying to protect?
- No “time of day” restrictions
- Harder to detect

Security in IT

- Authentication
- Authorisation
- Availability
- Confidentiality
- Integrity
- Non-repudiation

Authentication

- Is someone who they say they are?

EXAMPLES:

- Login / Password
- Public Key Infrastructure

Authorisation

- Is the person seeing what they're allowed to?

EXAMPLES:

- User permissions
- Access controls

Availability

- Is the data / system accessible?

EXAMPLES:

- Clusters / HA
- DR sites

Confidentiality

- Is the information safe from 3rd parties?

EXAMPLES:

- Encryption
- Secure methods of transmission

Integrity

- Is the information correct?

EXAMPLES:

- Hashes

Non-repudiation

- Did the communication happen between 2 legitimate parties?

EXAMPLES:

- Digital Certificates + Certificate Authorities

What is Security Testing?

- A type of “non functional” testing
- Outside the box
- Physical + Logical

- System Security, Network and Infrastructure, Web Application, Physical

- Vulnerability Assessment vs Pentesting

Vulnerability Assessment

- Build attack surface through various methods
- Scan for known vulnerabilities
- CVE
- Can be done with scanning software
- “Low hanging fruit”

Penetration Testing

- Digs deeper
- Tries to gain access by other means
- System loopholes / network vulnerabilities
- Has specific goals (access a certain system)
- Harder to automate
- Black box

Types of Security Threats

- People
  - Malicious
  - Negligent
- Malware
- Phishing
- Social Engineering

Injection

- The sending of untrusted data to the system / interpreter
- Simple text based attack
- Examples: SQL, LDAP, XML parsers
- Basically anything that accepts arguments
- Easy to exploit if you can see code, not so easy to detect

Injection

- Example:

- Get Customer Details

  SELECT * FROM customers WHERE customerID=‘” +
  $_GET[“customerID”] + “;

  http://www.myshop.org/getCustomerDetails.php?customerID
  =700

Injection

getCustomerDetails.php?customerID=‘ OR ‘1’=‘1 --

- SELECT * FROM customers WHERE customerID=‘’ OR ‘1’ = ‘1’

- ‘ causes statement to terminate
- -- comments out remainder of command
- OR 1 = 1 returns true
- Will run “SELECT * FROM customers”
- WebGoat Example

Cross Site Scripting (XSS)

- Simple script attack
- Caused by not validating user input
- Attackers execute scripts on victim machines to retrieve data / hijack sessions
- Come in 2 flavours. Stored and Reflected
- Can be run on server or client

Google Dorks

- Google is EXTREMELY powerful
- Can be a useful penetration testing tool
- Use Dorks to dig deeper
- Google Hacking Database

Google Dorks

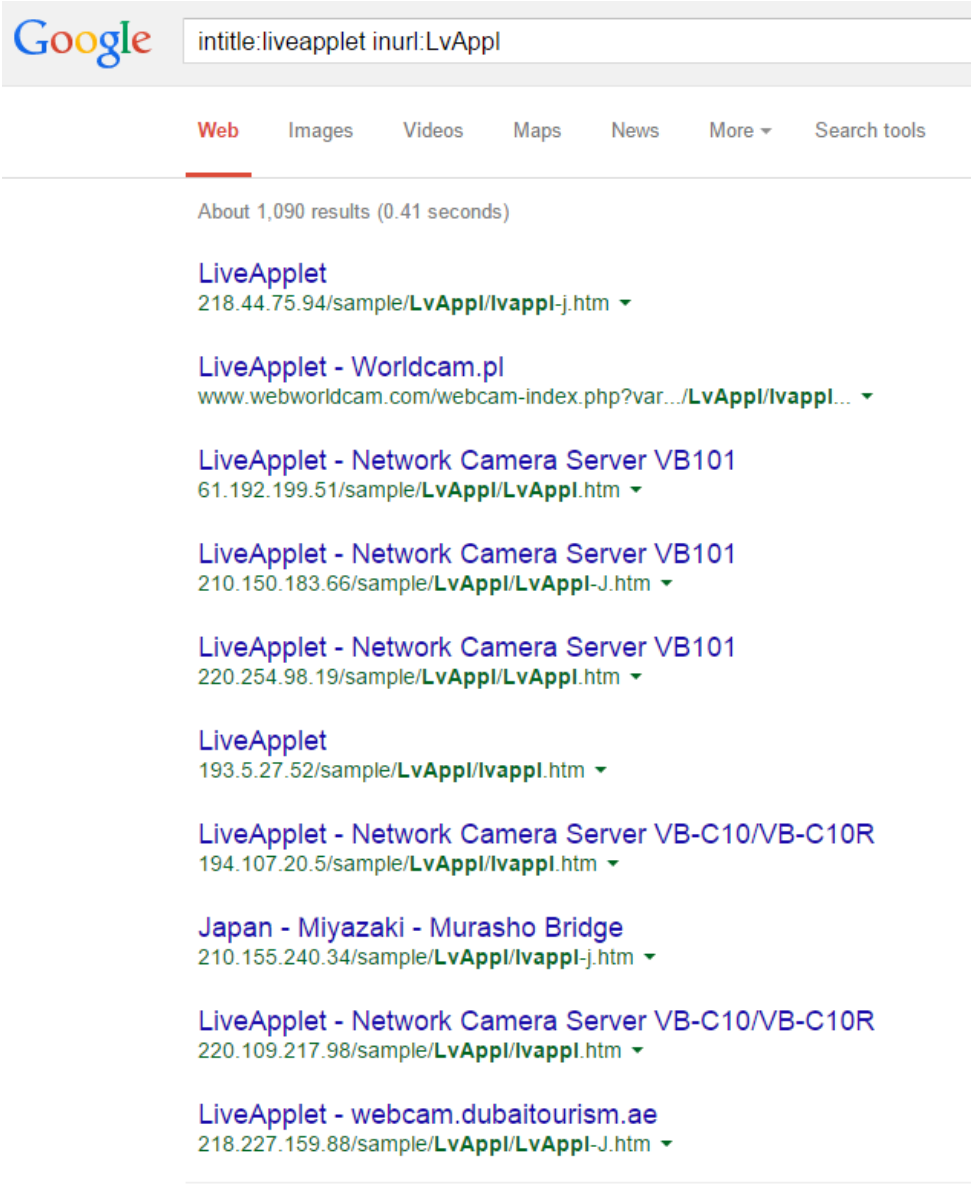
Operator	Purpose	Mixes with Other Operators?
intitle	Search page Title	yes
allintitle	Search page title	no
inurl	Search URL	yes
allinurl	Search URL	no
filetype	specific files	yes
allintext	Search text of page only	not really
site	Search specific site	yes
link	Search for links to pages	no
inanchor	Search link anchor text	yes
numrange	Locate number	yes
daterange	Search in data range	yes
author	Group author search	yes
group	Group name search	not really
insubject	Group subject search	yes
msgid	Group msgid search	

Google Dorks

- So??
- So….
- inurl:/wp-content/uploads/ filetype:sql
  - Locates .sql files in wp-content/uploads
  - Potentially backups of peoples WordPress sites

Google Dorks

- The possibilities are endless
- intitle:liveapplet inurl:LvAppl


Google
intitle:liveapplet inurl:LvAppl
Web
Images
Videos
Maps
News
More
Search tools
About 1,090 results (0.41 seconds)
LiveApplet
218.44.75.94/sample/LvAppl/lvappl-j.htm
LiveApplet - Worldcam.pl
www.webworldcam.com/webcam-index.php?var.../LvAppl/lvappl...
LiveApplet - Network Camera Server VB101
61.192.199.51/sample/LvAppl/LvAppl.htm
LiveApplet - Network Camera Server VB101
210.150.183.66/sample/LvAppl/LvAppl-J.htm
LiveApplet - Network Camera Server VB101
220.254.98.19/sample/LvAppl/LvAppl.htm
LiveApplet
193.5.27.52/sample/LvAppl/lvappl.htm
LiveApplet - Network Camera Server VB-C10/VB-C10R
194.107.20.5/sample/LvAppl/lvappl.htm
Japan - Miyazaki - Murasho Bridge
210.155.240.34/sample/LvAppl/lvappl-j.htm
LiveApplet - Network Camera Server VB-C10/VB-C10R
220.109.217.98/sample/LvAppl/lvappl.htm
LiveApplet - webcam.dubaitourism.ae
218.227.159.88/sample/LvAppl/LvAppl-J.htm

Thank you!!