SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Information Systems Security Audit & Control

4th Year 2nd Semester 2016

Name: Harshanath W.W.D.K

SLIIT ID: IT13069032

Practical Session: WE Friday

Practical Number: Lab 1

Date of Evaluation : _____

Evaluators Signature : _____

Google Hacking

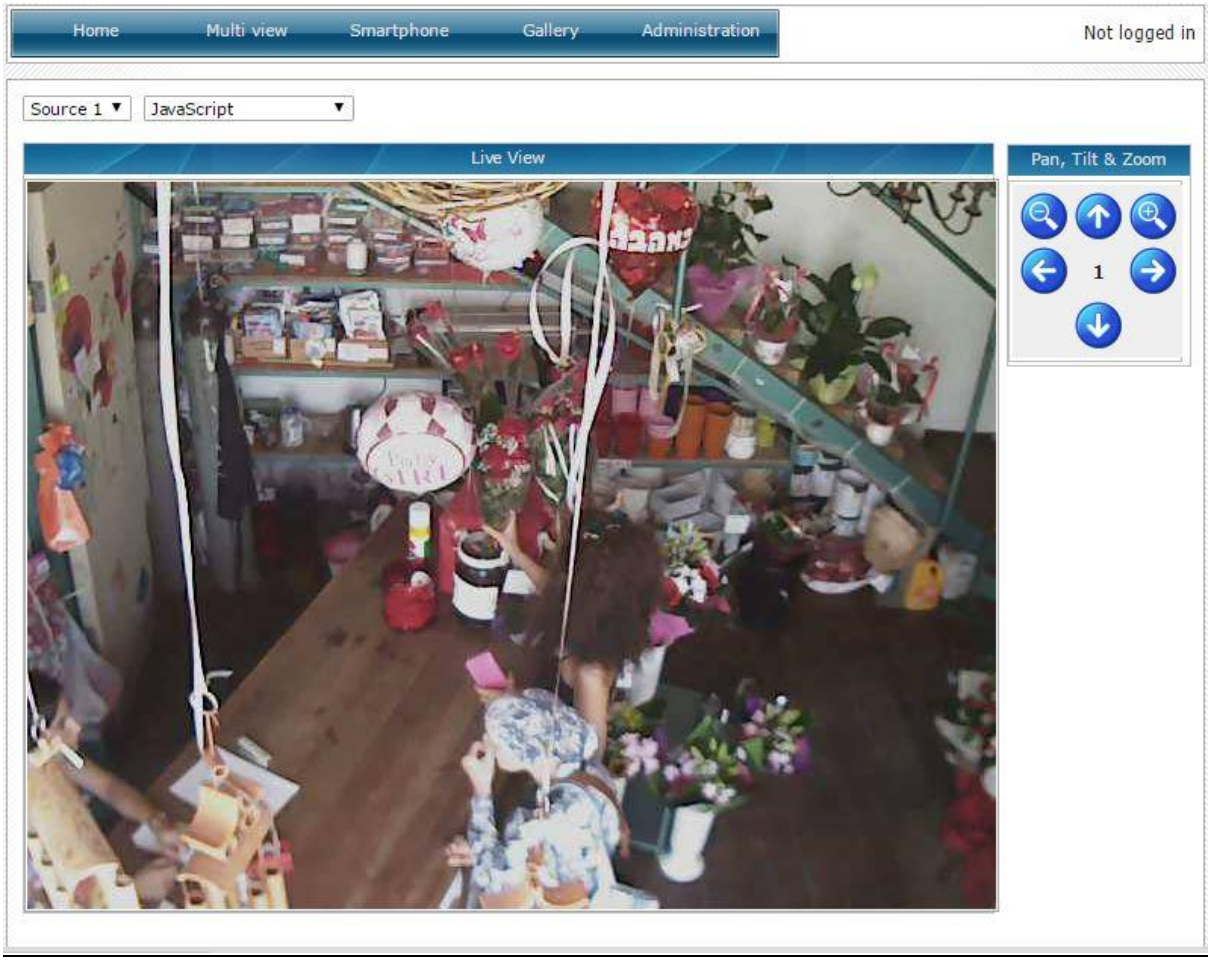
Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use. Google hacking involves using advanced operators in the Google search engine to locate specific strings of text within search results. Some of the more popular examples are finding specific versions of vulnerable Web applications.

Exploits Database by Offensive Security

The Exploit Database is the ultimate archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. Its aim is to serve as the most comprehensive collection of exploits gathered through direct submissions, mailing lists, and other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away.

We use Exploit database as a source for google hacking. It provides the corresponding search queries to hack each and every vulnerability over the internet. Here are some examples for Google hacking.

Webcams



Search query: intitle:webcam 7 inurl:8080 -intext:8080

Sources:

http://212.235.66.227:8080/home.html

http://81.7.87.107:8080/mobile.html?src=1&mode=1

http://73.185.88.15:8080/multi.html

http://206.45.110.113:8080/multi.html

Emails

Search query: intitle:index.of.mail

Sources:

https://www.ietf.org/mail-archive/text/

http://docs.freebsd.org/mail/archive/

Camera pictures

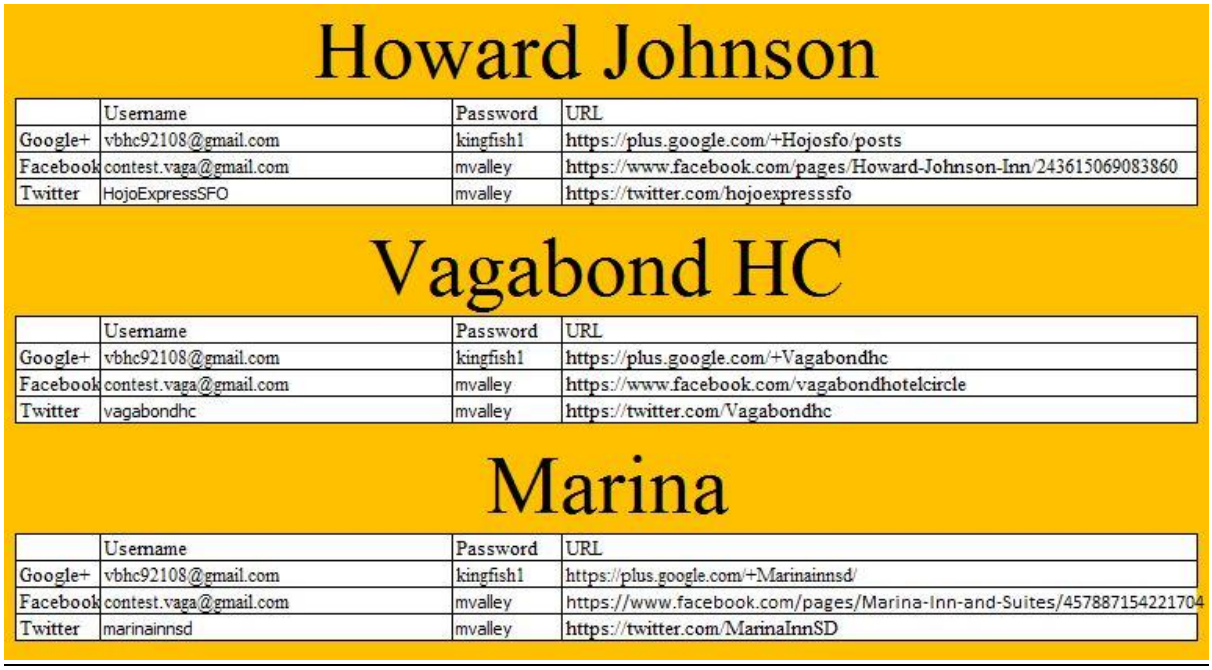
Search query: intitle:"Index of" "DCIM"

Sources:

http://www.augustomestieri.com.br/DCIM/Camera/

http://dchampagne.com/website/AcerLaptop/Documents/Phone/New%20folder/DCIM/Camera/

Files containing passwords



Howard Johnson

	Username	Password	URL
Google+	vbhc92108@gmail.com	kingfish1	https://plus.google.com/+Hojosfo/posts
Facebook	contest.vaga@gmail.com	mvalley	https://www.facebook.com/pages/Howard-Johnson-Inn/243615069083860
Twitter	HojoExpressSFO	mvalley	https://twitter.com/hojoexpresssfo

Vagabond HC

	Username	Password	URL
Google+	vbhc92108@gmail.com	kingfish1	https://plus.google.com/+Vagabondhc
Facebook	contest.vaga@gmail.com	mvalley	https://www.facebook.com/vagabondhotelcircle
Twitter	vagabondhc	mvalley	https://twitter.com/Vagabondhc

Marina

	Username	Password	URL
Google+	vbhc92108@gmail.com	kingfish1	https://plus.google.com/+Marinainnsd/
Facebook	contest.vaga@gmail.com	mvalley	https://www.facebook.com/pages/Marina-Inn-and-Suites/457887154221704
Twitter	marinainnsd	mvalley	https://twitter.com/MarinaInnSD

Search query: site:static.ow.ly/docs/ intext:@gmail.com | Password

Sources:

http://static.ow.ly/docs/MMMMasterLoginsandAccounts_2Q3T.pdf

Search query: site:github.com ext:csv userid | username | user -example password

Sources:

https://github.com/oaeproject/Hilary/blob/master/node_modules/oae-principals/tests/data/users-with-password.csv

https://github.com/cheetz/adobe_password_checker/blob/master/foundpw.csv

National Data

Annual Reports

Search query: site:lk filetype:pdf intitle:annual

Sources:

https://www.cse.lk/cmt/upload_report_file/388_1456910078.pdf

http://www.nestle.lk/asset-library/documents/annual-reports/nestle-annual-report-2015.pdf

NIC Numbers

Search query: site:lk filetype:pdf intitle:annual

Sources:

http://www.psc.gov.lk/web/images/pdf/english/5._Orders_Decisions/4_2_Appointment_Promotions/ne_slas_e.pdf

http://www.mrt.ac.lk/itum/PDF/ME.pdf

Phone Numbers

Search query: site:lk filetype:pdf intitle:phone

Sources:

http://www.pgia.ac.lk/files/about/CC_MEMBERS_CONTACTS.pdf