

This document tracks the time I spent to learn the Online Course "**Web Security**", course number **S111.23** taken at <http://www.eclasses.org/> from reading the text book, reading and documenting online lectures, reading online resources, and doing homeworks.

These online classes are primarily conducted via the web board interface - called Web Crossing. You can take a Virtual Tour of an Online Classroom at <http://www.eclasses.org/Demo/> (note: the ".23" in S111.23 refers to the number of times the course has been given).

Total number of hours I spent on Web Security (details below) = 49.75 hrs

*******Course Description*******

Web Security - course number S111.23

Start Date: 20-July-2009; **Duration:** 6 weeks; **CEUs:** 3.0; **Course Number:** S111.23; **Instructor:** Michael Chapple

How eClasses Work

The classroom environment is based on Lundeen & Associates Web Crossing technology, a threaded messaging system. Instructors post lectures, reading selections, and hands-on assignments once a week in the online classroom. Students can discuss the assignments with the instructor and amongst themselves in the classroom area. **This format has no set meeting time**, which allows students to attend class at a time most convenient to them, yet still provides logically organized communication between class participants. Students can apply for the completion certificate after finishing the class. Web Study certificate is also available. Click on the Certificates link on the top navigation bar for more information.

About eClasses.Org - Affordable Web Technology Learning

Since 1998 eClasses.Org has provided the very best in online training to 45,000 Web developers and other professionals. It offers a catalog of 40 online courses covering the breadth of Web work, from HTML to Flash; from CSS to XML. All classes are taught by fellow experts and working professionals in the field.

- Online, instructor-led web technology classes
- Affordable and flexible learning solution
- 4 Web certificate programs

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Course Outline: Web Security

Web Security offers an introduction to the computer security concepts important to those who develop web applications or supervise those who do. Students will learn the basics of secure coding, prevention of buffer overflow attacks, secure database integration as well as relevant legal/privacy issues. The course is taught in a platform-independent manner so that students using any technology will benefit.

Outline

Week 1: Principles of Information Security

- Explain the elements of the CIA Triad
- Explain how the rule of least privilege applies to web security
- Understand how common security devices may be combined to enhance security
- Know the proper placement of web servers in various security scenarios

Week 2: Malicious Code and Other Nasties

- Understand the risk posed by various malicious code objects
- Design a comprehensive defense against those threats
- Explain the special risks that denial of service and buffer overflow attacks pose to web applications

Week 3: Secure Web Development Practices

- Perform parameter checking to protect against buffer overflow attacks
- Implement change control processes to reduce risk
- Design a strong logging/auditing policy

Week 4: Secure Database Integration

- Explain the risks posed by inference and SQL injection attacks
- Develop a defensive posture against those issues
- Build web applications that securely integrate with back-end databases

Week 5: Introduction to Cryptography

- Explain the difference between symmetric and asymmetric cryptography
- Implement a secure website using HTTPS and SSL
- Understand the issues surrounding web cryptography

Week 6: Privacy and Legal Issues

- Understand the various laws and regulations that apply to websites
- Write a privacy policy for your organization
- Explain the impact of the Children's Online Privacy Protection Act
- Understand the safe harbor provisions of the COPPA

Prerequisites Basic understanding of web development techniques on any platform is a requirement. Basic familiarity with databases is desirable but not mandatory.

Requirements This course has no specific software or hardware requirements.

Required Book: [Information Security Illuminated](#) [] [by Michael Solomon and Mike Chapple, Paperback, 2nd edition, 600 pages, ISBN: 076372677X, **Publisher:** Jones & Bartlett Press, **Pub.Date:** April 25, 2005

Additional Information:

This online course is limited to 100 participants. Your place in the course is confirmed by your payment. Introductory courses are intended for students with no experience in the subject matter and are seeking beginner level training.

Refund Policy: Please read our ["Terms and Refund Policy"](#) before registering for this course.

Additional Cost: Book and software might be required for the course. Read the Requirements and Book section for more information. Course fee does not include the book and software cost .

Start Date: Click on the Register Now button to proceed to the registration page. You will see the start date of the class on that page. To get the start date of other courses, click on Open Classes link on the top navigation bar.

How eClasses Work: The classroom environment is based on Lundeen & Associates Web Crossing technology, a threaded messaging system. Instructors post lectures, reading selections, and hands-on assignments once a week in the online classroom. Students can discuss the assignments with the instructor and amongst themselves in the classroom area. **This format has no set meeting time**, which allows students to attend class at a time most convenient to them, yet still provides logically organized communication between class participants. Students can apply for the completion certificate after finishing the class. Web Study certificate is also available. Click on the Certificates link on the top navigation bar for more information.

Instructor: Mike Chapple

Mike Chapple is a computer/network security expert with over six years of experience in the public and private sectors. He formerly served as an information security researcher with the National Security Agency developing cutting-edge network intrusion detection systems and as a computer security officer with the U.S. Air Force. He currently oversees enterprise-wide security initiatives as Chief Information Officer of the Brand Institute, a Miami-based marketing consultancy.

Mike is the author/co-author of three computer security books: the TICSAs Training Guide from Que Publishing, the CISSP Study Guide from Sybex and the SANS GSEC Prep Guide from John Wiley & Sons.

Mike holds an M.S. in Computer Science with a concentration in Trusted and Secure Information Systems from the University of Idaho and a B.S. in Computer Science from the University of Notre Dame. His professional credentials include the CISSP, TICSAs, CCSA, MCSE, MCDBA and CCNA certifications.

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

How eClasses Work

About the Classroom

The classroom environment is based on Web Crossing technology, a threaded messaging system (message board). Instructors post lectures, reading assignment, and hands-on assignment once a week. Classes start on a certain date but this format has no set meeting time, which allows students to attend class at a time most convenient to them. Students only need to complete the assignment within one week and continue with another assignment in the following week.

The main benefit of our classes is the interaction among you, your instructor and other students in classroom (online message board). Students can post comments or questions to the instructor or other students, share ideas, communicate about your learning experience, or discuss topics of the course with other interested students.

How to Access Your Classroom

After you register for a class, you will get a receipt email and an instructional email. Simply follow the instructions to add yourself to the classroom (or grant yourself access to the classroom). After that, you can access your classroom at <http://interact.eclasses.org/cgi-bin/WebX?15@@>

How to Use the Classroom

The classroom is organized by folders and discussion. A folder is like a folder or directory on your hard disk. It contains discussions or other sub-folders. Every folder has a title and a heading which describe the folder. On top of each page, there is the path of the current folder, so you can see where you are. If you click on any folder or you will go to that page. Take a look at our [DEMO](#) to see how the classrooms look like.

A discussion has a title and heading that describe its purpose. Discussions are not 'chat-rooms', they are more like organized electronic mail. You can browse a discussion and post a message at any time. To post a message, just scroll down to the message form at the end of each discussion. Fill in the form, and then click on the 'Post Message' button following the form.

Someone else will see your post later, when they are browsing or when they check for new messages. You can always read the whole discussion from beginning to end, so you never have to wonder what people are talking about. Because a discussion may have many of messages posted to it, long discussions are split into smaller pieces. In a long discussion, you'll see buttons at the top and/or bottom that let you go back and forth.

The system automatically keeps track of messages as you view them. When you see a discussion in a folder, the listing includes how many messages are in the discussion, and how many are new messages. There is another way to check for new messages, through your 'Subscription List'. After you subscribe to a discussion or folder, you can later check your subscription list at any time. You'll then be shown the first new message, discussion, or folder that has been added since you last checked.

What are CEUs?

One Continuing Education Unit (CEU) is generally defined as ten contact hours of participation in an organized continuing education experience under responsible sponsorship and qualified instruction. For instructor-led online learning, each course is assigned a number of CEUs for that course which may not relate to the total number of hours an individual takes to complete the course. The number of CEUs awarded is the average number of hours required to complete a course.

Class Schedule

Almost every week, a group of classes is open for registration. A class is open about 1-2 months prior to its start date. Click on the Open Classes link to see the list of classes that are open for registration now. The same class is offered every 2-3 months.

If you are interested in a class but it's not on the Open Classes list, you can click on Class Catalog link and go to the description page for the class. Then click on Register Now button and put in your email address. We will send you an email when the class is open.

Student Center

[Student Center](#) is another online system which requires a different password (which students selected when they first register.) Below is the list of what you can do in the Student Center:

- Grant yourself access to your registered courses
- Register for new eClasses
- Get the list of your previous and current courses
- Get your payment history
- Check your final grades
- Apply for class completion certificates
- Apply for Web Study certificates
- Check your Web Study certificate application status
- Retake courses at special prices
- Update your email and mailing address

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

[What's the difference between 32-bit and 64-bit computing?](#) In a nutshell, the numbers refer to the amount of bits a computer can process in

one computation. They also translate into the amount of random access memory (RAM) a computer can address. A 32-bit Windows computer can address a maximum of 4GB of RAM, while a 64-bit Windows machine can address up to 128GB and even more (64-bit applications can address theoretically up to 16 billion gigabytes of memory). So the higher number of bit means better computing, both in terms of precision and capability.

Documentations: The documents - **file names** - that I wrote/created are:

1. TimeSpentToLearnWebSecurity.doc
2. Most Documents are in *.html (or *.htm) format.

Date	Time Spent (hrs)	Description (mainly)
Monday July 20, 2009	1.5	Start of Web Security -course number S111.23 Read and documented course materials at http://www.eclasses.org/ Documents created are located at: C:\Users\boutros\Documents\MyPrograms\eClasses.Org\Course_WebSecurity_S111.23\
Saturday July 25, 2009	3.75	Book: Information Security Illuminated - by Michael Solomon Read Chapters 1, 2, 3 [pages 1 - 81]. Read Week1 Online Lecture of Web Security class at http://www.eclasses.org/ + others .
Sunday July 26, 2009	5.25	Book: Information Security Illuminated - by Michael Solomon Read Chapter 8 [pages 191 - 214], Chapter 13 [pages 325 - 351].
Monday July 27, 2009	3.5	Finished week 1 Homework for Web Security class. Posted it online at: http://bacsoftwareconsulting.com/websecurity/wk1_homework.doc Read Week1 Online references: http://sourceforge.net/ http://www.pcmag.com/ http://www.attrition.org/security/commentary/ http://www.cert.org http://www.sans.org http://www.microsoft.com/security/ http://www.sans.org/resources/policies/ http://www.microsoft.com/windowsxp/pro/using/howto/security/accesscontrol.asp http://www.eskimo.com/~joelm/tempest.html http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html http://www.checkpoint.com/products/firewall-1/ http://www.juniper.net/products/glance/ http://www.pcmag.com http://www.zdnet.com http://www.netfilter.org/ http://www.linuxgazette.net/103/odonovan.html http://www.sans.org/rr/ http://www.snort.org http://www.securityfocus.com http://www.cerias.purdue.edu/about/history/coast_resources/intrusion_detection http://en.wikipedia.org/wiki/CIA_Triad#Key_concepts http://en.wikipedia.org/wiki/Intrusion_detection_system http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml http://www.bro-ids.org/ http://www.hhs.gov/ocr/privacy/index.html

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

Wednesday July 29, 2009

1.25

Book: Information Security Illuminated - by Michael Solomon
Read Chapter 7 [pages 165 - 189].

Thursday July 30, 2009

3.25

Book: Information Security Illuminated - by Michael Solomon
Read Chapter 12 [pages 303 - 324].

Read Week2 Online required references:

<http://pintday.org/whitepapers/dos-smurf.shtml>

<http://insecure.org/splotts/ping-o-death.html>

http://lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

Read Week2 Online references:

<http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf>

<http://www.cert.org/csirts/>

<http://www.auscert.org.au/render.html?it=2252&cid=1920>

http://www.sans.org/rr/catindex.php?cat_id=27

<http://www.first.org>

<http://isc.sans.org/>

<http://www.zonealarm.com/security/en-us/home.htm?lid=en-us>

<http://en.wikipedia.org/wiki/Nmap>

[http://en.wikipedia.org/wiki/Crack_\(software\)](http://en.wikipedia.org/wiki/Crack_(software))

<http://en.wikipedia.org/wiki/Rootkit>

http://en.wikipedia.org/wiki/MAC_address

<http://nmap.org/>

Friday July 31, 2009

4.0

Finished week 2 Homework for **Web Security** class.

Posted it in the classroom area and online at:

http://bacsoftwareconsulting.com/websecurity/form_unprotected.html

http://bacsoftwareconsulting.com/websecurity/form_protected.html

Read Week2 Homework References (for Buffer Overflow Attack):

http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html

<http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-05/0133.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2370>

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-2370>

http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=21663

<http://www.microsoft.com/technet/security/Bulletin/MS06-025.mspx>

Friday August 7, 2009

4.0

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 9 [pages 215 - 245], Chapter 10 [pages 246 -274].

Saturday August 8, 2009

2.25

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 11 [pages 275 - 291].

Sunday August 9, 2009

2.0

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 11 [pages 292 - 301].

Read Week3 Online references:

<http://www.sans.org/top20/>

<http://technet.microsoft.com/en-us/security/cc184924.aspx>

<http://www.pctools.com/guides/registry/>

<http://technet.microsoft.com/en-us/library/dd365874.aspx>

<http://www.microsoft.com/security/default.aspx>

http://en.wikipedia.org/wiki/Windows_registry

http://en.wikipedia.org/wiki/Domain_Name_System

<http://www.tripwire.org/>

http://en.wikipedia.org/wiki/Scripting_language

Read Week4 Online references:

<http://databases.about.com/od/security/l/aainference.htm>

<http://databases.about.com/od/security/a/sqlinjection.htm>
http://databases.about.com/od/security/a/sql_inject_test.htm
<http://www.youtube.com/watch?v=MJNJjh4jORY>
<http://www.youtube.com/watch?v=5FxiYafIV-g&NR=1>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.youtube.com/watch?v=NDx5MhwbLso>
<http://www.youtube.com/watch?v=JqzWPLq7bJY>
<http://unixwiz.net/techtips/sql-injection.html>
<http://st-curriculum.oracle.com/tutorial/SQLInjection/index.htm>
<http://coldfusion.sys-con.com/node/165921>
http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
<http://www.wwwcoder.com/main/parentid/258/site/2966/68/default.aspx>
<http://www.hostmysite.com/support/cfusion/cfsqlinjection/>

Monday August 10, 2009

4.75

Finished week 3 Homework for the **Web Security** class. Posted it at:

http://bacsoftwareconsulting.com/websecurity/wk3_homework.doc

Read Week3 Homework Online references:

http://www.pragmatics.com/Newsletters/newsletter_2004_06_SP.htm

http://www.amadeussolutions.com/english/practices/bp_change_control.htm

Finished week 4 Homework for the **Web Security** class. Posted it at:

<http://bacsoftwareconsulting.com/websecurity/week4/index.cfm>

Posted the source code as a doc file.

<http://bacsoftwareconsulting.com/websecurity/week4/index.doc>

<http://bacsoftwareconsulting.com/websecurity/week4/searchdatabase.doc>

http://bacsoftwareconsulting.com/websecurity/week4/employee_info.doc

Friday August 14, 2009

1.0

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 5 [pages 109 - 121].

Saturday August 15, 2009

3.25

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 5 [pages 122 - 134]; Chapter 6 [pages 135 - 164].

Sunday August 16, 2009

3.5

Read Week5 Online references:

<http://www.itl.nist.gov/fipspubs/fip46-2.htm>

<http://www.itl.nist.gov/fipspubs/index.htm>

<http://www.gnupg.org/>

<http://www.ietf.org/>

<http://www.ietf.org/rfc/rfc0768.txt>

<http://www.ietf.org/rfc/rfc0791.txt>

<http://www.ietf.org/rfc/rfc0792.txt>

<http://www.ietf.org/rfc/rfc0793.txt>

<http://www.ietf.org/rfc/rfc2821.txt>

<http://www.ietf.org/rfc/rfc2246.txt>

<http://www.standards.ieee.org/regauth/oui/oui.txt> (MAC addresses)

<http://web.mit.edu/Kerberos/>

<http://www.verisign.com/ssl/index.html>

<http://www.thawte.com/>

<http://filext.com/file-extension/ASC>

http://en.wikipedia.org/wiki/TCP/IP_model

<http://en.wikipedia.org/wiki/Ping>

http://en.wikipedia.org/wiki/Address_resolution_protocol

http://en.wikipedia.org/wiki/Reverse_address_resolution_protocol

http://en.wikipedia.org/wiki/Packet_analyzer

<http://www.ethereal.com/>

<http://www.wildpackets.com/>

<http://en.wikipedia.org/wiki/SSL>

<http://en.wikipedia.org/wiki/ISAKMP>

Read Week5-homework Online references:

<http://www.pgpi.org/download/gnupg/>

<http://www.pgpi.org/doc/>

ftp://ftp.pgpi.org/pub/pgp/2.x/doc/pgpdoc1.txt (PGP User's Guide)

ftp://ftp.pgpi.org/pub/pgp/2.x/doc/pgpdoc2.txt

<http://www.gnupg.org/gph/en/manual.html#AEN26>

<http://www.gnupg.org/gph/en/manual.html#AEN84>

<http://www.schwer.us/nblug/gpg/>

Finished week 5 Homework for the **Web Security** class. Posted it in the classroom section and at:

<http://bacsoftwareconsulting.com/websecurity/toMikeFromBoutros.asc>

Tuesday August 18, 2009

2.5

Book: Information Security Illuminated - by Michael Solomon

Read Chapter 4 [pages 83 - 107].

Read Week6 Online references:

<http://www.caru.org/program>

<http://www.esrb.org/privacy/index.jsp>

http://en.wikipedia.org/wiki/Children's_Online_Privacy_Protection_Act

<http://www.ftc.gov/coppa/>

<http://www.ftc.gov/ogc/coppa1.htm>

<http://www.ftc.gov/bcp/>

http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html

Wednesday August 19, 2009

2.5

Finished week 6 Homework for **Web Security** class.

Posted it online at:

http://bacsoftwareconsulting.com/websecurity/wk6_homework.doc

Monday September 7, 2009

1.5

Documented weeks 5 and 6 Misc. Materials for **Web Security** class.

Total = 49.75 hrs

***** *End of Web Security* *****
