Global Information Assurance Certification Paper

SANS INSTITUTE
GSEC Practical Assignment
Version 1.2d

Preparing for a Web Security Review

Peter Maung
May 29, 2001

Preparing for a Web Security Review

By Peter Maung

Introduction

The Internet can be thought of as the great social and business enabler in that it is generally useful, fairly user-friendly, and readily available. But the Internet is more than an evolving technology that has continued to grow over the past decade. It has changed the way we communicate with each other, conduct business and view the world. However, while the technological marvel that fuels the Internet continues to increase in sophistication, the security that protects the user has not.[1]

Generally, the proliferation of web sites and web applications can be attributed to the growing presence the Internet plays in our lives. According to one source, "as the Internet grows into an acceptable global medium for data exchange, communication connectivity and e-commerce, the risks and vulnerabilities associated with the Internet will increase in greater proportion."[3] "From 1997 to 2000, the number of governmental and commercial web sites hacked daily has increased."[1] So, why then are web sites continually compromised, even though we may be much better informed and prepared to deal with various web security vulnerabilities and exploits today?

The answer perhaps lies in not one, but a multitude of possible reasons such as new technology, poor security standards, and inexperienced web developers. At the forefront of this web security battle, opposite the web attacker, is the IT security professional charged with the security of the web site and its data. These professionals are basically responsible for leading the fight to ensure that web sites maintain confidentiality, integrity and availability (**Figure 1**).

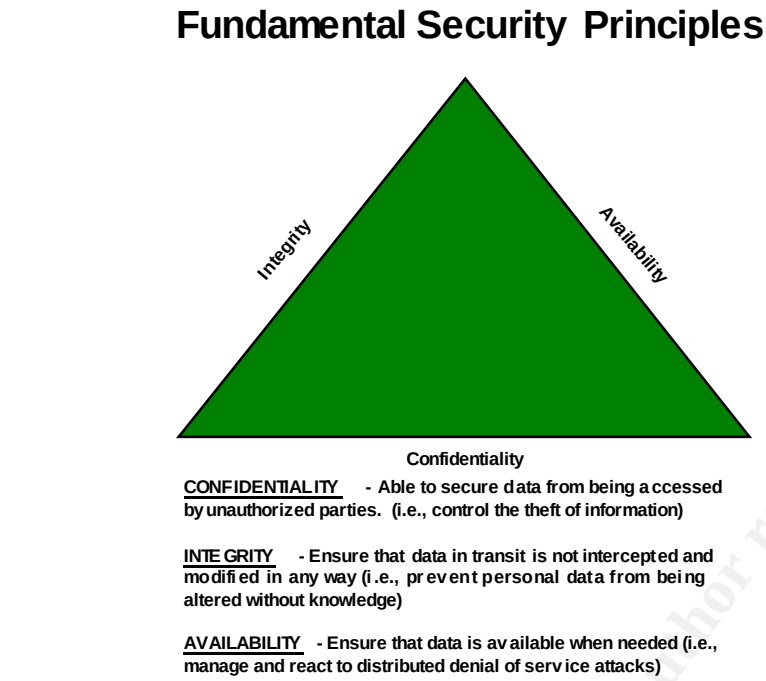
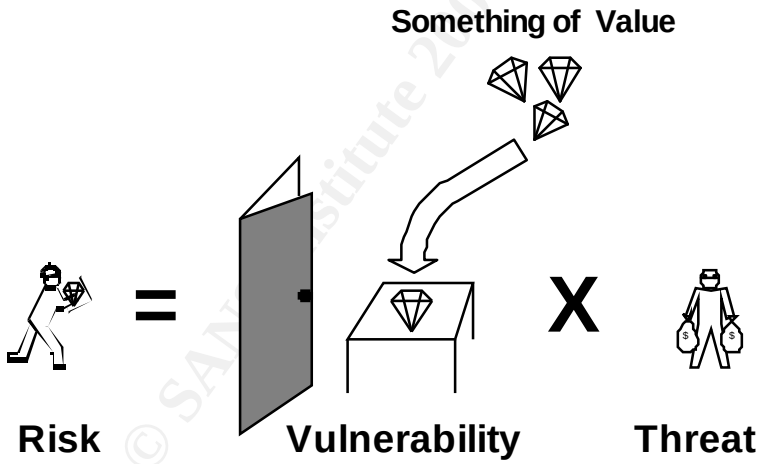


Figure 1 [5]

It is said that security is about managing risk to mitigate some business information you are trying to protect from unauthorized parties, and it is also about decreasing the number of opportunities for the attacker to gain entry to your protect data.[6] Managing risk as depicted in **Figure 2** is as much about technology as it is about the people.



Goldman, James E.
Applied Data Communications, 2nd Edition
p.553

Figure 2 [12]

Web site are conceptualized, created, deployed and financed by people. Although much has been written about securing web sites, many of the technical and non-technical

solutions assume that people will consistently do the right things at the right time. This paper looks at the preparation process necessary to perform a web security review. It addresses problems encountered in a security review, and a list of suggestions and considerations when performing a security review. This article is generally written for the novice IT security professional who needs to understand critical issues in preparing for a web security review.

Web and Security

Connection to the Internet has the potential of giving the Internet community access to your internal resources and systems. Generally, you may be dealing with unauthorized access, web defacement, theft of valuable information, or a host of attacks on your web site and related systems. If your web site is attacked, you may be impacted along with your customers, third-party vendors, partners and trusted systems. [9], [8] In fact, a computer is only safe when not connected to the Internet and turned off.[6] Unfortunately, the whole purpose of securing a web site is to enable, not disable business.

In its basic format, web security can be broken down and segregated into three parts: the host browser (client-side), the web server (server-side) and the connection between the two.[12] Each of these parts must be analyzed individually and then collectively to determine security risks and vulnerabilities that may be present in a web site. Security considerations for the client-side component include issues such as the web browser type, client operating system security, and authentication methodology, while server-side considerations may include issues such as host OS security, network security and database security. Connection between the client and server could raises security issues such as encryption strength, firewall configuration and network connectivity. In a typical web site configuration as illustrated in **Figure 3**, each component would have to be secured before a web site is in product. For example, the web server in the DMZ must be properly configured and updated.

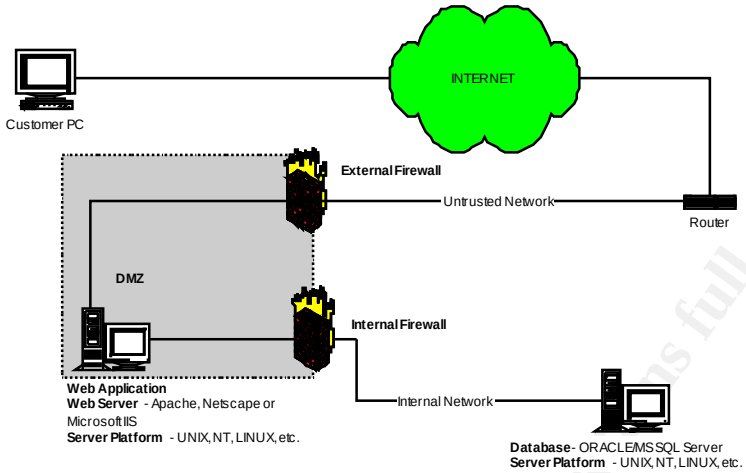


Figure 3

The level of security that should be applied to a web site is typically a balance between business productivity and security considerations. As illustrated in **Figure 4**, too much or too little of either business productivity or security could have undesired consequences.[11] Frequently companies are not aware of web vulnerabilities and crimes to justify strengthening their web security, so they either believe they would not be impacted or that the Internet is much safer today.[1]

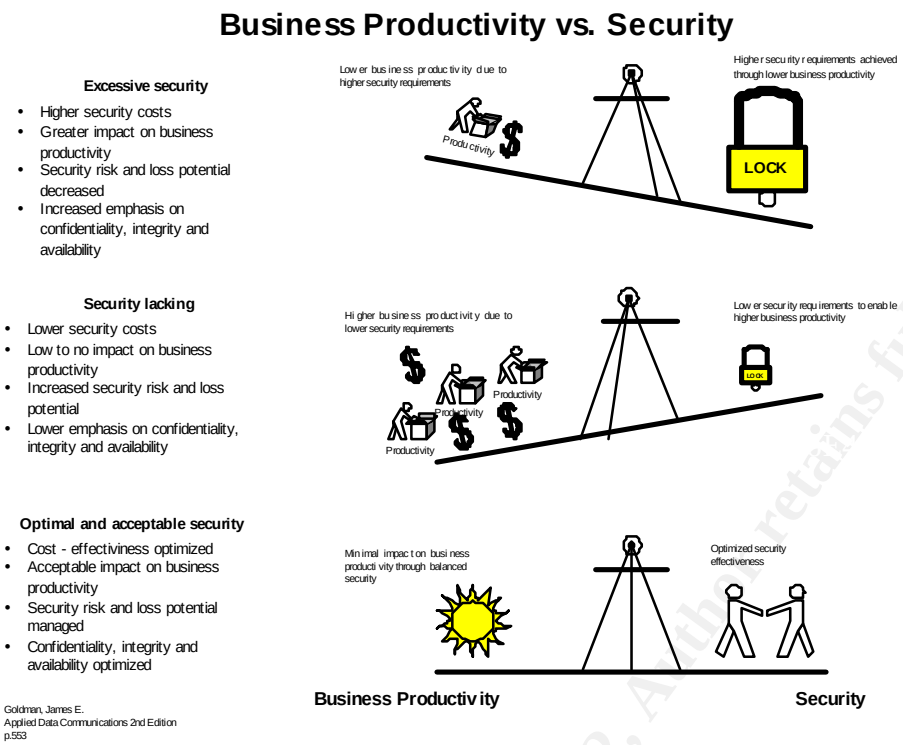


Figure 4 [11]

While these security issues are a part of a web site, analyzing, identifying and resolving web security issues cannot be accomplished without a set of preparatory guidelines. Therefore, it is important to understand factors that make a web security review challenging.

Challenges in performing a web security review

Security is not a new concept. However, the level of technological and computing sophistication that has impacted the Internet has progressively improved the Internet for better commerce activities as well as greater web security exploits. For example, web standardization of network and applications protocol such as TCP/IP, XML, Java, etc. which greatly enhances e-commerce is also prone to security vulnerabilities. [6] In addition, to accommodate greater business profitability and growth potential, security vulnerabilities and processes are often overlooked or ignored when developing a web site.

There are several possible reasons why implementing proper web security may be difficult. Some of these reasons are as follows:

- Web sites are developed in an environment that is fast paced and dynamic.
- Web sites are designed to be user-friendly with numerous functionalities and sophisticated capabilities, but are often impacted by security controls, if applied.
- IT security is often consulted after the project is completed, and it is often too costly to implement security once a web site is in production.

- IT security is often viewed or perceived as a support function that would eagerly impose costly security measures and restrictions to a web site.
- Web security is often perceived as solely an IT security problem.
- Talented IT security professionals may be scarce.
- Customers or web site owners do not believe that their web sites may be vulnerable to security breaches because it has never happened to them.
- Web site owners complain that they have always developed and maintained their web site without additional security.
- Web site owners are restricted by budgetary and time constraints from effectively implementing security solutions. Adequate security resources may not be included in the original project plan.

All these issues and many more are potential road blocks that the security practitioner needs to understand when assessing a web site. Web security is as much about working with other functional professionals as it is about assessing new technology. Technology alone is not security.[7]

Searching for a Solution

Although many web related security issues have been documented and made public by IT security professionals, the message is still lost or ignored by the public. Hence web related crimes and malicious acts such as credit card theft, web defacements, and numerous other known and unknown security exploits continues unabated. As we know, the frequency, sophistication and severity of future web related security exploits are expected to increase.

Before beginning a web security review, the following list of factors should be considered in developing a solution:

- Risk assessment is a crucial process that must be cost-effective, and management must approve actions that solve or mitigate risks.[3]
- Security is an endless cycle of protection, detection and response, and this is why the defense in depth concept is necessary to defend against threats.[2]
- Avoid using new tools that have not been reviewed and tested for security vulnerabilities. Use web tools that can be baseline or reviewed for security vulnerabilities
- The level of data security should be commensurate with the level of data classification. Once established, data classification should be continuously applied in all environments unless expressly changed by the data owner.
- Seek upper management approval and understanding in security matters.
- Security is a continuous process that is shared among individuals of all functional areas.
- Security should be considered a business enabler in that it is supposed to help build confidence for commerce over the Internet.[5]

Performing a Web Security Review

Web Business Case

In most web development projects, there is typically a web development project team responsible for designing and implementing a web site. As part of the project team, IT security may have a project or consulting presence. Before beginning a web security review, the IT security professional should consider asking a few questions to determine if the project team overlooked any critical information necessary for a security review. The following is a list of questions for the project team:

- Business owner or sponsor - who owns, funds and steers this project?
- Business purpose - what is the business purpose and impact to business entity? (i.e., process improvement, improve efficiency, increase productivity, etc.)
- Business or project scope - what is the extent of the web project? (i.e., domestic and/or foreign service/product offerings, web functionality/complexity, technology used, third-party applications used, etc.)
- Business or project documentation – what are the documents available for review (i.e., contract, statement of work, service line agreement, etc.)?
- Type of project – what is the nature of the web project (i.e., new customer requiring connectivity to company resources, existing customer requiring new system functionality, joint venture project requiring resource sharing, multiple vendors requiring complex web connectivity, etc.)?
- Project deliverable – what are the key project deliverables and critical success factors (i.e., develop an intranet web site for HR department in two months, provide third-party developers access to web databases, etc.)?
- Legal and contract review – what are the risks and concerns, if any, expressed by the legal or contracts department (i.e., contract is silent on third-party developer liabilities, legal has not reviewed contract for business exposure, etc.)?

Web Project Administration

Here are some suggested questions to ask when working on a web project with members of a multi-functional team.

- Are project team members identified and member list documented? (i.e., networking infrastructure support personnel, UNIX or NT administrators, Web/application developers, etc.)
- Are roles and responsibilities clearly identified and documented? (i.e., all project members aware of their roles and responsibilities with respect to web security in addition to their primary function)
- Is there a process to documented, escalated, resolved and archived web security issues? (i.e., security issues are identified, discussed and resolved by management in a timely manner)

- Are web security issues resolved with appropriate management input and approval? (i.e., process is in place to ensure that adequate and appropriate levels of management approval is sought to resolve web security issues)
- Is the project team aware of corporate IT Security policy, standards and procedures (i.e., project team has been apprised of the corporation's IT security requirements pertaining to web site security)
- Do support teams have a process in place to provide continuous security support for the web site while in production? (i.e., performance agreements are in place to ensure that all NT and MS - IIS web servers in support of a web site are patched within a reasonable time after a new patch is available)
- Does the web site owner have a process in place to assess the security impact to the enterprise network whenever there a change made to the original web site?
- Are the project hours necessary for web security reviews appropriately reflected in the project plan? (i.e., adequate time is allocated for web security review tasks)
- Are the IT security professionals maintaining adequate and appropriate communication log for the duration of the project? (i.e., IT security professional maintains a communication log for future reference)

Web Security Requirements

Once the business and administrative aspects of the web project have been addressed, the IT security professional would require additional information before beginning the analyzing and assessing web security issues. The following are suggested information to consider:

- Web project requirements are clearly communicated to the IT security professional to avoid any misunderstanding.
- Web data has been classified by the data owner to ensure proper levels of security are applied to the web site. (i.e., internal use, confidential, etc.)
- All relevant technical documentation is made available to the IT security professional. (i.e., network connectivity diagram, data flow diagram, external connectivity requirements, etc.)
- All industry-specific security requirements and regulations are adequately addressed. (i.e., Federal government may have specific guidelines and requirements for securing a governmental web site.)
- Where applicable, non-disclosure agreements (NDA) between the corporation and its third-party vendors are signed to mitigate any breach of security. (i.e., determine if project involves an external customer, partner or 3rd party and if so, ask project team if a NDA was completed before sharing information.)
- When IT security skills necessary to perform web review are limited or absent, management is informed immediately for support. (i.e., IT security professional may not have CORBA security experience, but management is addressing this deficiency.)
- The necessary technical security support is available to the IT security professional, if needed. (i.e., IT security professional has a subject matter expert in JAVA security identified to provide consultative services.

- IT security professional is given adequate time to perform and complete the web security review. (i.e., IT security professional has numerous projects and is not able to complete the web security assignment)

Web Security Analysis

Although each IT security professional may perform analysis in a variety of ways, each professional, varying in experience and background, would most certainly use some form of methodology. The following is a suggested list of tasks for performing web security reviews.

- Web security analysis should be performed in incremental steps with specific security objectives because security is a process and a destination.[5]
- Web security issues, risks, and exposures impacting the web project should be analyzed in layers, beginning with perimeter network security and working inwards to the data itself. (i.e., a web application that is open to the Internet and residing in the corporation's DMZ must be analyze to determine risk and exposure, if any, to the internal network)[4], [5]
- To determine web security issues, risks, and exposures, a security review should be performed based on established corporate IT security policy, standards and procedures. (i.e., what are the risks to company ABC when vendor XYZ's new web application for company ABC is residing on company YYY's web hosting server and is using MQSeries to access data on a database residing on ABC's internal network)
- Web security issues, risks and exposures for the web project should be identified, documented, and communicated to the project team or customer. (i.e., access controls poorly implemented, connectivity to third-party inadequately controlled, etc.)
- Knowledgeable IT security professionals or SME's should be consulted on challenging and complicated web security issues, if necessary.
- Web security solutions are validated, documented and presented to the project team or customer.
- Web security solutions should be approved by appropriate upper-level management, if necessary.

WEB SECURITY ASSESSMENT MATRIX

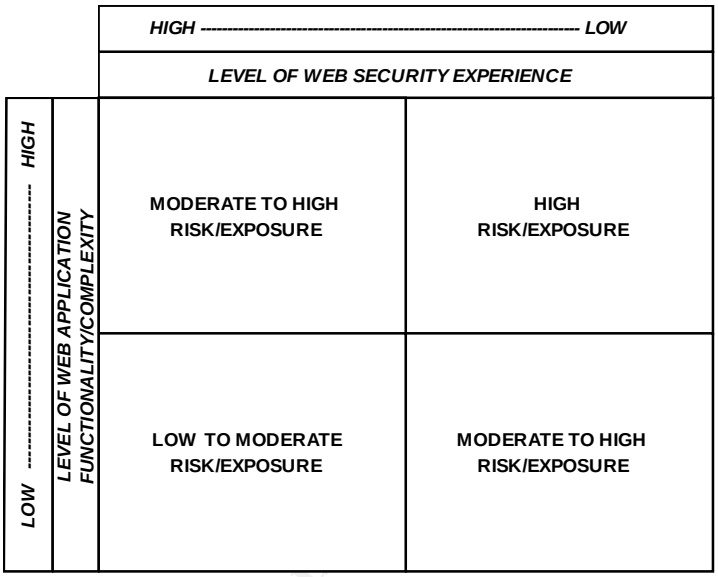


Figure 5

- Consider using business tools such as matrices and charts to improve security analysis and to help communicate security risks or solutions to the customer. For example, in **Figure 5**, a simple matrix depicting existing web security experience and web functionality could help the customer visualize and understand risk/exposure issues impacting a web site. Variations of the matrix could be used for other security issues.
- Post mortem review should be performed so that web security successes and failures for a web project are identified to improve review processes and to record lesson learned.
- Project documents should be archived, if necessary. Destroy project work papers according to corporate guidelines governing document destruction, otherwise.
- Web security may involve multiple systems, internal and external, so security analysis should determine how web project could impact the enterprise network.[5],[9]
- When analyzing web security, IT security professional should remember that security can never be perfect and human errors should never be underestimated.[10]

Summary

The number of hacking exploits perpetrated against web sites is expected to increase dramatically in the future as web sites continuously to proliferate. Before performing any web security review the IT security professional should consider asking critical questions to ensure he has adequate and accurate information. Furthermore, having a set of web security review guidelines would greatly assist in any subsequent security

analysis. Web security is an endless process design to secure data for people and by people.

REFERENCES

[1] Stewart, John. "Learning from History—Web Security in Review," WebTechniques. April 2000
http://www.webtechniques.com/archives/2001/04/conn/

[2] Norton, Stephen. "Circle of Security," SANS Institute. November 13, 2000
http://www.sans.org/infosecFAQ/securitybasics/circle.htm

[3] Johnson, John D. "Developing a Successful Information Security Process," SecurityPortal. March 29, 2001
http://www.securityportal.com/articles/risk20010329.html

[4] Peteanu, Razvan. "Practices for Secure Web Development: Technical Details," SecurityPortal. October 30, 2000
http://www.securityportal.com/articles/webdev20001103.html

[5] Mackey, Richard and Gossels, Jonathan. "MASTERING FUNDAMENTALS, PART 1," Information Security Magazine. January 2000
http://www.infosecuritymag.com/articles/january00/features3.shtml

[6] Mackey, Richard and Gossels, Jonathan. "MASTERING FUNDAMENTALS, PART 2," Information Security Magazine. February 2000
http://www.infosecuritymag.com/articles/february00/features3.shtml

[7] Mackey, Richard and Gossels, Jonathan. "MASTERING FUNDAMENTALS, PART 3," Information Security Magazine. March 2000
http://www.infosecuritymag.com/articles/march00/features3.shtml

[8] Worstell, Karen., Gerdes, Mike., and Kabay, Mich. "Net Present Value of Information Security: Part III," SecurityPortal. November 2, 2000
http://www.securityportal.com/articles/npv20001031.html

[9] Stein, Lincoln D. "The World Wide Web Security FAQ," The World Wide Web Consortium (W3C). March 24, 2000
http://www.w3.org/Security/Faq/www-security-faq.html

[10] Horowitz, Barry., Ph.D. "Managing the Security Risks of Your e-Business," eBizQ. August 2000
http://eai.ebizq.net/enterprise_integration/horowitz_1.html

[11] Goldman, James E. "Applied Data Communications: A business-Oriented Approach," 2nd Edition, John Wiley & Sons, Inc. 1998

http://isbn.nu/0471076791/price

[12] Stein, Lincoln D. "Web Security: A step-by-step reference guide," Addison-Wesley Longman, Inc. 1998
http://isbn.nu/0201634899/price

Other Suggested Reference

- Garfinkel, Simson with Spafford, Gene. "Web Security & Commerce," O'Reilly & Associates, Inc. June 1997.

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event