





# Teste de Invasão de Aplicações Web

## Abertura

# Teste de Invasão de Aplicações Web

Rio de Janeiro  
Escola Superior de Redes  
2013

*Nelson Uto  
Edson Kowask Bezerra*

**O curso apresenta uma metodologia de verificação da segurança por meio da simulação de ataques reais, explorando as vulnerabilidades de um ambiente, plataforma ou sistema, os quais são reconhecidamente os principais meios explorados para roubo de informações confidenciais e invasão de redes corporativas.**

**Para ser um profissional de pentest, é preciso muito mais do que utilizar ferramentas automatizadas: são necessários conhecimentos diferenciados e técnicas avançadas que permitam a compreensão ampla de cenários de vulnerabilidades.**

**Este livro apoia o curso de formação destes novos profissionais através das melhores práticas para testes de invasão, contendo atividades de simulação de ataques em ambiente de teste virtualizado. Ao final do curso, o aluno estará apto a avaliar a eficiência da segurança de sua organização, e a propor o modelo de maturidade em segurança de software mais adequado à sua necessidade.**


Curso voltado para técnicos, analistas e administradores de redes que desejam obter o conhecimento sobre técnicas, padrões internacionais e ferramental para realização de testes de invasão em aplicações web. Também indicado para técnicos e gestores responsáveis pelo desenvolvimento e suporte de sistemas, e para profissionais de computação interessados em adquirir conhecimento diferencial na área de segurança cibernética.




- 1 **Segurança em aplicações web**
- 2 **Reconhecimento e mapeamento**
- 3 **Teste do mecanismo de autenticação**
- 4 **Teste do gerenciamento de sessões**
- 5 **Cross-site scripting**




- 6 Injeção de SQL**
- 7 Ataques de injeção**
- 8 Teste do mecanismo de autorização e da lógica de negócio**
- 9 Mecanismos criptográficos**
- 10 Escrita de relatórios e exercício completo**




A filosofia pedagógica e a metodologia que orientam os cursos da ESR são baseadas na aprendizagem como construção do conhecimento por meio da resolução de problemas típicos da realidade do profissional em formação.




Os resultados obtidos nos cursos de natureza teórico-prática são otimizados, pois o instrutor, auxiliado pelo material didático, atua não apenas como expositor de conceitos e informações, mas principalmente como orientador do aluno na execução de atividades contextualizadas nas situações do cotidiano profissional.



A aprendizagem é entendida como a resposta do aluno ao desafio de situações-problema semelhantes às encontradas na prática profissional, que são superadas por meio de análise, síntese, julgamento, pensamento crítico e construção de hipóteses para a resolução do problema, em abordagem orientada ao desenvolvimento de competências.



Dessa forma, o instrutor tem participação ativa e dialógica como orientador do aluno para as atividades em laboratório. Até mesmo a apresentação da teoria no início da sessão de aprendizagem não é considerada uma simples exposição de conceitos e informações. O instrutor busca incentivar a participação dos alunos continuamente.



As sessões de aprendizagem onde se dão a apresentação dos conteúdos terão formato EaD utilizando metodologia estudo sala de aula invertida e práticas orientadas para o contexto de atuação do futuro especialista que se pretende formar.




## Gildásio Júnior

Sistemas de Informação @ **UFBA**  
Instrutor / Monitor / Tutor @ **ESR/RNP**  
Security Research @ **Allele**  
SOC Engineer @ **S21Sec**

Analista de Segurança @ **PoP-BA/RNP**  
Pesquisador de Segurança @ **CoSIC/UFBA**  
Líder @ **CERT.Bahia**  
Teaching Assistant @ **Cybrary**

 /gildasio

 /gildasio

 gildasiojunior  
@riseup.net

- ❑ BARKER, Elaine; BARKER, William; BURR, William; POLK, William e SMID, Miles. Recommendation for key management – part 2: Best practices for key management organization. NIST Special Publication 800-57, NIST, 2007b.
- ❑ BERNERS-LEE, Tim; FIELDING, Roy T. e MASINTER, Larry. RFC 3986: Uniform Resource Identifier (URI): Generic Syntax, 2005.
- ❑ FIELDING, Roy T.; GETTYS, James; MOGUL, Jeffrey C.; NIELSEN, Henrik Frystyk; MASINTER, Larry; LEACH, Paul J. e BERNERS-LEE, Tim. RFC 2616: Hypertext Transfer Protocol – HTTP/1.1, 1999.



- FRANKS, John; HALLAM-BAKER, Phillip M.; HOSTETLER, Jeffery L.; LAWRENCE, Scott D.; LEACH, Paul J.; LUOTONEN, Ari e STEWART, Lawrence C. RFC 2617: HTTP Authentication: Basic and Digest Access Authentication, 1999.
- KISSEL, Richard; STINE, Kevin; SCHOLL, Matthew; ROSSMAN, Hart; FAHLSING, Jim e GULICK, Jessica. Security considerations in the system development life cycle. NIST Special Publication SP 800-64, National Institute of Standards and Technology, 2008.
- LITCHFIELD, David. The Oracle Hacker's Handbook – Hacking and Defending Oracle. Wiley Publishing, Inc., 2007.

- ❑ MCGRAW, Gary. Software Security: Building Security In. Addison-Wesley Professional, 2006.
- ❑ MENEZES, Alfred J.; VAN OORSCHOT, Paul. C. e VANSTONE, Scott. A. Handbook of Applied Cryptography. CRC Press, 5th edition, 2001.
- ❑ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- ❑ ORACLE. Your First Cup: an Introduction to the Java EETM Platform. PartNo: 821–1770–10. Junho. Oracle, 2010.

- ❑ PCI. Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures – v. 1.2.1. PCI Security Standards Council, 2009a.
- ❑ PCI. Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) – version 1.2.1. PCI Security Standards Council, 2009b.
- ❑ SEACORD, Robert C. Secure Coding in C and C++. Addison-Wesley Professional, 2005.

- ▮ SHANNON, Claude. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, Vol. 28, p. 656-715, 1949.
- ▮ SHKLAR, Leon e ROSEN, Richard. Web Application Architecture: Principles, Protocols and Practices. 2<sup>a</sup>. Edição. Wiley, 2009.
- ▮ STEVENS, Marc; SOTIROV, Alexander; APPELBAUM, Jacob; LENSTRA, Arjen; MOLNAR, David; OSVIK, Dag Arne e DE WEGER, Benne. Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. In: Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology – LNCS. Vol. 5677. p. 55-69. Springer-Verlag, 2009.

- ▮ STUTTARD, Dafydd; PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.
- ▮ VAN DER STOCK, Andrew; CRUZ, Dinis; CHAPMAN, Jenelle; LOWERY, David; KEARY, Eoin; MORANA, Marco M.; ROOK, David; WILLIAMS, Jeff e PREGO, Paulo. OWASP code review guide v1.1. OWASP, 2008.
- ▮ WANG, Xiaoyun; YU, Hongbo. How to break MD5 and other hash functions. Eurocrypt 2005. Springer-Verlag, 2005.

- ❏ WIESMANN, Adrian; CURPHEY, Mark; VAN DER STOCK, Andrew e STIRBEI, Ray. A guide to building secure web applications and web services. OWASP, 2005.
- ❏ WYSOPAL, Chris; NELSON, Lucas; ZIVI, Dino Dai e DUSTIN, Elfriede. The Art of Software Security Testing: Identifying Software Security Flaws. Symantec Press, 2006.

- ▮ DOUPÉ, Adam; COVA, Marco e VIGNA, Giovanni. Why Johnny Can't Pentest: An Analysis of Black-box Web Vulnerability Scanners. In: Proceedings of Seventh Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2010). Bonn, Germany, 2010.
- ▮ HERZOG, Pete. OSSTMM 3 – The Open Source Security Testing Methodology Manual – Contemporary Security Testing and Analysis. ISECOM, 2010.

- ❑ LONG, Johnny; TEMMINGH, Roelof; STEWART, Jeff; PETKOV, Petko D. e LANGLEY, Ryan. Google Hacking for Penetration Testers: Volume 2 – a completely new volume of Google hacking techniques. Syngress, 2008.
- ❑ MCGRAW, Gary. Software Security: Building Security In. Addison-Wesley Professional, 2006.
- ❑ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- ❑ NETMARKETSHARE. Browser market share. Disponível em: <http://marketshare.hitslink.com/report.aspx?qprid=0>. Data de acesso: 28/12/2010.



- ❑ PCI. Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures – v. 1.2.1. PCI Security Standards Council, 2009a.
- ❑ PCI. Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) – version 1.2.1. PCI Security Standards Council, 2009b.
- ❑ POSTEL, Jon. RFC 793 – Transmission Control Protocol – DARPA Internet Program – Protocol Specification. 1981.

- ❑ SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda e OREBAUGH, Angela. Technical Guide to Information Security Testing and Assessment – Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-115, National Institute of Standards and Technology, 2008.
- ❑ STATCOUNTER. Top 5 browsers from Nov 09 to Nov 10. Disponível em: <http://gs.statcounter.com/>. Data de acesso: 28/12/2010.
- ❑ STATOWL. Web browser market share. Disponível em: [http://www.statowl.com/web\\_browser\\_market\\_share.php](http://www.statowl.com/web_browser_market_share.php). Data de acesso: 28/12/2010.

- STUTTARD, Dafydd; PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.

- ❑ DUC, Nguyen Minh e MIHN, Bui Quang. Your face is NOT your password – Face Authentication ByPassing Lenovo – Asus – Toshiba. Relatório Técnico, Bkis, 2009.
- ❑ HAMANN, E.; HENN, Horst; SCHÄCK, Thomas e SELIGER, Frank. Securing e-business applications using smart cards. IBM Systems Journal, Vol. 40, número 30, p. 635-647, março de 2001.
- ❑ HARRIS, Shon. All in One CISSP – Exam Guide. McGraw Hill – Osborne, 4ª edição, 2008.

- ❏ HELLMAN, Martin. A Cryptanalytic Time-Memory Trade-Off. In: IEEE Transactions on Information Theory, volume 26, número 4, páginas 401-406, julho de 1980.
- ❏ HOWARD, Michael; LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security – Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.
- ❏ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.

- ❑ OECHSLIN, Philippe. Making a Faster Cryptanalytic Time-Memory Trade-Off. In: Advances in Cryptology – CRYPTO 2003 – 23rd Annual International Cryptology Conference, volume 2729 de Lecture Notes in Computer Science, p. 617-630, Springer, 2003.
- ❑ PCI. Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures – v. 1.2.1. PCI Security Standards Council, 2009.
- ❑ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.

- ULUDAG, Umut e JAIN, Anil K. Attacks on Biometric Systems: A Case Study in Fingerprints. In: Proceedings of SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, p. 622-633, San Jose, CA, janeiro de 2004.

- ▮ BALDUZZI, Marco; EGELE, Manuel; KIRDA, Engin; BALZAROTTI, Davide e KRUEGEL, Christopher. A Solution for the Automated Detection of Clickjacking Attacks. In: ASIACCS '10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010.
- ▮ BARRALL, Darrin. Automated Cookie Analysis – Are your web applications vulnerable?. SPI Dynamics, 2005.
- ▮ BURNS, Jesse. Cross Site Reference Forgery – An introduction to a common web application weakness. Information Security Partners, LLC, 2005.



- ❑ BURNS, Jesse. Cross Site Request Forgery – an introduction to a common web application weakness. Information Security Partners, LLC, 2007.
- ❑ ENDLER, David. Brute-Force Exploitation of Web Application Session IDs. iAlert White Paper, iDEFENSE Labs, 2001.
- ❑ ESPOSITO, Dino. Take Advantage of ASP.NET Built-in Features to Fend Off Web Attacks.
- ❑ Disponível em: <http://msdn.microsoft.com/en-us/library/ms972969.aspx>. Data de acesso: 25/07/2011. MSDN Library, 2005.

- ❏ HANSEN, Robert e GROSSMAN, Jeremiah. Clickjacking. Disponível em: <http://www.sectheory.com/clickjacking.htm>. Data de acesso: 25/07/2011. SecTheory, 2008.
- ❏ JOVANOVIĆ, Nenad; KIRDA, Engin e KRUEGEL, Christopher. Preventing Cross Site Request Forgery Attacks. In: 2006 SecureComm and Workshops, IEEE, 2006.
- ❏ KOLŠEK, Mitja. Session Fixation Vulnerability in Web-based Applications. Version 1.0, ACROS Security, 2002.

- ❑ KOLŠEK, Mitja. Session Fixation Vulnerability in Web-based Applications. Version 1.0 – revision 1, ACROS Security, 2007.
- ❑ KRISTOL, David e MONTULLI, Lou. HTTP State Management Mechanism. RFC 2965, 2000.
- ❑ KUPPAN, Lavakumar. Attacking with HTML5. Attack & Defense Labs, 2010.
- ❑ MAHEMOFF, Michael. Explaining the “Don’t Click” Clickjacking Tweetbomb. Disponível em: <http://softwareas.com/explaining-the-dont-click-clickjacking-tweetbomb>. Data de acesso: 25/07/2011. Mahemoff’s Podcast/Blog, 2009.

- MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- MORGAN, Timothy D. Weaning the Web off of Session Cookies – Making Digest Authentication Viable. Version 1.0, VSR, 2010.
- PALMER, Chris. Secure Session Management with Cookies for Web Applications. iSEC Partners, Inc., 2008.
- RYDSTEDT, Gustav; BURSZTEIN, Elie; BONEH, Dan e JACKSON, Colling. Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites. In: IEEE Web 2.0 Security and Privacy (W2SP), 2010.

- ❑ SCHRANK, Michael; BRAUN, Bastian e POSSEGA, John Joachim. Session Fixation – The Forgotten Vulnerability? In: Sicherheit 2010: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 5. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 2010.
- ❑ SCHREIBER, Thomas. Session Riding a Widespread Vulnerability in Today's Web Applications. SecureNet, Whitepaper, 2004.
- ❑ SILES, Raúl. SAP: Session (Fixation) Attacks and Protections (in Web Applications). Taddong S. L., Black Hat Europe 2011, 2011.

- ▮ STONE, Paul. Next Generation Clickjacking – New attacks against framed web pages. White Paper, Context Information Security Ltd., 2010.
- ▮ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.

- ❑ BOJINOV, Hristo; BURSZTEIN, Elie e BONEH, Dan. XCS: Cross Channel Scripting and its Impact on Web Applications. In: CCS'09: Proceedings of the 16th ACM Conference on Computer and Communications Security (New York, USA), pág. 420-431, Association for Computing Machinery, 2009.
- ❑ BOJINOV, Hristo; BURSZTEIN, Elie e BONEH, Dan. The Emergence of Cross Channel Scripting. In: Communications of the ACM, volume 53, número 08, p. 105-113, Association for Computing Machinery, 2010.
- ❑ CHIEN, Eric. Malicious Yahoooligans. White Paper: Symantec Security Response, Symantec, 2006.

- ❑ ENDLER, David. The Evolution of Cross-Site Scripting Attacks. iALERT White Paper, iDEFENSE Labs, 2002.
- ❑ GROSSMAN, Jeremiah. Cross-Site Tracing (XST) - The New Techniques and Emerging Threats to Bypass Current Web Security Measures Using TRACE and XSS. WhiteHat Security, 2003.
- ❑ GROSSMAN, Jeremiah. Cross-Site Scripting Worms & Viruses - The Impending Threat & the Best Defense. White Paper, White Hat Security, 2007a.



- ❏ GROSSMAN, Jeremiah. Hacking Intranet Websites from the Outside (Take 2) - Fun with & without Javascript Malware. White Paper, White Hat Security, 2007b.
- ❏ GROSSMAN, Jeremiah; HANSEN, Robert “RSnake”; PETKOV, Petko “pdp”, RAGER, Anton e FOGIE, Seth. XSS Attacks – Cross Site Scripting Exploits and Defense. Syngress, 2007.
- ❏ HOFFMAN, Billy. Stealing Search Engine Queries with JavaScript. SPI Labs Research Brief, SPI Labs, 2006.
- ❏ HOFFMAN, Billy e SULLIVAN, Bryan. Ajax Security. Addison-Wesley Professional, 2007.

- ▮ HOWARD, Michael; LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security – Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.
- ▮ JOHNS, Martin. SessionSafe: Implementing XSS Immune Session Handling. In: ESORICS 2006, Lecture Notes in Computer Science 4189, p. 444-460. Springer-Verlag, 2006.
- ▮ KAMKAR, Samy. Technical explanation of The MySpace Worm – Also called the “Samy worm” or “JS.Spacehero worm”. 2005. Disponível em: <http://namb.la/popular/tech.html>. Data de acesso: 30/07/2011.

- ❏ KIRDA, Engin; KRUEGEL, Christopher; VIGNA, Giovanni e JOVANOVIC, Nenad. Noxes: a Client-Side Solution for Mitigating Cross-Site Scripting Attacks. In: SAC '06: Proceedings of the 2006 ACM symposium on Applied computing, Association for Computing Machinery, 2006.
- ❏ KLEIN, Amit. Cross Site Scripting Explained. Sanctum Security Group, 2002.

- ❑ KLEIN, Amit. DOM Based Cross Site Scripting or XSS of the Third Kind - A look at na overlooked flavor of XSS. Web Application Security Consortium, 2005. Disponível em: <http://www.webappsec.org/projects/articles/071105.html>. Data de acesso: 30/07/2011.
- ❑ KUPPAN, Lavakumar. Attacking with HTML5. Attack & Defense Labs, 2010.
- ❑ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.

- ▮ SHAH, Shreeraj. Hacking Browser's DOM - Exploiting Ajax and RIA. Blackhat, 2010. Disponível em:  
<https://media.blackhat.com/bh-us-10/whitepapers/Shah/BlackHat-USA-2010-Shah-DOM-Hacks-Shreeraj-wp.pdf>. Data de acesso: 30/07/2011.
- ▮ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.
- ▮ SUN, Fangqi; XU, Liang e SU, Zendhong. Client-Side Detection of XSS Worms by Monitoring Payload Propagation. In: ESORICS'09: Proceedings of the 14th European Conference on Research in Computer Security, Springer-Verlag, 2009.

- ❏ VAN DER STOCK, Andrew; CRUZ, Dinis; CHAPMAN, Jenelle; LOWERY, David; KEARY, Eoin; MORANA, Marco M.; ROOK, David; PREGO, Paulo e WILLIAMS, Jeff. OWASP Code Review Guide v1.1. OWASP, 2008.

- ▮ ANLEY, Chris. Advanced SQL Injection in SQL Server Applications. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software Ltd, 2002a.
- ▮ ANLEY, Chris et al. Advanced SQL Injection. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software Ltd, 2002b.
- ▮ ANLEY, Chris. Hackproofing MySQL. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software Ltd, 2004.

- CLARKE, Justin. SQL Injection Attacks and Defense. Syngress, 2009.
- DOUPÉ, Adam; COVA, Marco e VIGNA, Giovanni. Why Johnny Can't Pentest: An Analysis of Black-box Web Vulnerability Scanners. In: Proceedings of Detection of Intrusions and Malware, and Vulnerability Assessment, 7th International Conference, DIMVA 2010. Lecture Notes in Computer Science 6201, Springer, 2010.
- GUIMARÃES, Bernardo Damele Assumpção. Advanced SQL Injection to operating system full control. Black Hat Europe Briefings, 2009.



- ❏ GUIMARÃES, Bernardo Damele Assumpção e STAMPAR, Miroslav. SQL map user's manual – version 0.9. Manual, 2011.
- ❏ HALFOND, Willian G. J.; VIEGAS, Jeremy e ORSO, Alessandro. A Classification of SQL Injection Attacks and Countermeasures. In: Proceedings of the International Symposium on Secure Software Engineering, 2006.
- ❏ HOWARD, Michael; LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security - Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.

- ❑ KOST, Stephen. An Introduction to SQL Injection Attacks for Oracle Developers. Integrity Corporation, 2004.
- ❑ LEIDECKER, Nico. Having Fun With PostgreSQL. Portcullis Computer Security Limited, 2007.
- ❑ LITCHFIELD, David. Data-mining with SQL Injection and Inference. NGSSoftware Insight Security Research (NISR) Publication, Next Generation Security Software Ltd, 2005.

- ❑ LITCHFIELD, David; ANLEY, Chris; HEASMAN, John e GRINDLAY, Bill. The Database Hacker's Handbook: Defending Database Servers. Wiley Publishing, Inc., 2005.
- ❑ LITCHFIELD, David. The Oracle Hacker's Handbook - Hacking and Defending Oracle. Wiley Publishing, Inc., 2007.
- ❑ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- ❑ SPETT, Kevin. SQL Injection - Are your web applications vulnerable?, SPI Dynamics, 2002.

- SPETT, Kevin. Blind SQL Injection - Are your web applications vulnerable?, SPI Dynamics, 2003.
- STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.

- ▮ ALONSO, Chema; BORDÓN, Rodolfo; GUZMÁN, Antonio e BELTRÁN, Marta. LDAP Injection & Blind LDAP Injection in Web Applications. Black Hat Europe 08, 2008.
- ▮ BALDUZZI, Marco 'embyte'. HTTP Parameter Pollution Vulnerabilities in Web Applications. Black Hat Europe, 2011.
- ▮ BALDUZZI, Marco; GIMENEZ, Carmen Torrano; BALZAROTTI, Davide e KIRDA, Engin. HTTP Parameter Pollution Vulnerabilities in Web Applications. In: Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, The Internet Society, 2011.

- ▮ BAROR, Yuval; YOGEV, Ayal e SHARABANI, Adi. Flash Parameter Injection – A Security Advisory. Whitepaper, IBM Rational Application Security Team, 2008.
- ▮ BERGLUND, Anders; BOAG, Scott; CHAMBERLIN, Don; FERNÁNDEZ, Mary F.; KAY, Michael; ROBIE, Jonathan e SIMÉON, Jérôme. XML Path Language (XPath) 2.0 (Second Edition), W3C Recommendation, dezembro de 2010.
- ▮ BURSZTEIN, Elie; GOURDIN, Baptiste; RYDSTEDT, Gustav e BONEH, Dan. Bad Memories. Black Hat USA, 2010.

- ❑ CARETTONI, Luca e DI PAOLA, Stefano. HTTP Parameter Pollution. OWASP EU09 Poland, The OWASP Foundation, 2009.
- ❑ CLARK, James e DEROSE, Steve. XML Path Language (XPath) – Version 1.0, W3C Recommendation, novembro de 1999.
- ❑ DANIEL, Chrysostomos. HTTP Parameter Pollution. White Paper, Acunetix, 2012.
- ❑ DI PAOLA, Stefano e DABIRSIAGHI, Arshan. Expression Language Injection, White Paper, 2011.

- ❑ DÍAZ, Vicente Aguilera. MX Injection – Capturing and Exploiting Hidden Mail Servers. White Paper, Internet Security Auditors, 2006.
- ❑ FAUST, Sacha. LDAP Injection – Are your web applications vulnerable? White Paper, SPI Dynamics, Inc., 2003.
- ❑ FORBES, Thomas e SIDDHARTH, Sumit. Hacking XPath 2.0. Black Hat Europe, 2012.
- ❑ GRZELAK, Daniel. Log Injection Attack and Defence. SIFT Special Publication, SIFT Information Security Services, 2007.



- ❏ GUILLARDOY, Esteban, DE GUZMAN, Facundo e ABBAMONTE, Hernan. LDAP Injection – Attack and Defense Techniques. White Paper, Ridabeo Hack Lab, 2010a.
- ❏ GUILLARDOY, Esteban, DE GUZMAN, Facundo e ABBAMONTE, Hernan. LDAP Injection – Attack and Defense Techniques. Em HITB Magazine, Volume 1, Issue 1, 2010b.
- ❏ HOWARD, Michael, LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security – Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.

- ❑ JOURDAN, Guy-Vincent. Securing Large Applications Against Command Injections. Em Aerospace and Electronic Systems Magazine, Volume 24, Issue 6, Pág. 15-24, IEEE, 2009.
- ❑ KLEIN, Amit. “Divide and Conquer” – HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics. White Paper, Sanctum, 2004a.
- ❑ KLEIN, Amit. Blind XPath Injection. White Paper, Sanctum, 2004b.
- ❑ KLEIN, Amit. Blind XPath Injection. White Paper, Watchfire, 2005.

- ▮ LARANJEIRO, Nuno, VIEIRA, Marco e MADEIRA, Henrique. Protecting Database Centric Web Services against SQL/XPath Injection Attacks. Em Database and Expert Systems Applications, 20th International Conference, DEXA 2009, Linz, Austria, 31 de agosto – 4 de setembro, 2009. Proceedings. Lecture Notes in Computer Science 5690, Springer, 2009.
- ▮ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.

- ▮ MITROPOULOS, Dimistris, KARAKOIDAS, Vassilios e SPINELLIS, Diomidis. Fortifying Applications Against Xpath Injection Attacks. Em The 4th Mediterranean Conference on Information Systems, MCIS 2009, 2009.
- ▮ PINTER, Dominik. Kentico CMS Security White Paper. Kentico Software s.r.o., 2011.
- ▮ SMITH, Mark e HOWES, Tim. RFC 4515: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters, 2006.

- ❑ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.
- ❑ SU, Zhendong e WASSERMANN, Gary. The Essence of Command Injection Attacks in Web Applications. Em POPL '06 Conference record of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, ACM, 2006.
- ❑ VAN DER VLIST, Eric. XQuery Injection – Easy to exploit, easy to prevent.... Em XML Prague 2011 – Conference Proceedings, p. 177-189, 2011.

- ZEILENGA, Kurt. RFC 4514: Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, 2006a.
- ZEILENGA, Kurt. RFC 4512: Lightweight Directory Access Protocol (LDAP): Directory Information Models, 2006b.

- ❏ ANDERSON, James P. Computer Security technology planning study. Relatório Técnico ESDTR- 73-51, Air Force Electronic Systems Division, 1972.
- ❏ BISHOP, Matt. Race Conditions, Files, and Security Flaws; or the Tortoise and the Hare Redux. Technical Report CSE-95-9, Dept. of Computer Science, University of California at Davis, Davis, CA 95616-8562, 1995.
- ❏ GROSSMAN, Jeremiah. Seven Business Logic Flaws That Put Your Website At Risk. WhiteHat Security Whitepaper, 2007.

- ▮ HOWARD, Michael, LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security – Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.
- ▮ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- ▮ NETZER, Robert H. B. e MILLER, Barton P. What are Race Conditions? - Some Issues and Formalizations. ACM Letters on Programming Languages and Systems, Volume 1, 1992.



- ▮ PALEARI, Roberto; MARRONE, Davide; BRUSCHI, Danilo e MONGA, Matia. On Race Vulnerabilities in Web Applications. In: DIMVA '08 Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Lecture Notes in Computer Science, Volume 5137, Springer-Verlag, 2008.
- ▮ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.

- ❑ BARKER, Elaine, BARKER, William, BURR, William, POLK, William e SMID, Miles. Recommendation for Key Management – Part I: General. NIST Special Publication SP800-57, National Institute of Standards and Technology, 2007.
- ❑ CARMICHAEL, Mary. Como Conter o Parasita Mais Letal do Mundo. Em Scientific American Brasil, Ano 8, número 103, dezembro de 2010.
- ❑ DWORKIN, Morris. Recommendation for Block Cipher Modes of Operation – Methods and Techniques. NIST Special Publication SP800-38A, National Institute of Standards and Technology, 2001.

- ❏ FRIEDMAN, William F. The index of coincidence and its applications in cryptology. Department of Ciphers. Publ 22. Geneva, Illinois, EUA. Riverbank Laboratories, 1922.
- ❏ GAINES, Helen Fouché. Cryptanalysis – A study of ciphers and their solution. Dover Publications, 1939.
- ❏ HOWARD, Michael, LEBLANC, David e VIEGA, John. 19 Deadly Sins of Software Security – Programming Flaws and How to Fix Them. McGraw-Hill/Osborne, 2005.

- ❏ Kleinjung, Thorsten, Aoki, Kazumaro, Franke, Jens, Lenstra, Arjen K., Thomé, Emmanuel, Bos, Joppe W., Gaudrym, Pierrick, Kruppa, Alexander, Montgomery, Peter L., Osvik, Dag Arne, Riele, Herman te, Timofeev, Andrey e Zimmermann, Paul. Factorization of a 768-bit RSA modulus. Cryptology ePrint Archive 2010/006. IACR, 2010.
- ❏ KNUDSEN, Lars. SMASH – A Cryptographic Hash Function. Em Fast Software Encryption: 12th International Workshop, FSE 2005, volume 3557 de Lecture Notes in Computer Science, páginas 228–242. Springer, 2005.

- ❑ KOST, Stephen. Security Analysis – Hashing Credit Card Numbers: Unsafe Application Practice. Relatório Técnico de Integrigy Corporation, 2007.
- ❑ LENSTRA, Arjen, VERHEUL, Eric. Selecting Cryptographic Key Sizes. Journal of Cryptology, volume 14, 1999.
- ❑ MENEZES, Alfred, VAN OORSCHOT, Paul C. e VANSTONE, Scott A. Handbook of Applied Cryptography. 5th edition. CRC Press, 2001.
- ❑ MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- ❑ OAKS, Scott. Java™ Security. 2nd edition. O'Reilly, 2001.

- ❑ PCI. Payment Card Industry (PCI) Data Security Standard – Requirements and Security Assessment Procedures – v. 1.2.1. PCI Security Standards Council, 2009a.
- ❑ PCI. Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) – version 1.2.1. PCI Security Standards Council, 2009b.

- ❑ PRAMSTALLER, Norbert, RECHBERGER, Christian e RIJMEN, Vincent. Breaking a New Hash Function Design Strategy Called SMASH. Em Selected Areas in Cryptography, 12th International Workshop, SAC 2005, volume 3897 de Lecture Notes in Computer Science, páginas 234–244. Springer, 2005.
- ❑ RIBEIRO, Ronaldo. Código Postal | Águas Claras, DF 71900-000 – Ficção Urbana. Em National Geographic Brasil, janeiro de 2011.
- ❑ SAVALICH, William. Evolution in the Revolution. Em Digital Photo Pro, março/abril de 2009.

- ❑ SINGH, Simon. The Code Book – The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography. Doubleday, 1999.
- ❑ SMART, Nigel. ECRYPT II Yearly Report on Algorithm and Keysizes (2009-2010) – Revision 1.0. ECRYPT, março de 2010.
- ❑ STALLINGS, William. Cryptography and Network Security – Principles and Practice. 4th edition. Prentice Hall.



- ▮ STEVENS, Marc, SOTIROV, Alexander, APPELBAUM, Jacob, LENSTRA, Arjen, MOLNAR, David, OSVIK, Dag Arne e DE WEGER, Benne. Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate. Em Advances in Cryptology – CRYPTO 2009 – 29th Annual International Cryptology Conference, volume 5677 de Lecture Notes in Computer Science, páginas 55–69, Springer, 2009.
- ▮ STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.
- ▮ SWENSON, Christopher. Modern Cryptanalysis – Techniques for Advanced Code Breaking. Wiley Publishing, Inc., 2008.

- WAGNER, David e SCHNEIER, Bruce. Analysis of the SSL 3.0 Protocol. Em Proceedings of the Second USENIX Workshop on Electronic Commerce, 1996.
- WANG, Xiaoyun, YAO, Andrew e YAO, Frances. New Collision Search for SHA-1. Rump Session de Crypto'05, 2005.
- WANG, Xiaoyun, YIN, Yiqun Lisa e YU, Hongbo. Finding Collisions in the Full SHA-1. Em CRYPTO 2005: 25th Annual International Cryptology Conference, volume 3621 de Lecture Notes in Computer Science. Springer, 2005.

- ▮ WANG, Xiaoyun e YU, Hongbo. How to Break MD5 and Other Hash Functions. Em EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, volume 3494 de Lecture Notes in Computer Science, pages 19–35. Springer, 2005.
- ▮ WONG, Kate. Twilight of the Neandertals. Em Scientific American, volume 301, número 2, agosto de 2009.

- ▮ AUGER, Robert et al. WASC Threat Classification – Version 2.00. Web Application Security Consortium, 2010.
- ▮ GORDEYCHIK, Sergey, GROSSMAN, Jeremiah, KHERA, Mandeep, LANTINGA, Matt, WYSOPAL, Chris, ENG, Chris, SHAH, Shreeraj, LEE, Lawson, MURRAY, Campbell e EVTEEV, Dmitry. Web Application Security Statistics 2008. Web Application Security Consortium, 2008.
- ▮ MELL, Peter, SCARFONE, Karen e ROMANOSKY, Sasha. CVSS – A Complete Guide to the Common Vulnerability Scoring System – Version 2.0. FIRST, 2007.

- MEUCCI, Matteo et al. OWASP testing guide v3.0. OWASP, 2008.
- STUTTARD, Dafydd e PINTO, Marcus. The Web Application Hacker's Handbook. Wiley Publishing, Inc., 2007.



# Teste de Invasão de Aplicações Web

## Abertura