ModSecurity - Development and Management of Web Application Firewall rules.

1. Training description.
2. Key learning objectives.
3. Who should attend.
4. Prerequisite knowledge.
5. HW / SW requirements.
6. Full agenda.
7. Time duration.
8. Training keywords.
9. Trainer Bio.
10. Customers.
11. Contact.

TRAINING DESCRIPTION:

- *ModSecurity - Development and Management of Web Application Firewall rules* is a dedicated training which helps you understand the basics and deploy later complex web application firewall rules and hardened configuration against modern flaws in your web application infrastructure. During hands-on labs we will cover in details every important aspect and functionality of ModSecurity vs current attacker's techniques, vulnerabilities and server misconfigurations. Various examples such as Command Execution, SSRF, SQL Injection or Cross Site Scripting are just a few of the most commonly used bugs. Types of susceptibility are dozens. The most dangerous, however, are the so-called hybrid-attacks which are chained attacks consisting of misconfiguration or vulnerabilities in many different layers - and we want to focus on that! Within the labs we will examine features that lie in the open design of ModSecurity project: configuration, rule syntax, logs, tuning and troubleshooting. In addition to that we will build our own dedicated rules and create virtual patches. There are also abs from other areas of application (in)security: web-based honeypots in central Reverse Proxy architecture, secure HTTP headers, Appsensor approach, Content Security Policy, HMAC, SRI, upload security, Tomcat / PHP /DB hardening and many more. The whole web application security material is preserved in a "protection vs. attack" model.

KEY LEARNING OBJECTIVES → We will explore in details how to:

- Test and protect your web applications against different classes of vulnerabilities and bugs → based on OWASP Top 10, Testing Guide, ASVS and Bug Bounty writeups.
- Install, setup and secure Apache/Nginx with ModSecurity.
- Gain insight into ModSecurity Rule syntax and Apache/nginx internals
- Use and tweak OWASP ModSecurity Core Rules and prepare your own dedicated rules against attacks.
- Create virtual patches using negative and positive security model
- Collect and analyze full HTTP traffic coming to and from the secured backed webapp without rules (monitoring mode)
- Run threat hunting actions against web applications → ex. webshells vs yara
- secure API endpoints and other critical cloud-based assets from central place

---

WHO SHOULD ATTEND:

- Web Server Administrators and Hosting Providers
- Web Application Firewall Experts
- Linux Experts and System Engineers
- Network Security Engineers
- Penetration Testers
- IT Consultants
- SOC members

PREREQUISITE KNOWLEDGE:

- An intermediate level of command line syntax experience using Linux
- Fundament knowledge of Apache / Nginx
- Fundament knowledge of TCP/IP network protocols
- Penetration testing experience performing enumeration, exploiting, and lateral movement is beneficial, but not required
- Basic programming skills is a plus, but not essential

HW / SW REQUIREMENTS:

- At least 20GB of free disk space
- At least 8GB of RAM
- Students should have the latest Virtualbox installed on their machine
- Full Admin access on your laptop

FULL AGENDA:

1. Threats are everywhere → short introduction to the Web Application Security.
2. Analysis and practical use of exploits for popular web applications: Jenkins, Magento, Zimbra, PHPnuke, Joomla, Drupal, PHPmyadmin, OScommerce, Wordpress, dotProject, Bug Bounty writeups and others.

3. Hardened Apache/Nginx configuration:
    a. Modules in use, path / HTTP method restrictions and file system security.
    b. Secure HTTPS - how to achieve and verify a A+ status?
    c. Mutual and authenticated SSL between reverse proxy and backend servers
    d. Kerberos and LDAP for your web-based Single Sign On setup
    e. Security headers: Content Security Policy, Cross Origin Resource Sharing / Same Origin Policy, X-Frame-Options, X-Content-Type-Options, X-XSS-Protection, Fetch API, Service Workers, SRI, Per-page sub-origins, HSTS, HPKP, PFS.

    f. Cookies: Secure, Httponly, Domain, Path, Same_site, Clear Site Data Feature Policy, First-party cookies

    g. HTTP header anomalies and full HTTP auditing.
    h. LUA support for Apache/Nginx.
    i. ModSecurity syntax, scoring, collections and logs.
    j. Deep dive into OWASP CRS and tuning.
    k. Sensor approach - OWASP Appsensor within ModSecurity.
    l. ModSecurity rules against server misconfigurations, vulnerabilities and attacks:
        i. *Injections
        ii. Null bytes
        iii. Path/directory traversal
        iv. LFI/RFI->Command Execution
        v. Cross Site Scripting (XSS) vs CSP
        vi. Cross Site Request Forgery (CSRF)
        vii. Server Side Request Forgery (SSRF)
        viii. HTTP Parameter Pollution (HPP)
        ix. Open Redirect
        x. Insecure Direct Object Reference vs HMAC
        xi. Forceful Browsing vs HMAC
        xii. CSWSH - Cross Site Websocket Hijacking
        xiii. Session Security
        xiv. Brute force
        xv. Slow DOS
        xvi. GEO restrictions
        xvii. Central Error handling
        xviii. Leakage detection

xix. Secure file upload
xx. Secure log out / forgot password form
xxi. Web honeypots
xxii. Bot/scan protection
xxiii. AV protection
xxiv. PHP and Tomcat Security
xxv. MySQL / PGSQL Hardening vs data exfiltration
xxvi. Tools in use:
    1. Sqlmap, sqlninja
    2. Xsser
    3. Dominator
    4. XXEinjector
    5. Skipfish
    6. ZAP / Burp
    7. Wafdetect
    8. Joomscan, wpscan, drupwn
    9. Dirbuster, dirb
    10. Nikto
    11. JSDetox
    12. Brakeman
    13. Browser plugins and others

xxvii. Central logging and hunting with ELK.
xxviii. Commercial & cloud WAF.

TIME DURATION:

- 2 days of very intensive training (9:00-17:00)

REVIEWS:

- “Excellent content, great stuff and awesome knowledge from the trainer.”
- “Excellent balance between breadth and depth of contents, great materials.”
- “Awesome OSDS @brucon training, learned a lot! Was a pleasure to meet you.”
- “Very good course, the instructor was very knowledgeable and answered all our questions. Course exceeded my expectations, great job!”

TRAINER BIO:

- Leszek Miś is the Founder of Defensive Security (www.defensive-security.com) and VP, Head of Cyber Security in Collective Sense (www.collective-sense.com) where he is responsible for strategy, business analysis, and technical product security research & feature recommendations. He has over 13 years of experience in IT security market supporting the world's largest customers in terms of exfiltration simulations and penetration tests, infrastructure hardening and general IT Security consultancy services. Next, to that, he has 10 years of experience in teaching and transferring a deep technical knowledge and his experience. He has trained 500+ students with the average evaluation on a 1-5 scale: 4.9. He is an IT Security Architect with offensive love and recognized expert in enterprise Open Source Security solutions market. Leszek provides network data exfiltration simulation services, web application & infrastructure penetration tests and OSINT. He specializes in low-level Linux/OS hardening and defensive security of web application platforms (ex. think about integration of WAF+BeeF!). He is also known and respected trainer/examiner of Red Hat solutions and author of many IT Security workshops:

    - Open Source Defensive Security (OSDS)
    - ModSecurity → Web Application Firewall rules vs attacks
    - FreeIPA → Centralised identity management system
    - SELinux - Creating and managing of SELinux policies
    - Advanced RHEL/Centos Defensive Security & Hardening
    - Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques

- As a speaker, trainer or just a participant he attended many conferences like Brucon 2017/2018, OWASP Appsec USA, FloCon 2018("May the data stay with U!"), SuriCon 2017, HITBSecConf, AlligatorCon, Semafor, Exatel Security Days, Confidence 2016("Honey(pot) flavored hunt for cyber enemy), PLNOG 2016 ("Yoyo! It's us, packets! Catch us if you can"), NGSEC 2016 ("Many security layers for many defensive opportunities"), Open Source Day 2010/2011/2012/2013/2014, SysDay 2008 ("SELinux vs exploits"), Confitura 2014 ("Detection and elimination of threats in real time - OWASP Appsensor in action."), Red Hat Roadshow 2014, OWASP Chapter Poland 2015("Does your WAF can handle it?), ISSA, InfoTrams 2015, BIN Gigacon 2015("Mapping pen testers knowledge for the need to protect a critical IT infrastructure").

- The holder of many certificates:

- Offensive Security Certified Professional (OSCP)
- Red Hat Certified Architect (RHCA)
- Red Hat Certified Security Specialist (RHCSS)
- Splunk Certified Architect
- Comptia Security+

CUSTOMERS:

- PGNiG
- Stack Overflow
- Daily Motion
- Alior Bank
- Ministry of Finance
- Millennium Bank
- Nazwa.pl
- Rekord Systemy Informatyczne
- IBS S.A.
- Cinkciarz.pl
- Rockwell Automation
- Esky.pl
- LPP S.A.
- ARiMR
- TUV
- Polkomtel
- Biatel S.A.

CONTACT:

- Email: info@defensive-security.com
- Mobile: 0048 791 611 309 (Poland) / 0048 791 83 10 18 (Poland)
- Website: https://www.defensive-security.com