

WAPT like a Hacker

FR-Hack Training 2009



About Trainer:

Aditya K Sood is an independent Security Researcher and Founder of SecNiche Security. He has been working in security field for last 5 years. He is a Lead Author for Hakin9 group for writing security and hacking papers. His research has been featured in Usenix; login magazine and ELSEVIER Network Security and Computer Fraud Journals. His work has been quoted at EWeek, SCMagazine, Zdnet, Internetnews etc. Aditya's academic background holds a BE and MS in Cyber Law and Information Security from Indian Institute of Information Technology (IIIT-A). He had already spoken at conferences like EuSecWest, XCON, Xkungfoo, OWASP, CERT-IN, Clubhack etc. His other projects include Mlabs, CERA and Triosec. He has written number of security papers released at packetstorm security, Linux security, infosecwriters, Xssed portal etc. He has also given number of advisories to forefront companies. At present he is working as a Lead Penetration Tester in KPMG IT Advisory Services.

Web: <http://www.secniche.org>
Blog: <http://zeroknock.blogspot.com>

Basic Aim: - To present the real world problems with an insight of type of penetration tests to be conducted and to educate professionals. Our class is interactive. The targets are developed as a vulnerable application on Virtual Machines. We will be covering all web based flaws and provide a hand on experience to the users by interactive discussions and hand on targets. The point is to clear the basics.

Note: We will discuss real world hacks too as cited examples. We will go beyond OWASP Top 10 attacks to cover what else can be done with a vulnerable application. We will also run real world application flaw videos.

Target Audience

Security Managers, Security Consultants and Auditors, Administrators, Developers, QA team and Code reviewers. All concepts taught in this class are punctuated with hands-on exercises based on situations observed in real life. The class ends with a challenge exercise. Working within a limited time period, participants are expected to analyze the code, identify loopholes, exploit vulnerabilities present in the applications and suggest appropriate defense strategies.

Course Outline:

[1] Under standing the Spectrum of Web application:

In this we will cover about application security fundamentals and principles. The talk revolves around the evolution of applications and threats related to it.

[2] Breaking inside Application components

We will be covering:

- 2.1** Communication Protocols and application components.
- 2.2** Understanding multi-layered application architecture, programming languages used in applications.
- 2.3** Browser Interaction, the client side coding, pluggable protocol handlers execution etc.
- 2.4** Server Side Technologies and Languages PHP, ASP, JSP, J2EE,.Net.
- 2.5** Introduction to standard tools to execute the concepts practically.
- 2.6** Web Server configuration, web server vulnerabilities, fingerprinting web servers and application servers, security controls pertaining to web servers and their deployment

[3] Application Discovery and Mapping

- 3.1** Application Foot printing and Enumeration.
- 3.2** Discovering the functional structure of applications – the hacker’s viewpoint, advanced techniques.
- 3.3** Server Side attack points and Web server configuration checks.
- 3.4** Infrastructure tests for application running on servers.
- 3.5** Exploiting Search Engine functionalities: Advanced Keywords.
- 3.6** Web garbage dumping for finding information about the targets.
- 3.7** Detection of HTTP interfaces Embedded Devices etc.

[4] Application Attack Vectors

- 4.1** Understanding the assets and Mapping them to targets.
- 4.2** Walk along HTML source for extracting information.
- 4.3** Information leakage through error messages, source code disclosure, input tampering and input validation attacks.
- 4.4** SQL injection and attacks on the database, injecting malicious code and remote command exec, accessing the underlying file system.
- 4.5** Brute forcing HTTP authentication, Brute Forcing HTML form authentication, Session Hijacking, Cross Site Scripting (XSS) attacks, Cross Site Request Forgery (XSRF) attacks.
- 4.6** Remote File Inclusion and Local File Inclusion attacks.
- 4.7** HTTP Verb Tampering Attacks
- 4.8** Cookie Dissection and Analysis
- 4.9** Generic Secure Coding Flaws , Frame Injections , Hidden Frame Exploitations, Same Origin Policy etc.

[5] What about Threat Analysis – Impact on Business

- 5.1** Threat Modeling - Threat analysis, Architecture review, Technologies and Source Code.
- 5.2** Threat matrix, Security controls for code, Design analysis and review.

[6] Prerequisite Knowledge

- 6.1** Working knowledge of Windows or Unix Operating Systems and command-line tools
- 6.2** Working knowledge of HTTP, SSL and related protocols
- 6.3** Working knowledge of shell scripts, SQL, Perl and JavaScript

PREREQUISITE WARNING Each class has prerequisites for software loads and a laptop is mandatory. These individual class guides will list material the students are expected have knowledge about coming in and software tools that need to be pre-installed before attending so you get the maximum benefit from the focused intermediate or advanced level course. Please pay particular attention to the prerequisites, as the material listed there will not be reviewed in the courses, and will be necessary to get the maximum benefit out of these educational programs.

Training