Web Application Vulnerabilities - Attacks on servers

Course code: GOC542

This course will introduce you to the secrets of webhacking and web application vulnerabilities, which make it possible to attack application servers and to steal data stored on them. The course will allow you to fully understand the methods that are commonly used by attackers and try those methods in practice. Web application vulnerabilities, which we will discuss on the course, fall into the most common types of web vulnerabilities and web application developers and administrators should be thoroughly familiar with them. Misusage of this type vulnerability often leads to the complete takeover of control of the target system. Learn about these vulnerabilities and test the security of your web applications before an unwelcome intruder does it for you. We will teach you everything you need for this in our practical course.

Who is the course designed for?

The course is designed for developers and web application administrators who want to understand the attackers´ procedures during the web applications attacks. We will try out the procedures of attackers, in which the server and databases are compromised, on many practical examples.

The procedures discussed in this course target primarily on Apache, PHP, and MySQL technologies. However, even if presented principles can often be applied to other technologies, we particularly recommend attending the course to anyone who wants to get familiar with the common practices of attackers of web applications and servers. We also recommend it to anyone who wants to acquire the right security habits in the development and administration of web applications and servers.

What will you learn by taking this course?

Our unique course "Webhacking in practice 2 - Attacks against servers" will allow you to understand and, most importantly, try out the methods commonly used by attackers on practical examples. During the course, we will explain everything you need to know to defend against these security threats.

Required skills

Anyone with basic knowledge of HTTP, HTML and SQL can join the course.

Teaching methods

Expert interpretation with practical examples, practise on PC.

Teaching materials

Powerpoint handouts and module printouts.

Course outline

Environmental research

- Identification of technologies used
- Web Crawling / Spidering
- Search for non-public sources
- Repositories
- Open Directory listing
- IIS Tilde File Enumerate
- Apache Multiviews File Enumerate
- HTTP methods

Exploitation of used technologies

- Guessing
- Search for exploits
- Use of exploits

- Post-exploitation
- Shelly

Vulnerabilities and SSL attacks

- Vulnerabilities of individual encryption algorithms
- Heartbleed
- Poodle
- BEAST
- CRIME
- BREACH
- and others..

Attacks on the database

- Missing / Insufficient authorization
- Direct access to objects
- Data leakage during redirect
- Forced Browsing

Attacks on the database

- Union-Based SQL injection
- Boolean-Based SQL injection
- Error-Based SQL injection
- Time-Based SQL injection
- Stacked SQL injection
- Stored / Second-order SQL injection
- DNS exfiltration
- Multibyte SQL injection
- SQL injection via binary hash
- Local File Disclosure via SQL injection
- Command execute via SQL injection
- SQL Truncation

Hash cracking

- Hashing algorithms
- Salting hashes
- Hash cracking
- Brute Force / Dictionary attack / Rainbow tables

Vulnerabilities of XML parsers

- Denial of Services via XML
- Local File Disclosure via XML
- Command Execution via XML
- XML injection
- LDAP injection
- XPATH injection

Code Execution

- Unsecured upload
- Unsecured download
- Local File Disclosure
- Remote File Inclusion (RFI)

Web Application Vulnerabilities - Attacks on servers

- Local File Inclusion (LFI)
- LFI via file upload
- LFI via session storage
- LFI via environment
- LFI via log
- LFI via phpinfo
- Function Injection
- PHP Object Injection
- Code Execution
- Command Execution
- WebDav and misusage of HTTP methods
- PHP-CGI vulnerability
- SSI Injection

We will go through other attacks as well...

- Misuse of the webserver as a proxy
- HTTP request smuggling
- Privilege escalation / authorization bypass through cookies
- HTTP Request headers
- Host Header Injection
- Session Storage Attack
- Local Session Injection
- Session Puzzling
- ZIP bombs and DoS
- Attacks on shared servers
- Server-Side Request Forgery (SSRF)
- Shellshock vulnerability