Web Application Vulnerabilities - Attacks on users

Course code: GOC541

This course will introduce you to the secrets of webhacking and web application vulnerabilities that make end-users attacks possible. 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. Although it may not be obvious at first glance, these attacks can have very serious consequences, including a 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 attacks in which user accounts, login data and sessions are stolen on many practical examples. We will misuse requests submitted by the user and we will practice stealing and misusing each their click.
- We can also recommend the course to ordinary users with a basic knowledge of creating websites, who would like to learn about possible attacks that threaten them during normal surfing on the Internet. In this course, you will learn a lot of information on how to improve your web browsing safety habits to reduce your potential risks.
- The procedures discussed in this course are platform independent. You will apply the acquired knowledge in practice, regardless of which programming language you use to develop your application.

What will you learn by taking this course?

- Our unique course "Web Application Vulnerabilities 1 - Attacks against Users" 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 HTML, CSS and Javascript can join the course.

Teaching methods

- Expert interpretation with practical examples, practise on PC.

Teaching materials

- Powerpoint handouts and module printouts.

Course outline

Introduction and tools

- Introduction to HTTP protocol
- Introduction to Burp Suite platform
- Web Parameters Tampering / Hidden Fields

Authentication and Session Management

- User enumeration
- Authentication attacks / Guessing
- Captcha – usage and common mistakes
- Sensitive data in URL's
- Session Stealing
- Session Prediction
- Session Fixation
- Session Donation

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Cross-Site Cooking
- Cross-Subdomain Cooking
- Session Puzzling
- Insufficient Session Expiration
- Insufficient logout
- Logout action availabilty

Attacks on the users

- Cross-Site Request Forgery (CSRF)
- CSRF and GET / POST methods
- CSRF defense options
- HTTP verb tampering
- Stealing clicks using clickjacking
- Filling in and sending forms using clickjacking
- Clickjacking defense options

Client-side scripting

- Cross-Site Scripting (XSS)
- Persistent XSS
- Reflected XSS
- DOM based XSS
- Blind XSS
- Self XSS
- Bypass code
- Javascript, vbscript &data protocols
- XSS and Content-Type settings
- Cross-Site Flashing
- Introduction to BeEF
- XSS defense options
- Too long cookie value
- HttpOnly flag
- Cross-Site Tracing
- Reflected HTTP Request Header
- Open Redirect
- HTTP Response Splitting (CRLF injection)
- HTTP Response Smuggling
- File Download via Open redirect
- Content Spoofing
- Cross-Site Messaging

Stealing user data

- Refer data leak
- Data leakage during redirect
- CORS attacks
- JavaScript Hijacking
- Callback problems
- WWW-Authenticate attack
- Post &Back Attack
- Cross-site WebSocket hijacking

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Web Application Vulnerabilities - Attacks on users

We will go through other attacks as well...

- Local storage attacks
- Websocket attacks
- Cache Poisoning
- HTTP Parameter Pollution
- Host Header Injection
- Path Relative StyleSheet Import (PRSSI)
- Misuse of a user to attack an intranet
- Reflected File Download
- CSV injection
- HTTP Response headers for a secure website

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk