Web application attacks – practical demonstration

Ing. Pavol Lupták, CISSP, CEH

Agenda

- Unvalidates Parameters
- Access Control Flaws
- Session Management Flaws
- Cross Site Scripting (XSS)
- Injection flaws (bonus)
- Improper Error Handling (bonus)
- AJAX Security (bonus)

Access Controls Flaws

- Bypass a Path Based Access Control Scheme
- Bypass Data Layer Access Control
- Bypass Business Layer Access Control
- Remote Admin Access

AJAX Security

- DOM-based XSS
- Client Side Filtering
- Same Origin Policy (SOP) Protection
- XML Injection
- JSON Injection
- Silent Transaction Attacks
- Dangerous Use of Eval

Authentication flaws

- Forgot Password
- Multilevel Login 1
- Multilevel Login 2

Code Quality

- Discover Clues in the HTML code

Concurrency

- Shopping Card Concurrency Flaw

Cross Site Scripting (XSS)

- Stored XSS
- Reflected XSS
- Cross Site Request Forgery (CSRF)
- HTTPonly test

Improper Error Handling

- Fail Open Authentication Scheme

Injection flaws

- Blind SQL injection
- Numeric SQL injection
- String SQL injection
- XPATH injection

Parameter tampering

- Exploit Hidden Fields
- Exploit Unchecked Email
- Bypass Client Side JavaScript Validation

Session Management Flaws

- Spoof an Authentication Cookie
- Hijack a Session
- Session Fixation Attack

Used tools

- WebGoat project http://www.owasp.org/index.php/Category:OWASP_WebG
- WebScarab http://www.owasp.org/index.php/Category:OWASP_WebSc
- Tamperdata http://tamperdata.mozdev.org/
- LiveHTTPHeaders http://livehttpheaders.mozdev.org/
- Foxy Proxy http://foxyproxy.mozdev.org/

References

- New Web Applications Attacks
  http://www.nethemba.com/new_web_attacks-ne
- LAMP and PHP security hardening (in Slovak language)
  http://www.nethemba.com/php-sec.pdf

Thank you for listening!

Ing. Pavol Lupták, CISSP, CEH
pavol.luptak@nethemba.com