Securitatea PHP

Nivel: mediu

Durata: 28 ore

Infrastructura folosită: retroproiector, tablă, calculator personal cu o variantă de Windows sau Linux instalat și conexiune Internet

Cine poate participa: programatori PHP care doresc îmbunătățirea securității aplicațiilor pe care le dezvoltă

Efectul cursului: participanţii vor realiza importanța securității aplicațiilor PHP, vor învăța să identifice vulnerabilitățile și apoi să găsească soluții specifice pentru fiecare în parte.

Cerințe prealabile: noțiuni de bază legate de Internet: browsere, server web, protocolul HTTP, HTML, CSS, Javascript, cunoștințe de programare PHP și baze de date.

Cursuri conexe: Construirea aplicațiilor web cu Apache, PHP și MySQL, Introducere Linux, Programare Web folosind HTML5, Javascript & CSS

Verificarea cunoştinţelor: opţional, pe parcurs şi/sau test final

Suport de curs: da

Descriere:

Fiind unul dintre cele mai populare și mai utilizate limbaje pentru construirea aplicațiilor web, PHP a devenit automat și una din țintele predilecte ale atacatorilor de pretutindeni. Site-urile și forumurile de securitate abundă de rapoarte ale diverselor atacuri mai mult sau mai puțin celebre asupra diverselor aplicații PHP.

Orice programator PHP trebuie să conștientizeze rolul securității în dezvoltarea de aplicații PHP și faptul că ameliorarea caracteristicilor de securitate a aplicațiilor trebuie să fie o preocupare constantă și nu una episodică.

În cadrul cursului se vor studia cele mai frecvente breșe de securitate care țin atât de limbajul PHP cât și a celorlalte elemente cu care PHP interacționează: sistem de operare, server de baze de date, server web. Pentru fiecare dintre vulnerabilitățile studiate se vor studia soluții specifice.

Cursul are un pronunțat caracter practic, cursanții învățând să „spargă” un site vulnerabil și apoi odată identificată problema de securitate să aplice și soluția aferentă de ameliorare.

Bibliografie:

- Pro PHP Security (2nd Edition), 2010, Chris Snyder, Thomas Myer, Michael Southwell, Apress
- Hardening Apache, 2004, Tony Mobily, Apress
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Conţinut:

1. Ce este securitatea și de ce avem nevoie de ea?
   Să cunoaștem atacatorii și motivele lor.
   Open Web Application Security Project (OWASP)
   Managementul riscului

2. OWASP Top 10 (cele mai frecvente probleme de securitate)
   A1. Injection: SQL injection, code & command injection, SSI injection
   A2. Broken Authentication an Session Management
   A3. Cross Site Scripting (XSS)
   A4. Insecure direct object reference
   A5. Security misconfiguration
   A6. Sensitive data exposure
   A7. Missing function level access control
   A8. Cross-site Request Forgery (CSRF)
   A9. Using components with known vulnerabilities
   A10. Unvalidated redirects and forwards

3. Metode de prevenție
   a. Tehnici de autentificare
   b. HTTP vs HTTPS
   c. Stocare date confidențiale (hashing vs criptare)
   d. Validare/sanitizare input
   e. Controlul accesului: ACL, RBAC
   f. Utilizare captcha
   g. Token-uri și managementul sesiunilor
   h. Securizarea upload-ului de fișiere
   i. Ascunderea și logarea erorilor
   j. Securizarea serverului web și a serverului de baze de date