“Hack this workshop”

IntraWorlds s.r.o.
Oldřich Kaucký

INTRAWORLDS
STRONGER RELATIONS

Trocha teorie na začátek...

- Proč se zabývat bezpečností webových aplikací?
- Základní principy bezpečnosti
  - Důvěryhodnost
  - Integrita
  - Dostupnost

INTRAWORLDS
STRONGER RELATIONS

SQL Injection

- Útok je směřován na aplikaci
- Nechráněný uživatelský vstup, vstupní data jsou součástí dotazu
- *$query = “SELECT * FROM user WHERE login=$_GET[‘username’]”*
- *&username=oldakaucky AND 1=2 UNION SELECT table_schema, table_name, 1 FROM information_schema.table*
- ***SELECT * FROM user WHERE login=oldakaucky AND 1=2 UNION SELECT table_schema, table_name, 1 FROM information_schema.table***

IntraWorlds
STRONGER RELATIONS

SQL Injection - ochrana

- PDO, ORM, cokoliv (bezpečného) co oddělí data od dotazu
- *$stmt = $pdo->prepare(“SELECT * FROM user WHERE login= :login”);*
- *$stmt->execute([‘:login’ => $_GET[‘username’]]);*
- Více informací např.: https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

INTRAWORLDS
STRONGER RELATIONS

Chcete přestávku?

10minut?

IntraWorlds
STRONGER RELATIONS

XSS (Cross-site scripting)

- Obětí se stává uživatel
- Nechráněný uživatelský vstup, resp. jeho výpis
- *<script>alert(1);</script>*

INTRAWORLDS
STRONGER RELATIONS

XSS (Cross-site scripting) - ochrana

- “escapování” výstupu
- Twig, Latte, etc…
- Nastavení hlaviček
  - *X-XSS-Protection: 1; mode=block*
  - *Content-Security-Policy: default-src 'self';*
    img-src 'self' https://www.google-analytics.com;
    script-src 'self' https://www.google-analytics.com;
    frame-src https://www.youtube-nocookie.com;
    form-action 'self';
    report-uri https://….report-uri.io/r/…

INTRAWORLDS
STRONGER RELATIONS

XSS (Cross-site scripting) - ochrana

- Specifikace CSP: https://content-security-policy.com/
- https://www.michalspacek.cz/prednasky/xss-php-csp-etc-omg-wtf-bbq-phplive
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

IntraWorlds
STRONGER RELATIONS

Cross-Site Request Forgery (CSRF)

- Je nutné znát aplikaci na kterou útočím
- Uživatel provádí akci o které neví
  - *<img src="http://example.com/vote?option=1">*

INTRAWORLDS
STRONGER RELATIONS

Cross-Site Request Forgery (CSRF) - ochrana

- Hlavička:
  - Content-Security-Policy: frame-ancestors 'self'
  - X-Frame-Options: SAMEORIGIN
- Token

INTRAWORLDS
STRONGER RELATIONS

Chcete přestávku?

10minut?

INTRAWORLDS
STRONGER RELATIONS

Directory Traversal

- Procházení složek serveru
  - Nikdy nevypisovat na stránku nic co tam nepatří!
  -

Directory Traversal - ochrana

- Správné nastavení serveru
  - Např. pro apache: Require all denied

INTRAWORLDS
STRONGER RELATIONS

Odkazy...

- https://securityheaders.com/
- https://www.ssllabs.com/ssltest/
- https://content-security-policy.com/
- https://www.owasp.org/index.php/Main_Page
- https://www.michalspacek.cz/prednasky/xss-php-csp-etc-omg-wtf-bbq-phplive
- https://www.michalspacek.cz/prednasky/http-hlavicky-subresource-integrity-a pod-phplive
-

INTRAWORLDS
STRONGER RELATIONS

Co nás čeká příště?

?

RTsoft
informační systémy na míru

Informační systémy na míru | Business analytika | Mobilní aplikace | Weby a E-shopy

Standa Smitka uvádí workshop v Beer Factory na téma:

OOP, objektový návrh a návrhové vzory

Jak to vidím já po 38 letech programování aneb *„Názory programátorského dinosaura“.*

3. 4. 2019 od 18 hod


We’re hiring!