BEZIT – 5. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

14. 3. 2024

Cvičná webová stránka

- Máme k dispozici cvičný server s webovou aplikaci
  - `http://158.194.80.100/`
  - Použity velmi moderní technologie
- Aplikace má spoustu zranitelností
- Před vnějším světem je omezen přístup pomocí HTTP basic authentication
  - Pro zvídavé: Zkuste si odchytit, jak vypadají pakety s komunikací
- V Galerii lze prohlížet obrázky, ale také nahrávat nové
- V sekci Studenti lze řadit podle zadaných sloupců
- V knize návštěv můžete zanechat svůj vzkaz
- Administrace je tajná

Co by mělo jít

- Cross-site scripting
- Získat zdrojové kódy backendu
- Upravit zdrojové kódy backendu
- Získat hesla a uživatele do administrace
- Smazat databázi
- Session hijacking
- . . . ?

Úkol

- Využijte alespoň dvě zranitelnosti
- Navrhněte k nim vhodný způsob obrany
- Reset aplikace – načtením scriptu: `http://158.194.80.100/reset.php?reset=true`
  - Pokud vám něco povede, zapište si postup (pro replikaci) a resetujte aplikaci

Úkol

- Využijte alespoň dvě zranitelnosti
- Navrhněte k nim vhodný způsob obrany
- Reset aplikace – načtením scriptu: `http://158.194.80.100/reset.php?reset=true`
  - Pokud vám něco povede, zapište si postup (pro replikaci) a resetujte aplikaci
- HTTP basic auth user: `test`, heslo: `Heslo`