Bezpečnostná analýza školského informačného systému EduPage

Matej Novota
Vedúci: RNDr. Richard Ostertág, PhD.
Konzultant: RNDr. Michal Rjaško, PhD.

Fakulta matematiky, fyziky a informatiky
UNIVERZITA KOMENSKÉHO V BRATISLAVE

novota9@uniba.sk, matej.novota@g.fmph.uniba.sk

23. júna 2021

EduPage

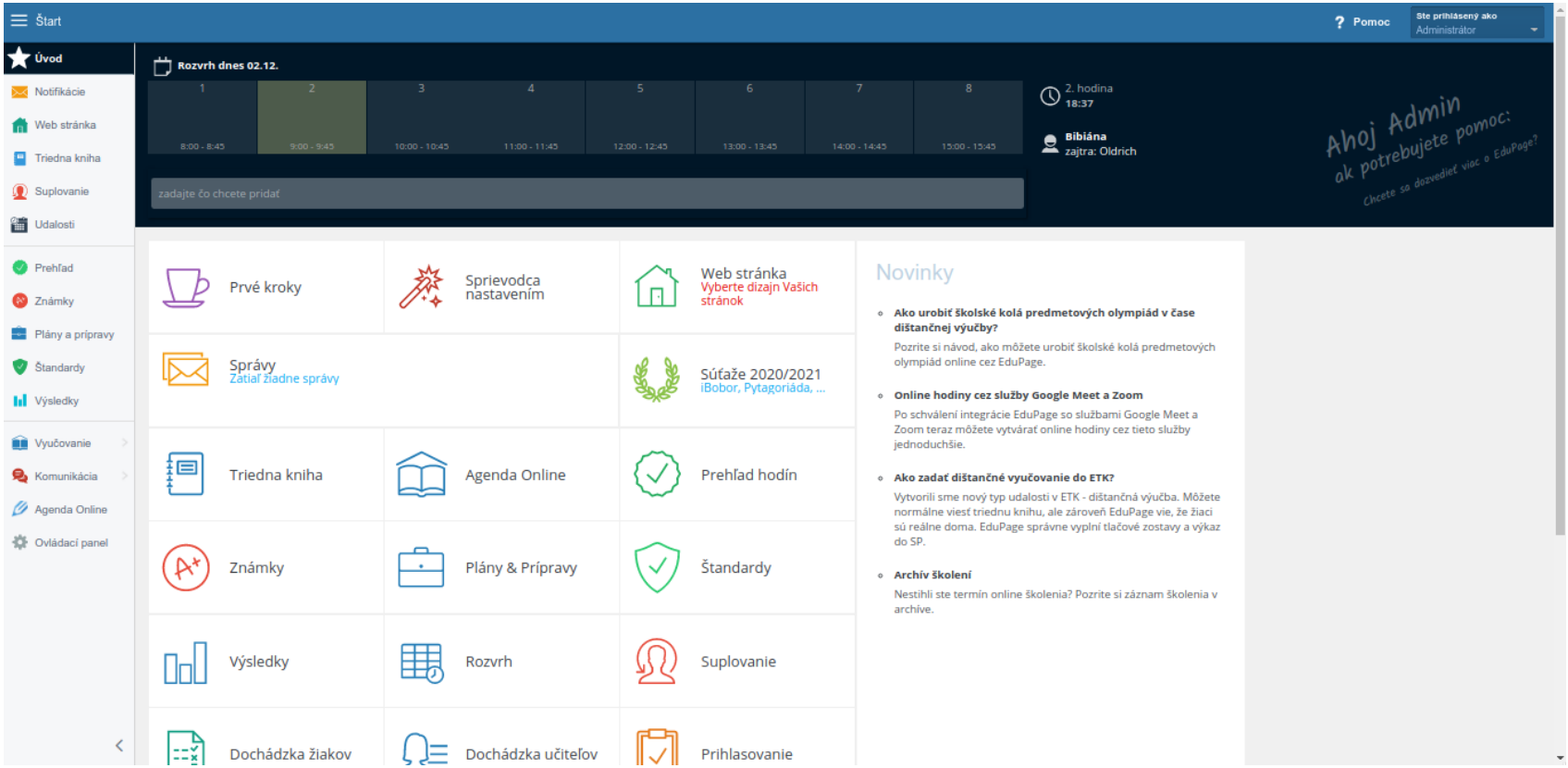
Školský informačný systém

- Webová stránka a mobilná aplikácia
- pre stredné, základné ale aj materské školy
- 173 krajín, 150 000 škôl

Podobne ako

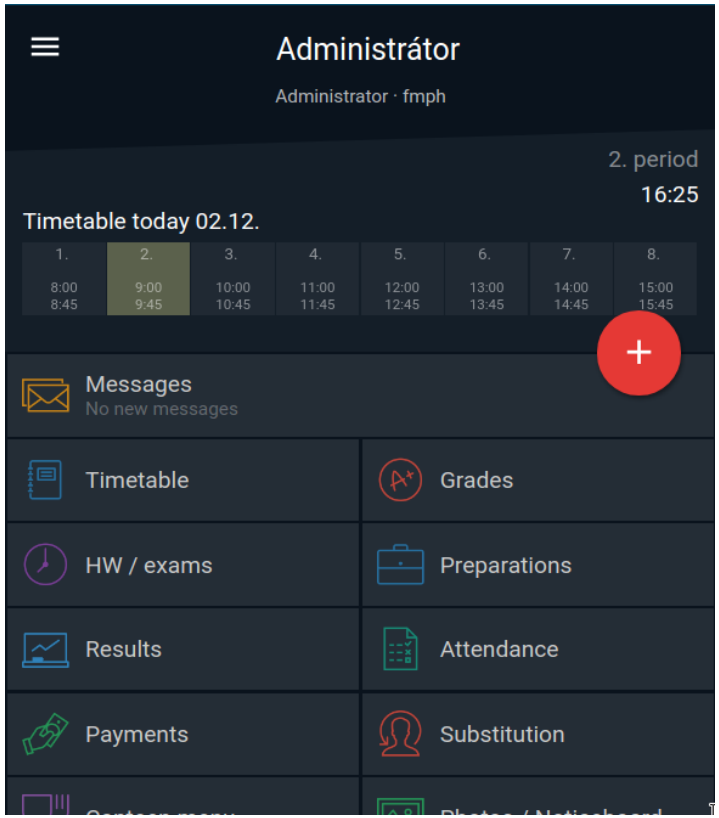
- AIS2
- Moodle
- MS Teams

EduPage



Obr. 1: Webové UI pre prihláseného používateľa

EduPage



Obr. 2: Mobilná aplikácia

Funkcie alebo moduly

- Známky
- Triedna kniha, dochádzka
- Rozvrh
- Suplovanie
- Platby
- Vyučovacie plány
- Písomky, domáce úlohy
- Jedáleň
- Potvrdenia o návšteve školy
- a 91 ďalších funkcii[1]

[1] Aspoň podľa edupage.org.

EduPage

Typy používateľov

- Administrátor
- Učiteľ
- Žiak
- Rodič
- Hosť alebo „guest“

Obr. 3: Nastavovanie práv učiteľov

Cieľ práce

„Pozrieť sa na jednotlivé moduly systému EduPage a otestovať ich odolnosť voči rôznym útokom a overiť, či existuje možnosť povýšenia používateľských práv.[2] *“*

[2] So zameraním na osobné údaje.

Komunikačný protokol

- base64
- komprimácia
- json

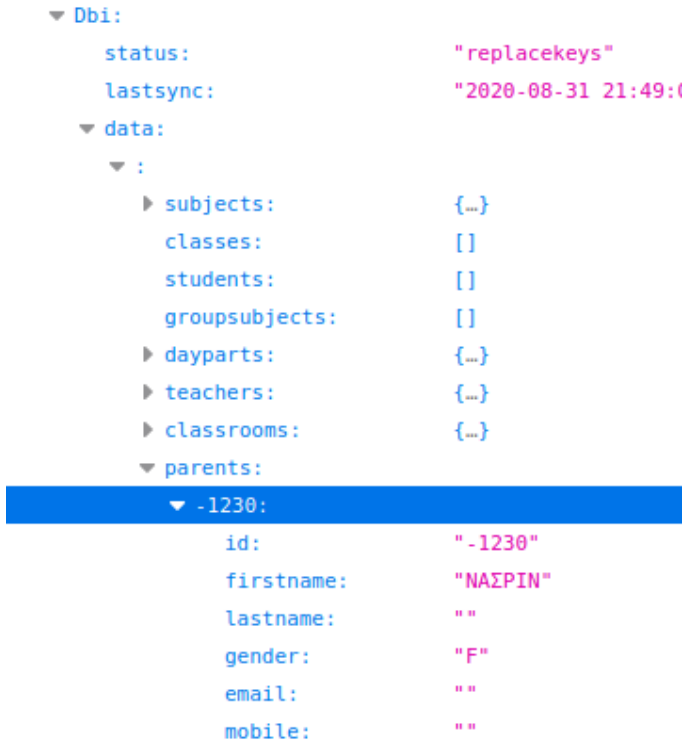
```
try {
  var encoder = new TextEncoder()
  var gz = new Zlib.RawDeflate(encoder.encode(DATA));
  var compressed = gz.compress();
  var cs1 = '';

  for (var i = 0; i < compressed.length; i += 10000) {
    cs1 += String.fromCharCode.apply(null, compressed.subarray(i, i + 10000));
  }
  eqap = 'dz:' + btoa(cs1);
} catch (e) {
  eqap = Base64.encode(DATA, true);
}
```

Obr. 4: Predspracovanie správy

Objavené zraniteľnosti

Dáta používateľov

Mobilná aplikácia posiela zoznam všetky žiakov, rodičov a učiteľov všetkým prihláseným používateľom.



Obr. 5: Výsek z dát poslaných aplikáciou

Objavené zraniteľnosti

Push notifikácie

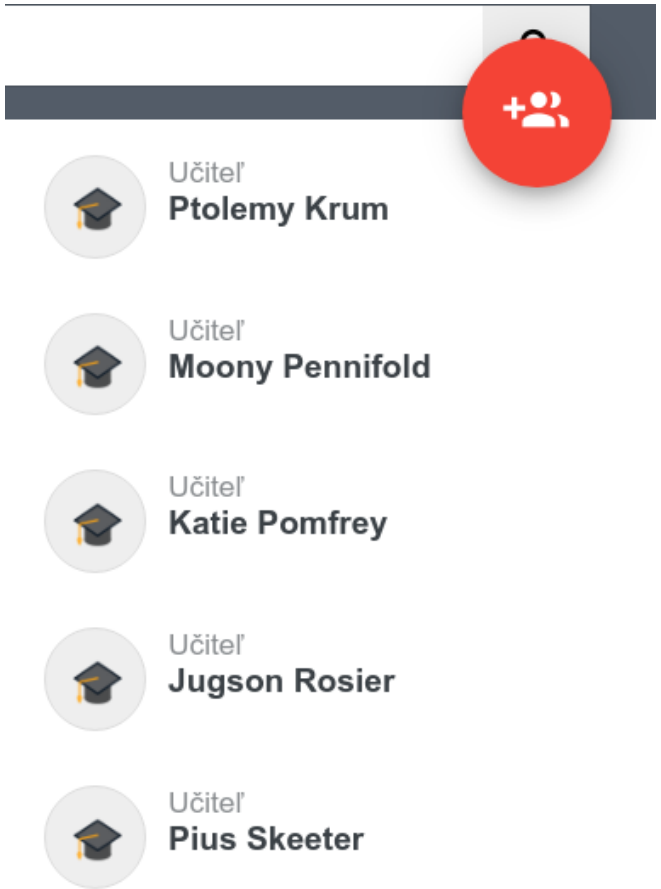
„Guest“ dostáva notifikácie ohľadom správ adresovaných celej škole.

Obr. 6: Ukážka notifikácie pre celú školu

Objavené zraniteľnosti

Posielanie správ

„Guest“ vie posielať správy komukoľvek. Žiak nie.

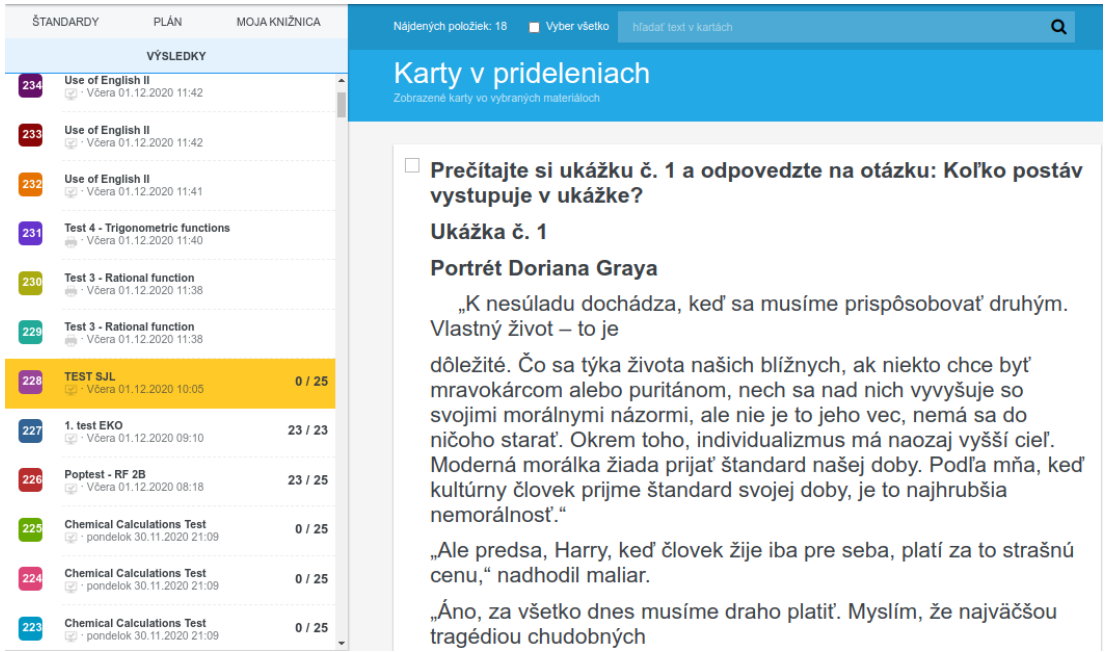


Obr. 7: Výsek zo chatového zoznamu

Objavené zraniteľnosti

Prístup k testom

„Guest“ si vie prezerať všetky testy na škole aj so správnymi odpoveďami.

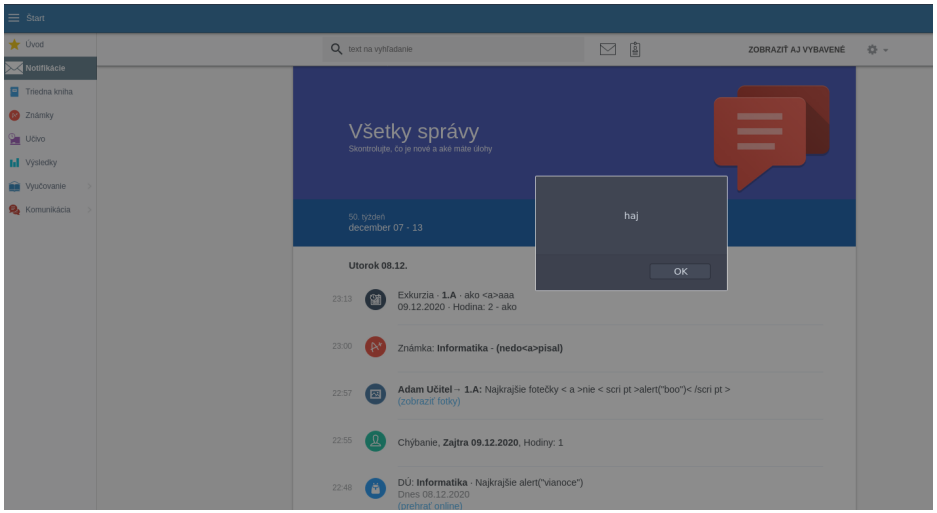


Obr. 8: Ukážka testu na bližšie nemenovanej škole

Objavené zraniteľnosti

XSS v zozname udalostí

Učiteľ vie pridať udalosť, ktorá v sebe bude mať skrytý kód. Týmto spôsobom vie získať prístup do účtov žiakov ale aj iných učiteľov či admina danej školy.

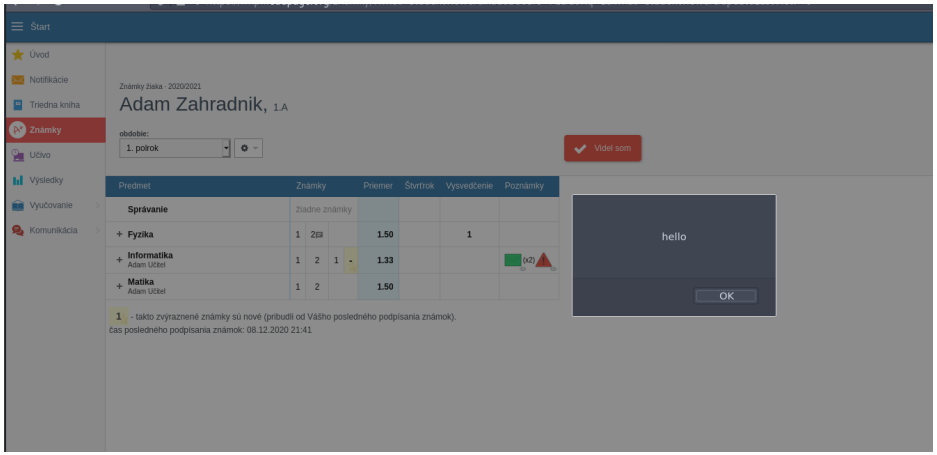


Obr. 9: Vytvorenie alertu pocou XSS

Objavené zraniteľnosti

XSS v zámkach

Učiteľ môže pridať do popisu známky akýkoľvek HTML kód. Týmto spôsobom vie získať prístup do účtov žiakov alebo rodičov.

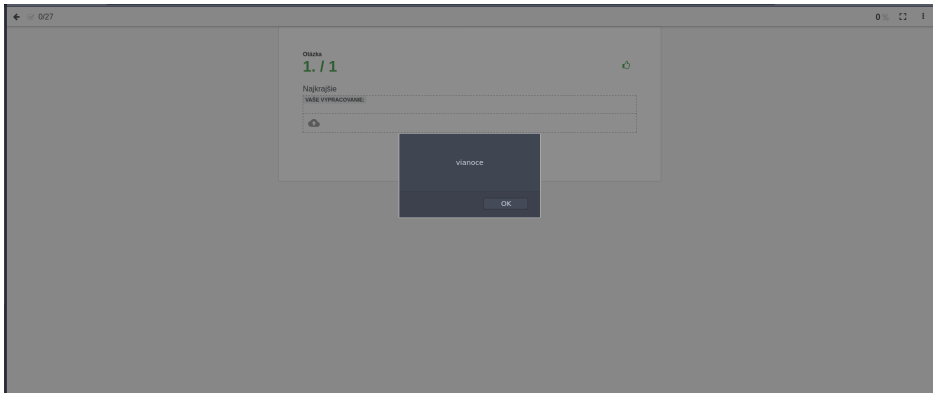


Obr. 10: Ukážka XSS v Známkach

Objavené zraniteľnosti

XSS v teste

Pri tvorbe testu môže učiteľ priamo upraviť zdrojový kód testu.

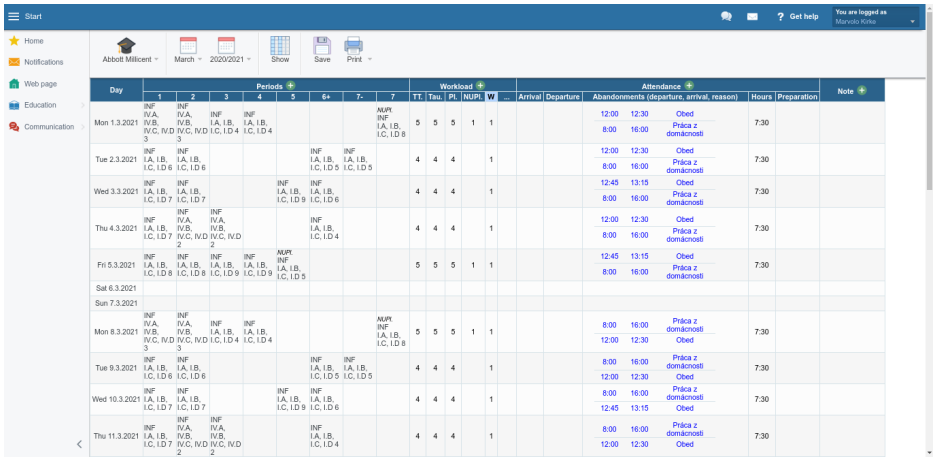


Obr. 11: Ukážka XSS v Teste

Objavené zraniteľnosti

Dochádzka učiteľov

„Guest“ má prístup k pracovným výkazom učiteľa. Potrebuje iba jeho verejne dostupný identifikátor.



Obr. 12: Ukážka dochádzky fiktívneho učiteľa

Ďakujem za pozornosť

SQL

```php
<?php
$db->query("INSERT INTO pouzivatelia (meno, heslo, typ) VALUES ('".
    $_POST['meno']."', '".$_POST['heslo']."', 'guest')");
?>
```

Obr. 13: Ukážka zraniteľného php kódu jednoduchej registrácie používateľa

Akonáhle máme prístup ku SQL dotazu, môžme ho ľubovoľne upraviť, napríklad pridať za neho daľší. V tomto prípade stačí zadať správne meno.

```sql
INSERT INTO pouzivatelia (meno, heslo, typ) VALUES ('jozko', 'heslo123
    ', 'admin'); DROP TABLE pouzivatelia /*', '', 'guest')
```

Obr. 14: Vyhodnotenie príkazu

SQL

```php
<?php
$stmt = $db->prepare("INSERT INTO pouzivatelia (meno, heslo, typ)
    VALUES (?, ?, 'guest')");
$stmt->bind_param("ss", $_POST['meno'], $_POST['heslo']);
$stmt->execute();
$stmt->close();
?>
```

Obr. 15: Ukážka opraveného kódu

XSS

Alternatívou `<script>` HTML tagu je použitie napríklad `on...` v inom HTML tagu.

pri explicitnej kontrole textu `<script>` je možné tento tag zamaskovať. Napríklad použiť veľké písmená, znaky, ktoré prehliadač ignoruje alebo mať ho viac krát v sebe vnorený.