

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

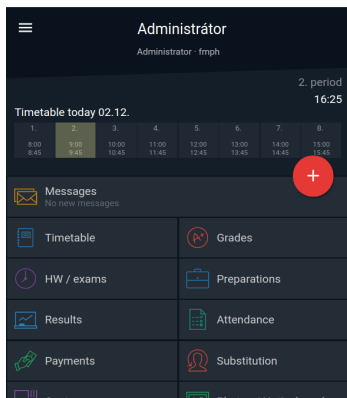
Podobne ako

- AIS2
- Moodle
- MS Teams

EduPage

Obr. 1: Webové UI pre prihláseného používateľa

EduPage



Obr. 2: Mobilná aplikácia

¹Aspoň podľa edupage.org.

Funkcie alebo moduly

- Známky
- Triedna kniha, dochádzka
- Rozvrh
- Suplovanie
- Platby
- Vyučovacie plány
- Písomky, domáce úlohy
- Jedáleň
- Potvrdenia o návšteve školy
- a 91 ďalších funkcií¹

EduPage

Typy používateľov

- Administrátor
- Učiteľ
- Žiak
- Rodič
- Host' alebo „guest“

The screenshot shows the 'Používateľské práva' (User Rights) configuration page in EduPage. It features a sidebar with navigation options like 'Uvod', 'Notifikácie', 'Web stránka', 'Viecha kniha', 'Spracovanie', 'Udalosti', 'Prehľad', 'Ziarsky', 'Plány a prípravy', 'Standardy', 'Výsledky', 'Vyučovanie', 'Komunikácie', 'Agenda Online', and 'Ovládač panel'. The main area displays a table with columns for various permissions and rows for individual users. The permissions are represented by green checkmarks in the table cells.

Meno	Prístup k učebnici	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)	Prístup k učebnici (prístup k učebnici)
Abbott, Milcent	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bryce, Janus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Goshawk, Sybil	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hooch, John	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katlebun, Augustus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kirke, Marvok	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Koum, Phalemy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Maxime, Marcus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Penniford, Moony	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Peverell, Tamin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pomfrey, Katie	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rabbot, Peeves	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rosier, Jugson	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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“

²So 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 posielala zoznam všetky žiakov, rodičov a učiteľov všetkým prihláseným používateľom.

```
▼ Db1:
  status: "replacekeys"
  lastsync: "2020-08-31 21:49:(
  ▼ data:
    ▼ :
      ▶ subjects: {}
      ▶ classes: []
      ▶ students: []
      ▶ groupsubjects: []
      ▶ dayparts: {}
      ▶ teachers: {}
      ▶ classrooms: {}
      ▼ parents:
        ▼ -1230:
          id: "-1230"
          firstname: "NAŠPIN"
          lastname: ""
          gender: "F"
          email: ""
          mobile: ""
```

Obr. 5: Výsek z dát poslaných aplikáciou

Objavené zraniteľnosti

Push notifikácie

„Guest“ dostáva notifikácie
ohľadom správ adresovaných
celej škole.

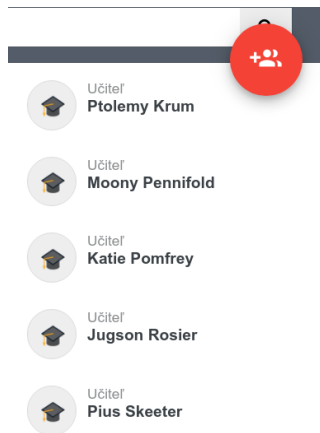


Obr. 6: Ukážka notifikácie pre celú školu

Objavené zraniteľnosti

Posielanie správ

„Guest“ vie posilať 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.

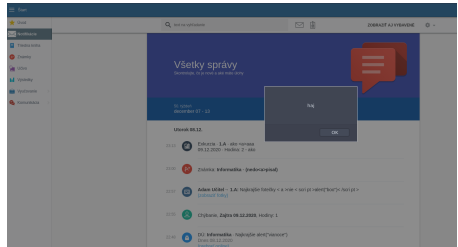
The screenshot shows the EduPage interface. On the left, there is a table of tests with columns for 'STANDARDY', 'PLÁN', and 'MOU KNIŽNICA'. The table lists various tests, including 'Use of English II', 'Test 4 - Trigonometric functions', 'Test 3 - Rational function', and 'TEST 3.A.1'. The 'TEST 3.A.1' row is highlighted in yellow and shows a score of '0 / 25'. Below the table, there is a detailed view of a test question. The question is in Slovak and asks the user to identify the correct answer to a question about the author of the text 'Portrait of Doriana Gray'. The text of the question is: 'Prečítajte si ukážku č. 1 a odpovedzte na otázku: Kofko postáv vystupuje v ukážke? Ukážka č. 1 Portrét Doriana Graya „K nesúladu dochádza, keď sa musíme prispôbovať druhým. Vlastný život – to je dôležité. Čo sa týka života našich blízkych, ak niekto chce byť mravokárcom alebo purtánom, nech sa nad nich vyvyšuje so svojimi morálnymi názormi, ale nie je to jeho vec, nemá sa do ničoho starať. Okrem toho, individualizmus má naozaj vyšší cieľ. Moderná morálka žiada prijať štandard našej doby. Podľa mňa, keď kultúrny človek prijme štandard svojej doby, je to najhrubšia nemoralnosť.“ Ale predsa, Harry, keď človek žije iba pre seba, platí za to strašnú cenu,“ nadhodil maliar. „Áno, za všetko dnes musíme draho platiť. Myslím, že najväčšou tragédiou chudobných

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.

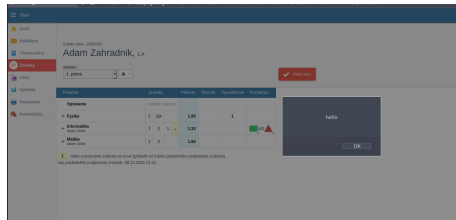


Obr. 9: Vytvorenie alertu pocou XSS

Objavené zraniteľnosti

XSS v zámkach

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

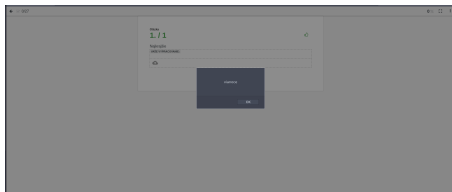


Obr. 10: Ukážka XSS v Známkach

Objavené zraniteľnosti

XSS v teste

Pri tvorbe testu môže učiteľ priamo upraviť zdrojový kód testu.



Obr. 11: Ukážka XSS v Teste

Objavené zraniteľnosti

Dochádzka učiteľ'ov

„Guest“ má prístup k
pracovným výkazom učiteľ'a.
Potrebuje iba jeho verejne
dostupný identifikátor.

Day	Prítomnosť	Prítomnosť
Mon 3.2021	0 0 0 1 1	Guest
Tue 8.2021	4 4 4 1	Guest
Wed 10.2021	0 0 0 0	Guest
Thu 4.2021	4 4 4 1	Guest
Fri 5.2021	0 0 0 1 1	Guest
Sat 7.2021	0 0 0 0	Guest
Sun 13.2021	0 0 0 0	Guest
Mon 19.2021	4 4 4 1	Guest
Tue 22.2021	0 0 0 0	Guest
Wed 24.2021	4 4 4 1	Guest
Thu 25.2021	0 0 0 0	Guest
Fri 26.2021	4 4 4 1	Guest

Obr. 12: Ukážka dochádzky fiktívneho učiteľ'a

Ďakujem za pozornosť

SQL

```
1 <?php
2 $db->query("INSERT INTO pouzivateliam (meno, heslo, typ) VALUES ('.
   $_POST['meno'].'', '$_POST['heslo'].'', 'guest')");
3 ?>
```

Obr. 13: Ukážka zraniteľného php kódu jednoduchej registrácie používateľa

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

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

Obr. 14: Vyhodnotenie príkazu

SQL

```
1 <?php
2 $stmt = $db->prepare("INSERT INTO pouzivatelicia (meno, heslo, typ)
   VALUES (?, ?, 'guest')");
3 $stmt->bind_param("ss", $_POST['meno'], $_POST['heslo']);
4 $stmt->execute();
5 $stmt->close();
6 ?>
```

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.