

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

31. augusta 2022

EduPage

Školský informačný systém

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

Podobne ako

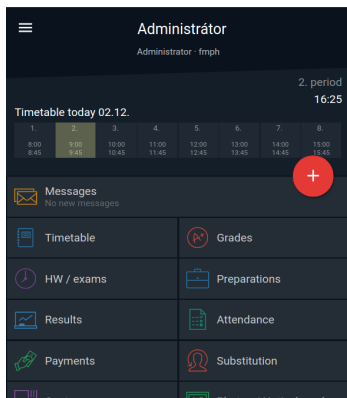
- AIS2
- Moodle
- MS Teams

EduPage

The screenshot shows the EduPage web interface for a logged-in user. The top navigation bar includes 'Start', a search icon, and the user's name 'Anhoj Admin' with the role 'ak potrebujete pomoc:'. Below the navigation bar is a calendar for 'Rozvrh dnes 02.12.' showing a grid of days from 1 to 8. A sidebar on the left contains a menu with categories like 'Úvod', 'Notifikácie', 'Web stránka', 'Triedna kniha', 'Suplovanie', 'Učebnice', 'Prehľad', 'Známky', 'Plány a prípravy', 'Standarty', 'Výsledky', 'Vyučovanie', 'Komunikácia', 'Agenda Online', and 'Ovládači panel'. The main content area features a grid of 12 tiles: 'Prvé kroky', 'Sprievodca nastavením', 'Web stránka', 'Správy', 'Súťaž 2020/2021', 'Triedna kniha', 'Agenda Online', 'Prehľad hodín', 'Známky', 'Plány & Prípravy', 'Standarty', 'Výsledky', 'Rozvrh', 'Suplovanie', 'Dochádzka žiakov', 'Dochádzka učiteľov', and 'Prihlasovanie'. A 'Novinky' (News) section on the right contains several articles with titles like 'Ako urobiť školské kóla predmetových olympiád v čase dŕžaného výučfy?' and 'Online hodiny cez služby Google Meet a Zoom'. A dark banner at the top right of the main area says 'Anhoj Admin ak potrebujete pomoc:'. The bottom of the interface has a navigation bar with icons for back, forward, and search.

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', 'Správovanie', 'Udávateľ', 'Přehľad', 'Známsky', 'Plány a prípravy', 'Štandardy', 'Výsledky', 'Využovanie', 'Komunikácie', 'Agenda Online', and 'Ovládač panel'. The main area displays a table with columns for various permissions and rows for different users. The permissions are represented by green checkmarks in the table cells.

Meno	Prístup k učebniciam	Prístup k učebniciam (pre učiteľov)	Prístup k učebniciam (pre rodičov)	Prístup k učebniciam (pre žiakov)	Prístup k učebniciam (pre učiteľov)	Prístup k učebniciam (pre rodičov)	Prístup k učebniciam (pre žiakov)	Prístup k učebniciam (pre učiteľov)	Prístup k učebniciam (pre rodičov)	Prístup k učebniciam (pre žiakov)
Abbott, Milcent	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bryce, Janus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Goshawk, Sybil	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hooch, John	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Katlebun, Augustus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kirke, Marvok	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kum, Phalemy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Maxime, Marcus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pennfold, Moory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pevenell, Tamsin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Pomfrey, Katie	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rabnett, Peewes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
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.

Skúmané zraniteľnosti

- SQL injection
- zvýšenie používateľských práv
- XSS

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.

```
▼ Dbí:  
  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.

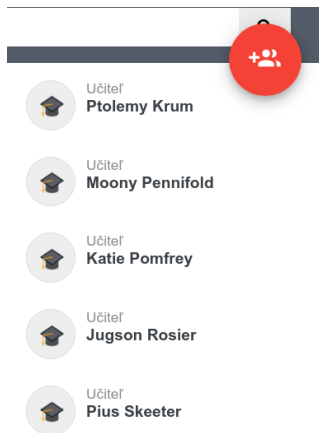


Obr. 6: Ukážka notifikácie pre celú školu

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 such as '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'. On the right, there is a detailed view of a test question titled 'Karty v prideleniach'. The question asks to read a passage and answer a question. The passage is about Dorian Gray and the importance of living for others. The question is: 'Prečítajte si ukážku č. 1 a odpovedzte na otázku: Koľko postáv vystupuje v ukážke?'. The answer is '1'.

STANDARDY	PLÁN	MOU KNIŽNICA
VYSLEDKY		
214	Use of English II	0 / 25
215	Use of English II	0 / 25
222	Use of English II	0 / 25
231	Test 4 - Trigonometric functions	0 / 25
234	Test 3 - Rational function	0 / 25
236	Test 3 - Rational function	0 / 25
238	TEST 3.A.1	0 / 25
237	1. test EKO	23 / 23
226	Pretest - RP 2B	23 / 25
227	Chemical Calculations Test	0 / 25
224	Chemical Calculations Test	0 / 25
223	Chemical Calculations Test	0 / 25

Najbližších pokusov: 18 | Všetky výsledky | Všetky testy v kurzoch

Karty v prideleniach

Zobrazované karty vo výberových materiáloch

Prečítajte si ukážku č. 1 a odpovedzte na otázku: Koľko 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.

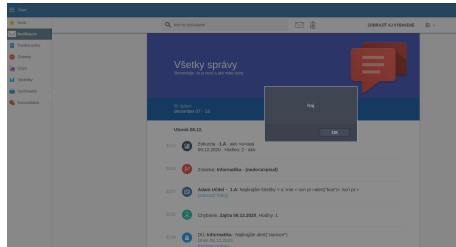
„Áno, za všetko dnes musíme draho platiť. Myslím, že najväčšou tragédiou chudobných

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.

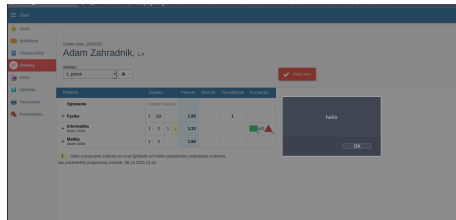


Obr. 9: Vytvorenie alertu pocou XSS

Objavené zraniteľnosti

XSS v zámkach

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

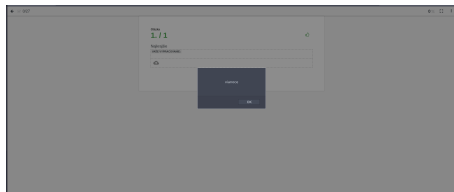


Obr. 10: Ukážka XSS v Známkach

Objavené zraniteľnosti

XSS v teste

Pri tvorbe testu môže učiteľ priamo upraviť zdrojový kód testu.



Obr. 11: Ukážka XSS v Teste

Ďakujem za pozornosť