Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Bezpečnostná analýza školského informačného systému EduPage

Bakalárska práca

2021
Matej Novota

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Bezpečnostná analýza školského informačného systému EduPage

Bakalárska práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	RNDr. Richard Ostertág, PhD.
Konzultant:	RNDr. Michal Rjaško, PhD.

Bratislava, 2021
Matej Novota

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Matej Novota
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Bezpečnostná analýza školského informačného systému EduPage
Security analysis of school information system EduPage

Anotácia: EduPage je modulárny školský systém, ktorý v posledných rokoch používa veľa slovenských (ale aj množstvo zahraničných) stredných a základných škôl. Cieľom práce je pozrieť sa na jednotlivé moduly systému EduPage a otestovať ich odolnosť voči rôznym útokom a overiť, či existuje možnosť povýšenia používateľských práv. Ďalším cieľom je analyzovať, aké dáta sú v jednotlivých moduloch dostupné učiteľom, študentom, rodičom, neprihláseným a prihláseným návštevníkom (so zameraním na osobné údaje).

Vedúci: RNDr. Richard Ostertág, PhD.
Konzultant: RNDr. Michal Rjaško, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
dočasne neprístupná, po uplynutí bez obmedzenia

Dátum zadania: 29.10.2020

Dátum schválenia: 31.10.2020 doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie: Najviac by som chcel poďakovať Adamovi Záhradníkovi, ktorý ma naviedol robiť túto prácu. A taktiež mi pomohol s overením niektorých zraniteľností spomenutých v práci na nezávyslej inštancii systému EduPage. Okrem toho by som chcel poďakovať všetkým, ktorý ma motivovali spísať čo najporiadnejšie túto prácu aj napriek tomu ako náročná činnosť to pre mňa bola.

Abstrakt

EduPage je modulárny školský systém, ktorý v posledných rokoch používa veľa slovenských (ale aj množstvo zahraničných) stredných a základných škôl. V práci sme sa na bližšie pozreli na niektoré časti tohto systému. Primárne sme testovali odolnosť systému voči rôznym útokom a taktiež sme odhalili niekoľko bezpečnostných zraniteľností. Tieto zraniteľností umožňovali prístup ku osobným údajom iných užívateľov systému. Väčšinu sa však podarilo opraviť.

Kľúčové slová: EduPage, bezpečnosť, cross-site scripting, osobné údaje

Abstract

EduPage is a modular school system, which is used in most of Slovak (but also a large number of foreign) secondary and elementary schools. In this paper, we take a closer look at some parts of this system. We primarily tested the resilience of the system to various security attacks. We detected some safety issues. These vulnerabilities have allowed access to the personal information of other users. However, most of the issues were successfully fixed.

Keywords: EduPage, security, cross site scripting, personal information

Obsah

Zoznam obrázkov

Úvod

V posledných rokoch prebieha pomerne silná informatizácia. Čoraz viac dokumentov a činností sa presúva do elektronickej podoby. Tento trend vidno aj v školstve. Väčšina slovenských škôl v dnešnej dobe používa nejaký elektronický systém na správu triednych kníh, známok, zoznamov študentov, ale aj učebných plánov, či archiváciu študijných výsledkov žiakov.

Napriek tomu, že informačných systémov existuje viacero, na trhu jednoznačne dominuje Slovenská aplikácia aSc EduPage. Keďže táto internetová aplikácia pracuje s citlivými údajmi, ako sú kontaktné údaje, známky, výsledky testov, ale aj údaje na vysvedčení, ako rodné číslo, národnosť a občianstvo, je potrebné preveriť, ako s nimi nakladá, kto a za akých podmienok sa k ním vie dostať.

Cieľom tejto práce je preveriť, aké údaje sú dostupné učiteľom, študentom, rodičom, neprihláseným a prihláseným používateľom, či existuje možnosť povýšenia používateľských práv. Teda, či má každý používateľ prístup iba k nevyhnutým dátam, alebo či nevie upravovať nejaké dáta bez oprávnenia. Prípadne, či takýto prístup nevie získať.

EduPage využíva 150 000 škôl po celom svete [1]. Pre predstavu na Slovensku máme dokopy 6 188 stredných, základných a materských škôl [2]. Pri takomto množstve zákazníkov by mala byť každá zraniteľnosť alarmujúca a čo možno najrýchlejšie odstránená. Všetky zraniteľnosti sme nahlásili pred zverejnením práce, Preto je možné, že v čase zverejnenia tejto práce budú niektoré nižšie spomínané zraniteľnosti už opravené.

V nasledujúcej kapitole 1 nájdete podrobnejšie informácie o systéme EduPage. Druhá kapitola pojednáva o bežných bezpečnostných zraniteľnostiach. V kapitole 3 nájdete informácie o testovacej metodike. V kapitole 4 nájdete odhalené zraniteľnosti a v poslednej kapitole zhrnieme zistené výsledky a ich dôsledky.

Kapitola 1

EduPage

V tejto kapitole sa podrobnejšie pozrieme na informačný systém EduPage. Vysvetlíme si, za čo sú zodpovedné jednotlivé časti systému a aké možné riziko prinášajú. Všetky informácie uvedené v tejto kapitole pochádzajú zo systému samotného.

1.1 História

Školský informačný systém EduPage vytvorila spoločnosť ASC Applied Software Consultants, s.r.o., ktorá vznikla v roku 1993 [3]. Pôvodne sa spoločnosť venovala najmä poskytovaniu softvéru v oblasti stavebníctva [4]. Postupne však začala s vývojom ich prvého akademického programu aSc Rozvrhy, ktorý vyhral hlavnú cenu medzinárodného veľtrhu PEDAGOGIKA 98 ako najlepší exponát [5]. Ako meno programu napovedá, tento program bol určený iba na generovanie rozvrhov. Neskôr spoločnosť vytvorila ďalší program aSc Agenda. Tento program umožňoval základnú školskú evidenciu a tlač zopár vybraných dokumentov [6]. Nakoniec pribudol samotný aSc EduPage. Z počiatku išlo iba o službu v programoch aSc Rozvrhy a aSc Agenda, ktorá umožňovala zverejnenie vybraných údajov z týchto programov na webovej stránke [7]. Schopnosti systému EduPage sa postupne rozrastali a v roku 2014 ich doplnila mobilná aplikácia pre operačné systémy iOS a Android. Najnovšia výrazná zmena systému prebehla v auguste 2020, keď pôvodné aplikácie nahradila nová aplikácia využívajúca React Native [8]. Zaujímavosťou je, že táto nová mobilná aplikácia je dostupná aj pomocou obyčajného internetového prehliadača.

1.2 Súčasnosť

Všetky programy existujú do dnešného dňa a stále sa na nich pracuje. EduPage sa stal samostatnou internetovou službou a hlavným produktom firmy ASC Applied Software Consultants. EduPage totiž poskytuje väčšinu funkcionality programov aSc Rozvrhy

a aSc Agenda priamo v internetovom prehliadači, bez nutnosti inštalácie programu. Avšak stále je možné využívať aj tieto programy. Na Slovensku sa predávajú spoločne v rámci jedného balíčka ascAgenda, avšak v zahraničí spoločnosť ponúka aj bezplatnú verziu aSc EduPage samostatne.

Samotná služba aSc EduPage beží na niekoľkých serveroch spoločnosti Hetzner Online GmbH a každej registrovanej škole poskytuje doménu tretieho rádu `<nazov skoly>.edupage.org`. Na tejto adrese beží webová stránka, ktorej serverová časť je napísaná prevažne v jazyku PHP, zatiaľ čo časť bežiaca v internetovom prehliadači využíva JavaScript, s externými knižnicami jQuery a React.

1.3 Typy používateľov

EduPage podporuje niekoľko typov používateľov. Najnižšie práva by mal mať „guest“. Tento účet si na ktorejkoľvek škole môže vytvoriť ktokoľvek pomocou mobilnej aplikácie. S takto vytvoreným účtom sa však vie prihlásiť aj do štandardného webového rozhrania. Takýto účet vie byť viacmenej anonymný a školský administrátor ho nijak nevie zablokovať.

Potom sú účty pre žiakov a rodičov. Medzi ich právami sú minimálne rozdiely. Žiaci napríklad vidia testy a úlohy, rodičia až výsledné známky.

Následne sú účty učiteľov. Tie môžu mať veľmi rozdielne právomoci v závislosti od nastavenia školy. V minimálnej konfigurácii učiteľ vidí v princípe iba veci, s ktorými musí priamo interagovať: svojich žiakov, dochádzku na jeho hodinách, svoj rozvrh, ... V najvoľnejšej konfigurácii môže vidieť takmer akékoľvek dáta na škole.

Nakoniec tu máme školského administrátora. Ten môže byť iba jeden a existuje zopár vecí, ktoré sa dajú robiť iba z tohoto účtu. Napríklad potvrdzovanie učebných plánov.

1.4 Modulárny systém

EduPage je ucelený školský systém, ktorý využíva takzvaný systém modulov. Niektoré moduly sú nevyhnutné na správne fungovanie systému a nedajú sa deaktivovať. Medzi takéto moduly patria napríklad známky, plány, mobilná aplikácia, ... Avšak veľké množstvo modulov môže školský administrátor aktivovať/deaktivovať, podľa toho, či má škola záujem danú funkcionalitu využívať alebo nie.

1.4.1 Plány a prípravy

Jedným z primárnych modulov, ktorý umožňuje základnú funkcionalitu EduPage sú plány a prípravy. V tomto module si každý učiteľ vytvára svoj učebný plán. Modul

má pomôcť s rozložením učiva do školského roku. Každý plán sa skladá z celkov, ktoré môžu obsahovať niekoľko tém. Pričom každej téme možno priradiť počet vyučovacích hodín, textový popis, „výkonový štandard“ podľa štátneho vzdelávacieho programu, alebo nejakú formu testu. Tieto informácie sa ďalej využívajú v moduloch triedna kniha a testy.

Samotné plány neobsahujú veľmi citlivé informácie, ak si do textovej poznámky učiteľ vyslovene nepoznačuje takéto informácie, napríklad o zdravotnom stave žiakov. Avšak tento modul taktiež umožňuje prístup k testom, ktoré by pre žiakov nemali byť dopredu viditeľné. Preto treba preskúmať, či tento modul neumožňuje prístup k iným, citlivejším modulom.

Tento modul využíva cesty `/elearning` a `/plany`.

1.4.2 Rozvrh

Ďalším z hlavných modulov je modul rozvrh. Tento modul sa stará o vytvorenie a zobrazovanie rozvrhu. Rozvrh má pomerne komplikovaný vstup. Program využíva dáta z iných modulov, napríklad, ktorý učiteľ učí aký predmet. Ale taktiež umožňuje zadať rôzne požiadavky, od úplne základných, ako interval pre obednú prestávku, cez podmienky, čo po sebe nesmie nasledovať, až po rovnomerné vyťaženie žiakov, ale aj učiteľov. Výsledkom týchto podmienok je sada rozvrhov pre jednotlivých učiteľov, učebne, triedy, alebo v prípade potreby aj konkrétnych žiakov. Tento modul umožňuje veľké množstvo automatizácie, avšak škola môže fungovať aj bez neho.

V istom zmysle sa by sme mohli rozvrhy chápať, ako citlivé informácie. Obsahujú totiž pomerne presnú polohu človeka v danom čase a teda sa s ich pomocou dá zistiť, kto kedy prichádza a odchádza zo školy. Preto sa dá v systéme EduPage nastaviť, kto vidí aké rozvrhy. Napríklad, či žiak vidí iba svoj rozvrh, alebo si môže pozrieť aj rozvrhy svojich učiteľov a spolužiakov. Treba však preveriť, či sa k rozvrhom nedá dostať aj ak školský administrátor zakáže zobrazovanie cudzích rozvrhov.

Tento modul využíva cestu `/timetable`.

1.4.3 Suplovanie

Tento modul umožňuje dočasné úpravy rozvrhu z dôvodu absencie učiteľa. Dá sa nastaviť spôsob informovania zastupujúceho učiteľa, či už pomocou elektronickej pošty alebo SMS.

Podobne, ako rozvrh, aj informácie o jeho dočasných zmenách sa dajú chápať ako citlivé údaje. Z tohto dôvodu sa dá nastaviť miera viditeľnosti suplovania samostatne pre žiakov, aj učiteľov. Podobne ako pri module rozvrhov treba preveriť, či sa k údajom nedá dostať aj napriek nastaveniam zadaným školským administrátorom.

Tento modul využíva cestu `/substitution`.

1.4.4 Známky

Pre takmer každú školu je nevyhnutné mať spôsob ako hodnotiť žiakov. Túto funkcionalitu umožňuje modul známky. Modul podporuje niekoľko rôznych spôsobov hodnotenia, tak aby každý učiteľ mohol zvoliť spôsob ktorý mu vyhovuje. Školský administrátor taktiež môže zvoliť formát výsledného hodnotenia, či už sú to známky od 1 po 5 alebo od A po Fx. Pri správnom nastavení učiteľ už nemusí ručne rátať výslednú známku, ktorú program automaticky zráta zo všetkých zadaných známok. Modul sa taktiež stará o podpisy známok rodičmi a žiakmi.

Hodnotenie žiakov sa považuje za citlivú informáciu, preto by k nemu nemal mať prístup nikto kto ho nutne nevyžaduje. Teda žiak by mal mať prístup iba ku svojim známkam a nemal by ich vedieť samovoľne meniť. Rodič by mal vidieť hodnotenie svojich detí. Podobne učiteľ by mal mať prístup iba ku známkam svojich študentov a to iba z predmetov, ktoré ich vyučuje.

Tento modul využíva cestu `/znamky`.

1.4.5 Triedna kniha

Ďalším zo základných modulov je triedna kniha. Triedna kniha je jedným z pedagogických dokumentov školy, ktoré škola musí viesť. V triednej knihe sa uvádza dochádzka žiakov a téma prebraného učiva na hodine. So správnym nastavením stačí potvrdiť údaje zo systému dochádzky žiakov a modulu plány a prípravy.

Tento modul umožňuje prístup k iným modulom s čiastočne citlivými údajmi, ako príchody do školy.

Tento modul využíva cestu `/dashboard`.

1.4.6 Testy

Modul testy umožňuje vytvoriť rôzne testy, projekty a domáce úlohy. Učiteľ môže nastaviť časové obmedzenie na vyplňovanie testu a počet pokusov. Väčšina typov úloh je automaticky kontrolovaná. Výsledky testu sa automaticky nahrávajú medzi známky.

Keďže tieto testy sú z väčšej časti automaticky kontrolované, tak niekde existujú správne odpovede, ku ktorým žiaci nesmú mať prístup. Toto predstavuje pomerne veľké riziko, keďže v prípade úniku týchto dát môže žiak získať lepšiu známku bez toho aby si to ktokoľvek všimol.

Tento modul využíva cestu `/elearning`.

1.4.7 Webová stránka

Modul webovej stránky umožňuje vytvorenie statickej webovej stránky školy. Administrátor môže vybrať štýl z niekoľkých návrhov alebo vytvoriť vlastný. Modul obsahuje

jednoduchý editor, v ktorom sa dá pomerne jednoducho vytvoriť nová pod stránka. Okrem toho tento modul poskytuje zopár menších modulov, ktoré umožňujú vytvorenie viac špecializovaných pod stránok.

Novinky

Tento modul je určený na zobrazovanie verejných oznamov na školskej stránke. Začiatky oznamov sa chronologicky zobrazujú na hlavnej stránke, po kliknutí za zobrazí celí oznam. Používa cestu `/news`.

Ocenenia a úspechy

Tento modul je určený na zobrazovanie úspechov žiakov na školskej stránke. Používa cestu `/awards`.

2 percentá

Tento modul vytvorí stránku so všetkými potrebnými informáciami pre ľudí, ktorý chcú škole darovať svoje dve percentá z dane. Používa cestu `/percenta2`.

Zoznamy

Tento modul poskytuje pod stránky so zoznamami všetkých žiakov, učiteľov ale aj tried, krúžkov, miestností a predmetov. Taktiež umožňuje vytvoriť osobnú stránku pre každú vec v zozname. Modul používa niekoľko url, konkrétne: `/classrooms`, `/kruzky`, `/students`, `/subjects`, `/forms` a `/teachers`.

Fotoalbum

Tento modul umožňuje škole zverejniť fotoalbum na svojej webovej stránke. Používa url `/album`.

Mapa

Tento modul zobrazuje polohu školy na mape. Používa url `/map`.

Kalendár

Tento modul zobrazuje kalendár nadchádzajúcich udalostí na školskej stránke. Udalosti za zobrazujú na základe práv používateľov. Používa url `/calendar`.

O škole

Tento modul vytvorí stránku so základnými informáciami o škole. Používa url `/about`.

Napíšte nám

Tento modul vytvorí kontaktný formulár na webovej stránke školy. Používa url `/writeus`.

Pracovné ponuky

Tento modul vytvorí stránku so zoznamom voľných pracovných miest na danej škole. Používa cestu `/job`.

Všetkým vyššie spomínaným modulom pod stránok možno nastaviť či ich škola vôbec používa a v prípade, že áno, kto ich môže zobraziť.

1.4.8 Informačná obrazovka

Tento modul vytvorí špecializovanú stránku, na ktorej sa zobrazujú vybrané informácie. Primárne je určená na premietanie na informačnej obrazovke v škole.

Modul môže mať prístup k rôznym citlivým informáciám, konkrétne ku kalendáru, rozvrhom a suplovaniu. Práva na otvorenie tejto stránky sa dajú nastaviť iba pre administrátora, učiteľov, heslo pre prihlásených používateľov, konkrétne IP adresy alebo stránka môže byť úplne verejná.

Používa cestu `/infoscreen`.

1.4.9 Mobilná aplikácia

V module Mobilnej aplikácie ide zobraziť takmer všetky dáta. Tento modul však vznikol v priebehu leta 2020 a zatiaľ je v relatívne aktívnom vývoji (takmer každý deň sa v ňom niečo menilo), preto som sa tomuto veľkému modulu nijak významne neskôr nevenoval.

Používa cestu `/app`.

1.4.10 Jedáleň

Tento modul má v sebe zabudovanú takmer kompletnú výbavu pre školskú jedáleň. Dá sa cez neho manažovať tovar v sklade. Sú v ňom nahrané aj všetky materiálno-spotrebné normy a receptúry pre školské stravovanie. Dá sa doň nahrávať jedálny lístok, rieši platby za obedy, ...

Avšak, žiadne s týchto informácii nie sú nijak zvlášť tajné alebo súkromné. Preto sme tomuto modulu nevenovali viac času.

Používa cestu `/menu`.

1.4.11 Zmluvy, faktúry a verejné obstarávanie

Tento modul je niečo ako transparentný účet školy. Škola v ňom môže zverejňovať zmluvy, ktoré uzatvára a príslušné faktúry a výberové konania k nim.

Všetky veci sú v ňom verejné, takže jediné riziko predstavuje nahranie nejakých falošných materiálov.

Používa cesty `/zmluvy` a `/obstaravanie`

1.4.12 Platby

Tento modul rieši platby žiakov/ich rodičov. Za záujmové akcie, krúžky alebo školské výlety.

Nakoľko testovanie tohto modulu je relatívne náročné, keďže zahŕňa posielanie peňazí medzi bankovými účtami venovať sa mu budeme iba veľmi povrchovo.

Používa cestu `/platby`.

1.4.13 Chat

Tento modul dovoľuje posielanie správ medzi používateľmi. Školský administrátor môže nastaviť práva jednotlivým používateľom, respektíve komu môžu písať žiaci, či učitelia.

Tomuto modulu sa budeme viac venovať. Keďže tento modul by mohol byť zneužitý na posielanie správ veľkému množstvu ľudí, prípadne vydávať sa za inú osobu, podobne ako elektronická pošta. Avšak v tomto prípade neexistuje žiadna možnosť filtrovania správ, či niečo ako kôš alebo spam.

Používa cestu `/chat`.

1.4.14 Správy

Tento modul zobrazuje všetky notifikácie, oznamy a správy čo danému používateľovi prišli. Kvôli tejto funkcionalite modul komunikuje s modulom kalendáru. Zaujímavé však je, že správy nie sú to isté ako Chat. Tieto správy majú podobné nastavenia a funkcie. Avšak v skutočnosti ide o dva nezávislé moduly a preto ich bude nutné nezávisle preskúmať.

Používa cestu `/timeline`.

1.4.15 Olympiády a sútaže

Tento modul je relatívne nový a umožňuje prihlasovanie žiakov na vybrané predmetové olympiády a iné sútaže.

Používa cestu `/contest`.

Samotné sútaže sa už odohrávajú na špeciálne upravenom EduPage Iuventy, kde sú olympiádne zadania nahodené podobne, ako písomky na štandardnom EduPage. Na tomto EduPage sa dá rovnako, ako na iných EduPage stránkach vytvoriť „guest“ účet. Čo môže byť potencionálny zdroj útoku, ktorý neskôr preveríme.

1.4.16 Prijímačky

Tento modul rieši presun účtov medzi jednotlivými školami a väčšinu byrokracie okolo prihlášok na stredné školy.

Jeho testovanie je však pomerne náročné, keďže ide o interakciu medzi dvomi školami.

Používa cestu `/prihlaska` a `/register`.

1.4.17 Ankety

Tento modul umožňuje všetkým používateľom odpovedať na anonymné ankety alebo prieskumy. Niekoľko ankiet je dopredu vytvorených, ale dajú sa pridať aj ďalšie. Po odpovedaní na anketu sa používateľovi zobrazia súhrnné výsledky.

Používa cestu `/anketa`.

1.4.18 Prihlasovanie na školské akcie

Tento modul sa stará o prihlasovanie na rôzne školské akcie ako výlety, krúžky, konzultačné hodiny alebo kloktacie testy.

Používa cestu `/singin`.

1.4.19 Dochádzka učiteľov

Tento modul nahrádza klasický pracovný výkaz učiteľa. Zobrazuje jeho odpracované hodiny, prestávky, suplovania, návštevy u doktora a podobne.

Tieto údaje sa dajú považovať za citlivé informácie, keďže z nich ide teoreticky dorátať plat učiteľa, zistiť jeho zdravotný stav, alebo zistiť, kde sa v danom čase nachádzal.

Používa cesty `/empattendance` a `/inside`.

1.4.20 Knižnica

Tento modul umožňuje zdieľanie dokumentov medzi viacerými školami. Učitelia tam môžu nahrávať svoje spracované poznámky, písomky, či celé plány. Tie potom môžu využívať učitelia iných škôl, či už priamo alebo ako inšpiráciu.

Používa cestu `/kniznica`.

1.4.21 Maturita

Tento modul rieši časť byrokracie okolo maturít. Keďže však nemáme k dispozícii na testovanie skutočnú školu s týmto modulom sa toho veľa nedá spraviť.

Používa cestu `/maturita`.

1.4.22 eGoverment

Tento modul pribudol v roku 2021. Umožnuje škole používanie schránky na `slovensko.sk`. Táto schránka sa používa na komunikáciu s roznymi úradmi. Taktiež sa tento modul používa na hromadné podpisovanie prihlášok, zmlúv a iných elektronických dokumentov.

Podrobnejšiemu testovaniu tohoto modulu sa však taktiež nebudeme venovať, keďže nechceme náhodou neúmyselne nahrať chybné údaje na `slovensko.sk`.

Používa cestu `/egov`.

Kapitola 2

Bežné bezpečnostné zraniteľnosti

V tejto kapitole si ukážeme príklady niektorých bežných zraniteľností, ktoré sa pokúsime využiť pri odhaľovaní chýb v informačnom systéme EduPage.

2.1 Vkladanie neoprávnených SQL dotazov

Každá stránka obsahujúca väčšie množstvo dynamického obsahu potrebuje nejakú databázu na uloženie dát potrebných na jeho generovanie. Napriek klesajúcemu trendu stále trhu jednoznačne dominujú SQL[1] databázy [9]. Z tohoto dôvodu sa dá predpokladať, že aj EduPage využíva niektorú z bežne používaných implementácii SQL databáz.

2.1.1 Vysvetlenie útoku

Pri tomto type útoku ide o pokus používateľa položiť databáze iný dotaz ako autor stránky zamýšľal. Ukážme si to na jednoduchom príklade zlej implantácie registračného formulára.

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

Listing 2.1: Ukážka zraniteľného PHP kódu jednoduchej registrácie používateľa

Takýto formulár je nevhodný hneď z viacerých dôvodov, napríklad nekontroluje, či používateľ vôbec na server odoslal nejaké používateľské meno či heslo alebo ukladá heslo ako text, nie ako jeho hash. To však nie je primárnym problémom v tejto ukážke.

Predstavme si, že Jožko sa pokúsi registrovať používateľa s menom `jozko', 'heslo123', 'admin') /*`. V takomto prípade sa SQL dotaz vyhodnotí

[1] Structured Query Language

na príkaz `INSERT INTO pouzivatelia (meno, heslo, typ) VALUES ('jozko', 'heslo123', 'admin') /*', '', 'guest')`, ktorý Jožkovi úspešne vytvorí účet. Avšak s inými parametrami ako sme mohli na prvý pohľad očakávať. Jožko sa totiž stal administrátorom stránky, nech to už znamená čokoľvek.

Takýto typ útoku je však ešte nebezpečnejší ako sa môže zdať. Pretože umožňuje používateľovi plný prístup ku databáze. Podobne, ako si v našom príklade Jožo vytvoril administrátorský účet, mohol zmazať, upraviť alebo zobraziť akékoľvek dáta uložené v databáze.

2.1.2 Ochrana pred útokom

Pred takýmto útokom sa dá chrániť rôznymi spôsobmi. Keďže problémom je vstup od používateľa, najjednoduchším riešením je takýto vstup vôbec nemať, avšak to znemožňuje väčšinu funkcionality čo od moderných stránok očakávame.

Inou, stále veľmi striktnou možnosťou je zakázať všetky „nebezpečné“ znaky. Ak by totiž používateľ mohol vložiť iba alfanumerické znaky, bez úvodzoviek, čiarok, zátvoriek, ... útok by sa nikdy nepodaril. Je však dôležité, aby sa kontrola robila až na serveri, keďže kontrola na strane webového prehliadača sa dá obísť. Takéto riešenie môže byť dostatočné pri zadávaní prihlasovacieho mena, no ak má databáza obsahovať komplexnejšie dáta, ako novinky na stránke alebo chat medzi používateľmi, je asi zrejmé, že takéto riešenie nebude ideálne.

Tretou možnosťou je takzvané „escapovanie“ vstupu. Ide o techniku ako označiť „nebezpečné“ znaky tak, aby ich databáza očakávala a teda, aby už neboli nebezpečné. Štandardne sa na tento účel používa znak \, ktorý sa umiestni pred všetky „nebezpečné“ znaky. Na tento problém mysleli aj tvorcovia väčšiny knižníc na komunikáciu z databázami. Teda nie je nutné programovať ošetrenie vstupu, ale stačí použiť vhodnú knižničnú funkciu a zároveň použitie takejto knižničnej funkcie umožňuje jednoduchšiu údržbu pri odhalení prípadných iných zraniteľností, keďže obvykle stačí prejsť iba na novšiu verziu knižnice. Takéto ošetrenie vstupu umožňuje používateľovi najväčšiu voľnosť a zároveň zabezpečuje server voči tejto zraniteľnosti.

Štvrtou možnosťou sú takzvané „prepared statements“. V tomto prípade sa SQL dotaz na databázu neposiela ako text ale v špeciálnom binárnom formáte, v ktorom sa dotaz rozdelí na dve časti. Najprv server pošle databáze šablónu SQL príkazu, ktorý bude chcieť niekedy v budúcnosti vykonať. Táto šablóna môže obsahovať definíciu parametrov, ktoré sa pošlú neskôr, až keď server chce dotaz vykonať. Šablóna sa teda spracuje iba raz, a to na začiatku pred tým ako ju upraví vstup od používateľa. Ten sa posiela až potom a nespracováva sa ako SQL príkaz. Tým pádom ho nie je nutné nijak upravovať alebo obmedzovať ako v predchádzajúcich možnostiach ochrany.

Náš príklad zraniteľného kódu by sme mohli opraviť pomocou techniky „prepared

statements“ takto.

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

Listing 2.2: Ukážka bezpečného PHP kódu jednoduchej registrácie používateľa

2.2 Zvýšenie používateľských práv

Obvykle sa pod týmto pojmom myslí zneužitie chyby v operačnom systéme, vďaka ktorej získa útočník (alebo jeho program) práva ku zdrojom, ktoré by nemal mať. V našom prípade však myslíme obdobný problém v rámci webovej aplikácie. Teda, že používateľ získa prístup k dátam, ku ktorým by prístup mať nemal.

Typickým príkladom takéhoto útoku je pokus používateľa o prístup k časti stránky, ku ktorej by štandardne namal mať prístup.

Táto zraniteľnosť je obvykle spôsobená nedostatočnou, alebo úplne chýbajúcou, kontrolou používateľských práv v niektorej časti stránky.

2.3 Cross-site scripting

Cross-site scripting alebo XSS[2] je typ bezpečnostnej zraniteľnosti, pri ktorej je umožnené útočníkovi vložiť do stránky vlastný kód. Tento kód sa následne môže spustiť pri návšteve stránky iným používateľom.

Na prvý pohľad tento útok môže vyzerať relatívne nevinne, avšak kód môže napríklad ukradnúť prihlasovacie údaje iných, nič netušiacim používateľov stránky. Čo je vcelku závažný problém.

2.3.1 Vysvetlenie útoku

Obvykle sa tento útok vyskytuje na miestach, kde používateľ môže zadať nejaký vstup, ktorý neskôr uvidia aj iný používatelia stránky. Typickým príkladom zraniteľných miest je napríklad posielanie správ medzi používateľmi alebo zverejňovanie oznamov, prípadne iného obsahu stránky.

[2]Pôvodne označovaný ako CSS, neskôr zmenený na XSS. Aby sa skratka odlíšila od skratky kaskádových štýlov.

Útok môže pozostávať z vloženia rôznych HTML tagov, tak aby sa nakoniec spustil nejaký kód v jazyku JavaScript. Na tento účel sa za normálnych okolností v HTML používa tag `<script>`. Avšak dajú sa použiť napríklad aj argumenty `onload` alebo `onmouseover` na iných tagoch.

2.3.2 Ochrana pred útokom

Podobne ako pri vkladaní neoprávnených SQL dotazov aj v tomto prípade je účinnou ochranou kontrola vstupu od používateľa. Napríklad úplným odstránením HTML tagov. Avšak rovnako nestačí kontrolovať vstup pri jeho načítaní na strane webového prehliadača ale až na servery, prípadne ešte neskôr až pri kroku zobrazenia vstupu u iného používateľa stránky.

Problémom však je, že častokrát chceme umožniť používateľom použiť nejaké HTML tagy. Napríklad tag `<b>` iba zobrazí text hrubým písmom. Ukazuje sa, že riešenie tohoto problému je vcelku komplexné a aj preto OWASP[3] odporúča použiť exterternú knižnicu DOMPurify (`https://github.com/cure53/DOMPurify`)[11].

[3]Open Web Application Security Project - nezisková organizácia, ktorej cieľom je zvýšenie bezpečnosti softvéru.[10]

Kapitola 3

Metodika odhalovania zraniteľností

V tejto kapitole uvedieme, ako sme postupovali pri odhaľovaní zraniteľností v systéme EduPage.

3.1 Postup

3.1.1 Celková analýza systému

Predtým, ako môžme začať odhaľovať zraniteľnosti systému, musíme systém aspoň čiastočne spoznať, a pochopiť ako funguje.

Prístup k zdrojovým kódom sme síce nedostali, avšak firma ASC Applied Software Consultants, s.r.o. nám poskytla jednu bezplatnú inštanciu systému EduPage na naše testovanie. V tejto inštancii sme dostali aj administrátorský účet, vďaka ktorému sme sa v systéme mohli lepšie zorientovať a vytvoriť si ľubovoľných ďalších používateľov. Výstup z tohoto kroku je popísaný v kapitole 1.

3.2 Analýza komunikačného protokolu

V tejto sekcii spomenieme akým spôsobom komunikuje „frontend“ aplikácie so serverom. Túto vedomosť využijeme neskôr pri odhaľovaní zraniteľností.

Väčšina komunikácie prebieha pomocou upraveného jQuery [12]. Konkrétne sa používa metóda `post` z knižnice jQuery. Táto metóda posiela špeciálu správu na server, ktorá v hlavičke obsahuje autentifikačné cookie a správu, ktorá vznikne upravenou metódou `post`. Tá je upravená tak, že ku správe stránka vždy pridáva dva GET parametre.

- Parameter `eqav`, ktorý má väčšinou hodnotu 1.
- Parameter `maxEqav`, ktorý má vždy hodnotu 7.

V prípade, že sa hodnoty týchto parametrov rovnajú správa sa odošle na server bez zmeny.

V opačnom prípade sa vypočítajú dve pravdivostné hodnoty `useEncryption` a `useZip`, ktoré menia vzhľad tela správy.

Hodnota `useEncryption` nám hovorí, či sa používa „encryption“, ktoré sa štandardne používa (Nepoužíva sa iba v prípade, keď je aktívny `MobileAppBridge.isActive()`.). Pod „encryption“ autori EduPage mysleli konverziu správy do `base64` formátu.

Hodnota `useZip` je pravdivá, ak je `eqav` nepárne. V takom prípade sa používa na telo správy „zipovanie“. Konkrétne sa na obsah správy aplikuje algoritmus `deflate` z knižnice Zlib.

Nakoniec vznikne objekt, ktorý sa pošle po sieti s troma parametrami v tele správy:

- Parameter `eqap` obsahuje samotné „telo“ správy, ktorá môže byť v rôznych formátoch podľa hodnoty `useEncryption` a `useZip` ako bolo spomenuté vyššie.
- Parameter `eqacs`, ktorý obsahuje hash, konkrétne `sha1` parametru `eqap`. V niektorých prípadoch `eqacs` server ignoruje, väčšinou je však vyžadovaný a bez neho server nepošle naspäť správnu odpoveď.
- Parameter `eqaz`, ktorý je ekvivalentný hodnote `useEncryption`.

Neúspešná odpoveď na takúto správu začína „eqwd:“ táto odpoveď znamená, že požiadavka bola neúspešná. V takomto prípade sa stránka pokúsi požiadavku zopakovať so zvýšením `eqav` o jedna.

V prípade, že je odpoveď úspešná a použili sme „encryption“ dáta sa vrátia vo formáte „eqz:“ a skutočná odpoveď vo formáte `base64`.

3.3 Modifikácia odosielanej správy

V tejto sekcii popíšeme akým spôsobom sme upravovali komunikáciu, aby sme odhalili konkrétne zraniteľnosti.

Najprv sme spravili normálnu požiadavku na daný modul pomocou webového prehliadača, v ktorom sme boli normálne prihlásený. Popritom sme odchytávali internetovú komunikáciu. Následne sme sa pokúsili spraviť rovnakú požiadavku však z autentifikačným „cookie“ od iného typu používateľa. Takýmto spôsobom sme overovali, či nemajú niektoré typy používateľov prístup ku modulom, ku ktorým by prístup mať nemali.

Podobným spôsobom sme potom skúsili aj vkladanie neoprávnených SQL dotazov. Teda pre rovnakú správu sme tentokrát nezmenili autentifikačný „cookie“ ale obsah správy tak, aby v upravenom formáte obsahoval niekoľko štandardných neoprávnených SQL dotazov.

3.4 Cross-site scripting

V tejto sekcii popíšeme akým spôsobom sme testovali XSS zraniteľnosti.

Pri tejto zraniteľnosti sme sa pokúsili vložiť nejakú formu `<script>` tagu do každého vstupného textového poľa.

Najprv sme skúsili základný formát `<script>alert("nejaky text")</script>`, ak sa nám nepodarilo odhaliť zraniteľnosť skúsili sme neuzavreté úvodozvky a zátvorky `"><script>alert("nejaky text")</script>`, ktoré HTML prekladaču z webového priehliadaču nevadia ale ochrana proti XSS by ich nemusela rozoznať. Potom sme skúsili rôzne veľkosti písma `"><scRiPt>alert("nejaky text")</scRiPt>`, iné kódovanie `"\%3cscri pt\%3ealert("nejaky text")\%3c/scri pt\%3e` a vnorené tagy `<scr<script>ipt>alert("nejaky text")</script>`.

Pokiaľ žiaden z týchto vstupov nefungoval, skúsili sme ešte niekoľko iných HTML tagov. Pokiaľ nefungovalo `<a src="http://example.com/̈a</a>` neskúšali sme ďalšie variany tohoto tagu. Potom sme skúsili ešte základné verzie tagov `<b>`, `<p>`, `<i>`. Ale kedže ani v takomto formáte tagy nefungovali, neskúšali sme pridať parametre ako `onload`, `onmousehover`, `onclick`.

Taktiež ak nejaký JavaScript vo webovom prehliadači overoval, či je text v správnom formáte, tak sme ho dočasne odstránili aby sme mohli našu správu odoslať. Takýmto spôsobom sme overili, či by bolo možné využiť XSS na danej podstránke. Nešlo nám totiž o skutočnú krádež autentifikačných „cookie“, prihlasovacích údajov alebo podobných dát ale iba o otestovanie, či by bol takýto útok možný.

Nakoniec sme skontrolovali, či sa daný text správne zobrazil ako text a nie ako html kód.

Kapitola 4

Objavené zraniteľnosti

V tejto kapitole vysvetlíme všetky zraniteľnosti, ktoré sme v systéme EduPage objavili. A spomenieme možné návrhy ich riešenia, prípadne čas kedy bola zraniteľnosť opravená.

4.1 Verejne dostupné používateľské dáta

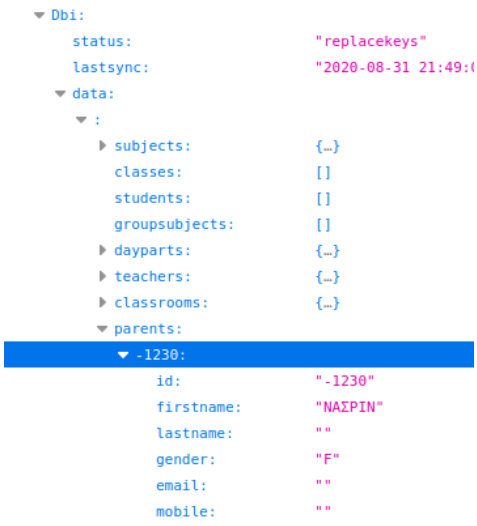
4.1.1 Popis zraniteľnosti

Pri prihlásení sa do mobilnej aplikácie server zasielal všetkým prihlásením používateľom, teda aj „guest“ účtom, ktoré možno vytvoriť na akejkoľvek škole, kompletný stav systému.

Tento stav obsahoval základné informácie o škole ako časy začiatkov hodín, aké hodiny na danej škole vyučujú, denný rozvrh prihláseného používateľa, ... Avšak okrem týchto informácií bol v stave uložený aj zoznam všetkých účtov na danej škole. Išlo o účty všetkých typov používateľov, teda učiteľov ale aj žiakov a rodičov. Ku každému účtu bol dostupný zoznam osobných informácií ako meno, fotka, email, telefónne číslo, pohlavie a v prípade žiakov trieda, ktorú navštevuje. Aj keď veľké množstvo informácií mohlo byť nevyplnených, tak ak škola tieto informácie mala v systéme, tak boli dostupné.

4.1.2 Riešenie

Zoznam používateľov bol v priebehu novembra 2020 z tohoto stavu odstránený.



Obr. 4.1: Výsek z dát poslaných aplikáciou, zámerne bez údajov

4.2 Push notifikácie

4.2.1 Popis zraniteľnosti

Mobilná aplikácia dostáva notifikácie na správy, ktoré by používateľ nemal vidieť. Konkrétne „guest“ používateľ dostáva notifikácie ohľadom správ adresovaných celej škole. Napriek tomu, že tieto správy v aplikácii samotnej nevidí.

Obr. 4.2: Ukážka notifikácie pre celú školu

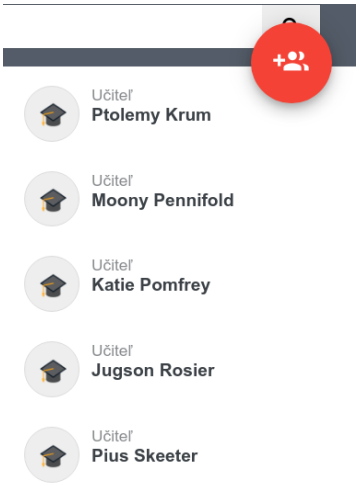
4.2.2 Riešenie

Stačí na servery vypnúť odoberanie notifikácií pre „guest“ účty. Pôvodne boli správy viditeľné aj v aplikácii a na stránke, čo sa vyriešilo v priebehu októbra 2020.

4.3 Posielanie správ

4.3.1 Popis zraniteľnosti

Chatovací modul 1.4.13 umožňoval používateľom typu „quest“ vytvoriť spoločný chat s akýmikoľvek účtami na rovnakej škole, napriek tomu, že žiakom môže byť takáto funkcionalita zakázaná. Následne do tohoto chatu môžu všetci zúčastnený posielať správy. Používateľ však musel poznať správnu adresu pre tvorbu chatu `chat/?cmd=NewChat`.



Obr. 4.3: Výsek zo chatového zoznamu

Táto zraniteľnosť je obzvlášť závažná v kontexte nedávneho škandálu, podľa ktorého boli odcudzené prihlasovacie údaje jedného žiaka, cez ktorého účet boli neskôr rozoslané nevhodné fotografie 22 jeho spolužiakom [13].

4.3.2 Riešenie

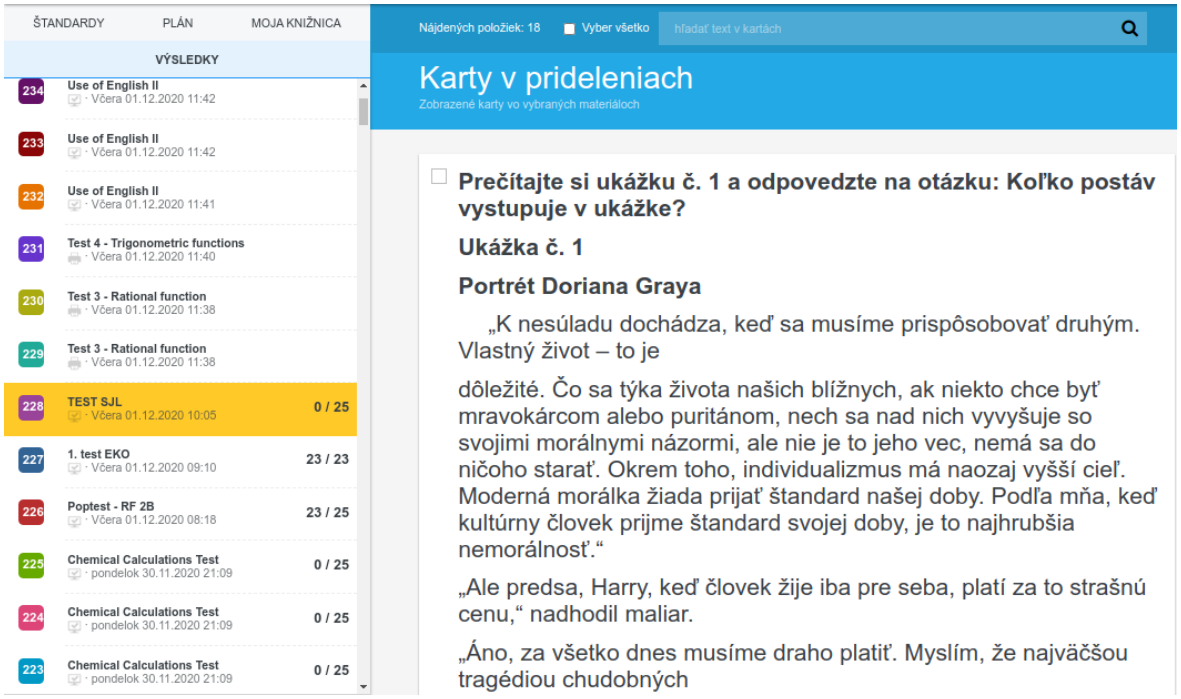
Napriek tomu, že vyššie spomínaný incident údajne nevyužíval túto zraniteľnosť, tak bola krátko po jeho zverejnení aj táto zraniteľnosť opravená.

4.4 Prístup k testom

4.4.1 Popis zraniteľnosti

Modul elearning umožňuje „guest“ používateľom zobraziť zoznam všetkých testov na škole. Žiak na rovnakej adrese vidí iba zoznam jemu pridelených testov. Tieto testy sa zobrazujú ako keby v nich nič nebolo. Avšak „guest“ má možnosť editovať takýto test (aj keď zmeny neskôr nebude môcť uložiť). Počas editovania stále nevidí skutočný obsah testu ale môže do testu pridať otázku z iného testu. Pri pridávaní otázky si môže rozklknúť ľubovoľný test a zobrazia sa mu otázky daného testu aj z odpoveďami. Toto

však platí iba za predpokladu, že je otázka označená ako „verejná“, čo boli až do konca januára 2021 všetky otázky, pokiaľ učiteľ pri tvorbe testu neodznačil nenápadné políčko pri každej úlohe. Čo podľa môjho prieskumu nikto nerobil.



Obr. 4.4: Ukážka testu na bližšie nemenovanej škole

4.4.2 Riešenie

Nutnosť označenia otázky za verejnú rozhodne pomohla. Napriek tomu by bolo rozumné varovať učiteľa predtým než toto políčko zaškrtne. Alebo zneviditeľniť úlohu pokiaľ test nebude ukončený.

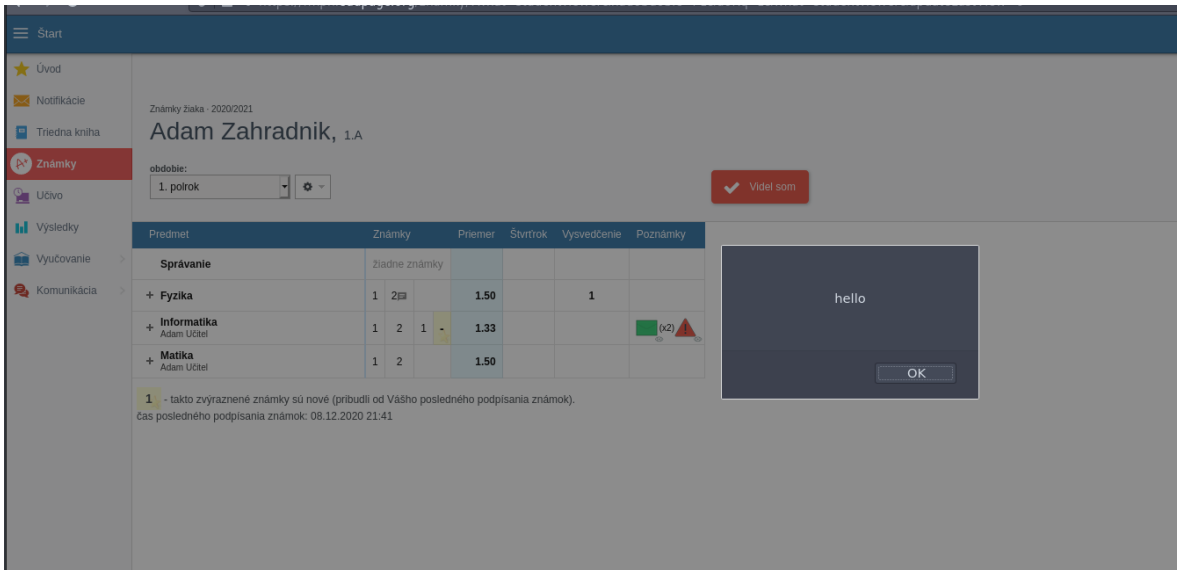
4.5 XSS v Známkach

4.5.1 Popis zraniteľnosti

Učiteľ môže pridať do popisu známky akýkoľvek HTML kód. Tento kód sa správne „escapuje“ pre mobilnú aplikáciu aj pre cez učiteľské rozhranie. Avšak u žiaka a rodiča sa tento kód spustí.

4.5.2 Riešenie

Treba správne „escapovať“ popis známky aj pre žiaka a rodiča. V čase písania práce táto zraniteľnosť nebola ešte opravená.

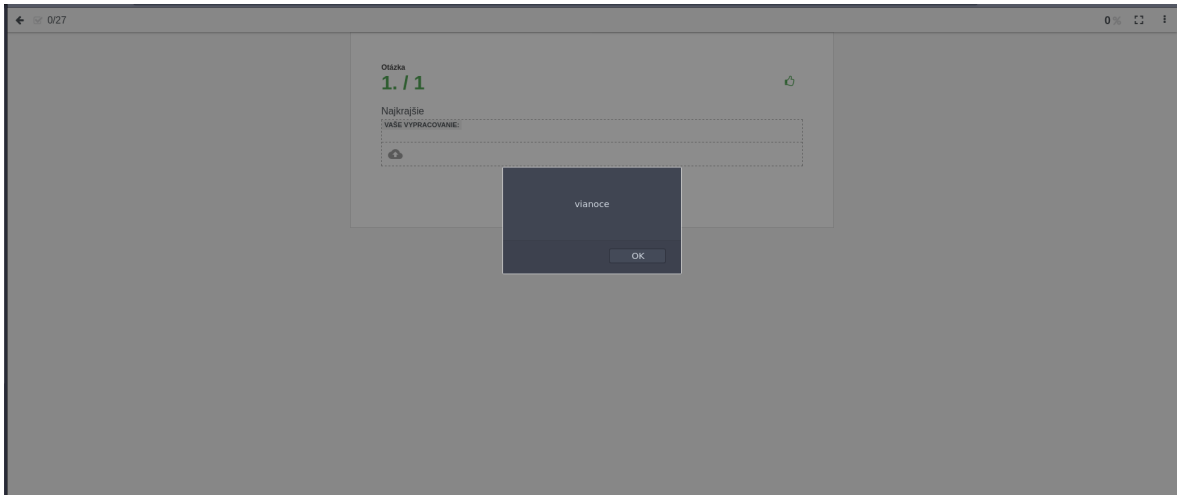


Obr. 4.5: Ukážka XSS v Známkach

4.6 XSS v Teste

4.6.1 Popis zraniteľnosti

Pri tvorbe testu môže učiteľ priamo upraviť zdrojový kód testu. Tento kód sa ďalej „neescepuje“.



Obr. 4.6: Ukážka XSS v Teste

4.6.2 Riešenie

Jedným možným riešením je zakázať učiteľom priamo editovať kód testu ale umožniť im používať iba WYSIWYG[1] editor. Inou alternatívou je zaistiť aby kód testu neobsahoval

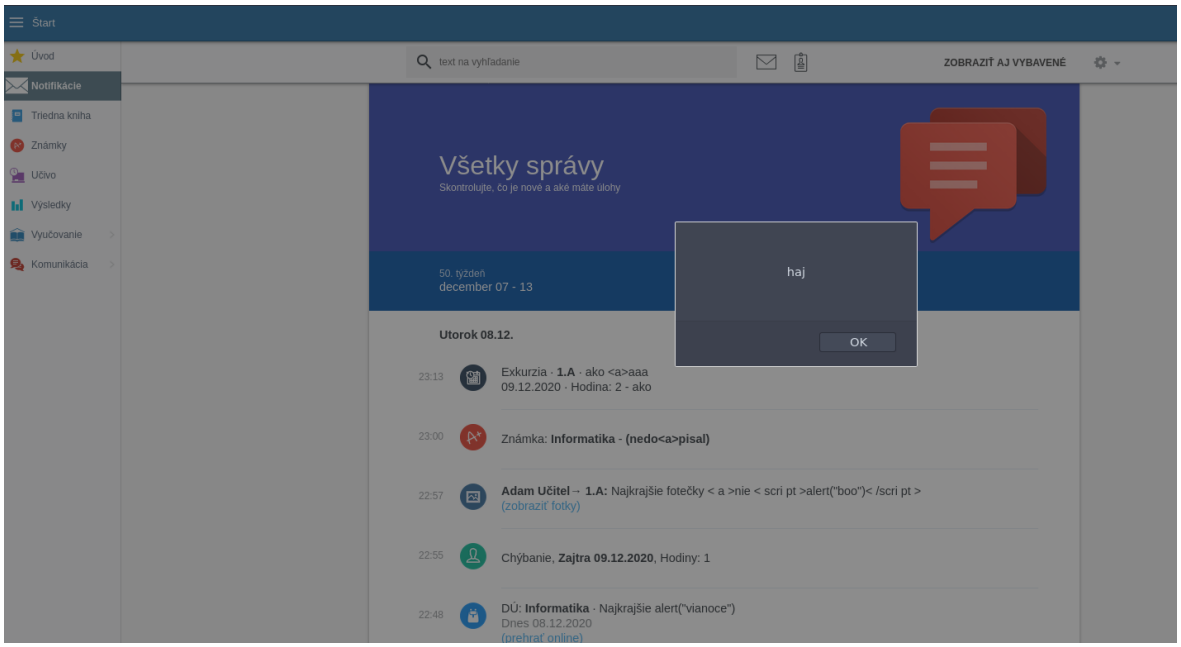
[1]What You See Is What You Get, teda „čo vidíš, to dostaneš“, je typ editoru, v ktorom iba vyzuálne vytvárame výsledný kód.

žiaden JavaScript. V čase písania práce táto zraniteľnosť nebola ešte opravená.

4.7 XSS medzi správami

4.7.1 Popis zraniteľnosti

Učiteľ môže pridať ľubovoľnú udalosť (výlet, exkurzia...). Pole „správa od učiteľa“ sa zobrazuje ako notifikácia v module 1.4.14 a nie je „escapované“. V aplikácii skript nefunguje, ale na normálnej stránke funguje.



Obr. 4.7: Ukážka XSS medzi správami

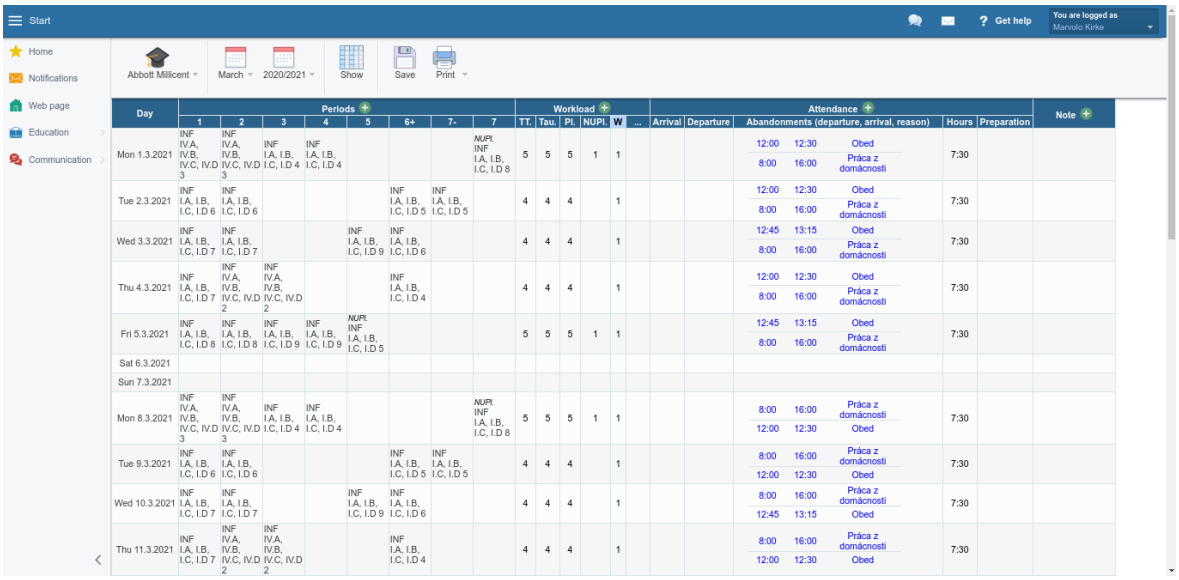
4.7.2 Riešenie

Nevidím dôvod prečo by sa tento text nemohol „escapovať“. V čase písania práce táto zraniteľnosť nebola ešte opravená.

4.8 Dochádzka učiteľov

4.8.1 Popis zraniteľnosti

Dochádzka učiteľov 1.4.19 poskytuje prístup ku všetkým pracovným výkazom bez dostatočnej verifikácie práv. Teda aj „guest“ používateľ má prístup k týmto výkazom, pokiaľ pozná identifikátor učiteľa. Tento identifikátor je však verejne dostupný na stránke so zoznamom učiteľov 1.4.7.



Day	Periods 1	2	3	4	5	6+	7-	7	Workload TT.	Tau.	Pl.	NUPI.	W	...	Attendance Arrival	Departure	Abandonments (departure, arrival, reason)			Hours	Preparation	Note
Mon 1.3.2021	INF IV.A, IV.B, IV.C, IV.D 3	INF IV.A, IV.B, IV.C, IV.D 3	INF I.A, I.B, I.C, I.D 4	INF I.A, I.B, I.C, I.D 4				NUPI. INF I.A, I.B, I.C, I.D 8	5	5	5	1	1				12:00 8:00	12:30 16:00	Obed Práca z domácnosti	7:30		
Tue 2.3.2021	INF I.A, I.B, I.C, I.D 6	INF I.A, I.B, I.C, I.D 6				INF I.A, I.B, I.C, I.D 5	INF I.A, I.B, I.C, I.D 5		4	4	4		1				12:00 8:00	12:30 16:00	Obed Práca z domácnosti	7:30		
Wed 3.3.2021	INF I.A, I.B, I.C, I.D 7	INF I.A, I.B, I.C, I.D 7			INF I.A, I.B, I.C, I.D 9	INF I.A, I.B, I.C, I.D 6			4	4	4		1				12:45 8:00	13:15 16:00	Obed Práca z domácnosti	7:30		
Thu 4.3.2021	INF I.A, I.B, I.C, I.D 7	INF IV.A, IV.B, IV.C, IV.D 2	INF IV.A, IV.B, IV.C, IV.D 2			INF I.A, I.B, I.C, I.D 4			4	4	4		1				12:00 8:00	12:30 16:00	Obed Práca z domácnosti	7:30		
Fri 5.3.2021	INF I.A, I.B, I.C, I.D 8	INF I.A, I.B, I.C, I.D 8	INF I.A, I.B, I.C, I.D 9	INF I.A, I.B, I.C, I.D 9	NUPI. INF I.A, I.B, I.C, I.D 5				5	5	5	1	1				12:45 8:00	13:15 16:00	Obed Práca z domácnosti	7:30		
Sat 6.3.2021																						
Sun 7.3.2021																						
Mon 8.3.2021	INF IV.A, IV.B, IV.C, IV.D 3	INF IV.A, IV.B, IV.C, IV.D 3	INF I.A, I.B, I.C, I.D 4	INF I.A, I.B, I.C, I.D 4				NUPI. INF I.A, I.B, I.C, I.D 8	5	5	5	1	1				8:00 12:00	16:00 12:30	Práca z domácnosti Obed	7:30		
Tue 9.3.2021	INF I.A, I.B, I.C, I.D 6	INF I.A, I.B, I.C, I.D 6				INF I.A, I.B, I.C, I.D 5	INF I.A, I.B, I.C, I.D 5		4	4	4		1				8:00 12:00	16:00 12:30	Práca z domácnosti Obed	7:30		
Wed 10.3.2021	INF I.A, I.B, I.C, I.D 7	INF I.A, I.B, I.C, I.D 7			INF I.A, I.B, I.C, I.D 9	INF I.A, I.B, I.C, I.D 6			4	4	4		1				8:00 12:45	16:00 13:15	Práca z domácnosti Obed	7:30		
Thu 11.3.2021	INF I.A, I.B, I.C, I.D 7	INF IV.A, IV.B, IV.C, IV.D 2	INF IV.A, IV.B, IV.C, IV.D 2			INF I.A, I.B, I.C, I.D 4			4	4	4		1				8:00 12:00	16:00 12:30	Práca z domácnosti Obed	7:30		

Obr. 4.8: Ukážka dochádzky fiktívneho učiteľa

4.8.2 Riešenie

Stačí pridať dodatočnú verifikácie používateľských práv. V čase písania práce táto zraniteľnosť nebola ešte opravená.

Záver

Cieľom tejto práce bolo zoznámiť sa so systémom EduPage a analyzovať ho z bezpečnostného hľadiska. Nakoniec sme objavili niekoľko bezpečnostných zraniteľností, z ktorých sa väčšinu už podarilo opraviť.

Napriek tomu, že sme testovali väčšinu systému vlastne na 3 typy zraniteľností, nakoniec sa nám podarilo objaviť iba relatívne malé množstvo zraniteľností.

Pričom principiálne boli všetky dvoch typov. Buď sa týkali „guest“ používateľov alebo išlo o XSS zneužiteľné zo strany učiteľov. Pričom žiadna zraniteľnosť sa netýkala vkladania neoprávnených SQL dotazov.

Osobne úplne nerozumieme prečo existuje typ používateľov „guest“, keďže ani nie je nikde prezentovaný. Preto by sme odporúčali ho úplne odstrániť zo systému, keďže prináša iba niekoľko relatívne veľkých zraniteľností a dá sa predpokladať, že existujú aj ďalšie, ktoré sme v tejto práci neodhalili.

Druhý typ problémov považujeme za problémy menej vážneho typu. Keďže takýmto spôsobom môžu učitelia získať prístup k žiackym účtom čo by nemali. Avšak tieto účty im nepridávajú takmer žiadne informácie, ku ktorým by predtým nemali prístup.

V práci sme nenašli vhodné miesto, kde by sme spomenuli všetky moduly systému, ktoré podľa analýzy fungujú správne. Taktiež teraz spomenieme, že sme sa bližšie nevenovali modulom jedáleň, faktúry a zmluvy, verejné obstarávanie, platby, prijímačky, maturity, príchody do školy a eGoverment. Tieto moduly sú teda vhodné na prípadnú ďalšiu analýzu. A všetky ostatné v čase nášho testovania fungovali správne, alebo sme v nich žiadnu chybu okrem tých spomínaných v predchádzajúcej kapitole neodhalili.

Bibliografia

[1] *aSc EduPage*. 2022. URL: https://edupage.org.

[2] *Štatistická ročenka - súhrnné tabuľky*. Sept. 2020. URL: https://www.cvtisr.sk/cvti-sr-vedecka-kniznica/informacie-o-skolstve/statistiky/statisticka-rocenka-publikacia/statisticka-rocenka-suhrnne-tabulky.html?page_id=9603.

[3] *Výpis z obchodného registra SR*. 2022. URL: https://www.orsr.sk/vypis.asp?ID=8267&SID=2&P=1.

[4] *aSc Info About aSc*. Archív: https://web.archive.org/web/19970412040415/http://www.asc.sk/about.html. Apr. 1997. URL: http://www.asc.sk/about.html.

[5] *aSc Rozvrhy*. Archív: https://web.archive.org/web/19991009115405/http://www.asc.sk:80/rozvrhy/sk/index.htm. Okt. 1999. URL: http://www.asc.sk/rozvrhy/sk/index.htm.

[6] *aSc Agenda*. Archív: https://web.archive.org/web/20040909191713/http://agenda.skoly.org:80/index.php?file=home.html. Sept. 2004. URL: http://agenda.skoly.org/index.php.

[7] *aSc EduPage*. Archív: https://web.archive.org/web/20060520075449/http://www.edupage.org/text/?text=text/info4school. Máj 2006. URL: http://www.edupage.org/text/?text=text/info4school.

[8] *React Native*. 2022. URL: https://reactnative.dev/.

[9] *Prieskum používanosti databáz*. 2020. URL: https://insights.stackoverflow.com/survey/2020#technology-databases.

[10] *Open Web Application Security Project*. 2022. URL: https://owasp.org.

[11] *Cross Site Scripting Prevention*. 2022. URL: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.

[12] *jGuery*. 2022. URL: https://jquery.com/.

[13] Ingrid Timková. „ŠKANDÁL v prešovskej základnej škole: Pozrite sa, aká fotografia sa dostala k žiakom!“ In: *Plus JEDEN DEŇ* (2021). URL: https://www1.pluska.sk/krimi/sokovani-rodicia-cez-stranku-urcenu-vzdelavanie-ktosi-rozposlal-detom-porno.