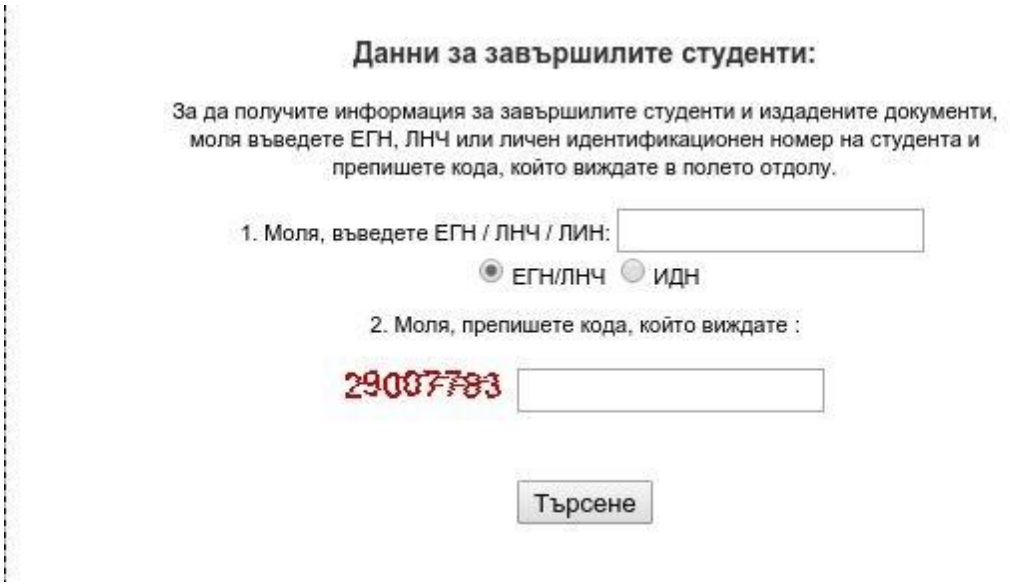
Уязвимост в сигурността на “Регистъра на завършилите студенти”

“Регистърът на завършилите студенти” - www2.mon.bg/AdminRHE2, съдържа данни за студентите, завършили образователно-квалификационна степен "бакалавър" или "магистър" след 1 януари 2012 година. Регистърът съдържа данни за завършената специалност, професионално направление, форма на обучение, както и сканирано изображение на дипломата.

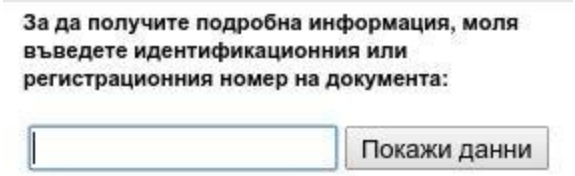
Уязвимостта в online регистъра се състои в това, че потребители с неоторизиран достъп имат лесната възможност да се сдобият с абсолютно всички сканирани копия на дипломите регистрирани в базата данни. По-долу ще наблегна на техническите детайли.

Автентикацията в портала става посредством въвеждането на ЕГН / ЛНЧ / ЛИН и случайно генерираната captcha (проверка против ботове).



След успешната автентикация, системата генерира cookie, което има за цел да оторизира заявките на съответния потребител към страницата с персонална информация. По долу е даден пример за такова cookie:

Cookie name: ASPSESSIONIDSSHBTTBT;
Cookie value: FNPFBLDCENCNCLOBFDBHHBGO;



След като потребителят бъде пренасочен към страницата с персонална информация, той има възможност да прегледа своите дипломи като въведе номера на желаната диплома в полето изобразено по-горе. Ако въведеният номер е валиден, потребителят ще бъде пренасочен към страницата с информация за съответната диплома, която съдържа и сканираните копия.

Когато потребителят селектира някое от сканираните изображения, той бива препращан към подобен URL:
https://www2.mon.bg/AdminRHE2/default.asp?action=s_img&intID=123456&fromRNV=0

И точно на тази стъпка е допусната сериозната уязвимост, която предоставя свалянето на всички дипломи. **intID** представлява уникалният номер на сканираното изображение. Ако се загледаме по-внимателно върху това ID ще стигнем до извода, че това са последователни числа, което ни предоставя възможността да ги променяме и по този начин да визуализираме различни сканирани дипломи. Какво ще се случи ако вместо 12345**6** (което е ID-то да моята диплома) въведем 12345**7**? Просто системата ще ни покаже съответната диплома с това ID.

От изложените факти може да се направят няколко извода:

1) Генерираната captcha е изключително лесна за bypass-ване от ботовете, което позволява написването на клиент (бот), който да се автентицира в системата.

2) Тъй като достъпът до дадена сканирана диплома не изисква оторизация, това позволява на случайни хора да боравят с личните данни на бившите студенти.

По-долу ще предоставя няколко такива дипломи за доказателство:

НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ
София
Бакалавърски факултет

ДИПЛОМА

на [redacted]

ЗА ВИСШЕ ОБРАЗОВАНИЕ
НА ОБРАЗОВАТЕЛНО-КВАЛИФИКАЦИОННА СТЕПЕН

БАКАЛАВЪР

по специалност
РЕКЛАМА

с професионална квалификация
рекламен мениджър

ДЕКАН: (подпис)

РЕКТОР: (подпис и печат с държавен герб)

Университет за Национално и Световно Стопанство
София

Факултет Икономика на инфраструктурата

ДИПЛОМА

на [redacted]

ЗА ВИСШЕ ОБРАЗОВАНИЕ
НА ОБРАЗОВАТЕЛНО-КВАЛИФИКАЦИОННА СТЕПЕН

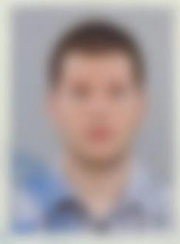
Бакалавър

по специалност
Икономика на търговията

с професионална квалификация
Бакалавър по икономика на търговията

Декан: *(проф.д.ик.н. Хр. Терзиев)*

Ректор: *(проф.д.ик.н. Стати Статев)*



Science & critical thinking

РУСЕНСКИ УНИВЕРСИТЕТ "АНГЕЛ КЪНЧЕВ"
ТРАНСПОРТЕН ФАКУЛТЕТ
РУСЕ

ДИПЛОМА

ЗА ВИСШЕ ОБРАЗОВАНИЕ

на

[redacted]

образователно-квалификационна степен:
МАГИСТЪР

по специалност:

ТЕХНОЛОГИЯ И УПРАВЛЕНИЕ НА ТРАНСПОРТА

с професионална квалификация:
МАГИСТЪР ИНЖЕНЕР

РУСЕНСКИ УНИВЕРСИТЕТ * РЕПУБЛИКА БЪЛГАРИЯ * "АНГЕЛ КЪНЧЕВ"

ДЕКАН: /Проф. д-р Р. Иванов/

РЕКТОР: /Проф. дтн Хр. Белоев/