Klienta drošība Latvijas interneta veikalos

Aigars Naglis
IT drošības konsultants

2015. gada 5. oktobris

Cik bieži iepērkamies internetā?

23% Reizi mēnesī

35% Dažas reizes gadā

18% Reizi gadā vai retāk

Dati no http://www.gemius.lv/e-komercija-zinas/interneta-ieperkas-latvijas-interneta-lietotaju.html

Vai bieži iepērkamies internetā?

58% Latvija

64% Eiropa

Dati no http://www.gemius.lv/

Kāpēc ne biežāk?

Kas ir būtiski drošībai?

Tehniski:

- Komunikācija starp jūsu pārlūku un portālu ir šifrēta
- Neuzrāda tehniskus kļūdu paziņojumus
- Paroles garuma un sarežģītības noteikumi
- Paroli iespējams atgūt drošā veidā
- Izmantota atjaunināta tīmekļa servera programmatūra

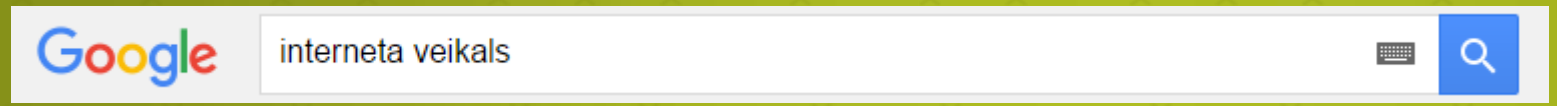
```
if (isset($votingstep)) {
     function ShowTheStuff($item, $itemvoted, $graph_width, $graph_height) {
        $hector=count($itemvoted);$totalvotes=0;$in=0;$stepstr='';
        $totalvotes=SumArray($itemvoted);
        $in=0;
        if ($totalvotes==0) { $totalvotes=0.0001; }
        while ($in<$hector) {
            $stepstr=$stepstr.stripslashes($item[$in]).':
            '.(int)(($itemvoted[$in]/$totalvotes)*100).'%<br>';
            $timesred=(int)((($itemvoted[$in]/$totalvotes))*$graph_width);
            $stepstr=$stepstr.'<img height='.$graph_height.' width='.$timesred.'
            src="lp_1.gif"><img height='.$graph_height.'
            width='.($graph_width-$timesred).' src="lp_0.gif"><br><br>';
            $in++;
        }
        return $stepstr;
    }
}
```

Kas ir būtiski drošībai?

Likumiski un Uzticamībai:

- Atrodama privātuma atruna
- Lietotāju atsauksmes neatkarīgos portālos
- Preču atgriešanas noteikumi - preci iespējams atgriezt
- Aktīvs tālruņa numurs, norādīta adrese, reģistrēts uzņēmums
- Tiek akceptēti ne tikai pārskaitījumi, bet arī banku kartes

Ierobežojumi



1. 1a.lv
2. 220.lv
3. Expresshop.lv
4. Xnet.lv
5. Ololo.lv
6. Sexystyle.lv
7. Galaxy.lv
8. 1shop.lv
9. Vertulux.lv
10. elektroniks.lv

EXPRESSSHOP

GalaXy

www.1a.lv

1 shop.lv

TAVS LABĀKAIS
www.220.lv
INTERNETA VEIKALS

SexyStyle

Xnet

Ololo.lv!

Elektroniks.lv

Komunikācija starp pārlūku un portālu ir šifrēta

- SSL tiek izmantots veikala visās sadaļās (3 punkti)
- SSL izmantots tikai ievadot jūtīgu informāciju (2 punkti)
- Komunikācija netiek šifrēta (1 punkts)

Pozīcija	Veikals	legūtie punkti
1.	www.220.lv	2
2.	www.xnet.lv	2
3.	www.1shop.lv	2
4.	www.1a.lv	2
5.	www.sexystyle.lv	2
6.	www.ololo.lv	1
7.	www.expressshop.lv	1
8.	www.vertulux.lv	1
9.	www.elektroniks.lv	1
10.	www.galaxy.lv	1

Komunikācija starp pārlūku un portālu ir šifrēta

Neuzrāda tehniskus kļūdu paziņojumus

- Netiek uzrādīti kļūdu paziņojumi, pārbaudītās saites strādā (3 punkti)
- Nenozīmīgas nepilnības (2 punkti)
- Lietošanu bieži kavē tehniskas problēmas (1 punkts)

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.xnet.lv	3
3.	www.1shop.lv	3
4.	www.1a.lv	3
5.	www.ololo.lv	3
6.	www.sexystyle.lv	2
7.	www.vertulux.lv	2
8.	www.galaxy.lv	2
9.	www.expressshop.lv	1
10.	www.elektroniks.lv	1

expressshop.lv

SELECT * FROM users WHERE ((email='\') or (mob_phone='\') or (mob_phone='2\')) AND (password='\') LIMIT 1:
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
syntax to use near '\') or (mob_phone='2\')) AND (password='\') LIMIT 1' at line 1Paroles nesakrīt!

sexystyle.lv

ololo.lv

		Preces nosaukums	Cena	Daudzums	Summa
✖		Samsung M3 2.5" 1TB USB3, Black	50 €	0.001	0.05 €
✖		BRAUN D4.010	7.70 €	1	7.70 €
✖		RAVANSON K04T	25 €	1	25 €
				Summa:	32.75 €

Piegāde:

- ○ Bez piegādes
- ◉ Piegāde Rīgā (7 €)
- ○ Rīga (Bolderāja), Jūrmala (20 €)
- ○ Piegāde Latvijā (cena ir atkarīga no attāluma, preces svara un izmēriem)

Pārrēķināt | Noformēt pirkumu

1shop.lv

Apple MacBook Pro ME665LL/A

0.00 €

Ielikt grozā

Ātrais pirkums

Asus X401U 14/AMDC60/2GB/320GB/HD6290/ WIN8

0.00 €

Ielikt grozā

Ātrais pirkums

Asus X401A 14/B820/2GB/320GB/INTELHD/WI N8

0.00 €

Ielikt grozā

Ātrais pirkums

HP ProBook 4540s

0.00 €

HP 650 15.6/B830/2GB/500GB/INTELHD/ LINUX (C1N22EA)

0.00 €

HP 650 15.6/B980/2GB/320GB/INTELHD/ LINUX (C1M79EA)

0.00 €

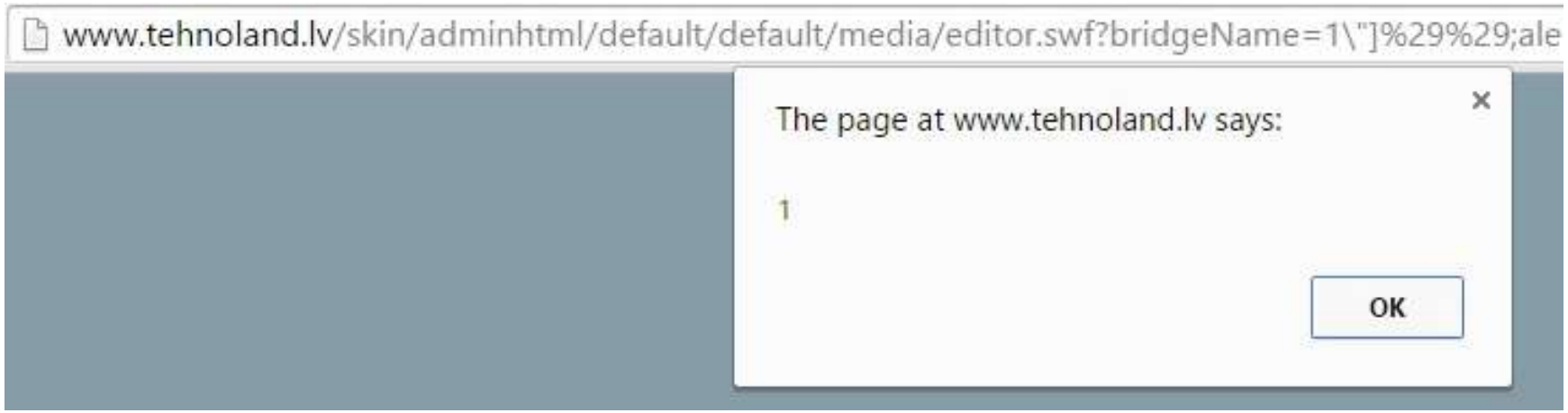
707.lv

	Nosaukums	Skaits	Cena	Kopā
🗑	CM9740 moderna mini mūzikas sistēma	0.2	733.65 EUR	146.73 EUR
🗑	Desire 310 DUAL matte blue EU	1	105.00 EUR	105.00 EUR
	Kopā:	1.2		251.73 EUR

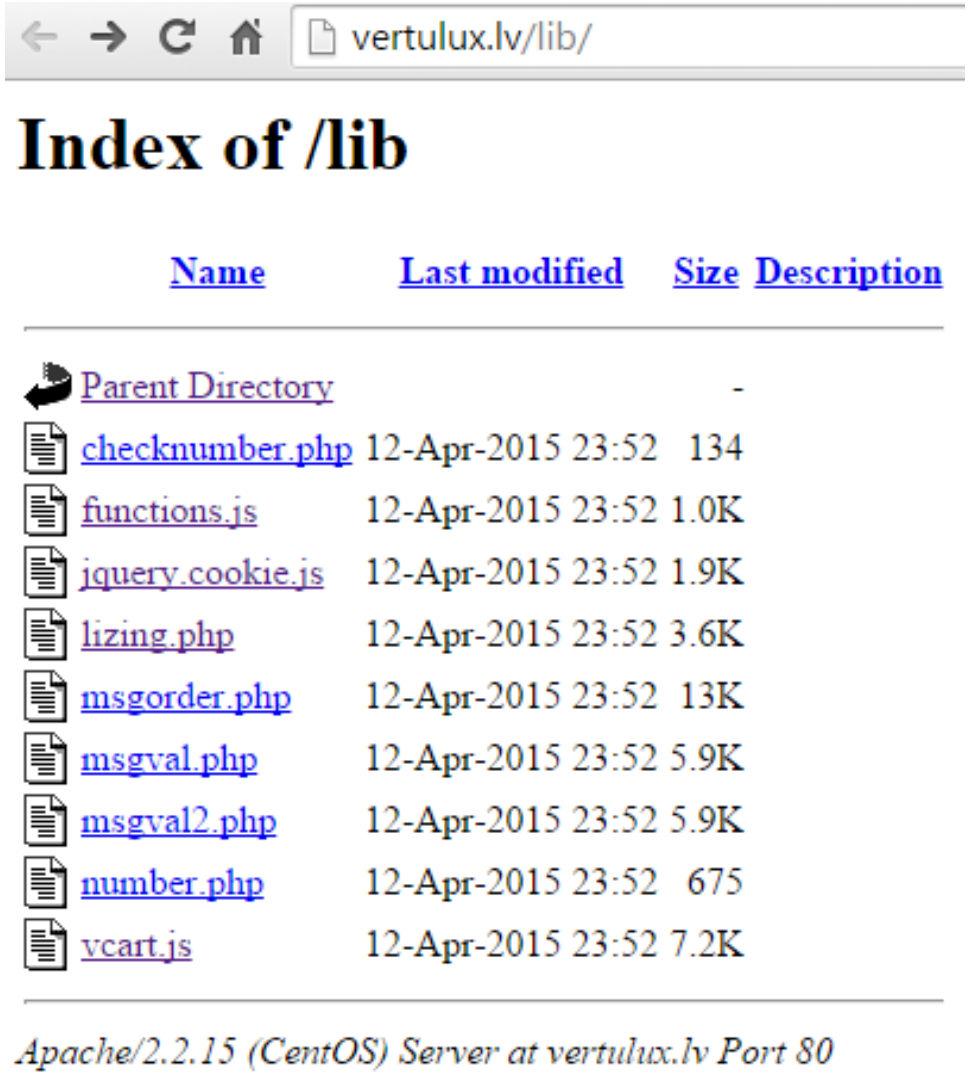
tera.lv

☑	4TER890843	LENOVO ThinkPad W541(20EF000S) 15.5" 3K (2880x1620) IPS, Intel Core i7-4910MQ 2.9GHz/8MB, vP...	3 438.80*	0.01	34.39	Noliktavā: 1
☑	0TER900141	SAMSUNG 3D 85" ULTRA HD 4K LED LCD televizors,	25 752.40*	0.01	257.52	Noliktavā: 2

tehnoland.lv



vertulux.lv


vertulux.lv/lib/
Index of /lib
Name
Last modified
Size
Description
Parent Directory -
checknumber.php 12-Apr-2015 23:52 134
functions.js 12-Apr-2015 23:52 1.0K
jquery.cookie.js 12-Apr-2015 23:52 1.9K
lizing.php 12-Apr-2015 23:52 3.6K
msgorder.php 12-Apr-2015 23:52 13K
msgval.php 12-Apr-2015 23:52 5.9K
msgval2.php 12-Apr-2015 23:52 5.9K
number.php 12-Apr-2015 23:52 675
vcart.js 12-Apr-2015 23:52 7.2K
Apache/2.2.15 (CentOS) Server at vertulux.lv Port 80

vertulux.lv

vertulux.lv/x/IMG_3315.JPG

Paroles garuma un sarežģītības noteikumi

- Paroles minimums 8 simboli, viens cipars, lielais burts un speciālais simbols (3 punkti)
- Tiek uzspiesti paroles veidošanas noteikumi, tomēr tie neatbilst labākajai praksei (2 punkti)
- Paroli var izvēlēties brīvi (1 punkts)

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	2
2.	www.1shop.lv	2
3.	www.sexystyle.lv	2
4.	www.expressshop.lv	2
5.	www.elektroniks.lv	2
6.	www.xnet.lv	1
7.	www.1a.lv	1
8.	www.ololo.lv	1
9.	www.vertulux.lv	1
10.	www.galaxy.lv	1

1a.lv

E-pasta adrese: *

koki@daba.lv

Tālrunis: *

[redacted]

Dzimšanas datums (Diena/Mēnesis/Gads): *

4 | Aprīlis | 1984

Dzimums: *

Sieviete

Parole: *

Parole atkārtoti: *

REĢISTRĀCIJA

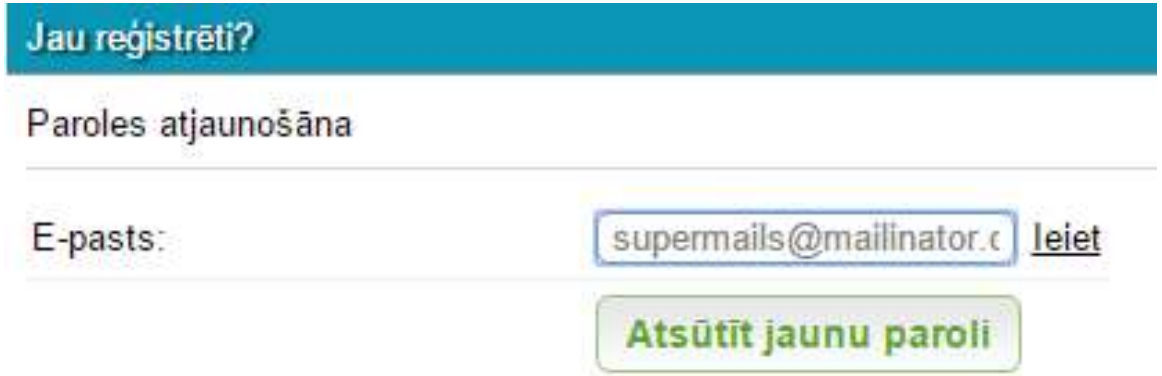
Lietotāja reģistrācija veiksmīga! Aktivizācijas atslēga tika nosūtīts uz e-pastu: "koki@daba.lv"!

Paroli iespējams atgūt drošā veidā

- Paroli iespējams atgūt salīdzinoši drošā veidā (3 punkti)
- Paroli nav iespējams atgūt vai tā tiek nosūtīta lietotājam nešifrētā veidā (1 punkts)

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.xnet.lv	3
3.	www.1shop.lv	3
4.	www.ololo.lv	1
5.	www.1a.lv	1
6.	www.sexystyle.lv	1
7.	www.expressshop.lv	1
8.	www.vertulux.lv	1
9.	www.elektroniks.lv	1
10.	www.galaxy.lv	1

Paroli iespējams atgūt drošā veidā



Paroles atjaunošāna

Lietotājvārds: super

Parole: 03516

Ololo.lv

Atjaunin--ta tīmekļa servera programmatūra

- Izmanto atjauninātas versijas (3 punkti)
- Izmanto pāris, iespējams, novecojušas komponentes (2 punkti)
- Izmanto novecojušas komponentes, vai komponentes ar būtiskām ievainojamībām (1 punkts)

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.1shop.lv	3
3.	www.sexystyle.lv	3
4.	www.xnet.lv	2
5.	www.1a.lv	2
6.	www.ololo.lv	2
7.	www.elektroniks.lv	2
8.	www.galaxy.lv	2
9.	www.expressshop.lv	1
10.	www.vertulux.lv	1

expressshop.lv

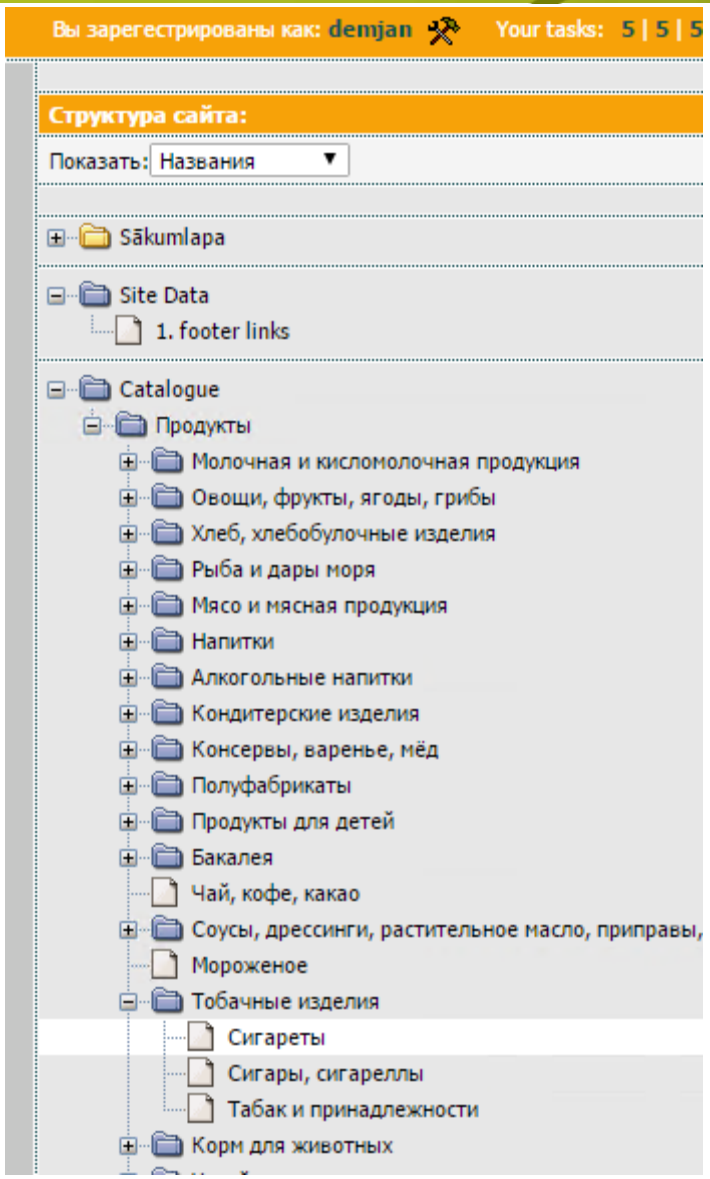
sexystyle.lv

Vulnerabilities in In-Portal CMS

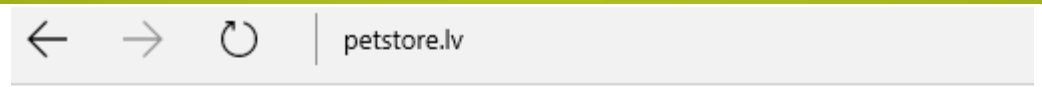
From: "MustLive" <mustlive () websecurity com ua>
Date: Tue, 16 Sep 2014 00:55:43 +0300

```
Hello list!

These are Cross-Site Scripting and Brute Force vulnerabilities in In-Portal CMS.
```


www
/in_site/
inSite
Login
1' or '1'='1
Password
Enter


Вы зарегестрированы как: demjan
Your tasks: 5 | 5 | 5
Структура сайта:
Показать: Названия
Sākumlapa
Site Data
1. footer links
Catalogue
Продукты
Молочная и кисломолочная продукция
Овощи, фрукты, ягоды, грибы
Хлеб, хлебобулочные изделия
Рыба и дары моря
Мясо и мясная продукция
Напитки
Алкогольные напитки
Кондитерские изделия
Консервы, варенье, мёд
Полуфабрикаты
Продукты для детей
Бакалея
Чай, кофе, какао
Соусы, дрессинги, растительное масло, приправы,
Мороженое
Тобачные изделия
Сигареты
Сигары, сигареллы
Табак и принадлежности
Корм для животных

petstore.lv



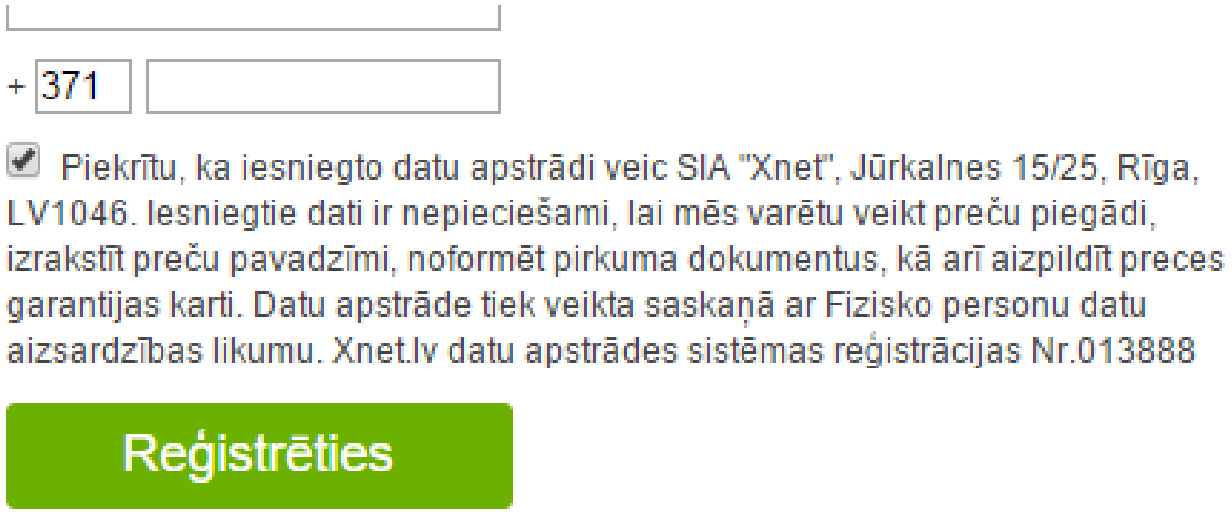
Index of /

[ICO]	Name	Last modified	Size	Description
[DIR]	clipspreview/	25-Aug-2015 05:08	-	
[ ]	combine.php.encrypted	25-Aug-2015 05:09	5.0K	
[DIR]	css/	25-Aug-2015 05:09	-	
[TXT]	design.html.encrypted	25-Aug-2015 05:09	9.4K	
[ ]	dummy.php.encrypted	25-Aug-2015 05:09	626	
[DIR]	fckeditor/	25-Aug-2015 05:07	-	

```
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret server on the Internet.  After

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 4.6 bitcoins (~1000 USD)
Without key, you will never be able to get your original files back.

-------------------------------------------

!!!!!!!!!!!!!!!!!!!!  PURSE FOR PAYMNET: 13JqaSsVg2tVBpbbvbwgF2jzdK5Sn2rQ68      !!!!!!!!!!!!!!!!!!!!
```

Atrodama privātuma atruna

- Pieprasīts nepieciešamais datu minimums, skaidrota vajadzība, uzglabāšana (3 punkti)
- Nav privātuma atrunas vai tiek pieprasīti lieki personas dati (1 punkts)



Pozīcija	Veikals	Iegūtie punkti
1.	www.xnet.lv	3
2.	www.1a.lv	3
3.	www.220.lv	1
4.	www.1shop.lv	1
5.	www.sexystyle.lv	1
6.	www.ololo.lv	1
7.	www.expressshop.lv	1
8.	www.vertulux.lv	1
9.	www.elektroniks.lv	1
10.	www.galaxy.lv	1

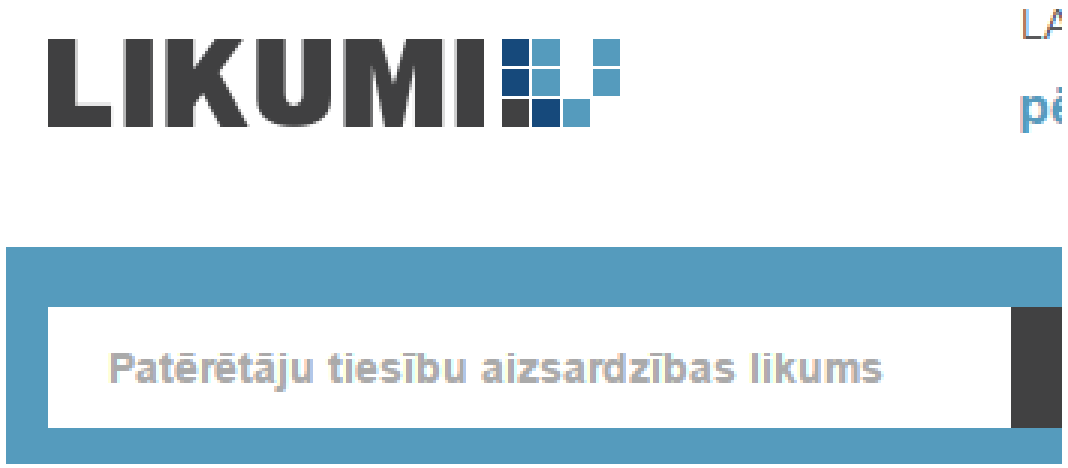
Lietotāju atsauksmes neatkarīgos portālos

- Salīdzini.lv vērtējums 3.5-5 (3 punkti)
- Salīdzini.lv vērtējums 2-3.5 (2 punkti)
- Salīdzini.lv vērtējums 1-2 (1 punkts)

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.xnet.lv	3
3.	www.1shop.lv	3
4.	www.1a.lv	3
5.	www.sexystyle.lv	3
6.	www.expressshop.lv	3
7.	www.elektroniks.lv	3
8.	www.ololo.lv	2
9.	www.vertulux.lv	2
10.	www.galaxy.lv	1

Preču atgriešanas noteikumi - preci iespējams atgriezt

- Noteikumi ir – pieļauj preces atgriešanu un naudas atdošanu (3 punkti)
- Noteikumi pieļauj preci tikai apmainīt pret citu (2 punkti)
- Prece nav atgriežama vai nav informācijas (1 punkts)



Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.xnet.lv	3
3.	www.1shop.lv	3
4.	www.1a.lv	3
5.	www.sexystyle.lv	3
6.	www.ololo.lv	3
7.	www.expressshop.lv	3
8.	www.vertulux.lv	3
9.	www.elektroniks.lv	1
10.	www.galaxy.lv	1

Aktīvs tālruņa numurs, norādīta adrese, reģistrēts uzņēmums

- Pieejams tālruņa numurs (++1 punkts)
- Portālā atrodama fiziskā adrese (++1 punkts)
- Veikala darbībai ir reģistrēts uzņēmums (++1 punkts)

3/3 !!!

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	3
2.	www.xnet.lv	3
3.	www.1shop.lv	3
4.	www.1a.lv	3
5.	www.sexystyle.lv	3
6.	www.ololo.lv	3
7.	www.expressshop.lv	3
8.	www.vertulux.lv	3
9.	www.elektroniks.lv	3
10.	www.galaxy.lv	3

Tiek akceptēti ne tikai pārskaitījumi, bet arī banku kartes

- Tiek pieņemtas kredītkartes, debetkartes un pārskaitījumi (3 punkti)
- Tiek pieņemti tikai pārskaitījumi (2 punkti)
- Tiek pieņemta tikai skaidra nauda (1 punkts)

Pozīcija	Veikals	legūtie punkti
1.	www.220.lv	2
2.	www.xnet.lv	2
3.	www.1shop.lv	2
4.	www.1a.lv	2
5.	www.sexystyle.lv	2
6.	www.ololo.lv	2
7.	www.expressshop.lv	2
8.	www.vertulux.lv	2
9.	www.elektroniks.lv	2
10.	www.galaxy.lv	2

Rezultāti

Pozīcija	Veikals	Iegūtie punkti
1.	www.220.lv	25
2.	www.xnet.lv	25
3.	www.1shop.lv	25
4.	www.1a.lv	23
5.	www.sexystyle.lv	22
6.	www.ololo.lv	20
7.	www.expressshop.lv	18
8.	www.vertulux.lv	17
9.	www.elektroniks.lv	17
10.	www.galaxy.lv	16
	Vidēji par veikalu	21,7
	Vidēji par pārbaudi	2.2/3

Tad kāpēc vēl neesmu šeit:

Vai veikalniekus nepilnības uztrauc?

Reply Reply All Forward IM

Pk 2015. gada .24.07 17:33

Aigars Naglis

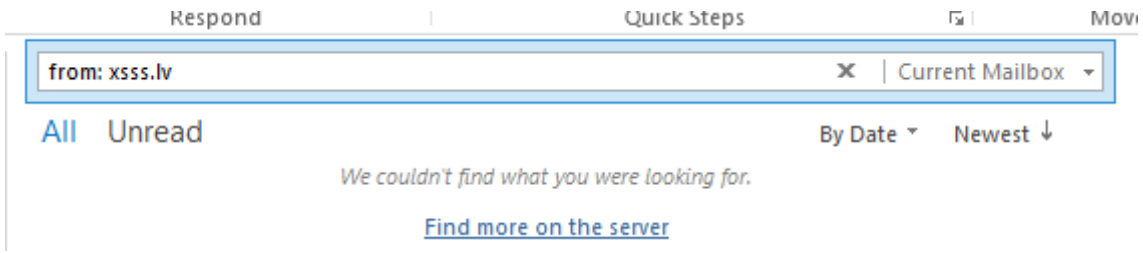
Drošības problēmas?

To veikals@xsss.lv

Labdien!

Rakstu sakarā ar jūsu internetveikala iespējamām drošības nepilnībām.

. . .



Tad vai ir droši iepirkties Latvijas e-veikalos?

Preci piegādās, garantija būs un naudu atgriezīs

- Pieejama kontaktinformācija – 3/3
- Preces iespējams atgriezt – 2.6/3
- Klientu vērtējums – 2.7/3

Personas dati un pirkuma vēsture var tikt nopludināta

- Komunikācijas šifrēta – 1.6/3
- Paroļu politika – 1.5/3
- Privātuma politika – 1.6/3
- Drošas tehnoloģiju versijas – 2/3

Paldies

blogs.dpa.lv

Aigars Naglis
IT drošības konsultants