

OWASP Top 10 Latvijā

Biežākās drošības problēmas tīmekļa lietojumos

Agris Krusts, IT Centrs, SIA

28.03.2019

Par mani

- Agris Krusts, SIA IT Centrs dibinātājs, drošības konsultants
 - Drošības auditi un testi, apmācība
 - E-pasts: Agris.Krusts@itcentrs.lv
 - Twitter: [@agris_krusts](https://twitter.com/agris_krusts)
 - www.itcentrs.lv

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Datu avots

- Tīmekļa lietojumu drošības testi laika posmā 2015-2018
- ~ 130 sistēmas
- Parasti testa vides
- Klasificēts atbilstoši OWASP Testing Guide v4
- Detalizētāka statistika tikai par "populārākajām" problēmām
- Salīdzinājums ar līdzīgiem datiem par 2011 - 2014

Par pašu prezentāciju

- No OWASP Top 10 2017 neapskatīju
 - A8:2017-Insecure Deserialization
 - A10:2017-Insufficient Logging & Monitoring
- Netulkoju OWASP Top 10 virsrakstus

Injekcijas

- Samazinājās no ~40% līdz aptuveni 10%
- Vēl ar vien lielākā daļa ir SQLi (7)
- Pārējās: XML un koda injekcijas
- Lielākā daļa ir grūti atrodamas aklās vai pilnīgi aklās (*totally blind*)

Totally blind injekcijas

- SQL Server: `1;waitfor delay '0:0:10'--`
- Postgress: `(SELECT pg_sleep(10))`
- MySQL:
``select * from users where id = (select 1 union select sleep(1) limit 1)`

Broken Authentication and session management

ievainojamas sistēmas

Sesijas fiksācija	11%
Logout problēmas	15%
Sesiju dzīves ilgums	13%
Autentifikācijas apiešana	18%
Problēmas paroles atjaunošanas funkcionalitātē	7%
Vājas paroles	13%

Broken Authentication and session management

- Sesijas fiksācija samazinājās no 30% līdz 11%
- Iztrūkstoši sīkdatņu parametri Secure un HttpOnly down samazinājās no 44% līdz 5%
- Vecākas sistēmas mēdz atstāt novārtā

www.manabalss.lv demo

FirefoxFileEditViewHistoryBookmarksToolsWindowHelp

ManaBalss.lv - līdzdalības platf...

←→↻🏠

🔒https://manabalss.lv

⌵⋮🔒🌟🔍Search

📺📅⚙️☰

📄

Par ManaBalss.lvPaveiktaisAtbalstītājiIniciatīvu iesniedzējiemPalīdzi mums!eucrowd project

LATVISKIRУССКИЙ



 Izveidot jaunu iniciatīvu

 Skatīt visas iniciatīvas



 Ienāc ManaBalss.lv

Atbalsti ManaBalss.lv

Ja katrs no mums ziedotu vismaz **5 eiro**, mēs varētu nosegt gada izmaksas un attīstīt jaunas digitālās demokrātijas platformas, lai tu varētu ietekmēt politiku Latvijā. Lūdzu palīdzi mums sasniegt iecerēto – kļūsti par ziedotāju!

VĒLOS ZIEDOT📄

ManaBalss.lv ziņas

skatīt visas ➤



Ne mīluma uzplūdi, bet ilgtermiņa atbildība

pirms 20 stundām

Paralēli mājdzīvnieku labturības normu izskatīšanai Saeimas komisijās trešdien, 27. martā, pie parlamenta notiek arī 25 dzīvnieku aizsardzības organizāciju atbalstīts pikets. Tā prasības sasaucas ar ManaBalss platformā virzīto iniciatīvu „Par mājdzīvnieku turēšanas likumu grozījumiem”.

Piketa rīkotāji – dzīvnieku patversme „Ulubele” – savā mājaslapā piketa sakarā ir publicējuši sekojošo uzsaukumu. Lasīt tālāk ...

Aktuālās iniciatīvas

skatīt visas ➤



AUKLES LĪDZFINANSĒJUMS ARĪ VECĀKIEM

Šobrīd vecāki nevar saņemt pašvaldības līdzfinansējumu, ja izvēlās paši pieskatīt bērnu mājās, nevis sūtīt uz privāto bērnu dārzu vai algot aukli.

10'000

KOPĀ PANĀKTAIS IEDVESMO

67.5%



NO INICIATĪVĀM, PAR KURĀM LEMTS, IR POZITĪVI IETEKMĒJUŠAS LIKUMUS

KĀ TU BALSOTU, JA BŪTU SAEIMAS DEPUTĀTS?

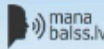
Vai ir jāaizliedz PSRS un nacistiskās Vācijas formastērpu izmantošanu sapulcēs, gājienos un piketos?

Par

Pret

1 / 4

 PAR vai PRET



11

www.manabalss.lv demo

- Youtube video

www.manabalss.lv

91	https://www.facebook.com	POST	/tr/	✓	200
92	https://manabalss.lv	GET	/auth/nordea/new		302
93	https://manabalss.lv	GET	/login?provider=nordea&service=htt...	✓	302
94	https://manabalss.lv	GET	/cauth/nordea/new		200
95	https://manabalss.lv	GET	/assets/application-81e33228bfd7e...		404
96	https://manabalss.lv	GET	/assets/application-31aed208d7d5c...		404
97	https://netbank.nordea.com	POST	/pnbeid/eidn.jsp	✓	302
98	https://netbank.nordea.com	GET	/pnbeid/eid.do?channel=WWW&new...	✓	302
99	https://netbank.nordea.com	GET	/pnbeid/eid_login.do?cs=b96e3b8b...	✓	200
102	https://netbank.nordea.com	GET	/scripts/jquery-1.4.2.min.js?v=13-1...	✓	200
104	https://netbank.nordea.com	GET	/scripts/util.js?v=13-1-3	✓	200
106	https://netbank.nordea.com	GET	/scripts/timeout_func.js?v=13-1-3	✓	200

Request	Response
---------	----------

Raw	Headers	Hex	HTML	Render
-----	---------	-----	------	--------

HTTP/1.1 302 Found
Server: nginx/1.10.1
Date: Wed, 27 Mar 2019 08:22:54 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
Location: https://manabalss.lv/login?provider=nordea&service=https%3A%2F%2Fmanabalss.lv%2Fauth%2Fnordea%2Fnew
Cache-Control: no-cache
Set-Cookie: mb_session=d68b496bb2db4400e9530374bfff18a2d; domain=.manabalss.lv; path=/; expires=Wed, 27 Mar 2019 08:22:54 GMT
X-Request-Id: 9b580d18-4fbe-4368-8e27-8a152d739d76
X-Runtime: 0.019993
Content-Length: 171

<html><body>You are being https://manabalss.lv/login?provider=nordea&service=https%3A%2F%2Fmanabalss.lv%2Fauth%2Fnordea%2Fnew

www.manabalss.lv

Burp Suite Professional v2.0.16beta - Temporary Project - licensed to SIA IT Centrs [single user license]

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
125	https://netbank.nordea.com	GET	/fonts/ApercuPro-Bold.otf			200	128324		otf		
126	https://netbank.nordea.com	POST	/pnbeid/eid_login1.do?ts=LV&am...	✓		200	1007	XML	do		
127	https://netbank.nordea.com	POST	/pnbeid/eid_login1.do?ts=LV&am...	✓		200	1007	XML	do		
128	https://netbank.nordea.com	POST	/pnbeid/eid_login2.do?act=auth&am...	✓		200	1379	XML	do		
129	https://netbank.nordea.com	GET	/pnbeid/switch_select_access.do?cs=...	✓		302	1078	HTML	do	302 Moved Temporarily	
130	https://netbank.nordea.com	GET	/pnbeid/eid_review.do?act=eid_revie...	✓		200	10955	HTML	do	Luminor Bank AS Latvija...	
132	https://netbank.nordea.com	POST	/pnbeid/redirect_to_partner.do?cs=2...	✓		302	1706	HTML	do	302 Moved Temporarily	
133	https://manabalss.lv	GET	/cauth/nordea?B02K_VERS=0002&B...	✓		303	729	HTML			
134	https://manabalss.lv	GET	/auth/nordea/login?ticket=ST-15536...	✓		302	612	HTML			
135	https://manabalss.lv	GET	/			200	41114	HTML		ManaBalss.lv - IĀ«dzdal...	
137	https://parvaipret.lv	GET	/widget			200	9375	HTML		Par vai Pret	
138	https://app.mailjet.com	GET	/widget/iframe/31IK/6ZE			200	4229	HTML		Widget Iframe	
139	https://manabalss.lv	GET	/initiatives/list?amount=11&offset=0...	✓		200	46622	HTML			
140	https://www.google-analytics....	GET	/r/collect?v=1&_v=j73&a=1144568...	✓		302	1003	HTML		302 Moved	
146	https://bam.nr-data.net	GET	/1/0d480a45bc?a=17823217&v=1...	✓		200	165	script			

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 303 See Other
Server: nginx/1.10.1
Date: Wed, 27 Mar 2019 08:23:44 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
Location: https://manabalss.lv/auth/nordea/login?ticket=ST-15536750244212-Rao3DyDMfFp7v8DZqax28Q9uw7cfjKHUfZwKEIrK
Cache-Control: no-cache
Set-Cookie: tgt=TGC-15536750244102-uydUCznjQZBJ4nduJRBfM1b6G001FLNdABIs9dcQ; path=/
X-Request-Id: 073aca08-5950-4891-a125-6f15712ba63c
X-Runtime: 0.032321
Content-Length: 170

<html><body>You are being redirected.</body></html>

0 matches

www.manabalss.lv

```
Date: Wed, 27 Mar 2019 08:23:44 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
Location: https://manabalss.lv/
Cache-Control: no-cache
Set-Cookie: _mb_session=d68b496bb2db4400e9530374bfff18a2d; domain=.manabalss.lv;
X-Request-Id: 6d815b76-d5ba-4e3d-89b4-4e61080de69c
X-Runtime: 0.064133
Content-Length: 87
```

```
<html><body>You are being <a href="https://manabalss.lv/">redirected</a>.</body>
```

www.manabalss.lv

The screenshot shows the website www.manabalss.lv in a browser window. The browser's address bar displays the URL. The website's header includes a navigation menu with links: "Par ManaBalss.lv", "Paveiktais", "Atbalstītāji", "Iniciatīvu iesniedzējiem", "Palīdzi mums!", and "eucrowd project". There are also language selection buttons for "LATVISKI" and "РУССКИЙ". The main navigation bar features the "mana balss.lv" logo, a button to "Izveidot jaunu iniciatīvu", a link to "Skatīt visas iniciatīvas", a search bar labeled "Meklēt", and a user profile for "Agris Krusts".

The main content area is divided into several sections:

- Atbalsti ManaBalss.lv**: A blue banner with text encouraging donations to support the platform. It includes a "VĒLOS ZIEDOT" button with a heart icon.
- ManaBalss.lv ziņas**: A section titled "ManaBalss.lv ziņas" with a link to "skatīt visas". It features a video of a kitten and a text article about animal welfare legislation. The article title is "Ne mīluma uzplūdi, bet ilgtermiņa atbildība" and it mentions a parliamentary session on March 27th.
- KOPĀ PANĀKTAIS IEDVESMO**: A red banner showing a "67.5%" success rate with a thumbs-up icon. The text reads: "NO INICIATĪVĀM, PAR KURĀM LEMTS, IR POZITĪVI IETEKMĒJUŠAS LIKUMUS".
- KĀ TU BALSOTU, JA BŪTU SAEIMAS DEPUTĀTS?**: A blue banner with a poll question: "Vai ir jāaizliedz PSRS un nacistiskās Vācijas formastērpu izmantošanu apulcēs, gājienos un piketos?". It has "Par" and "Pret" buttons and shows "1 / 4" votes.
- Aktuālās iniciatīvas**: A section titled "Aktuālās iniciatīvas" with a video player showing a video about "AUKLES LĪDZFINANSĒJUMS ARĪ VECĀKIEM". The video player shows a progress bar at 03:12 / 00:03.

www.manabalss.lv

- Sesijas sīkdatnes vērtība pirms autentifikācijas:
Cookie:
`_mb_session=d68b496bb2db4400e9530374bfff18a2d`
- Sesijas sīkdatnes vērtība pēc autentifikācijas:
Set-Cookie:
`_mb_session=d68b496bb2db4400e9530374bfff18a2d;
domain=.manabalss.lv; path=/; expires=Wed, 27
Mar 2019 08:38:44 -0000; HttpOnly`

Sensitive Data Exposure

Systems

Pārlūka kešatmiņa	21%
SSL problēmas	31%
Sensistīvas informācijas pārsūtīšana izmantojot HTTP	10%

Sensitive Data Exposure

- SSL problēmas palielinājās no 27% līdz 31%
- Sensitīvas informācijas pārsūtīšana ar HTTP samazinājās no 40% līdz 10%

Pārlūka kešatmiņa

https://patient.datamed.lv/patient/

...

Search

DM

DATAMED

MEDICAL DIAGNOSTICS INFORMATION
SYSTEM

LAT | ENG | RUS

PATIENT: KRUSTS AGRIS, 030474-1

LOGOUT

MY STUDIES

No studies found

INFORMATION

In DATAMED system are available only those studies, that medical institution stored in archive and which contain correct personal code in accordance with the standards of the Latvian Republic. Information about DATAMED Diagnostics information system customers can be found [here](#).

If you do not see your study here, it means that it was not sent to the DM archive, or it contains the wrong patient data. If you want to see this study in the DATAMED system, then please contact the appropriate medical institution in which this study was performed.

You can sign in to the DATAMED system using bank or eID card authentication. This type of authorization provides free access to your studies, which were performed in the last 30 days. At this time, you can save your studies on your data carrier (hard drive, CD/DVD or other). To get access to older studies (marked with lock icon), you can buy different types of portal subscription.

©DataMed

About DATAMED

Contacts

Usage rules

Display calibration

Questions & suggestions

Lapa pārlūkā

3326	https://patient.datamed.lv	GET	/		303
3327	https://patient.datamed.lv	GET	/patient/		200
3331	https://patient.datamed.lv	GET	/datamed.js?v=7	✓	200
3332	https://patient.datamed.lv	GET	/assets/jquery-1.9.1.min.js		200
3335	https://patient.datamed.lv	GET	/api/api_egl/documents_list/?patient...	✓	200
3336	https://patient.datamed.lv	GET	/favicon.ico		404

Request

Response

Raw

Headers

Hex

HTML

Render

```

HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 13 Mar 2018 14:00:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: lang=lv; path=/; domain=.datamed.lv; secure
Vary: Accept-Encoding
Content-Length: 4212

```

```

<!doctype html>
<html>
<head>
<title>DataMed portāls</title>

<link rel="stylesheet" type="text/css" media="screen" href="/assets/style.css?v=7">
<link rel="stylesheet" type="text/css" media="print" href="/assets/print-reset.css">
<link rel="stylesheet" type="text/css" media="print" href="/assets/print.css?v=1">

<link rel="shortcut icon" href="/favicon.ico">
</head>

```

Servera atbilde


```
akmbp2:9w2xfa9b.default akrusts$ find . -type f -exec grep 030474 {} /dev/null \;  
Binary file ./cache2/entries/FE783B0C0909BA855F46B0696072EAAA30DE1E89 matches  
Binary file ./cache2/entries/9FA5600A9E4AECEF92B4E258001619DEC9F4C3AE matches  
Binary file ./cache2/entries/152B4119E4C8B63CB3FB6EA01C60FEBF9A91F570 matches  
Binary file ./cache2/entries/BA8106F44A1A5CB18A39BBA7E62D9024E63E0072 matches  
Binary file ./cache2/entries/07CECF52C6AA6A86A7504C86E7967CC745646402 matches  
akmbp2:9w2xfa9b.default akrusts$ mate ./cache2/entries/BA8106F44A1A5CB18A39BBA7E62D9024E63E0072  
akmbp2:9w2xfa9b.default akrusts$  
akmbp2:9w2xfa9b.default akrusts$  
akmbp2:9w2xfa9b.default akrusts$  
akmbp2:9w2xfa9b.default akrusts$  
akmbp2:9w2xfa9b.default akrusts$  
akmbp2:9w2xfa9b.default akrusts$
```

Atrodam atbilstošu kešatmiņas failu


```
FE783B0C0909BA8...6072EAAA30DE1E89  BA8106F44A1A5CB1...E62D9024E63E0072  +
6 <link rel="stylesheet" type="text/css" media="screen" href="/assets/style.css?v=7">
7 <link rel="stylesheet" type="text/css" media="print" href="/assets/print-reset.css">
8 <link rel="stylesheet" type="text/css" media="print" href="/assets/print.css?v=1">
9
10 <link rel="shortcut icon" href="/favicon.ico">
11 </head>
12 <body>
13 <div id="main_content">
14 <!--[if IE 6]>
15 <div class="notice" id="ie6"><p>Jāsu pārlāķprogramma ir novecojusi, lāķdzu vai nu atjaunojiet savu pārlāķprogrammu vai izmantojiet Mozilla Firefox no
16 <![endif]-->
17 <div id="top" >
18 <div id="logo"><a href="/"></a></div>
19 <h1>MEDICAL DIAGNOSTICS <span>INFORMATION SYSTEM</span></h1>
20 <div id="lang_menu" >
21 <ul>
22 <li><a href="/lang/lv">Lat</a></li>
23 <li><a href="/lang/en">Eng</a></li>
24 <li class="last" ><a href="/lang/ru">Rus</a></li>
25 </ul>
26 </div>
27 <div class="clear" ></div>
28 </div>
29 <div id="header">
30 <div class="user">Patient: Krusts Agris, 03047 3</div>
31 <div id="nav" >
32 <ul>
33 <li class="last" ><a href="/logout" class="last">logout</a></li>
34 </ul>
35 </div>
36 <div class="clear" ></div>
37 </div>
38 <div id="status">
39 </div>
40 <div class="left_content" >
41 <div class="block" id="patient_documents" >
42 <div class="block_head" >
43 <h2>My studies</h2>
44 </div>
45 <div class="block_content" >
46 <p>No studies found</p>
47 </div>
48 </div>
```

Fails teksta redaktorā

```
EDVCHRT02 tH2LVj1ENdRkcm Q1bVqQbEW3Q550650p220tc1BBQ1ACF W0X173Hb1X1H0HbRdF W0Z17A21j EX1H0HbRdRd1X173BdgNVBA17C1bVCHRT02 tH2LVj1HkQMEg1bVqQbEW3Q550650p220tc
xGzAZBgNVBAMTEm5ldGJhbmsubm9yZGVhLmNvbTCBnzANBgkqhkiG9w0BAQEFAA0BjQAwYkCgYEAkQvfZtEoJd3Y7j2j7iXuiW/6RBdqrXIXrFxVSYbcbQCgxYUfAe3/aDCy09rmfGv6UXE+Bdx/DWuC9GH
LFc2ENpc4w9gbrb7FC04RpduHqsCrooKDPtVCSQ+kXq0VAoj6BLViWbrF8CAwEAAAMhMB8wHQYDVR0RBBywFIISbmV0YmFuay5ub3JkZWEuY29tMA0GCSqGSIb3DQEBCwUAA4GBAB398U1ELM5yIKo2Afiq9
774ArhbWqcNLqLKlKi+Qm6I27f60j6+VMQ6J7wCzqXReKRq+8R02anqbA8ZE7m1oCLnETkdy4Due4fpsgLPJ49FXMtG2RNjxc0VsU5oT9dn3XVAf6bFtAWCwC8DAwAAAAABAQAAAAAARub251AAAAEFJTQS1
od<NUL>POST<NUL>response-head<NUL>HTTP/1.1 302 Moved Temporarily
Date: Tue, 13 Mar 2018 14:00:58 GMT
Location:
https://api.datamed.lv/auth/nordea/return/ok/?B02K VERS=0002&B02K TIMESTMP=2002018031316002790&B02K IDNBR=636485&B02K STAMP=11482241711520949627&B02K CUSTNAI
B02K ALG=01&B02K CUSTID=03047. 3&B02K CUSTTYPE=01&B02K MAC=A14FA21C4C755F3F65C9718456F1868F
Content-Type: text/html
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 845
<NUL>original-response-headers<NUL>Connection: close
Date: Tue, 13 Mar 2018 14:00:58 GMT
Location:
https://api.datamed.lv/auth/nordea/return/ok/?B02K VERS=0002&B02K TIMESTMP=2002018031316002790&B02K IDNBR=636485&B02K STAMP=11482241711520949627&B02K CUSTNAI
B02K ALG=01&B02K CUSTID=03047. 03&B02K CUSTTYPE=01&B02K MAC=A14FA21C4C755F3F65C9718456F1868F
Content-Type: text/html
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Set-Cookie:
TS017c9029=01ab6b5143ab7feef9657e4a43718f846b8fb1495467620190d6cda6c87b43744db5dd1a5478cfa2faeb3f25c9f21a8cca423031fd775936d9a6fec237cec7691b1cd8aceb7992ac2
6f102f027c1d9c3f4a7b7cc9ee851a6176cbe5c9aee78ddc5c87e8ecfc27e83a1a06c4af9dbae0b5fe98bdca2973c224afe7ab7fe373338cb50a7b4; Path=/; Domain=.netbank.nordea.com;
Content-Length: 845
<NUL><NUL><NUL><NUL><NUL>
```

Bonuss: nedaudz autentifikācijas datu

Nedaudz par "*Sensitive data exposure*", kas nav minēts OWASP

588	https://stats.g.doubleclick.net	GET	/r/collect?t=dc&aip=1&r=3&v=1&...	✓		302	982	HTML	302 Moved	✓	64.233.165.154	lvp#lang=lv
592	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
593	https://www.latvija.lv	GET	/lv/PPK/Maja-un-vide			200	87151	HTML	Latvijas valsts portāls	✓	195.244.156.111	lvp#lang=lv; SC
595	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
599	https://www.latvija.lv	GET	/			200	95582	HTML	Latvijas valsts portāls	✓	195.244.156.111	SC_ANALYTICS_
601	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
605	https://bid.g.doubleclick.net	GET	/xbbe/pixel?d=KAE	✓		200	792	HTML		✓	74.125.205.155	
606	https://cm.g.doubleclick.net	GET	/pixel?google_nid=bidswitch_dbm&g...	✓		302	981	HTML	302 Moved	✓	172.217.18.130	
607	https://cm.g.doubleclick.net	GET	/pixel?google_nid=pubmatic&google_...	✓		302	1095	HTML	302 Moved	✓	172.217.18.130	
609	https://x.bidswitch.net	GET	/sync?dsp_id=16&user_id=CAESEOnl...	✓		302	703			✓	104.155.100.26	tuuid=94650e
610	https://x.bidswitch.net	GET	/ul_cb/sync?dsp_id=16&user_id=CA...	✓		302	632			✓	104.155.100.26	tuuid=94650e
612	https://www.latvija.lv	GET	/lv/PPK/Transports			200	84228	HTML	Latvijas valsts portāls	✓	195.244.156.111	lvp#lang=lv; SC
614	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
618	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
619	https://www.latvija.lv	GET	/lv/PPK/Transports/Darījumi-ar-tran...			200	392442	HTML	Latvijas valsts portāls	✓	195.244.156.111	lvp#lang=lv; SC
622	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
627	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
628	https://www.latvija.lv	GET	/			200	95582	HTML	Latvijas valsts portāls	✓	195.244.156.111	SC_ANALYTICS_
630	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
634	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
635	https://www.latvija.lv	GET	/Epakalpojumi/EP01/Apraksts			200	83796	HTML	Latvijas valsts portāls	✓	195.244.156.111	SC_ANALYTICS_
636	https://epakalpojumi.latvija.lv	GET	/STS/LVP.STS/IdentityProviders.js?ver...	✓		200	5565	script	js	✓	195.244.156.69	
638	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
642	https://www.latvija.lv	GET	/Epakalpojumi/EP01			200	96797	HTML	Latvijas valsts portāls	✓	195.244.156.111	SC_ANALYTICS_
644	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	✓		200	403	JSON		✓	195.244.156.111	lvp#lang=lv
645	https://epakalpojumi.latvija.lv	GET	/EServices/EP01-v1-1/Public/Lvp/Wr...	✓		200	1359	HTML		✓	195.244.156.69	LVP_Eservice_P
648	https://epakalpojumi.latvija.lv	GET	/EServices/EP01-v1-1/			302	3396	HTML	Object moved	✓	195.244.156.69	

Request Response

Raw Headers Hex HTML Render

```

HTTP/1.1 200 OK
P3P: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Date: Tue, 26 Sep 2017 11:11:01 GMT
Server: cafe
Cache-Control: private
X-XSS-Protection: 1; mode=block
Alt-Svc: quic=":443"; ma=2592000; v="39,38,37,35"
Accept-Ranges: none
Vary: Accept-Encoding
Connection: close

```

472	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
473	https://epakalpojumi.latvija.lv	GET	/STS/LVP.STS/IdentityProviders.js?ver...	☒	☐	200	5576	script	js
475	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
477	https://stats.g.doubleclick.net	GET	/r/collect?t=dc&aip=1&r=3&v=1&_...	☒	☐	302	982	HTML	
478	https://static.hotjar.com	GET	/c/hotjar-147868.js?sv=5	☒	☐	304	338	script	js
482	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
483	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
484	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
485	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
486	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
487	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
488	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	
489	https://www.latvija.lv	GET	/lv/Ajax/NetPipe/Counters/GetCount...	☒	☐	200	403	JSON	

RequestResponse

RawParamsHeadersHex

```

GET /r/collect?t=dc&aip=1&r=3&v=1&_v=j63&tid=UA-59465409-1&cid=2014358171.1506423588&jid=1072053006&gjid=1670770424&_gid=19249608
Host: stats.g.doubleclick.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://www.latvija.lv/Epakalpojumi/EP149/Apraksts
Cookie: IDE=AHWqTUmY0hCF9gLzad0ZMHEDiLZaKupTwap5Zqb0qc87dS9XtqBNQ1q7U8-11Lm6
Connection: close

```


XML External Entities

- Atsevišķa kategorija
- Reti sastopama Latvijā
- Izskatās līdzīgi ...

```
<?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>
```

Broken Access Control

Systems

Direktoriju apstaigāšana (../)	1%
Autorizācijas apiešana	9%
Tieša piekļuve objektiem	11%

invoice.pdf – Tor Browser

File Edit View History Bookmarks Tools Help

invoice.pdf

lv/files/orders/1301/invoice.pdf

Startpage HTTPS

Page: 1 of 1 Automatic Zoom



PASŪTĪJUMA RĒĶINS

Datums: 22.06.2014
Rēķina Nr. WBI436

Piegādātājs
Reģ. Nr.
Adrese
Banka
Kods
Konts

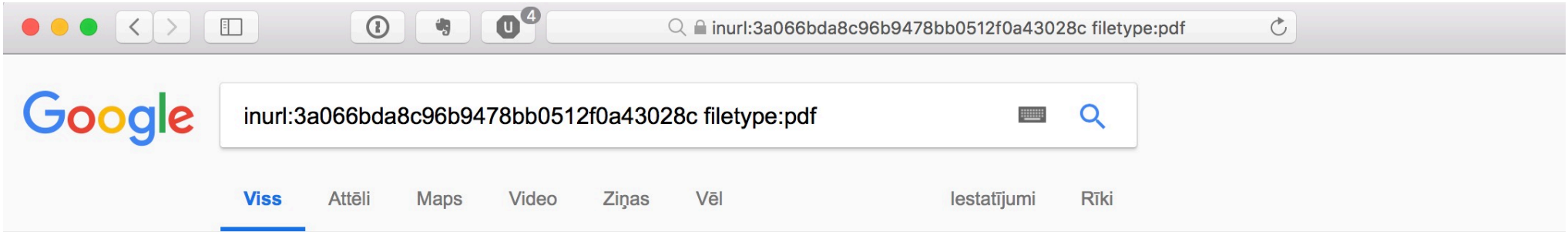
The White Book, SIA
50103429851
Tukuma iela 6, Rīga, LV-1002
AS Citadele banka
PARXLV22
LV74PARX0013271560001

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

21-51, Rīga

karti

Nr.	Nosaukums	Mērv.	Daudz.	Cena bez PVN	PVN	Cena ar PVN	Summa ar PVN
1	"Būs citi sūdi, šie aizmirsīsies"	gab.	1	3.57	12%	4.00	4.00
2	"Atslābsti un iedzer"	gab.	1	3.57	12%	4.00	4.00
3	"Krīti panikā un baidies"	gab.	1	3.57	12%	4.00	4.00
	Piegāde Latvijas teritorijā pa pastu		1	0.00	21%	0.00	0.00
Kopsumma bez PVN							10.71
Piegāde							0.00



[PDF] Resume Submission - asddddd

Page 1. asddddds. February 09, 2016 mosa hassan@beeieg.com. 1232312345235 (Other). Page 1/1.
2016-02-09 10:05:03.

okd.ukrintei.ua/view/okd/3a066bda8c96b9478bb0512f0a43028c ▼ Tulkot šo lapu

2018. gada 1. marts - Дисертація присвячена дослідженню можливості спекулятивного обґрунтування суб'єктивності («Я») та з'ясуванню епістемічного значення спекулятивного методу в контексті сучасних дискусій щодо апорій у самообґрунтуванні знання про себе. Дослідження являє собою спробу дати ...

www.dansservices.com/index/.../3a066bda8c96b9478bb0512f0a43028... ▼ Tulkot šo lapu

Date of Birth : February 24, 1985. Marital Status : Single. Current Age : 33 Years Old. Place of Birth : South Cotabato. No. of Children : none. Religion : Christian. Ages of Children : 0 to 0. Height: 151.00cm. Weight: 68.00kg. Educational Background : Bachelors Degree. Other Education/ Training : Recommended Salary : S\$.

www.shortbio.org/.../id/3a066bda8c96b9478bb0512f0a43028c.m8 ▼ Tulkot šo lapu

M.Eng.&Tech. Viktor Dmitriyev has graduated from Kazakh-British Technical University (KBTU), Kazakhstan in 2009 with the diploma in the Computer Systems and Software Engineering. He got his degree Master of. Information Systems in Engineering and Technology in 2010 from KBTU. Viktor Dmitriyev worked as an.

thekvinnatillkvinnafoundation.org/.../3a066bda8c96b9478bb0512f0a4... ▼ Tulkot šo lapu

5 Preface. 6 Introduction. 10 Background. 14 Organising for Peace. 18 Making Room for Change. 19 Challenging national identities. 21 Freedom from fear. 22 Creating space for return and reconciliation. 26 Crossing Borders. 28 Room for conversation. 32 Opening Doors for Activism. 32 Strengthening civil society and ...

Broken Access Control

- Autorizācijas problēmas kopumā samazinājušās no 40%
- Tieša piekļuve samazinājusies no 33% līdz 11%

Security Misconfiguration

	Systems
Konfigurācijas kļūdas	17%
Rezerves kopijas, nereferecēti faili ar sensitīvu informāciju u.c.	13%
Piekļuve administrācijas saskarnēm	9%
Iztrūkst HSTS galvenes	26%

Using Components with Known Vulnerabilities

- 239 komponenti 130 sistēmās!

Drupalgeddon

Drupal 7 and 8 core highly critical release on March 28th, 2018 PSA-2018-001

Posted by [Drupal Security Team](#) on *21 Mar 2018 at 19:13 UTC*

- Advisory ID: DRUPAL-PSA-2018-001
- Project: Drupal Core
- Version: 7.x, 8.x
- Date: 2018-March-21

Description

There will be a security release of **Drupal 7.x, 8.3.x, 8.4.x, and 8.5.x on March 28th 2018 between 18:00 – 19:30 UTC**, one week from the publication of this document, that will fix a highly critical security vulnerability. The Drupal Security Team urges you to reserve time for core updates at that time because exploits *might* be developed within hours or days. Security release announcements will appear on the [Drupal.org security advisory page](#).

While Drupal 8.3.x and 8.4.x are no longer supported and we don't normally provide security releases for [unsupported minor releases](#), given the potential severity of this issue, we *are* providing 8.3.x and 8.4.x releases that include the fix for sites which have not yet had a chance to update to 8.5.0. The Drupal security team strongly recommends the following:

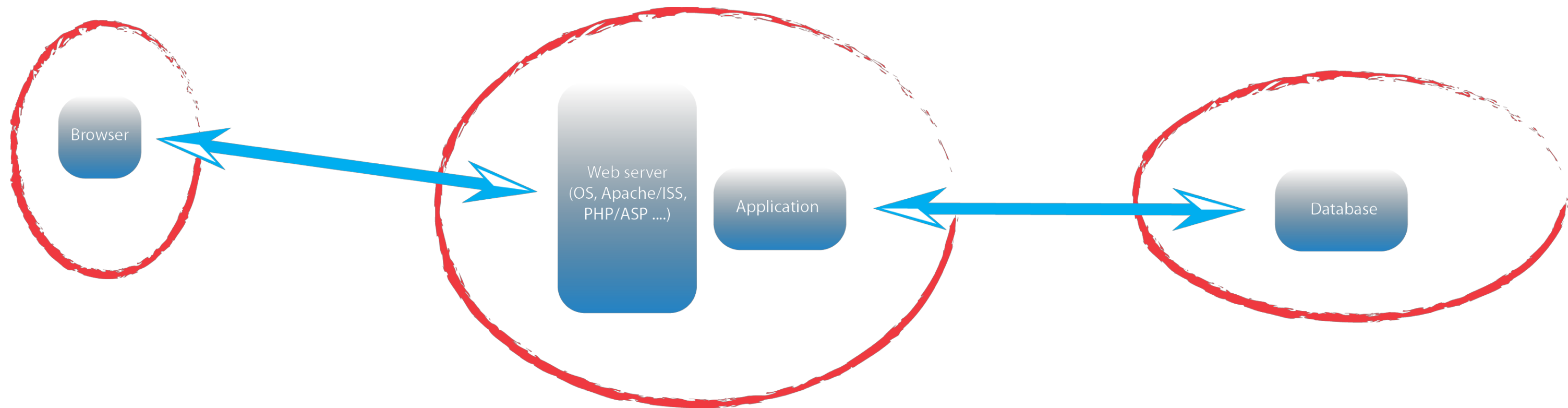
Cross-site scripting

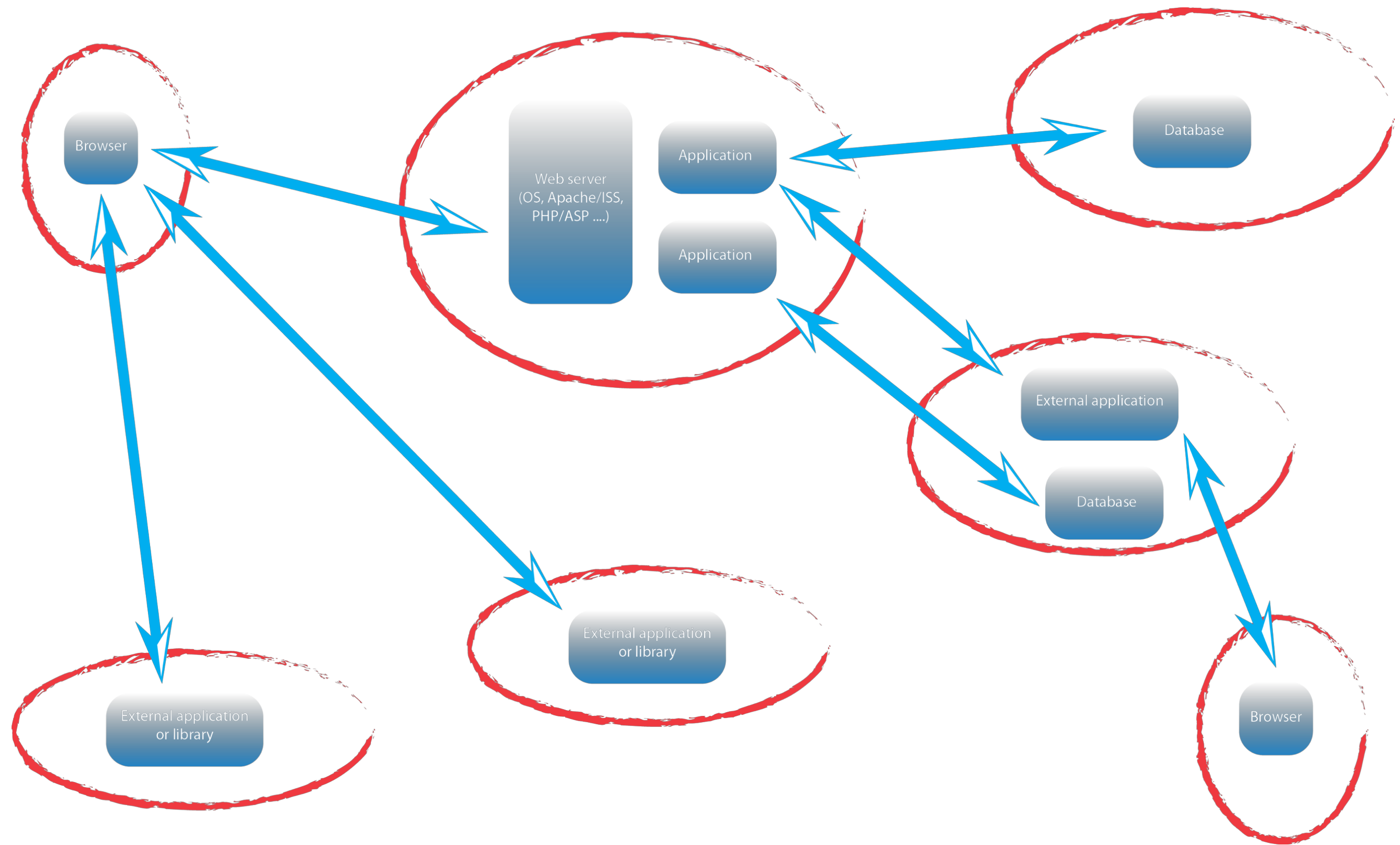
Systems

Dinamiskā	21%
DOM bāzētā	7%
Paliekošā	18%

Cross-site scripting

- Dinamiskā samazinājās no 46% un paliekošā no 36%
- Dinamiskā ir ar mazu risku, jo lielākā daļa pārlūko to bloķē
- Risks palielinās, jo dati parasti "ceļo" starp sistēmām





Kopsavilkums

Problēmu skaits

A1: Injection	10
A2: Broken Authentication and session management	134
A3 Sensitive Data Exposure	89
A4: XML External Entities	2
A5: Broken Access Control	27
A6: Security Misconfiguration	97
A7: Cross-Site Scripting	59
A9: Using Components with Known Vulnerabilities	239

Citi novērojumi

- Tīmekļa lietojumi paliek drošāki, vismaz daži
 - Visticamāk pateicoties ietvadiem
 - Bieži sistēmas drošība ir atkarīga no tā kuri izstrādātāji to ir viedojuši
- Drošības problēmas paliek ar vien grūtāk atrast un izmantot
- Jo jaunāka tehnoloģija, jo biežāk tā tiek ieviesta nedroši

Paldies par uzmanību!

Jautājumi!

P.S. Meklējam jaunus kolēģus

Agris.Krusts@itcentrs.lv, Twitter: @agris_krusts, +371 29151412