Root via XSS

Positive Technologies

November 2011

POSITIVE TECHNOLOGIES

How To Get into Troubles

Popular builds for web development:

- **Denwer;**
- **XAMPP;**
- **AppServ.**

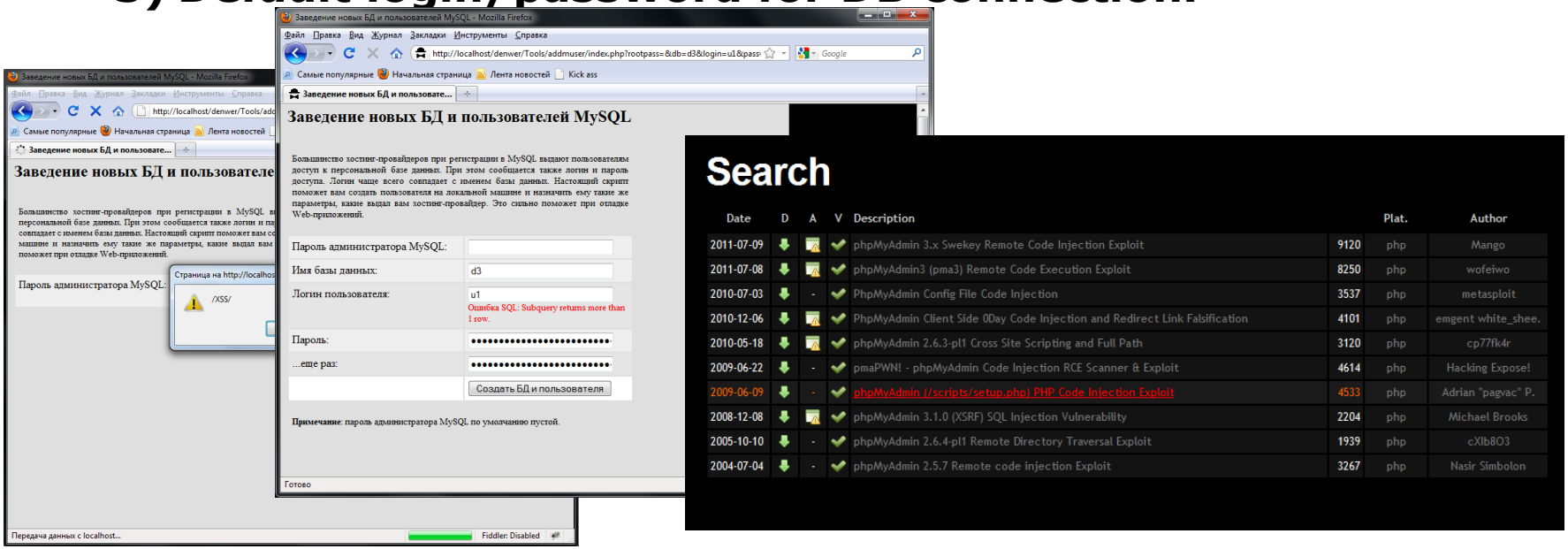
How to Use Them

Peculiarities:

- **usually run automatically;**
- **contain phpMyAdmin;**
- **have weak passwords;**
- **have full rights (for Windows systems);**
- **contain vulnerabilities;**
- **operate legitimately without alerting antiviruses.**

Denwer

- **Current versions have the following vulnerabilities:**
  1) **Service scripts: XSS and SQL Injection;**
  2) **PhpMyAdmin 3.2.3 (CVE 2011-2505, 2009-1151, and etc.);**
  3) **Default login/password for DB connection.**



Denwer XSS

Peculiarities:

- is present in the BD creation script;
- all parameters are vulnerable;
- is convenient for bypassing browser protections.

Examples:

- Chrome - /index.php?eBadRootPass=<script>/*&eSqlError=*/alert('XSS');</script>
- IE – /index.php?eBadRootPass=<img%0donerror=alert(1)%20src=s%20/>
- FF - /index.php?eBadRootPass=<script>alert(/XSS/);</script>

Using XSS

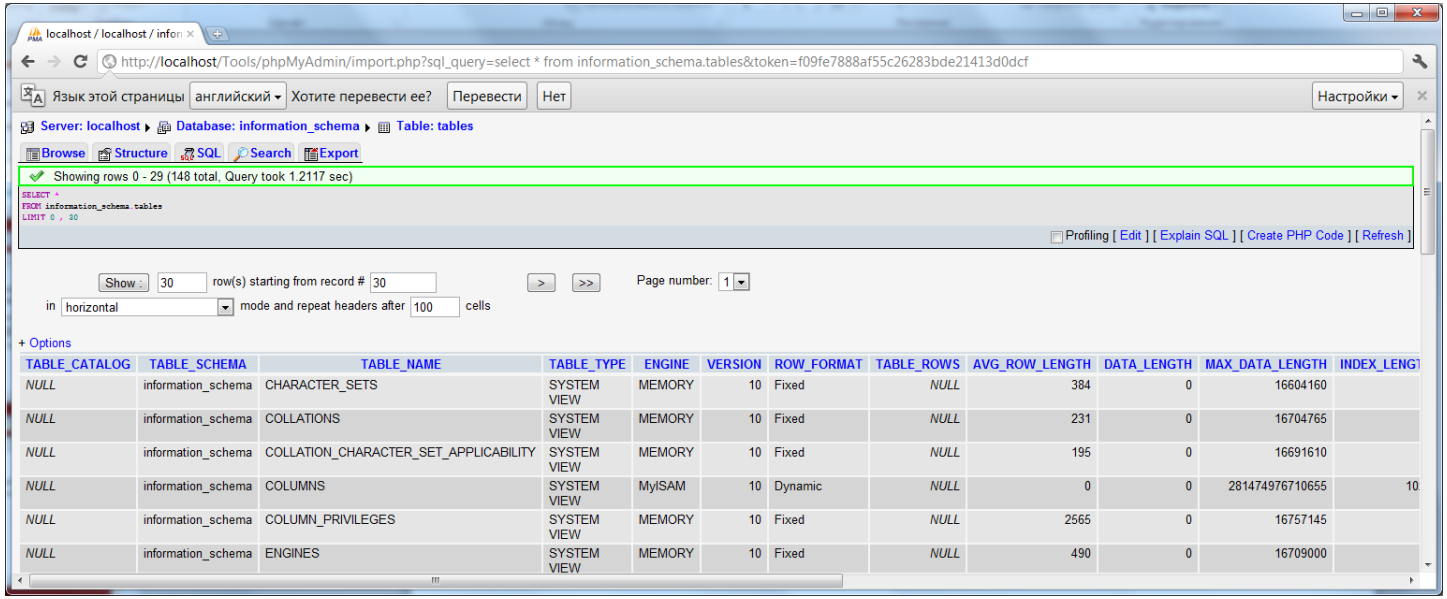
Implementation stages:

- **upload your JS file by means of XSS;**
- **add the SCRIPT tag into the HEAD to upload the file dynamically;**
- **the commands are passed over according to the reverse shell principle;**
- **Use a standard AJAX to address the scripts on the localhost;**
- **Use JSONP to address the script backconnect;**
- **Hide it in the IFRAME tag of the site.**

Operating PhpMyAdmin

Peculiarities:

- requires no authentication for the entrance;
- uses a token transferred in the body of the HTML response;
- you need just to pass over the token in the GET request to implement the SQL requests.



TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	VERSION	ROW_FORMAT	TABLE_ROWS	AVG_ROW_LENGTH	DATA_LENGTH	MAX_DATA_LENGTH	INDEX_LENG
NULL	information_schema	CHARACTER_SETS	SYSTEM VIEW	MEMORY	10	Fixed	NULL	384	0	16604160	
NULL	information_schema	COLLATIONS	SYSTEM VIEW	MEMORY	10	Fixed	NULL	231	0	16704765	
NULL	information_schema	COLLATION_CHARACTER_SET_APPLICABILITY	SYSTEM VIEW	MEMORY	10	Fixed	NULL	195	0	16691610	
NULL	information_schema	COLUMNS	SYSTEM VIEW	MyISAM	10	Dynamic	NULL	0	0	281474976710655	10
NULL	information_schema	COLUMN_PRIVILEGES	SYSTEM VIEW	MEMORY	10	Fixed	NULL	2565	0	16757145	
NULL	information_schema	ENGINES	SYSTEM VIEW	MEMORY	10	Fixed	NULL	490	0	16709000	

Access to the File System

Access to DB with root rights:

- granted rights on reading/writing files;
- MySQL located at the victim's home system.

Convenient to use:

- Use INTO OUTFILE to create a PHP web shell;
- After executing each request from JavaScript, the shell automatically deletes itself;
- No need to store the shell since, in general case, it is inaccessible from the outside (by default, Apache in Denwer processes only requests from localhost).

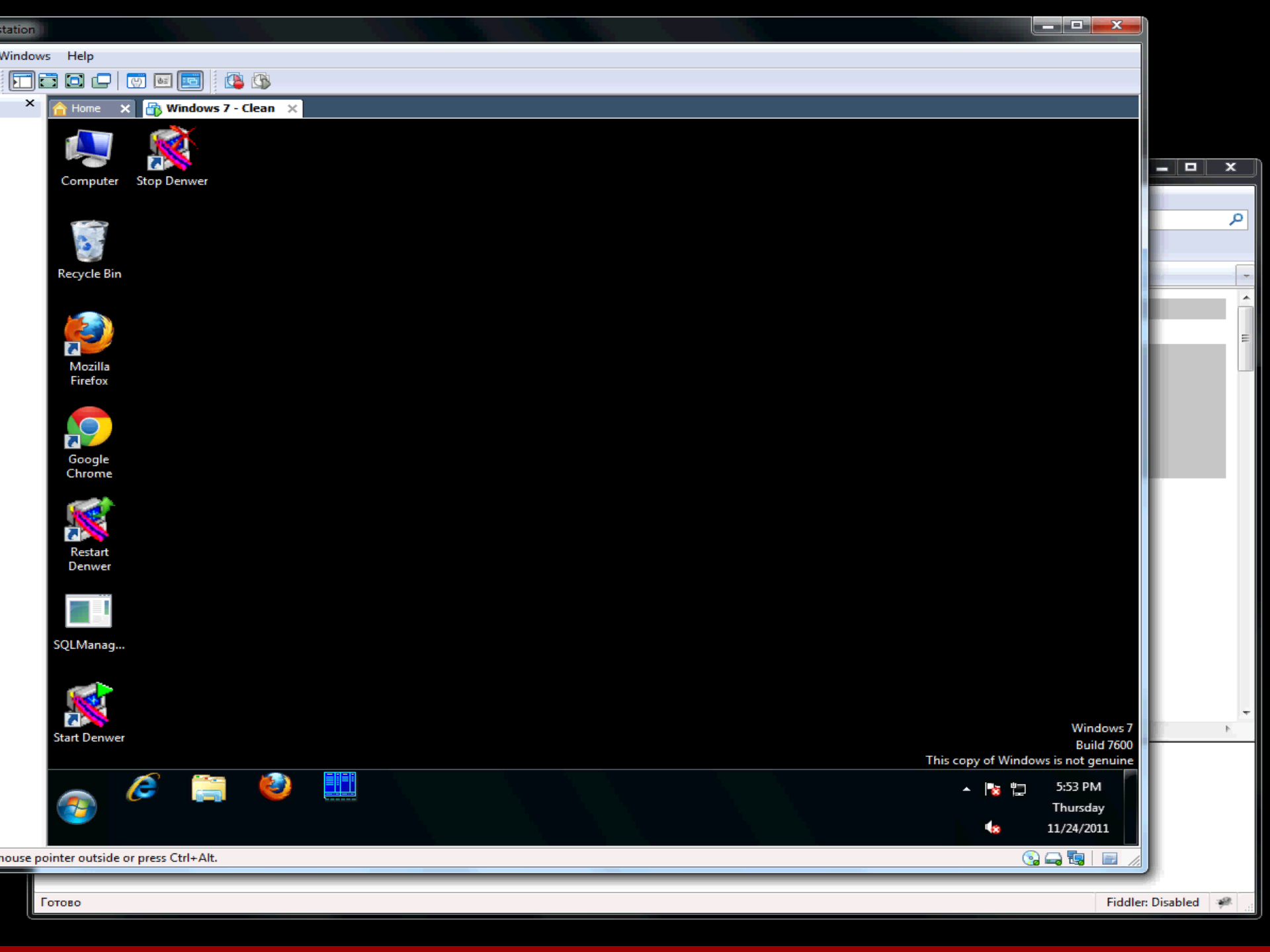
Implementing the Attack

Approach:

- user opens the attacker's page;
- the script is uploaded to IFRAME via XSS;
- the script requests commands from JSONP, its control server;
- when the command is received, the script addresses PhpMyAdmin to get a token, and then sends an SQL request for creating a web shell file;
- the web shell executes the command and deletes itself.

Hard-Coded Commands

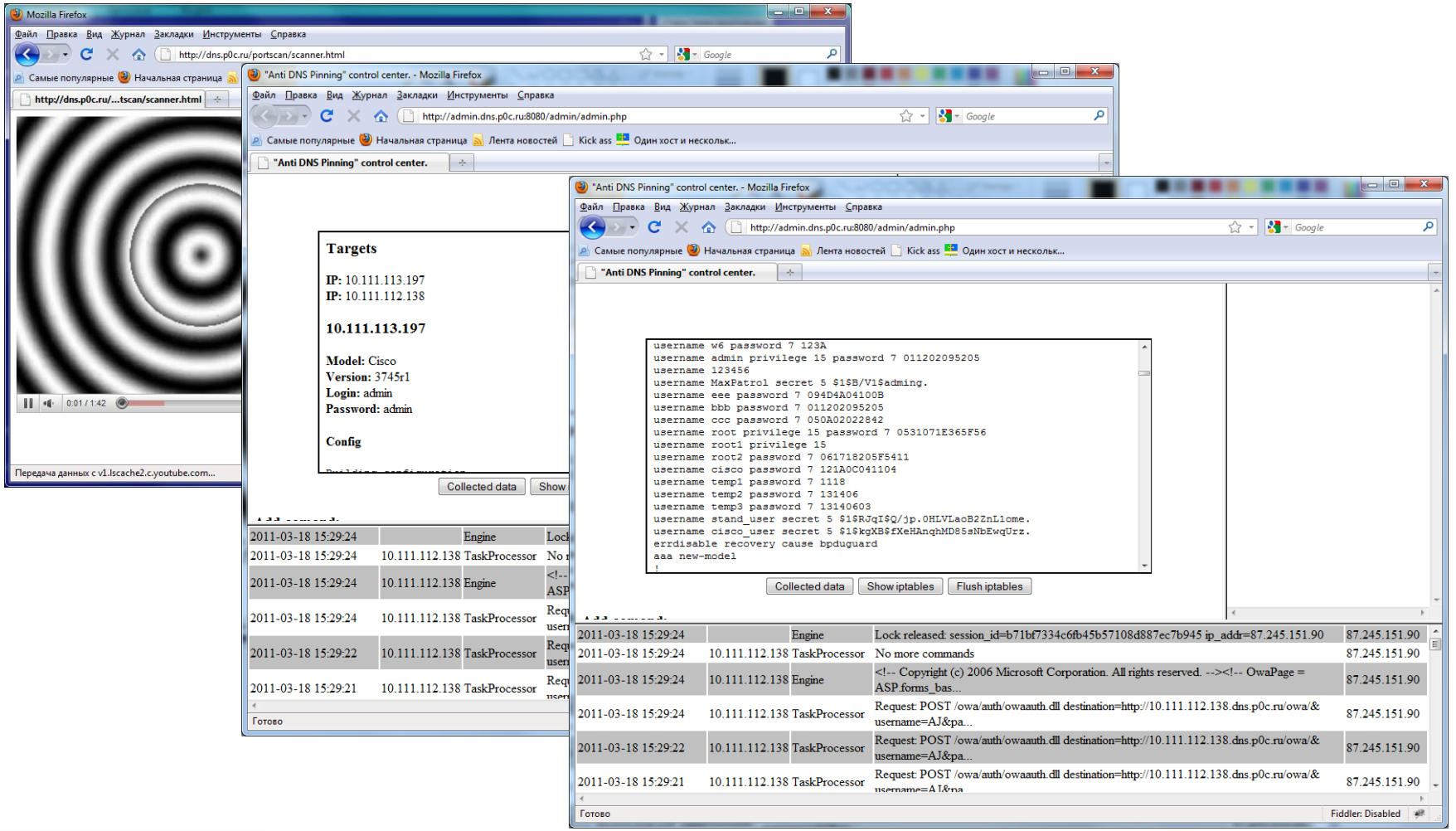
- **The script allows hard-coding the following:**
  - **certain sites and an IP router to visit (CSS History Hack);**
  - **a list of hard disks to obtain:**
    «echo list volume|diskpart»;
  - **ipconfig /ALL;**
  - **values of the environment variables to obtain;**
  - **a list of sites on the local system;**
  - **the obtained data can be processed on a Client to bypass directories automatically and for other reasons.**


Windows
Help
Home
Windows 7 - Clean
Computer
Stop Denwer
Recycle Bin
Mozilla Firefox
Google Chrome
Restart Denwer
SQLManag...
Start Denwer
Windows 7
Build 7600
This copy of Windows is not genuine
5:53 PM
Thursday
11/24/2011
house pointer outside or press Ctrl+Alt.
Готово
Fiddler: Disabled

Protection Against Attacks

- **Keep an eye on application updates, even on those used in builds**
- **Check the default configuration before using a program**
- **Use browser plugins analogous to «Noscript»**
- **For browser developers: use zone division**

Questions?



POSITIVE TECHNOLOGIES

Thank you for your attention!

dbaranov@ptsecurity.ru

POSITIVE TECHNOLOGIES