

# 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.**



## 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.

Заведение новых БД и пользователей MySQL

Большинство хостинг-провайдеров при регистрации в MySQL выдают пользователям доступ к персональной базе данных. При этом сообщается также логин и пароль доступа. Логин чаще всего совпадает с именем базы данных. Настоящий скрипт поможет вам создать пользователя на локальной машине и назначить ему такие же параметры, какие выдал вам хостинг-провайдер. Это сильно поможет при отладке Web-приложений.

Пароль администратора MySQL:

Имя базы данных: d3

Логин пользователя: u1

Пароль:

...еще раз:

Примечание: пароль администратора MySQL по умолчанию пустой.

Готово

Страница на http://localhost/

Передан данные с localhost...

Fiddler: Disabled

### Search

Date	D	A	V	Description	Plat.	Author
2011-07-09	↓	✓	✓	phpMyAdmin 3.x Swekey Remote Code Injection Exploit	9120	php Mango
2011-07-08	↓	✓	✓	phpMyAdmin3 (pma3) Remote Code Execution Exploit	8250	php wofeiwo
2010-07-03	↓	-	✓	PhpMyAdmin Config File Code Injection	3537	php metasploit
2010-12-06	↓	✓	✓	PhpMyAdmin Client Side 0Day Code Injection and Redirect Link Falsification	4101	php emgent white_shee.
2010-05-18	↓	✓	✓	phpMyAdmin 2.6.3-p11 Cross Site Scripting and Full Path	3120	php cp77fk4r
2009-06-22	↓	-	✓	pmaPWN! - phpMyAdmin Code Injection RCE Scanner & Exploit	4614	php Hacking Expose!
2009-06-09	↓	-	✓	phpMyAdmin (/scripts/setup.php) PHP Code Injection Exploit	4533	php Adrian "pagrac" P.
2008-12-08	↓	✓	✓	phpMyAdmin 3.1.0 (XSRF) SQL Injection Vulnerability	2204	php Michael Brooks
2005-10-10	↓	-	✓	phpMyAdmin 2.6.4-p11 Remote Directory Traversal Exploit	1939	php cXib803
2004-07-04	↓	-	✓	phpMyAdmin 2.5.7 Remote code injection Exploit	3267	php Nasir Simbolon



## 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>](#)



## Implementation stages:

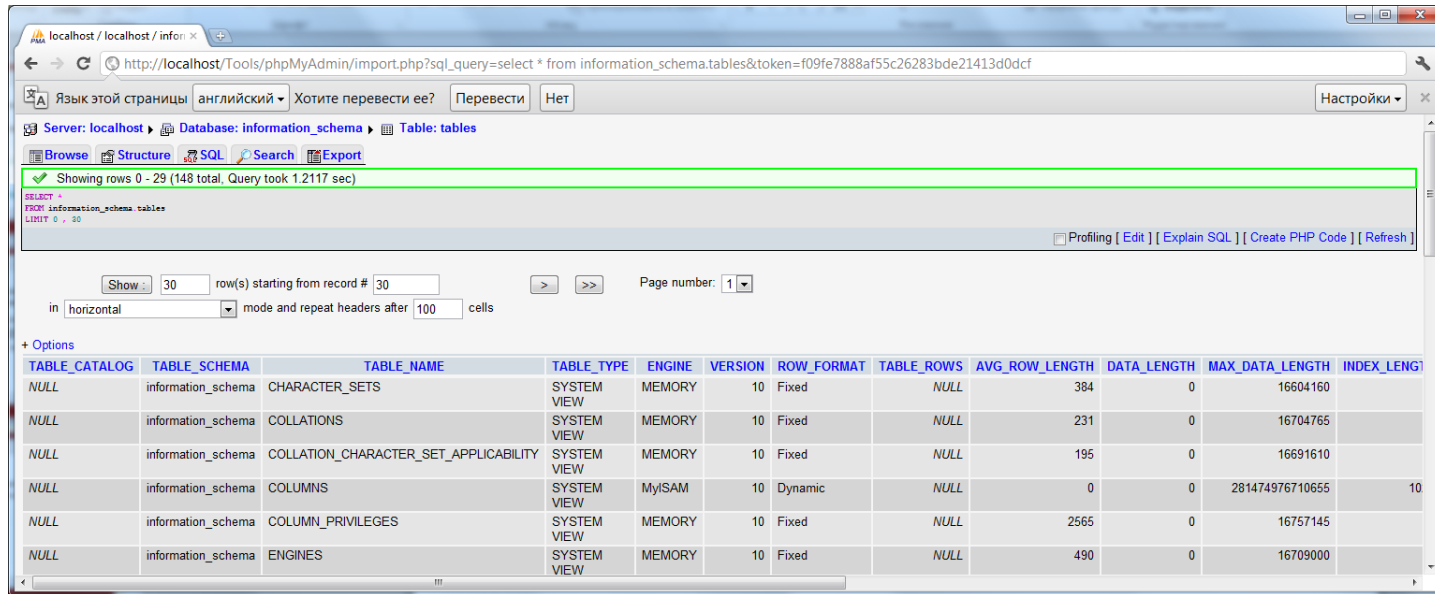
- **upload your JS file by means of XSS;**
- **add the SCRIPT tag into the HEAD to upload the file dynamically;**
- **the commands are passed over according to the reverse shell principle;**
- **Use a standard AJAX to address the scripts on the localhost;**
- **Use JSONP to address the script backconnect;**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



The screenshot shows the PhpMyAdmin interface in a browser window. The address bar contains the URL: `http://localhost/Tools/phpMyAdmin/import.php?sql_query=select * from information_schema.tables&token=f09fe7888af55c26283bde21413d0dcf`. The page title is "Server: localhost Database: information\_schema Table: tables". The main content area displays a table listing with the following data:

TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	VERSION	ROW_FORMAT	TABLE_ROWS	AVG_ROW_LENGTH	DATA_LENGTH	MAX_DATA_LENGTH	INDEX_LENGTH
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:

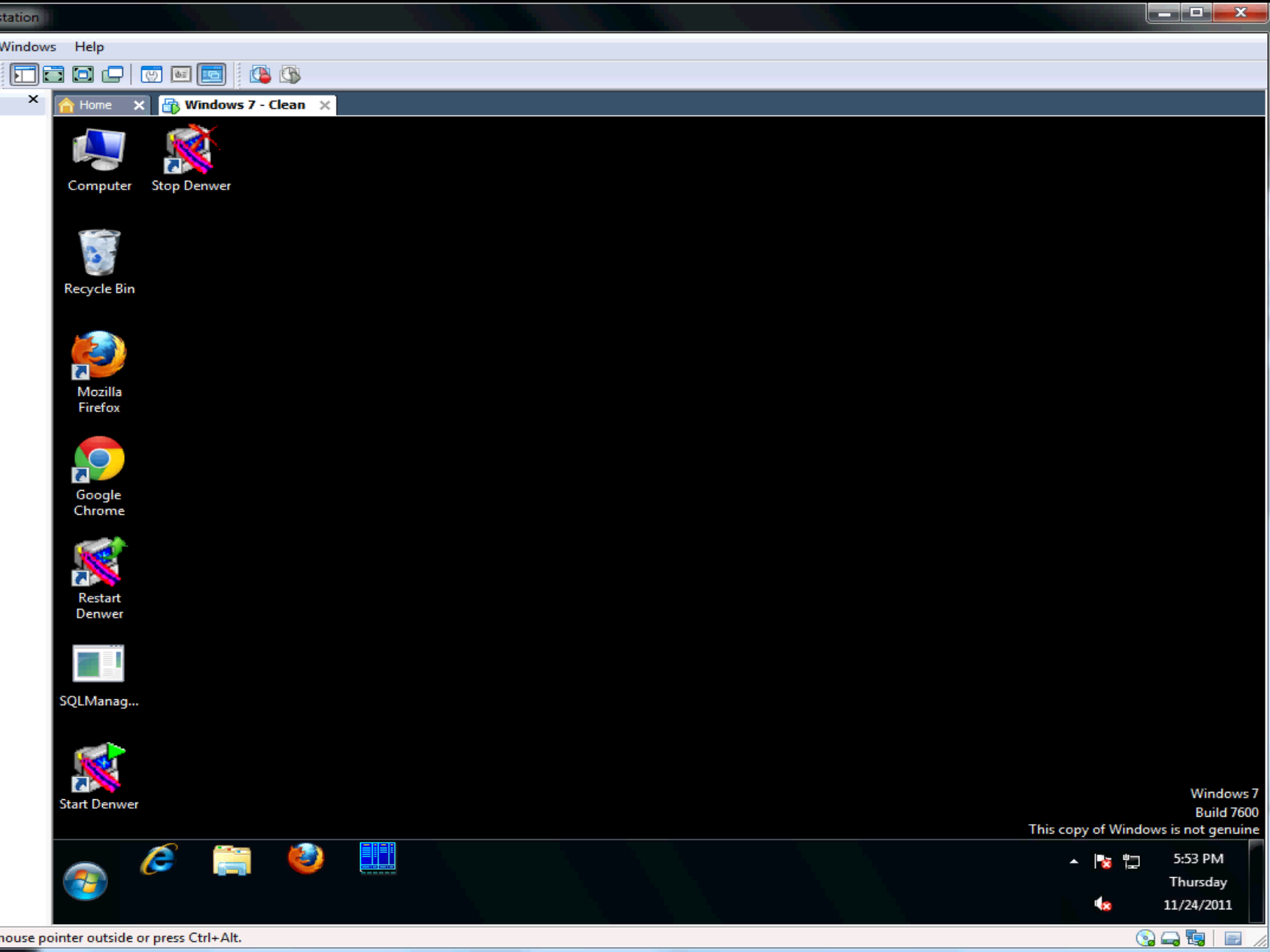
- **user opens the attacker's page;**
- **the script is uploaded to IFRAME via XSS;**
- **the script requests commands from JSONP, its control server;**
- **when the command is received, the script addresses PhpMyAdmin to get a token, and then sends an SQL request for creating a web shell file;**
- **the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









mouse 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?

**Targets**

IP: 10.111.113.197  
IP: 10.111.112.138

**10.111.113.197**

Model: Cisco  
Version: 3745r1  
Login: admin  
Password: admin

**Config**

```
username w6 password 7 123A
username admin privilege 15 password 7 011202095205
username 123456
username MaxPatrol secret 5 $1$B/V1$adming.
username eee password 7 094D4A04100B
username bbb password 7 011202095205
username ooo password 7 050A02022842
username root privilege 15 password 7 0531071E365F56
username root1 privilege 15
username root2 password 7 061718205F5411
username cisco password 7 121A0C041104
username temp1 password 7 1118
username temp2 password 7 131406
username temp3 password 7 13140603
username stand_user secret 5 $1$RjQI$9Q/jp.0HLVLaoB2ZnL1cme.
username cisco_user secret 5 $1$kgXB$fxeHAnqhMD85aNbEwgUrz.
errdisable recovery cause bpduguard
aaa new-model
!
```

2011-03-18 15:29:24		Engine	Lock
2011-03-18 15:29:24	10.111.112.138	TaskProcessor	No
2011-03-18 15:29:24	10.111.112.138	Engine	<!-- ASP
2011-03-18 15:29:24	10.111.112.138	TaskProcessor	Req
2011-03-18 15:29:22	10.111.112.138	TaskProcessor	Req
2011-03-18 15:29:21	10.111.112.138	TaskProcessor	Req

2011-03-18 15:29:24	Engine	Lock released: session_id=b71bf7334c6fb45b57108d887ec7b945 ip_addr=87.245.151.90	87.245.151.90	
2011-03-18 15:29:24	10.111.112.138	TaskProcessor	No more commands	87.245.151.90
2011-03-18 15:29:24	10.111.112.138	Engine	<!-- Copyright (c) 2006 Microsoft Corporation. All rights reserved. --><!-- OwaPage = ASP forms_bas...	87.245.151.90
2011-03-18 15:29:24	10.111.112.138	TaskProcessor	Request POST /owa/auth/owaauth.dll destination=http://10.111.112.138.dns.p0c.ru/owa/&username=AJ&pa...	87.245.151.90
2011-03-18 15:29:22	10.111.112.138	TaskProcessor	Request POST /owa/auth/owaauth.dll destination=http://10.111.112.138.dns.p0c.ru/owa/&username=AJ&pa...	87.245.151.90
2011-03-18 15:29:21	10.111.112.138	TaskProcessor	Request POST /owa/auth/owaauth.dll destination=http://10.111.112.138.dns.p0c.ru/owa/&username=AJ&pa...	87.245.151.90



# Thank you for your attention!

[dbaranov@ptsecurity.ru](mailto:dbaranov@ptsecurity.ru)



POSITIVE TECHNOLOGIES