Безопасность сайта

Факультет Интернета МФПУ СИНЕРГИЯ

Курс «Веб-разработка»

Илья Ершов

Зачем взламывают сайты?

- Заражение страниц сайта вирусами для последующих атак посетителей
- Взлом базы данных сайта, кража конфиденциальной информации
- Взлом сайта для размещения SEO ссылок
- Заказной взлом сайта
- Подмена информации на сайте
- Создание распределённой вычислительной сети

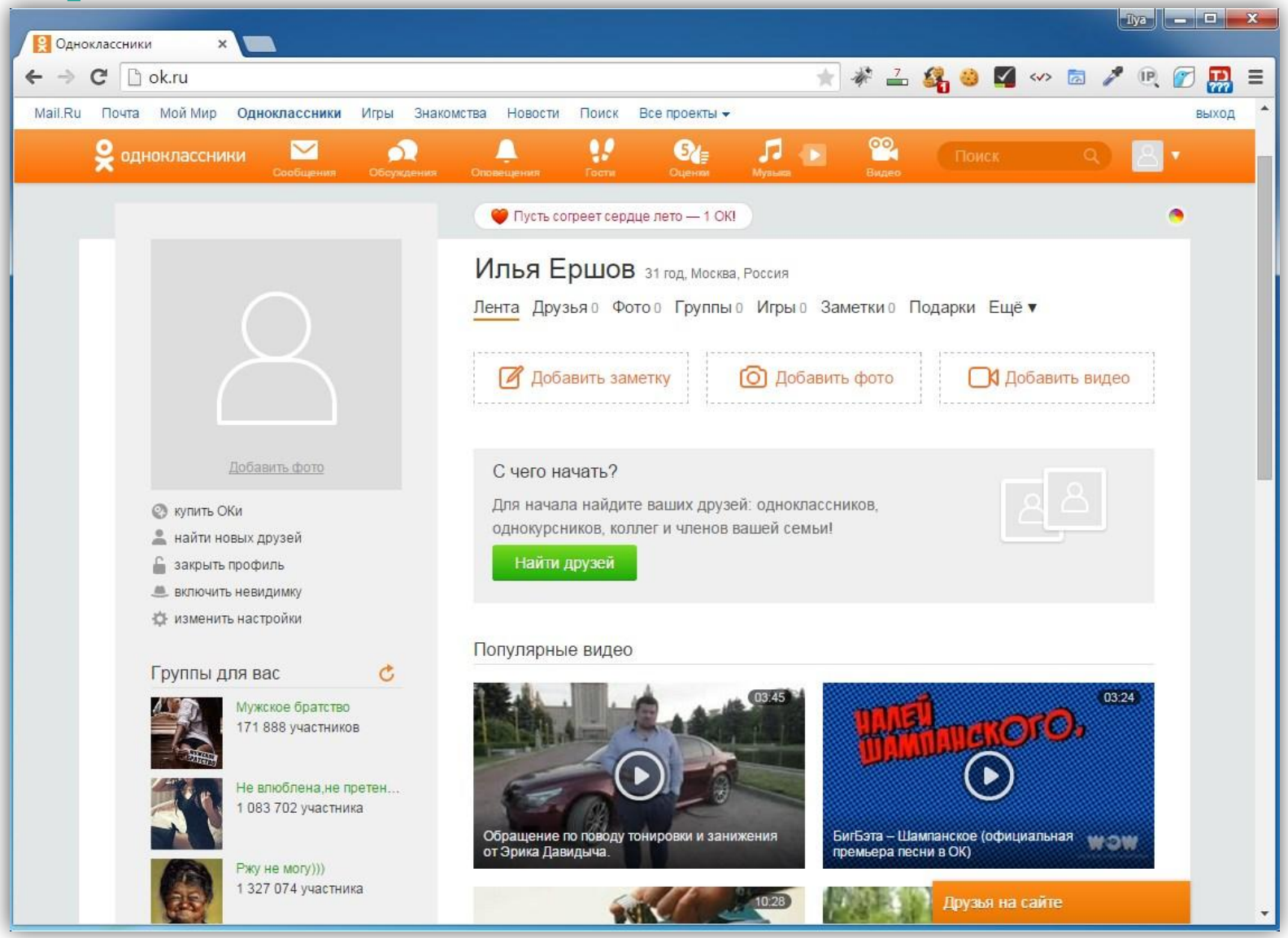
Как взламывают сайты?

1. Человеческий фактор
2. Подбор пароля
3. Кража Cookie
4. Подброс исполняемых файлов на хостинг
    1. Шеллы
    2. Вирусы
5. SQL-инъекция
    a) Для извлечения пароля админа
    b) Для прямого манипулирования БД
    c) Для подброса на сервер исполняемых файлов
7. Уязвимости серверного ПО

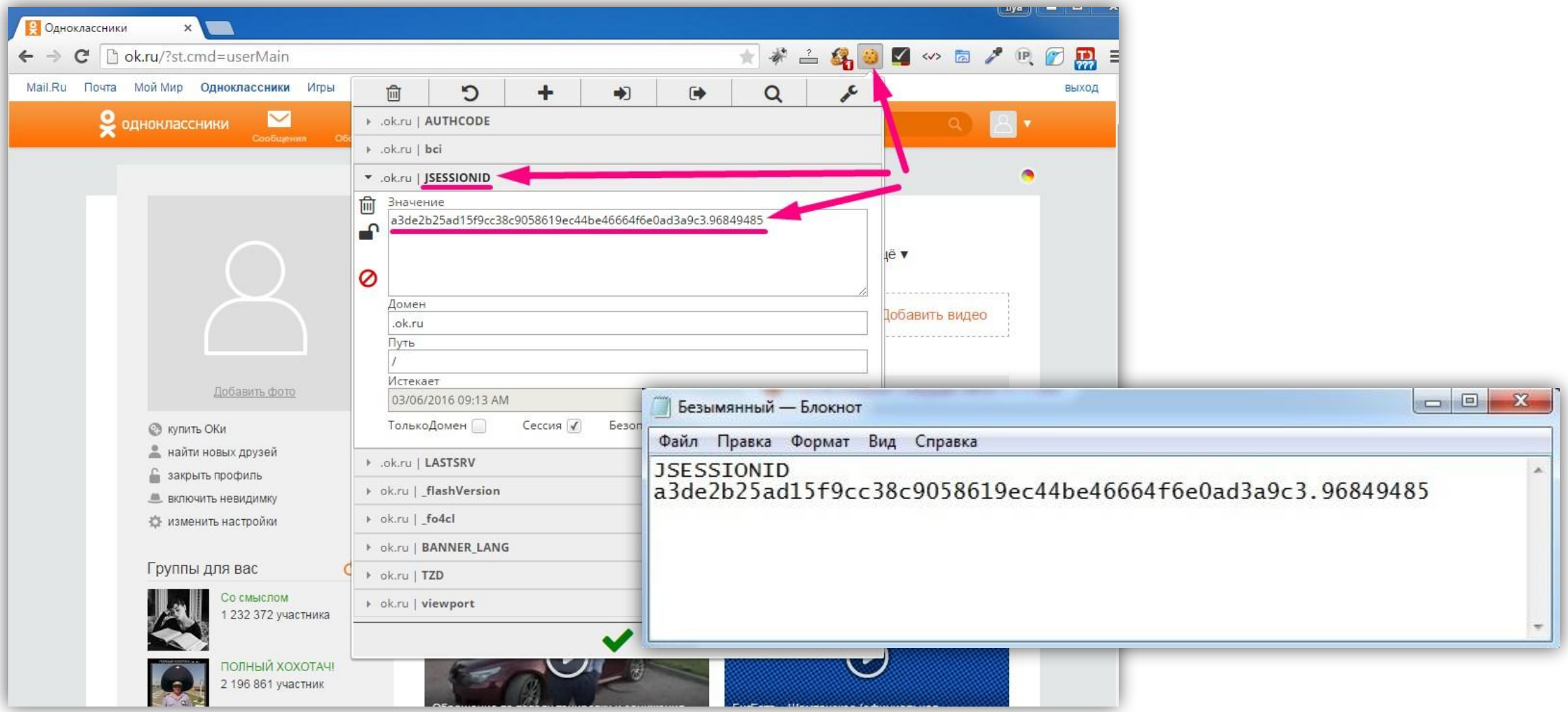
Как защититься?

1. Фильтруйте все данные поступающие от пользователей
2. Меняйте префиксы таблиц базы данных
3. Переопределяйте путь к админке
4. Закрывайте к уязвимым разделам доступ по IP адресу
5. Протоколируйте попытки проникновения
6. Обновляйте всё ПО

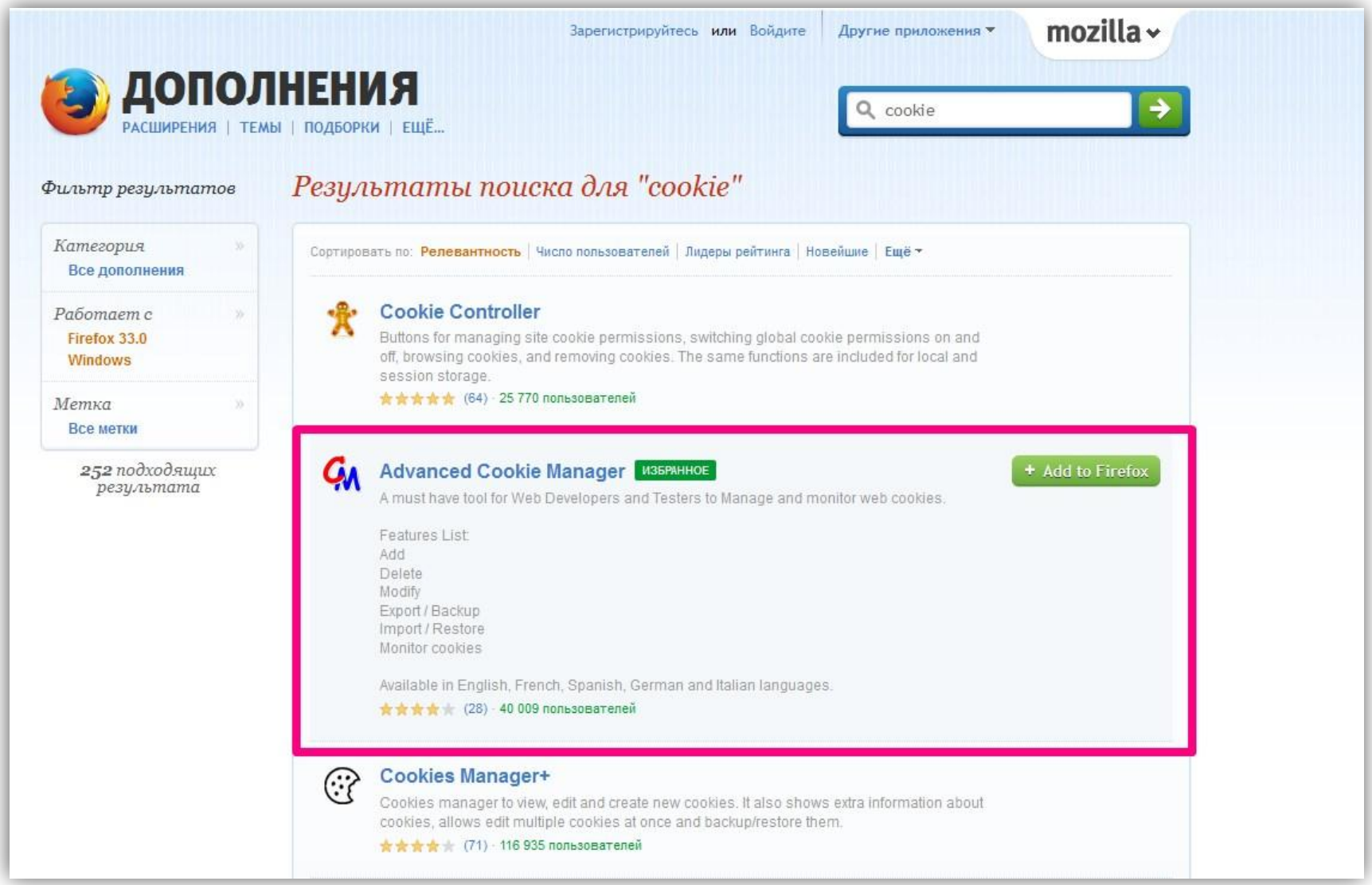
Кража Cookie



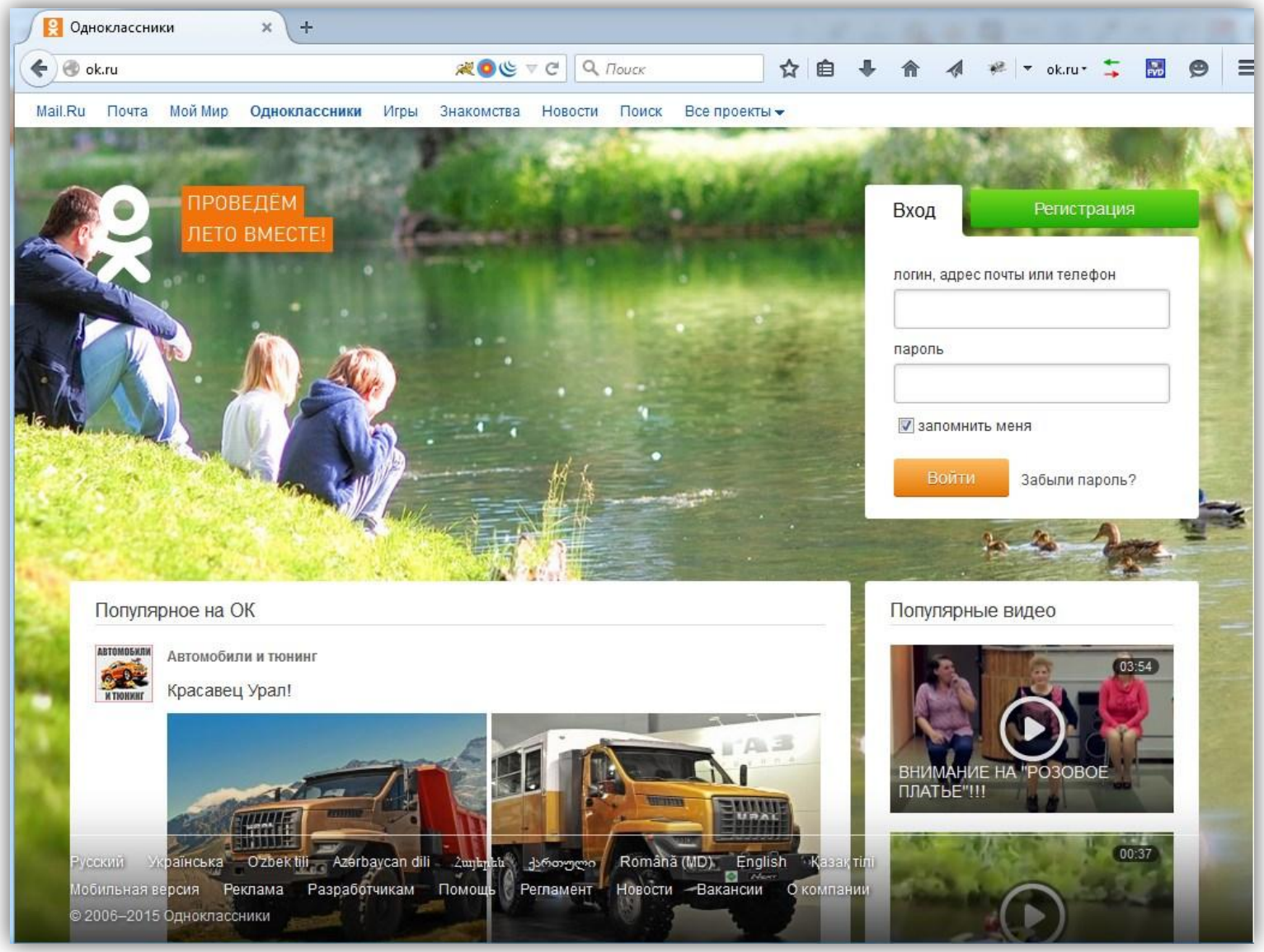
Кража Cookie



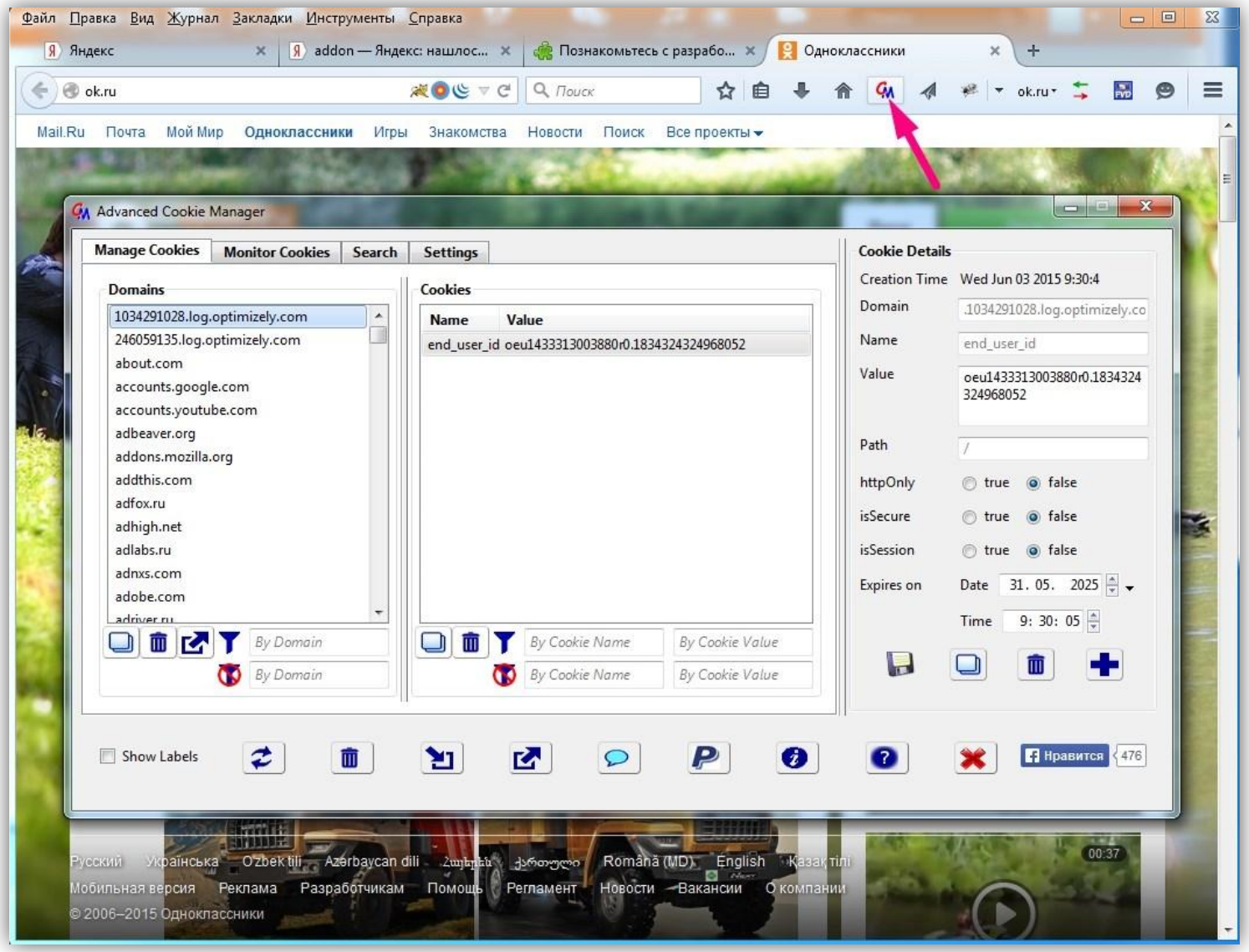
Кража Cookie



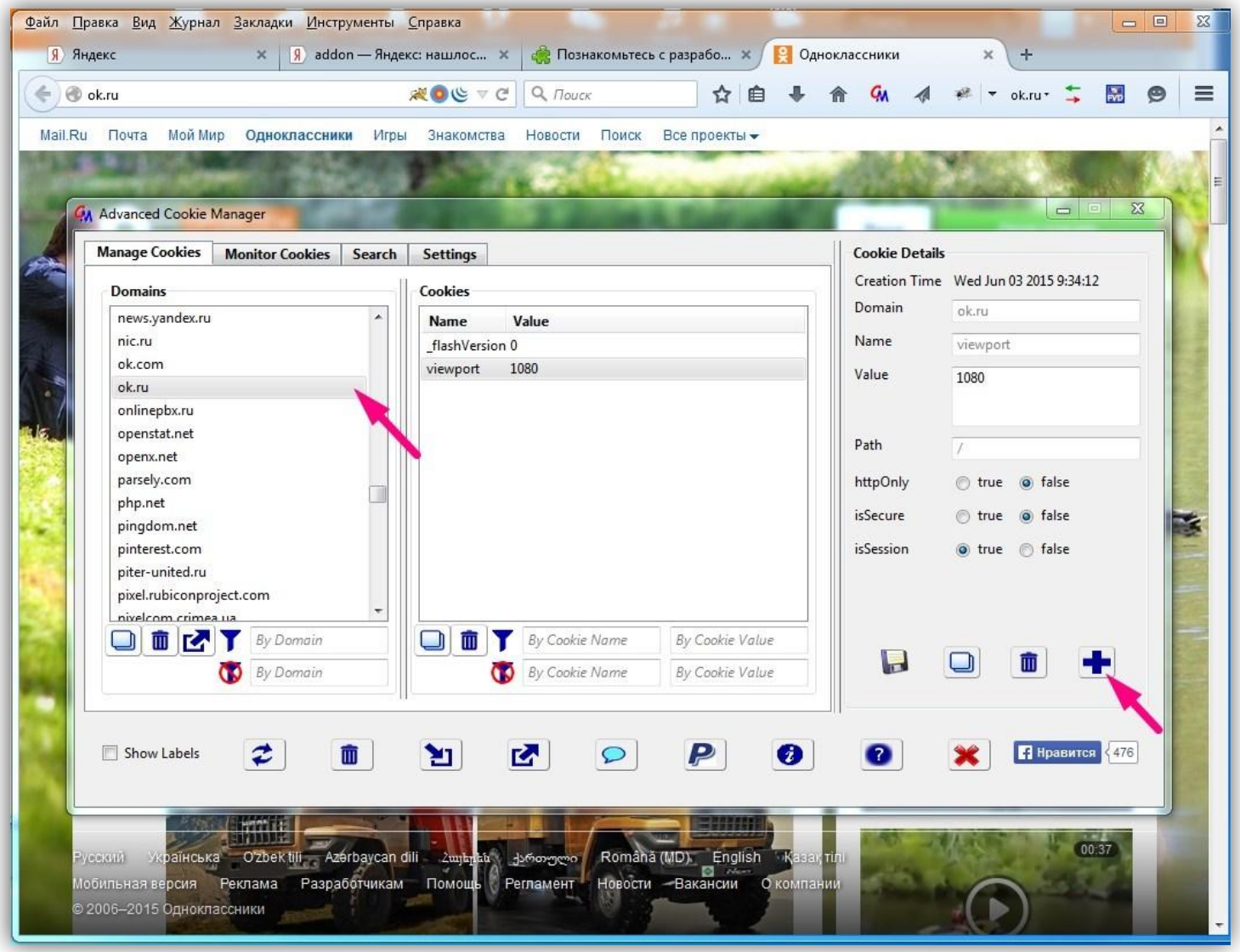
Кража Cookie



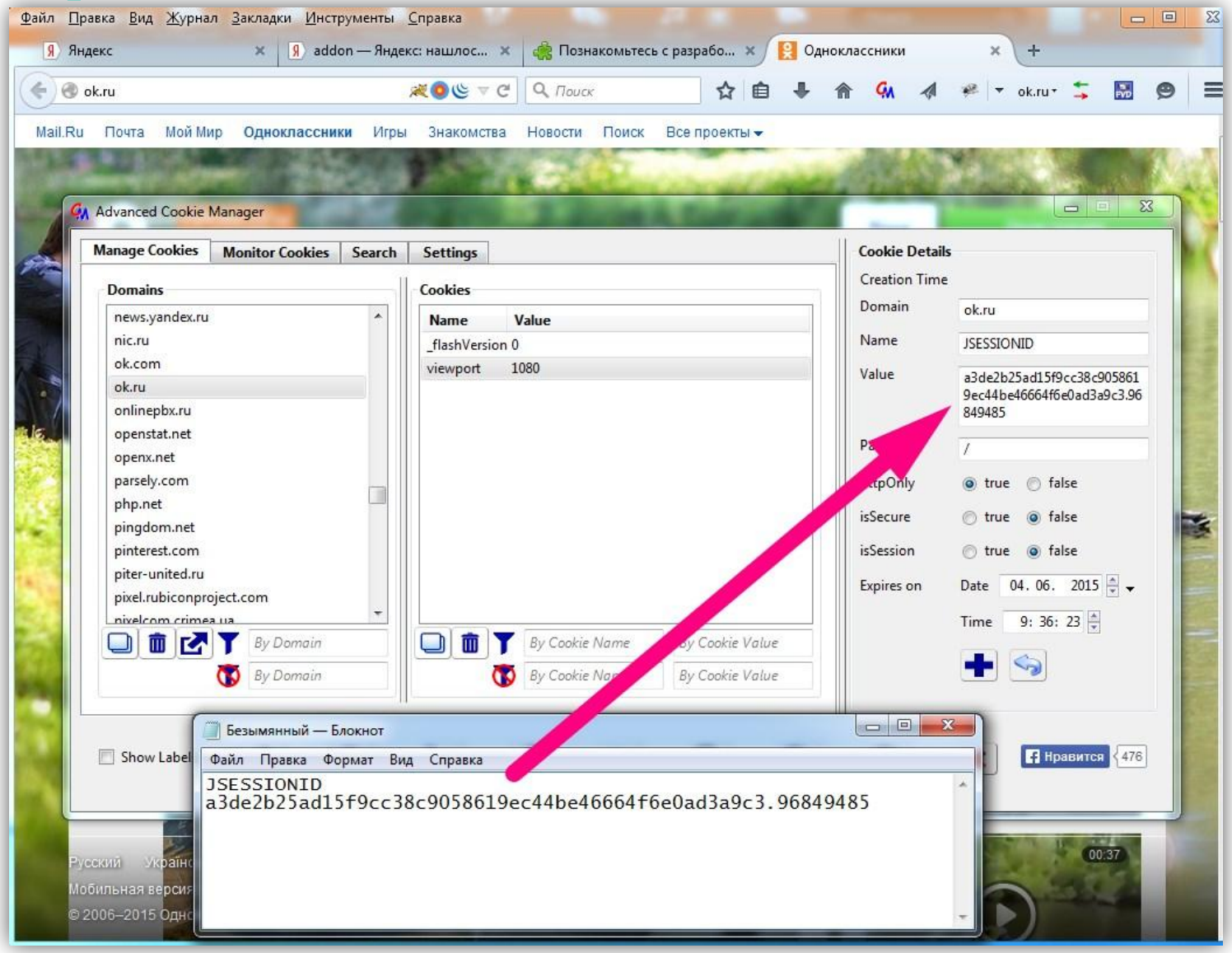
Кража Cookie



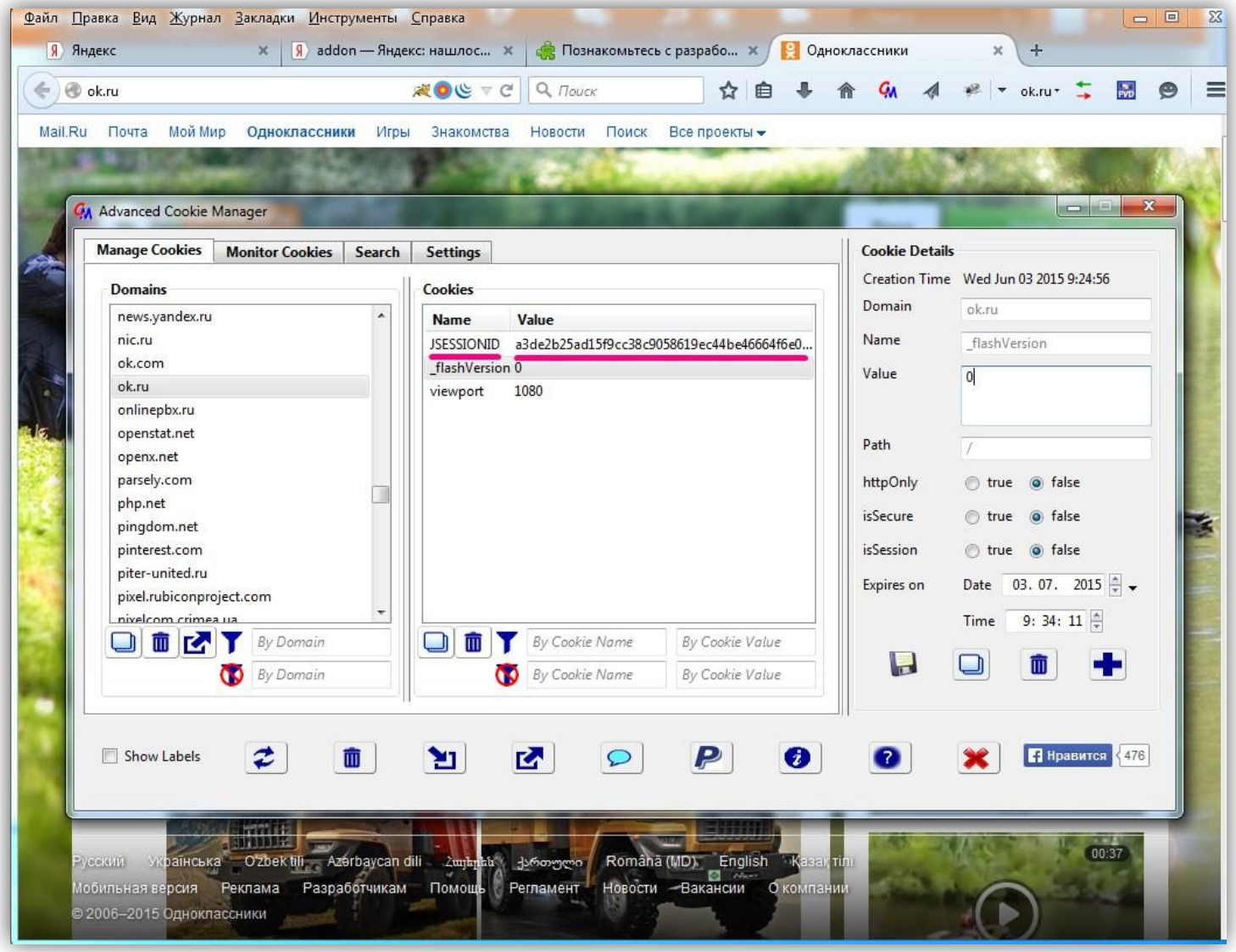
Кража Cookie



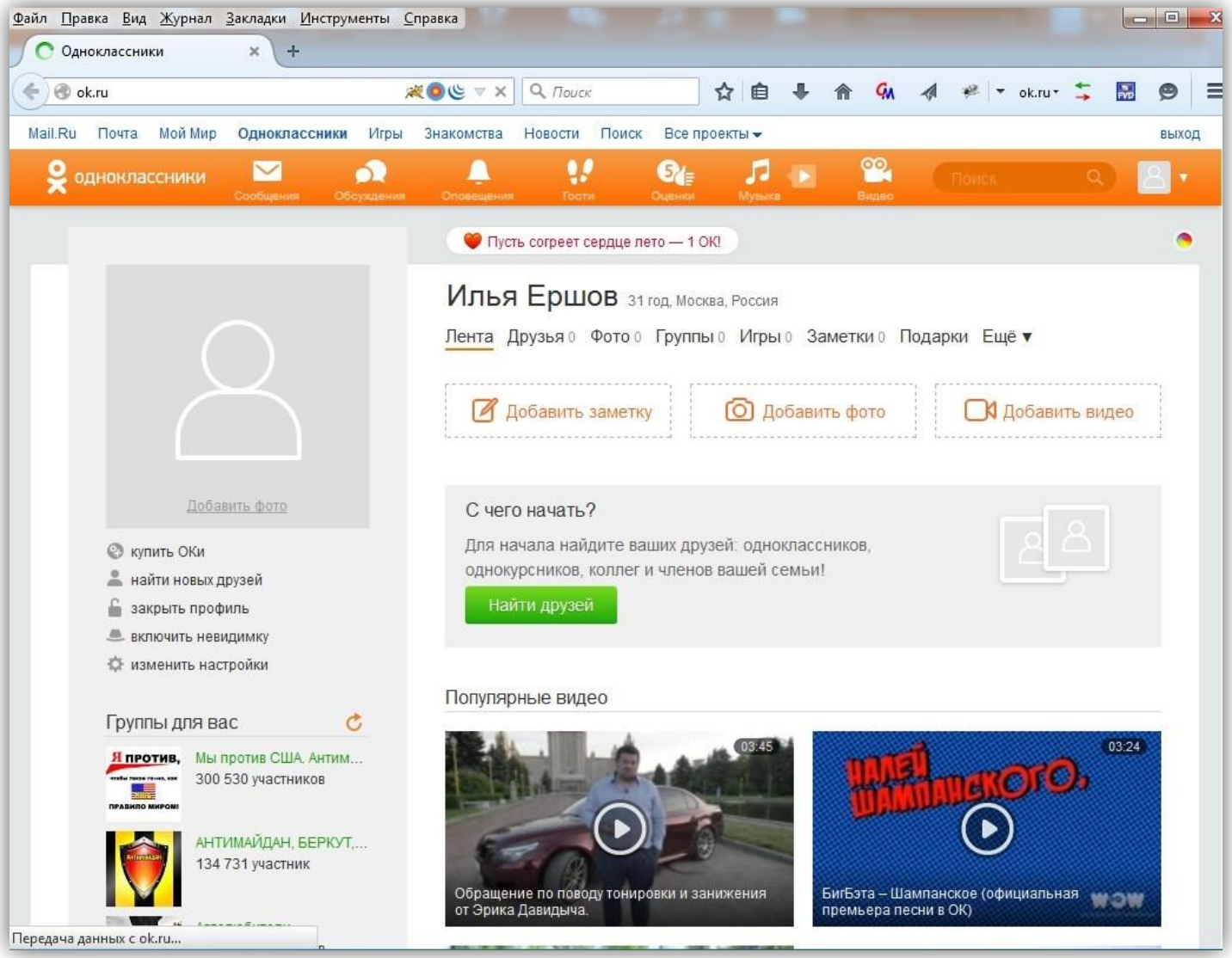
Кража Cookie



Кража Cookie



Кража Cookie



Перебор всех вариантов

Количество комбинаций

124164570546910030388582240001 = 29 разрядов

В день 1 сервер может перебрать 86400 комбинаций

Общее количество дней
1437089936885532759127l0 = 24 разряда

Количество лет
39372327037959801619 9

Количество сессий

Количество пользователей

42 600 000

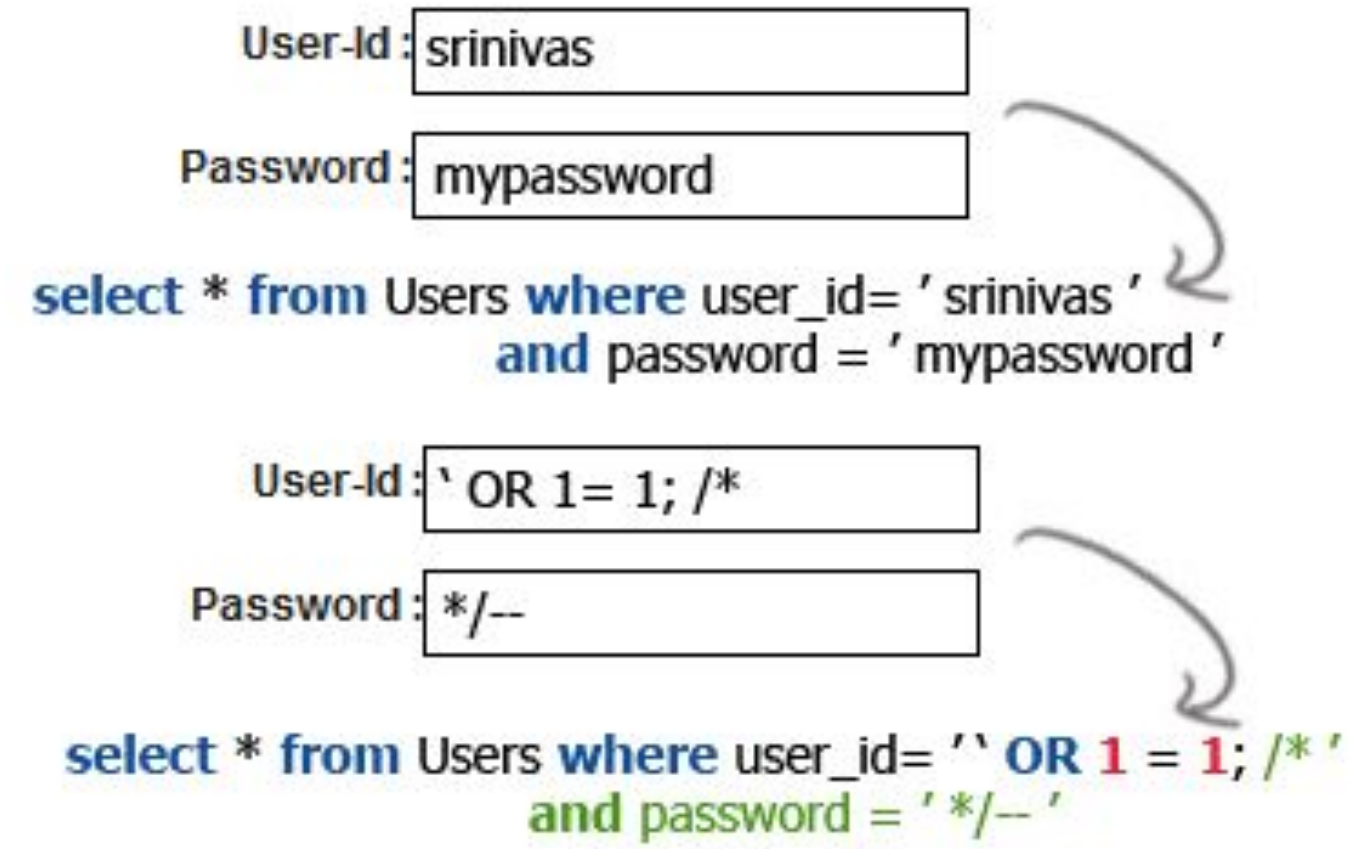
Количество сессий

127800000

Количество лет на подбор одной сессии

3080776763533

SQL-инъекция



Ссылки и дополнительные материалы на странице:
//j.mp/mfpa-links

Trap 4 hacker

Ссылки и дополнительные материалы на странице:
//j.mp/mfpa-links

REMOTE_ADDR 182.114.228.70

Попытка 1 от 21-05-2014 13:37:53

HOST DNS NAME hn.kd.ny.adsl

REQUEST_URI
/admin/fckeditor/editor/filemanager/browser/default/connectors/connector.php?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=/

Регион Китай - Чжэнчжоу

Trap 4 hacker

Ссылки и дополнительные материалы на странице:
//j.mp/mfpa-links

REMOTE_ADDR 208.79.95.226

Попытка 1 от 6-07-2014 20:47:21

HOST DNS NAME eeyore.smith-family.com

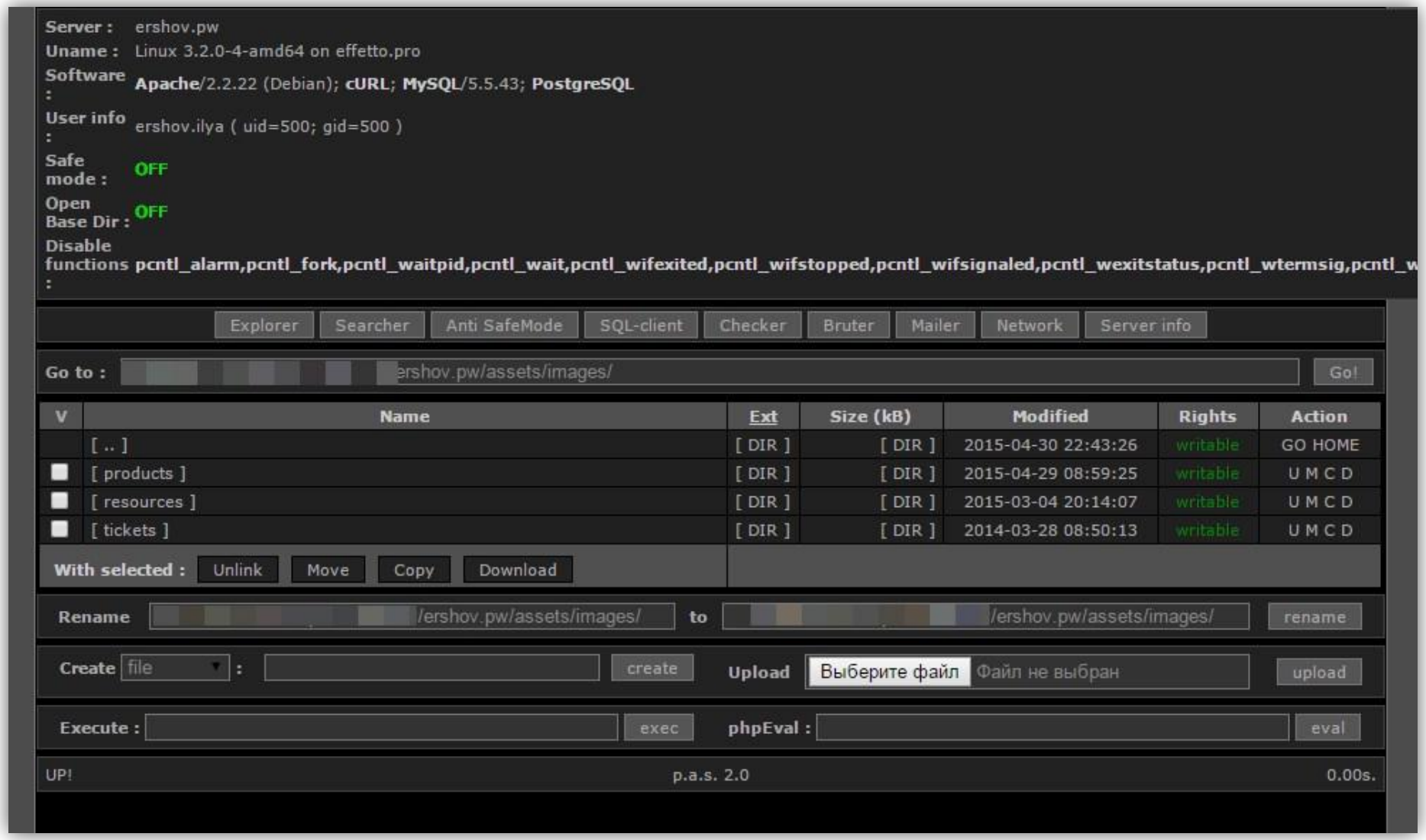
HTTP_USER_AGENT

REQUEST_URI
/administrator/components/com_extended_registration/admin.extended_registration.php?mosConfig_absolute_path=http://www.google.com/humans.txt?

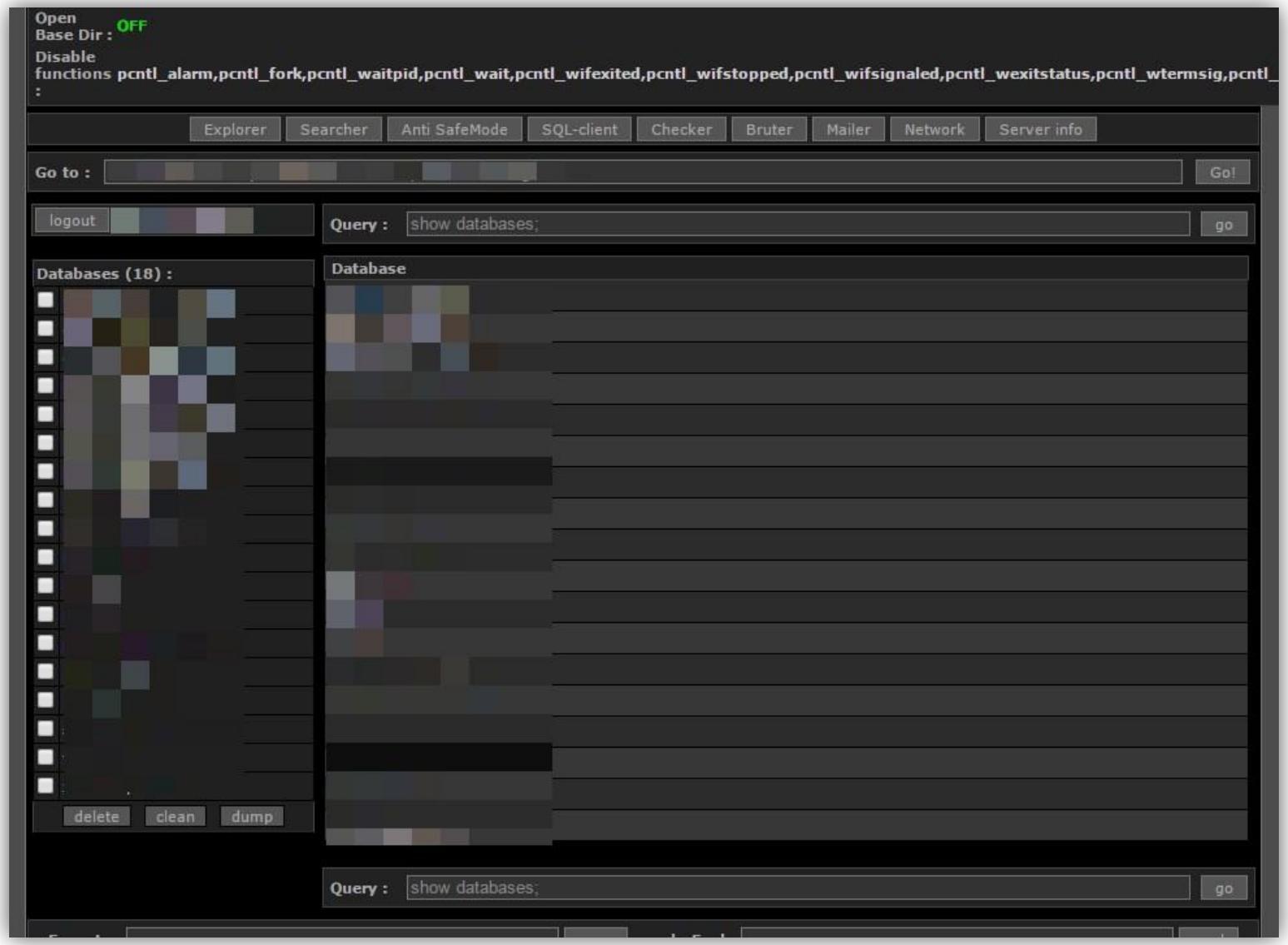
Регион США - Сильмар

Шелл p.a.s. 2.0

Шелл p.a.s. 2.0

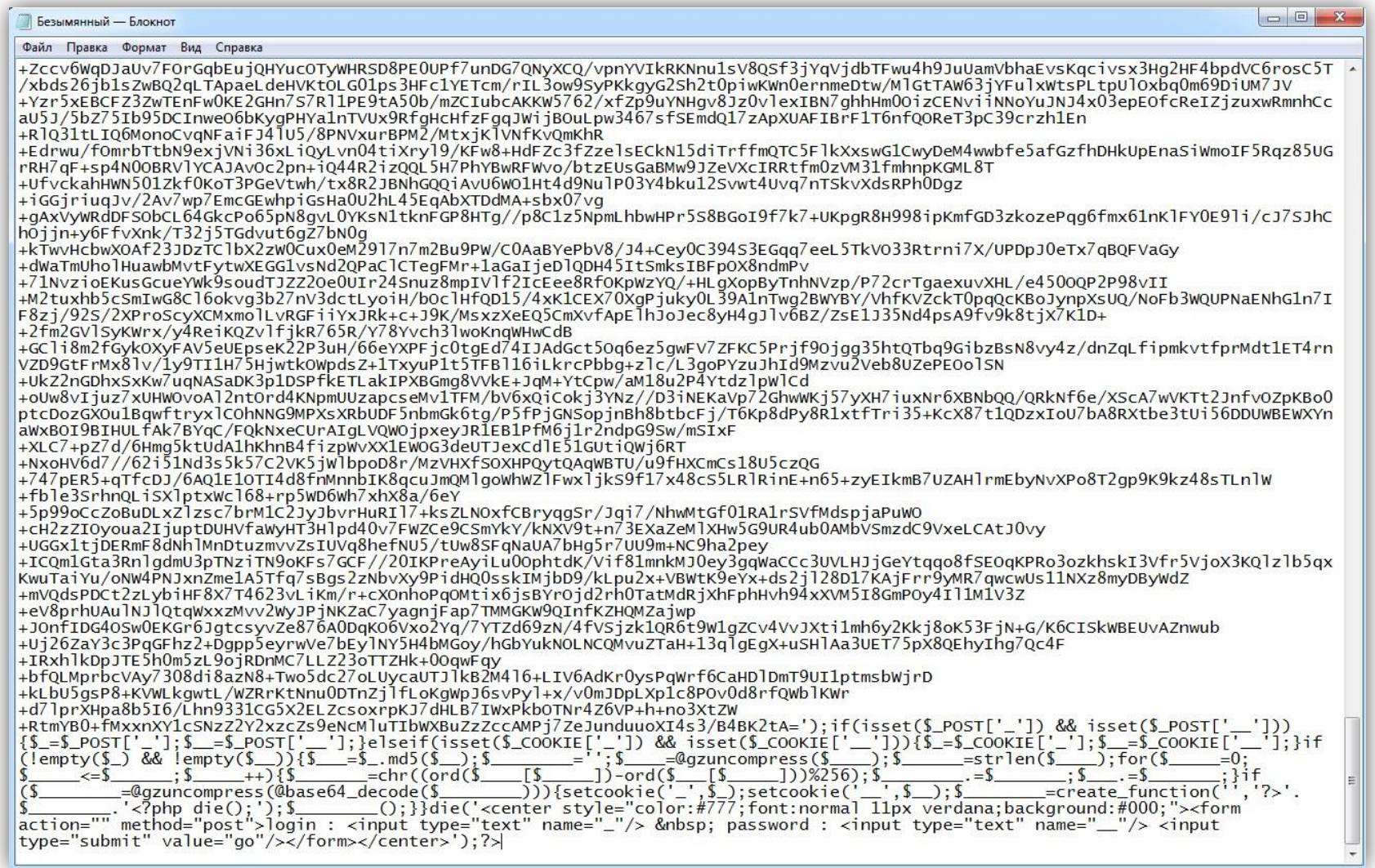

Server : ershov.pw
Uname : Linux 3.2.0-4-amd64 on effetto.pro
Software : Apache/2.2.22 (Debian); cURL; MySQL/5.5.43; PostgreSQL
User info : ershov.ilya (uid=500; gid=500)
Safe mode : OFF
Open Base Dir : OFF
Disable functions : pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_w
Explorer Searcher Anti SafeMode SQL-client Checker Bruter Mailer Network Server info
Go to : ershov.pw/assets/images/ Go!
V Name Ext Size (kB) Modified Rights Action
[..] [DIR] [DIR] 2015-04-30 22:43:26 writable GO HOME
[products] [DIR] [DIR] 2015-04-29 08:59:25 writable U M C D
[resources] [DIR] [DIR] 2015-03-04 20:14:07 writable U M C D
[tickets] [DIR] [DIR] 2014-03-28 08:50:13 writable U M C D
With selected : Unlink Move Copy Download
Rename /ershov.pw/assets/images/ to /ershov.pw/assets/images/ rename
Create file : create Upload Выберите файл Файл не выбран upload
Execute : exec phpEval : eval
UP! p.a.s. 2.0 0.00s.

Шелл p.a.s. 2.0


Open Base Dir : OFF
Disable functions pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_
Explorer
Searcher
Anti SafeMode
SQL-client
Checker
Bruter
Mailer
Network
Server info
Go to :
Go!
logout
Query :
show databases;
go
Databases (18) :
Database
delete
clean
dump
Query :
show databases;
go

Шелл p.a.s. 2.0

Обфускация (маскирование кода)



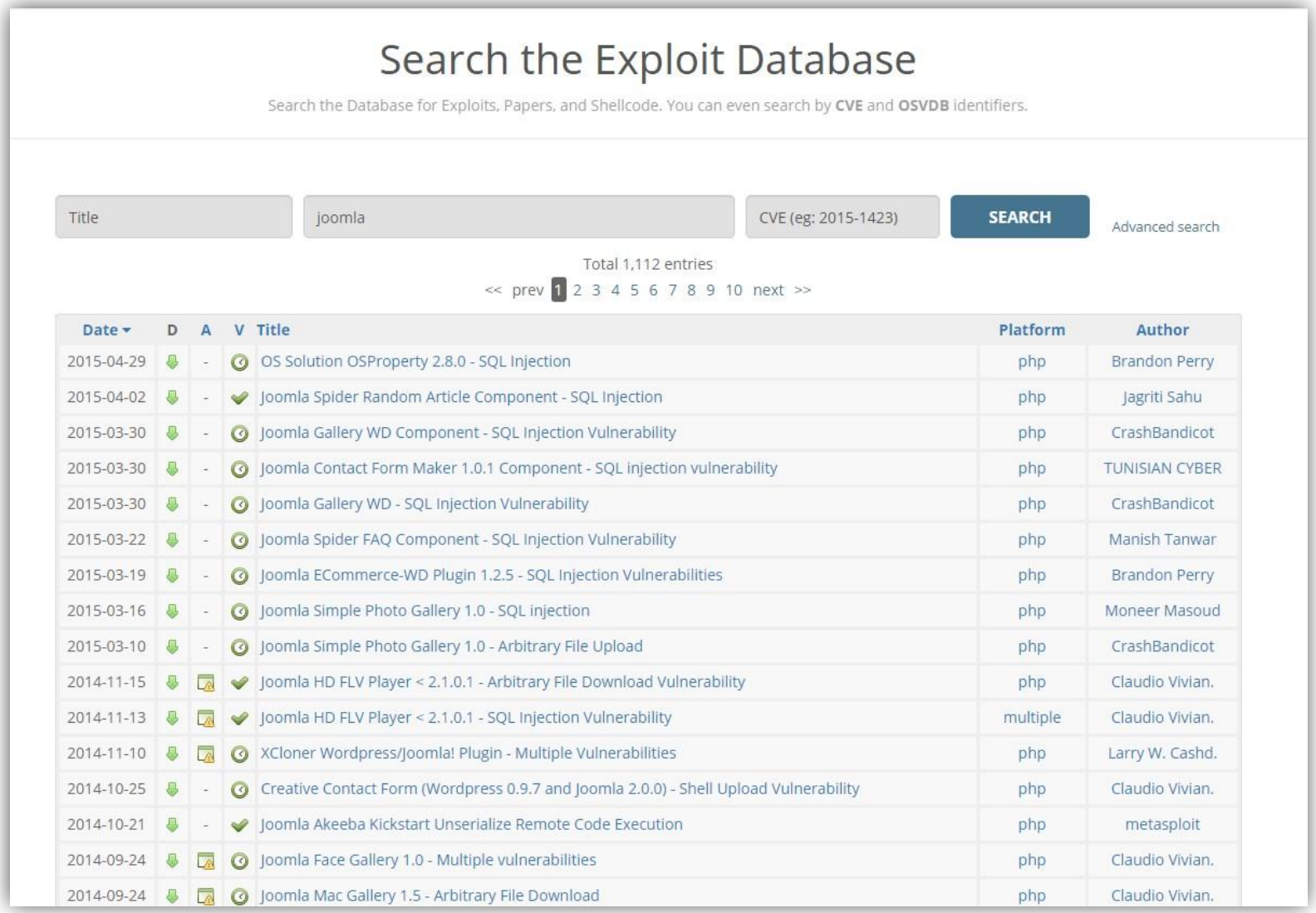
Безопасность

//exploit-db.com

Безопасность

Joomla

//exploit-db.com



Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

Title | joomla | CVE (eg: 2015-1423) | SEARCH | Advanced search

Total 1,112 entries

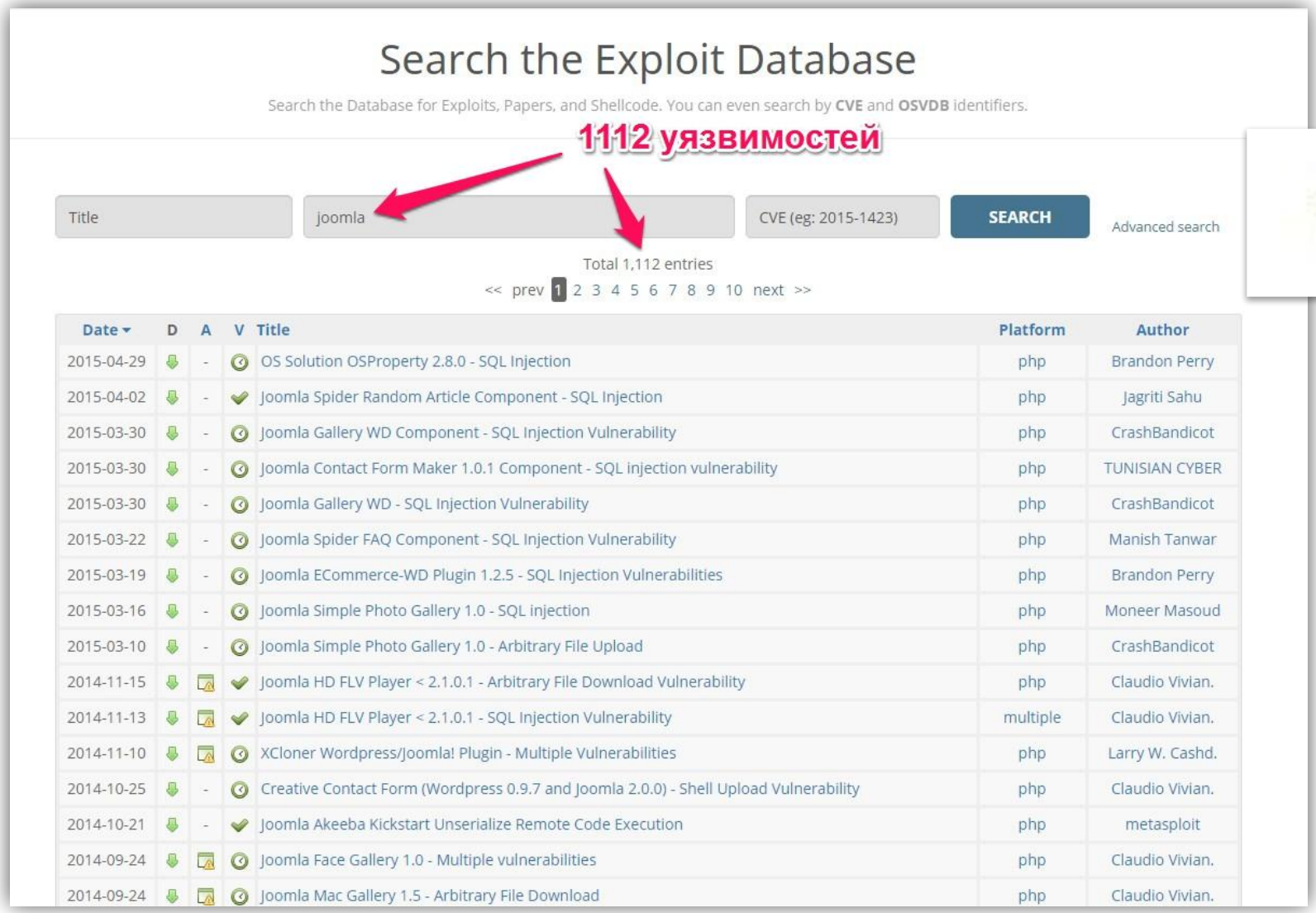
<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	D	A	V	Title	Platform	Author
2015-04-29		-		OS Solution OSProperty 2.8.0 - SQL Injection	php	Brandon Perry
2015-04-02		-		Joomla Spider Random Article Component - SQL Injection	php	Jagriti Sahu
2015-03-30		-		Joomla Gallery WD Component - SQL Injection Vulnerability	php	CrashBandicot
2015-03-30		-		Joomla Contact Form Maker 1.0.1 Component - SQL injection vulnerability	php	TUNISIAN CYBER
2015-03-30		-		Joomla Gallery WD - SQL Injection Vulnerability	php	CrashBandicot
2015-03-22		-		Joomla Spider FAQ Component - SQL Injection Vulnerability	php	Manish Tanwar
2015-03-19		-		Joomla ECommerce-WD Plugin 1.2.5 - SQL Injection Vulnerabilities	php	Brandon Perry
2015-03-16		-		Joomla Simple Photo Gallery 1.0 - SQL injection	php	Moneer Masoud
2015-03-10		-		Joomla Simple Photo Gallery 1.0 - Arbitrary File Upload	php	CrashBandicot
2014-11-15				Joomla HD FLV Player < 2.1.0.1 - Arbitrary File Download Vulnerability	php	Claudio Vivian.
2014-11-13				Joomla HD FLV Player < 2.1.0.1 - SQL Injection Vulnerability	multiple	Claudio Vivian.
2014-11-10				XCloner Wordpress/Joomla! Plugin - Multiple Vulnerabilities	php	Larry W. Cashd.
2014-10-25		-		Creative Contact Form (Wordpress 0.9.7 and Joomla 2.0.0) - Shell Upload Vulnerability	php	Claudio Vivian.
2014-10-21		-		Joomla Akeeba Kickstart Unserialize Remote Code Execution	php	metasploit
2014-09-24				Joomla Face Gallery 1.0 - Multiple vulnerabilities	php	Claudio Vivian.
2014-09-24				Joomla Mac Gallery 1.5 - Arbitrary File Download	php	Claudio Vivian.

Безопасность

Joomla

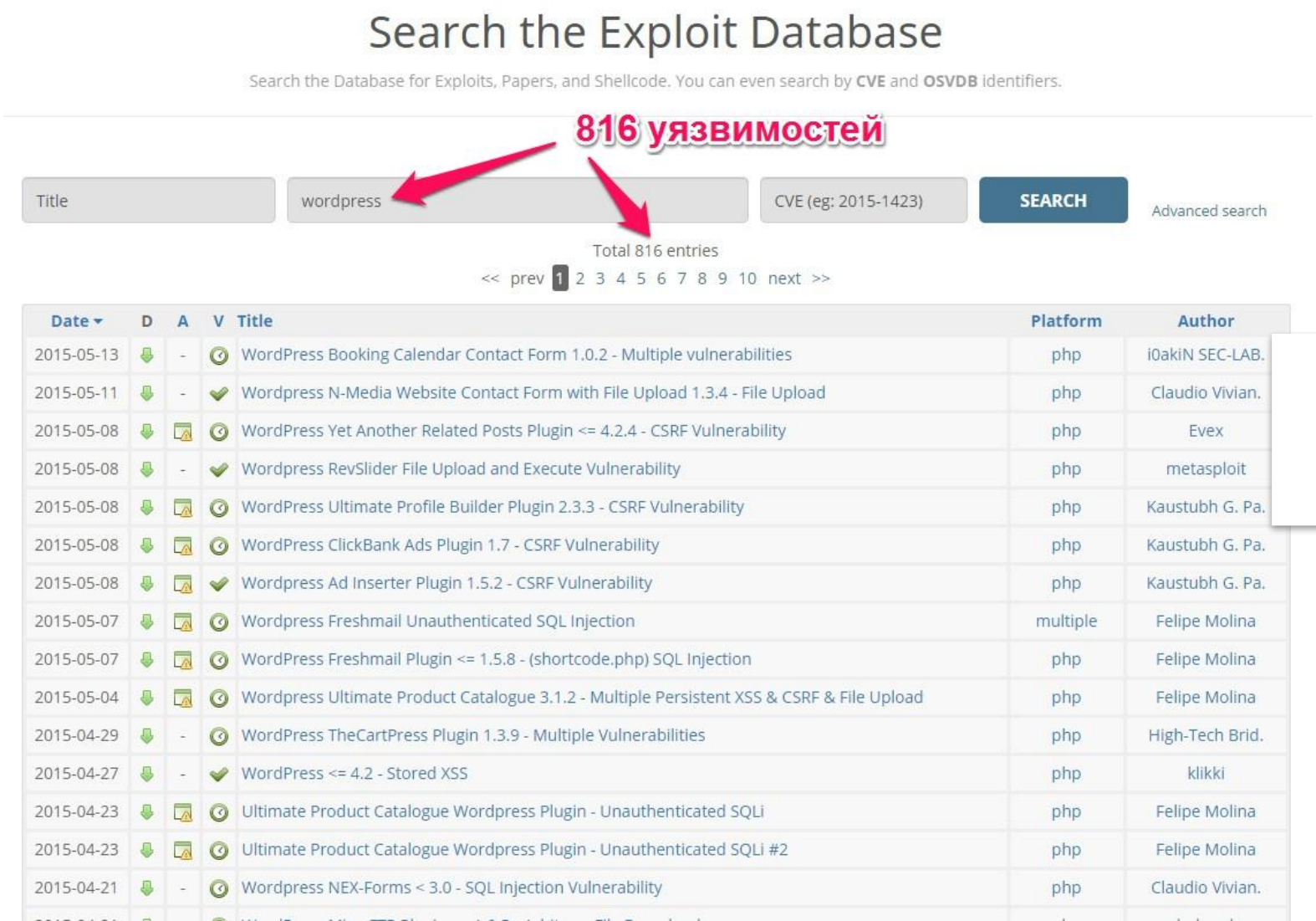
//exploit-db.com



Безопасность

Wordpress

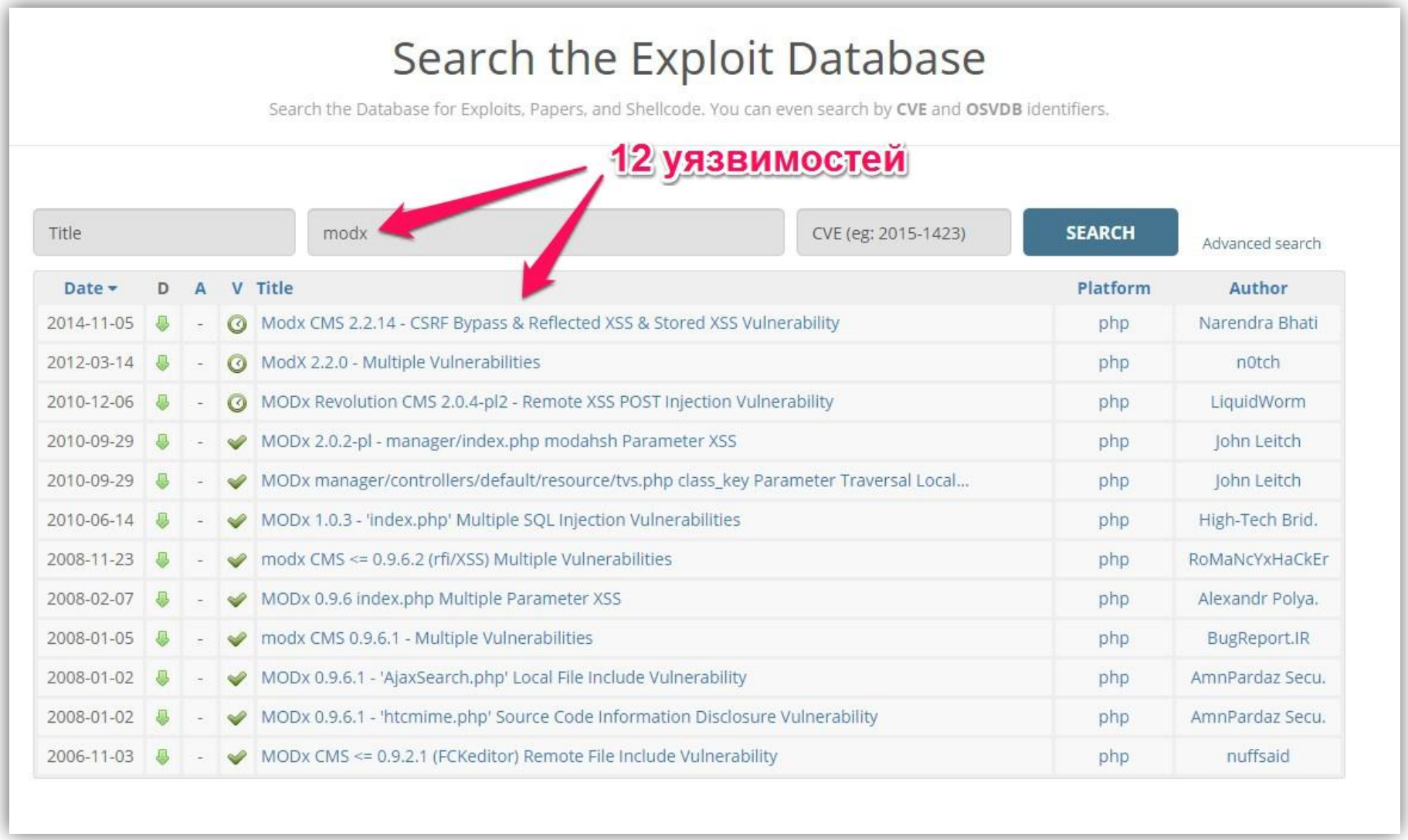
//exploit-db.com



Безопасность

MODX

//exploit-db.com

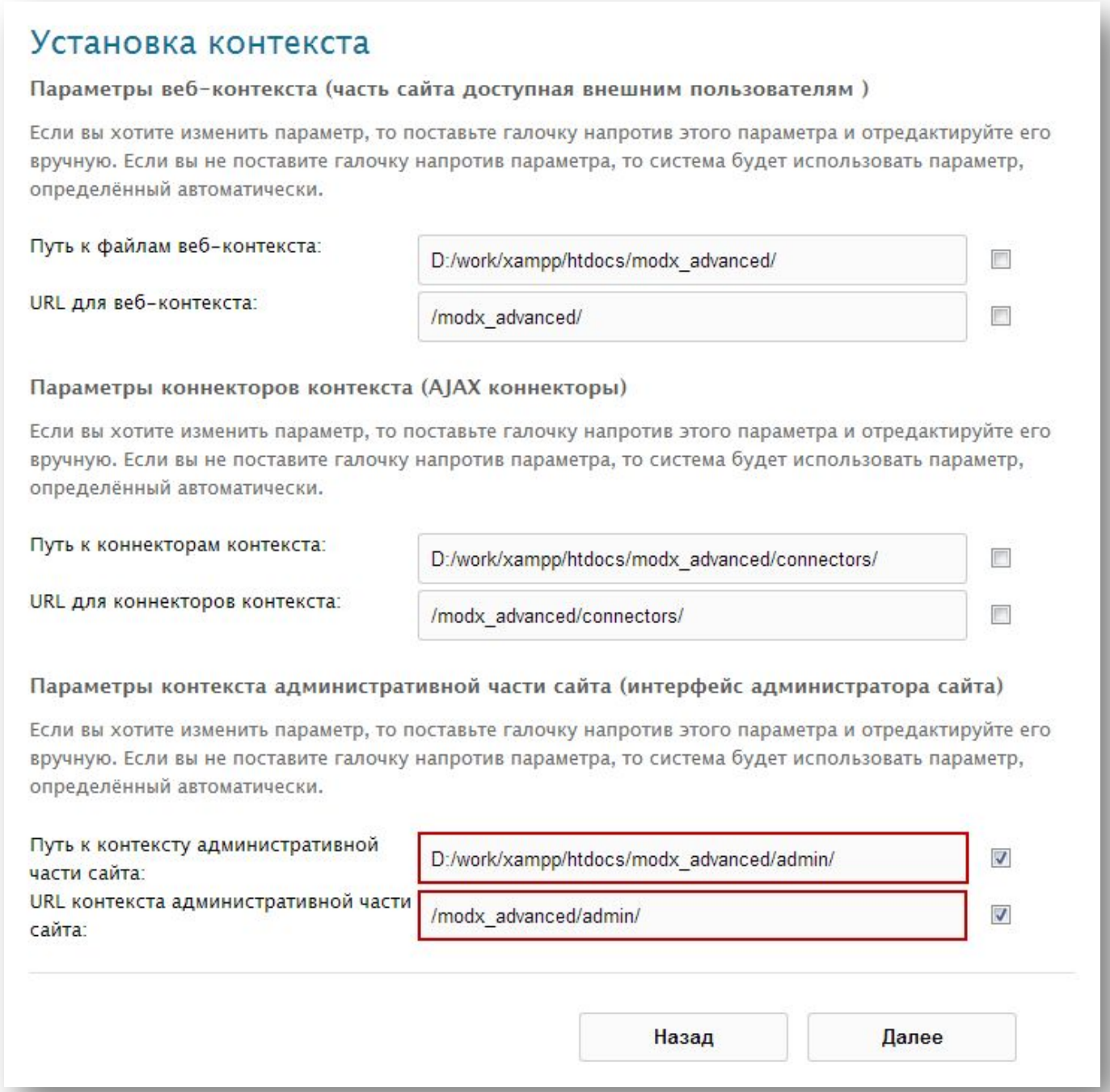


Как защититься?

1. Фильтруйте все данные поступающие от пользователей
2. Меняйте префиксы таблиц базы данных
3. Переопределяйте путь к админке
4. Закрывайте к уязвимым разделам доступ по IP адресу
5. Протоколируйте попытки проникновения
6. Обновляйте всё ПО

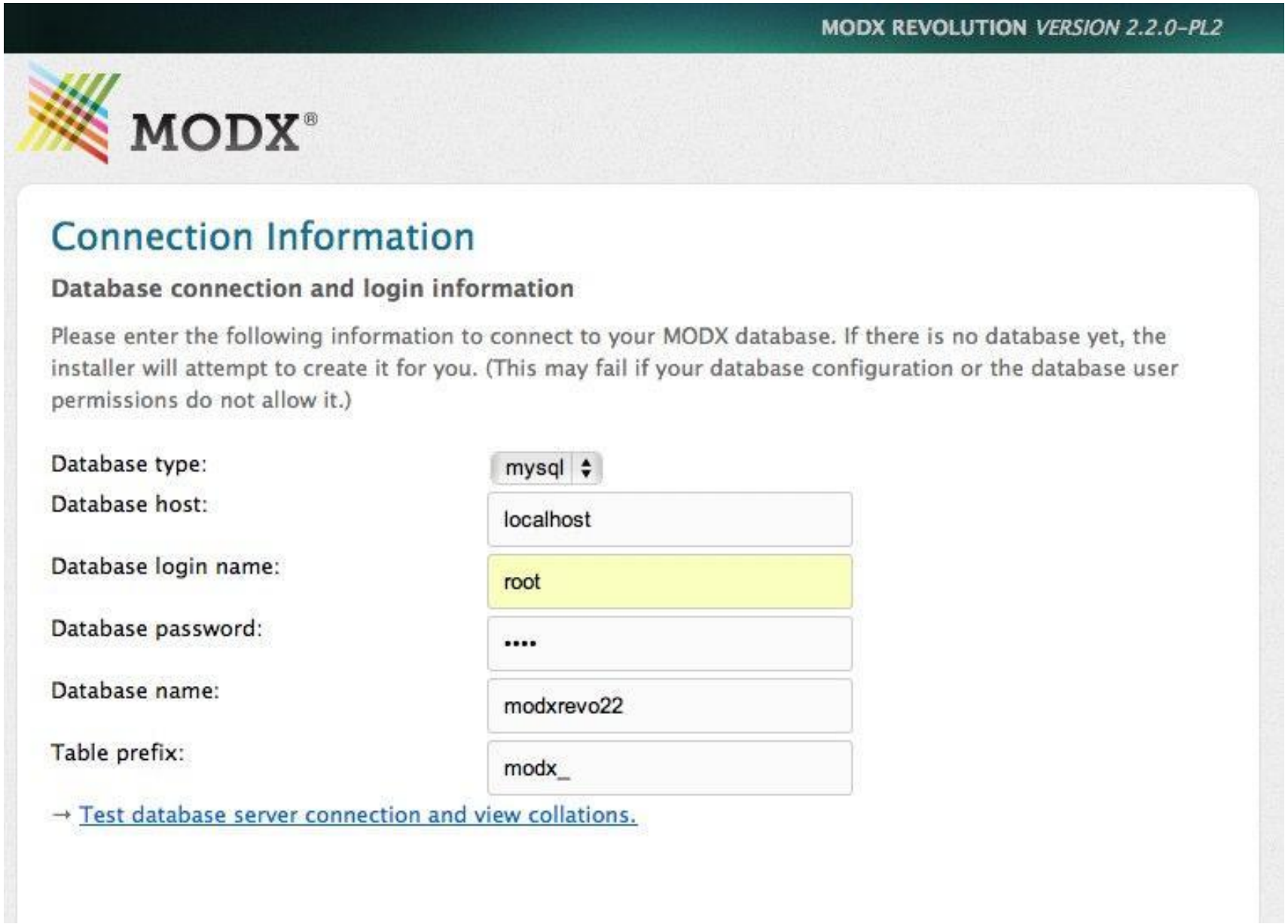
MODX

Подмена пути к админке



MODX

Подмена префикса таблиц



Запрет доступа чужим IP адресам

Файл admin/.htaccess

```
RewriteEngine Off
Order deny,allow
Deny from all
Allow from 122.233.122.223     # home
Allow from 122.233.122.224     # work
```

Илья Ершов

Веб-разработчик, руководитель интернет-проектов

ershov.ilya@gmail.com

Skype: ershov.ilya

www.ershov.pw

Спасибо за внимание