

УДК 003.26.7 004.9

## Защита от вредоносных междоменных запросов

*Волкович Е.К., студент  
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
Кафедра «Информационная безопасность»*

*Мессерле А.А., студент  
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
Кафедра «Информационная безопасность»*

*Научный руководитель: Алешин В.А., к. т. н., доцент  
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана  
[bauman@bmstu.ru](mailto:bauman@bmstu.ru)*

Рассмотрим типичное применение файла crossdomain.xml, который отвечает за политику безопасности сайта. Этот файл определяет, с каких доменов может производиться запрос к ресурсам сайта, если эти домены принадлежат другому серверу. Если данный файл отсутствует, то это означает, что к сайту запрещен доступ с других серверов, и, следовательно, они защищены от уязвимостей этого типа.

Рассмотрим, для начала, типичную структуру файла crossdomain.xml:

```
<cross-domain-policy>  
<site-control permitted-cross-domain-policies="all"/>  
<allow-access-from domain="*" />  
<allow-http-request-headers-from domain="*" headers="*" />  
</cross-domain-policy>
```

Поле «all» означает, что доступ разрешен любым сайтам, причем им могут быть предоставлены любые привилегии связей между доменами. Из этого следует, что при определенных обстоятельствах можно получить доступ ко всей информации пользователей, которая хранится на сайте, например, паролям, личным профилям с конфиденциальной информацией и прочему. Поле «\*» во второй строке говорит злоумышленнику о том, что к серверу разрешен доступ с произвольного домена. Это значит, что любой пользователь ПК может получить такой доступ.

Согласно проведенному нами исследованию, можно достаточно просто и быстро узнать о том, существует ли файл crossdomain.xml – достаточно зайти на главную страницу сайта и написать в конце «</crossdomain.xml»». Если такой файл существует, то

будет показано его содержимое, в противном случае на экране окажется «ошибка 404» - такого файла не существует. Используя последние данные за 01/03/2014 [2], мы провели оценку топ-75 наиболее популярных сайтов в России, с ежедневной средней посещаемостью не менее 500 тысяч пользователей. Результат отображен на диаграмме (см. рис.1).

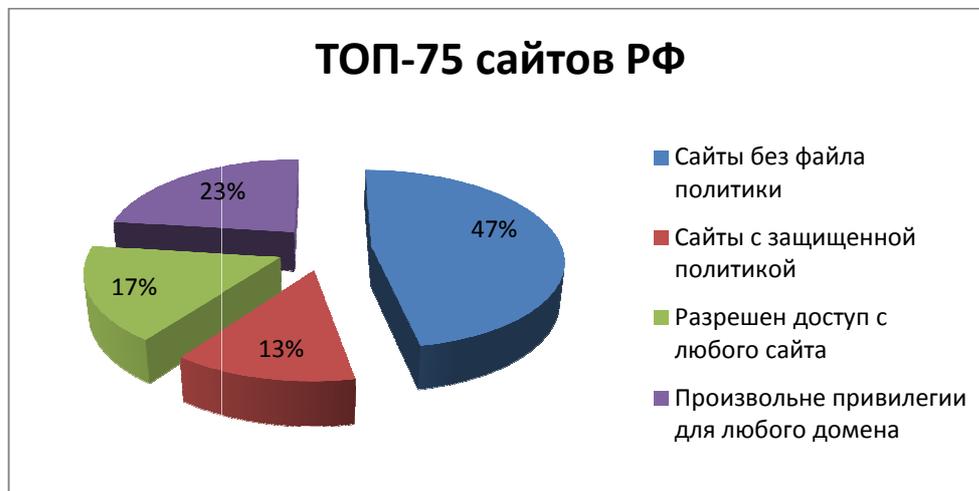


Рис.1. Оценка топ-75 наиболее популярных сайтов России

Проанализируем результаты. 53% сайтов имеют файл `crossdomain.xml`, то есть используют междоменную политику для своего контента, например, храня на сайте код, который вызывает файл формата `*.swf` (Flash), хранящийся на другом сервере. При этом только 13% сайтов используют в своей политике специальные домены, например сайт Adobe:

```
<?xml version="1.0"?>
<cross-domain-policy>
<site-control permitted-cross-domain-policies="by-content-type"/>
<allow-access-from domain="*.macromedia.com"/>
<allow-access-from domain="*.adobe.com"/>
<allow-access-from domain="*.photoshop.com"/>
<allow-access-from domain="*.acrobat.com"/>
</cross-domain-policy>
```

Как видно, доступ к серверу с произвольного домена запрещен. Получить доступ могут только сайты с сервера самого Adobe. Это является примером хорошей междоменной политики.

Далее, 17% разрешен доступ с любого сайта, то есть в файле содержится строка:

```
<site-control permitted-cross-domain-policies="all"/>
```

Это не очень опасно для пользователей, но все же благоразумно избегать таких выражений. Если в сети есть сайт, который может рассылать вредоносное содержимое, то он может попытаться прорваться и к этому сайту. Поэтому следует ограничивать произвольный доступ для сайтов, которые могут быть потенциально опасны, создавая правила или только для проверенных доменов, или только для «своих». В последнем случае обеспечивается наибольшая безопасность.

И, наконец, 23% сайтов предоставляют практически неограниченные привилегии для любого домена. Фактически, это означает, что эти сайты уязвимы, и защиты от такого рода уязвимостей у них пока нет. Следует задуматься, 23% сайтов с посещаемостью более полумиллиона в день оказываются уязвимыми. То есть, когда вы посещаете сайт и вводите какую-либо информацию или открываете Flash, или Silverlight содержимое, то ваши данные оказываются потенциально уязвимыми. Самая «убойная» комбинация получается, если файл crossdomain.xml имеет типичную структуру, как показано выше. В этом случае, сайт является абсолютно «открытым» для злоумышленника. Хакеру достаточно написать около 8 строк кода для эксплойта и залить код на сайт. Таким образом, может производиться «накрутка» голосов, популярности и прочих счетчиков сайтов. Просто представьте себе, что эта уязвимость возникнет на каком-нибудь федеральном сайте.

Вот часть файла crossdomain.xml, содержащего надежную политику кросс-доменных запросов:

```
<cross-domain-policy>
<site-control permitted-cross-domain-policies="master-only"/>
<allow-http-request-headers-from domain="odnoklassniki.ru" headers="*" />
<allow-access-from domain="odnoklassniki.ru" />
<allow-access-from domain="*.odnoklassniki.ru" />
</cross-domain-policy>
```

Видно, что доступ к контролю над сайтом разрешен только его создателям, и доступ допускается лишь с доменов самого сервера сайта. Таким образом, кросс-доменная политика этого сайта работает корректно, надежно храня свои секреты.

Теперь обратимся к следующему исследованию [3]. Хотя оно было проведено еще в 2006 году, оно позволяет, во-первых, сравнить динамику роста/падения угрозы, а, во-вторых, мы можем оценить масштабность этой уязвимости для РФ. Вот результаты Jeremian Grossman (см. рис.2):



Рис. 2. Оценка топ-100 наиболее популярных сайтов США

Как видно из диаграммы, в зарубежных странах более высок процент сайтов с отсутствующей кросс-доменной политикой. Процент сайтов, которые ограничивают список доменов, одинаков в обоих случаях. Однако доступ с любого домена разрешен гораздо меньшему количеству сайтов. Очевидно, что российский сегмент сети более склонен вести небезопасную междоменную политику.

Подводя итог, можно сказать, что в данной статье мы проанализировали ТОП-75 сайтов в РФ на уязвимость в файле `crossdomain.xml`. Результаты показали, что значительно число сайтов (23%) имеют небезопасные кросс-доменные политики, что может привести к некорректной работе сайта и утечкам персональных данных посетителей через эти уязвимости.

Метод защиты очень прост – достаточно отредактировать файл `crossdomain.xml` таким образом, чтобы доступ к контролю над сайтом имели только его создатели, а доступ к ресурсам мог осуществляться только с доменов своего сервера и проверенных доменов. Если кросс-доменные запросы на сайте не используются, то этот файл можно просто удалить.

### Список литературы

1. Lekies S., Nikiforakis N., Tighzert W., Piessens F., Johns M. DEMACRO: Defense against Malicious Cross-Domain Requests // Research in Attacks, Intrusions, and Defenses. Lecture Notes in Computer Science. Amsterdam. 2012. Vol. 7462. P. 254-273. DOI: 10.1007/978-3-642-33338-5\_13.
2. Рейтинг Top1000-RU: Все сайты. Режим доступа: <http://top1000-ru.hotlog.ru/> (дата обращения: 02.03.2014).

3. Jeremian Grossman: crossdomain.xml statistics. Режим доступа: <http://jeremiahgrossman.blogspot.ru/2006/10/crossdomainxml-statistics.html> (дата обращения: 02.03.2014).