Аудит безопасности сайта (тест на проникновение)

http://site.com

ATSEC.RU

01.02.2014

Суммарная информация об уязвимостях

SQL Injection

Элемент	Страница
/AJAX/infoartist.php	2
/listproducts.php	2

Cross Site Scripting

Элемент	Страница
/search.php	3
/t.php	3

Раскрытие исходного кода

Элемент	Страница
/showimage.php	4

Страница PHPinfo

Элемент	Страница
/phpinfo.php	5

WS_FTP log

Элемент	Страница
/pictures/WS_FTP.LOG	6

Directory Listing

Элемент	Страница
/Templates	7

SQL Injection

Опасность	**Высокая**

Описание

Внедрение SQL-кода (англ. SQL injection) — один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.

Возможные последствия

Внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере

Рекомендации

Для защиты от данного типа атак необходимо тщательно фильтровать входные параметры, значения которых будут использованы для построения SQL-запроса.

Уязвимость

Уязвимый скрипт: /AJAX/infoartist.php

Уязвимый параметр: id

Детали

GET запросом параметр id был установлен в 5’
Это привело к ошибке: You have an error in your SQL syntax
Пример эксплуатации уязвимости: http://site.com/AJAX/infoartist.php?id=9999+union+select+1,2,3,4,version()

Заголовки запросов HTTP

```
GET /AJAX/infoartist.php?id=5’ HTTP/1.1
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```

Уязвимый скрипт: /listproducts.php

Уязвимый параметр: cat

Детали

GET запросом параметр cat был установлен в 720‘
Это привело к ошибке: You have an error in your SQL syntax

Заголовки запросов HTTP

```
GET /listproducts.php?cat=720’ HTTP/1.1
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```

Cross Site Scripting

Опасность	**Высокая**

Описание

XSS (англ. Cross Site Scripting — «межсайтовый скриптинг») — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника.

Возможные последствия

Злоумышленники могут внедрять JavaScript, VBScript, ActiveX, HTML код в уязвимое приложение, получать данные пользователей. Например, злоумышленник может похитить cookies (куки). Кроме того, возможно изменять содержимое страницы, представленное пользователю.

Рекомендации

Для защиты от данного типа атак необходимо тщательно фильтровать данные, полученные от пользователей.

Уязвимость

Уязвимый скрипт: /search.php

Уязвимый параметр: searchFor

Детали

POST запросом параметр searchFor был установлен в 1<ScRiPt >alert(932032)</ScRiPt>
Таким образом, успешно внедрили javascript.

Заголовки запросов HTTP

```
POST /search.php?test=query HTTP/1.1
Content-Length: 71
Content-Type: application/x-www-form-urlencoded
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)

goButton=go&searchFor=1<ScRiPt >alert(932032)</ScRiPt>
```

Уязвимый скрипт: /t.php

Уязвимый параметр: test

Детали

GET запросом параметр test был установлен в 1<ScRiPt >alert(998881)</ScRiPt>
Таким образом, успешно внедрили javascript.

Заголовки запросов HTTP

```
GET /t.php?test=1<ScRiPt >alert(998881)</ScRiPt> HTTP/1.1
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```

Раскрытие исходного кода

Опасность	**Высокая**

Описание

Получение исходного кода скрипта.

Возможные последствия

Злоумышленник может получить важную информацию, для использования в дальнейшей атаке.

Рекомендации

Проанализируйте свой исходный код и устраните проблему.

Уязвимость

Уязвимый скрипт: /showimage.php

Уязвимый параметр: file

Детали

GET запросом параметр file был установлен в showimage.php
Был получен исходный код:

```
<?php
// header("Content-Length: 1" /*. filesize($name)*/);
if( isset($_GET["file"]) && !isset($_GET["size"]) ){
        // open the file in a binary mode
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];
        $fp = fopen($name, 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
elseif (isset($_GET["file"]) && isset($_GET["size"])){
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];
        $fp = fopen($name.'.tn', 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
?>
```

Заголовки запросов HTTP

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```

Страница PHPinfo

Опасность	**Средняя**

Описание

Функция phpinfo() выводит большое количество информации о текущем статусе PHP. Сюда входит информация об опциях компиляции PHP и о расширениях, версии PHP, информация сервера и окружения (если скомпилирован как модуль), окружение PHP, версия ОС, пути, master и локальные переменные опций конфигурации и т.д.

Возможные последствия

Злоумышленник может использовать информацию для дальнейшей атаки.

Рекомендации

Удалить файл.

Уязвимость

Детали
phpinfo() страница найдена по адресу: /phpinfo.php

WS_FTP log

Опасность	**Средняя**

Описание

WS_FTP популярный FTP клиент. Файл содержит информацию о расположении файлов, дате их изменение и другие подобные данные.

Возможные последствия

Злоумышленник может использовать информацию для дальнейшей атаки.

Рекомендации

Удалить файл или изменить настройки доступа к нему.

Уязвимость

Детали
WS_FTP.LOG файл найден по адресу: /pictures/WS_FTP.LOG

Directory Listing

Опасность	**Низкая**

Описание

Возможность просматривать список файлов и папок.

Возможные последствия

Раскрытие нежелательной информации.

Рекомендации

Загрузите в каталог Templates пустой файл index.htm

Уязвимость

Детали
Directory listing по адресу http://site.com/Templates

Контактные данные

Email: atsecru@gmail.com

Сайт: http://atsec.ru/