Дипломная работа

на тему:

апраркеркеркеркеркеркерке

Выполнил:

Дипломный руководитель:

Актуальность выбранной темы

В настоящее время основным информационным ресурсом является глобальная сеть интернет. В связи с этим растёт количество сайтов в международной виртуальной сети. По этой причине сейчас наиболее трудно уйти от шпионажа, взлома и порчи информации, которая подчас так необходима.

Объкт и предмет исследования

- Объектом курсовой работы выступает защита веб-приложений и сайтов.
- Предметом исследования является сеть интернет и защищённые сайты

Цель исследования

Изучить различные методы проникновения на сайты, привести практическую работу с SQL - инъекцией и XSS проникновением. Описать защиту от этих методов.

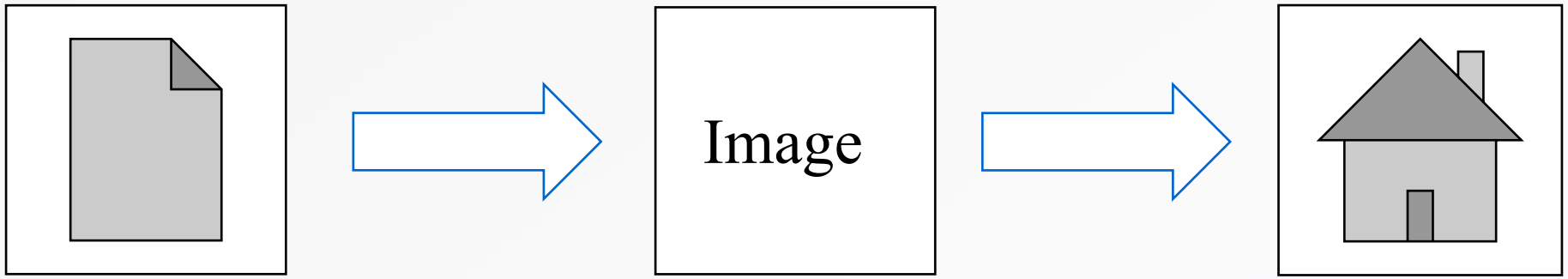
Задачи

Курсовая работа состоит из введения, двух основных глав, заключения и списка использованных источников.

- В первой главе рассматриваются методы проникновения на сайты.
- Во второй главе производится взлом логина и пароля двумя методами на разных сайтах с помощью с SQL - инъекцией и XSS проникновении.

Загрузка файлов

Сайт может позволять посетителям загружать свои файлы с последующим отображением на своих страницах. Это могут быть, к примеру, изображения в формате JPEG. Таким образом злоумышленник может вшить вредоностный файл в изображение разных форматов для последующего проникновения на сайт.



SQL-инъекции

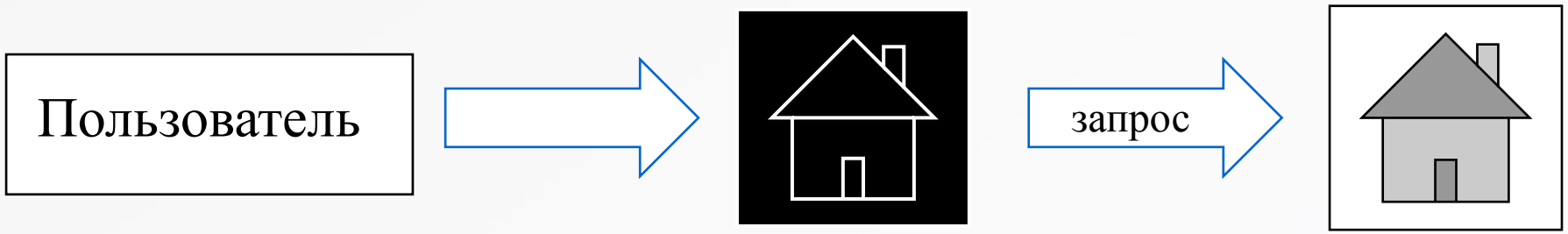
Это атака на базу данных, которая позволит выполнить некоторое действие, которое не планировалось создателем скрипта. На практическом примере получив доступ к базе данных сервера, можно получить любую входящую в него информацию, вместе с аторизационными данными пользователей.

XSS

Представляет собой атаку, при которой злоумышленник публикует на атакуемом сайте скрипт, который исполняется у пользователей сайта при открытии ими страниц. Поскольку этот скрипт выполняется в браузере у пользователя, то он имеет доступ к информации в его cookie, а также может производить на сайте действия от имени пользователя (если тот "залогинен"), к примеру, читать, писать и удалять сообщения.

Cross-Site Request Forgery

Атакой CSRF называется отправка запроса через браузер пользователя с одного сайта на другой, так что атакуемый сайт исполняет этот запрос, как будто он поступил от пользователя. То есть, если пользователь зайдет на заранее подготовленный хакером сайт, он может отправить сообщение от своего имени, перевести деньги на другой счет или сменить пароль в зависимости от команды, которую дал злоумышленник.



Отправка email с сайта

Функция mail позволяет отправлять письмо, указывая ему дополнительные заголовки, в которых можно прописать, в частности, адрес отправителя. К примеру можно взять такую форму, где хакер отправит от вашего имени сообщением на почту, которая указана после CC:

hacker@site.com
Cc: email@domain.com

DOS

Как правило, к этому классу атак принадлежат события, описываемые в новостях "Хакеры атаковали сайт X, нарушив его работу. Сайт не работал в течение Y часов". То есть это именно "атака", а не "взлом". На сервер производятся запросы, которые он не может обработать, в результате чего он не успевает обработать и запросы обычных посетителей выглядит для них как неработающий.

Отключение cookie

При отключении cookie у посетителя сайт вынужден дописывать идентификатор сессии к ссылкам и формам на страницах. К примеру человеку изначально может быть прислана ссылка с идентификатором сессии. И если человек перейдет по ссылке и авторизуется, то любой, кто воспользуется этой же ссылкой, сразу окажется авторизованным под чужим логином.

Описание практической части

С помощью первого метода удалось получить доступ к базе данных, которая была привязана к форме авторизации на сайте. Для этого использовался Ubuntu и список нужным команд.

С помощью второго метода был изъят cookie пользователя, введя который в код элемента был получен досуп к аккаунта без похождения авторизации.

Итоги дипломного проекта

Главной уязвимостью всех сайтов является недоработка самих администраторов и пользователей. Поэтому на примере двух методов SQL-инъекции и XSS я показал координально отличающиеся подходы для взлома данных.

Для разных сайтов существует ряд способов, которые в совокупности могут дать нужный результат. Также стоит учесть неосторожность или неосведомленность пользователя, которая приводит к ошибкам, с помощью которых злоумышленник способен получить доступ к любым его данным.

Спасибо за внимание.

Подготовил: Ганюшкин Данила Сергеевич