министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

*факультет Программной инженерии и компьютерной техники*

*Дисциплина «Информационная безопасность»*

**Лабораторная работа №4**

Взлом сервера IIS

Группа: P3417

Выполнил: Ореховский А.

Проверила: Маркина Т. А.

Санкт-Петербург,

2021г

# Взлом сервера IIS 5

Хакинг сервера IIS базируется на уязвимостях программных средств сервера, основанных на протоколах HTTP (Hypertext Transfer Protocol - Протокол передачи гипертекста) и CGI (Common Gateway Interface - Общий шлюзовой интерфейс), а также на уязвимых сценариях сервера IIS, открывающих доступ к ресурсам серверного компьютера.

Функция протокола HTTP - обеспечение взаимодействия сервера и клиента Web при запросе и получении текстовой информации. Для этого протокол HTTP предоставляет несколько методов, основным из которых является метод GET. Когда Web-браузер запрашивает у сервера информационный ресурс (скажем, текстовый файл), он использует метод GET, одновременно указывая адрес ресурса, например, **http://www.anyserver.com/documents/order.html**. Этот адрес указывает на файл **order.html** в каталоге **/documents** сервера IIS, которому соответствует каталог локальной файловой системы **c:\inetpub\wwwroot\documents**.

Протокол CGI регламентирует удаленные вызовы серверных сценариев со стороны клиентов. Вызовы сценариев выполняются с помощью запросов протокола HTTP, которые имеют такой вид:

**http://www.anysite.com/scripts/MyScript?Парaметр1+Параметр2**

Здесь **MyScript** - это название сценария, хранящегося в папке **/scripts** сервера IIS, а запись **?Параметр+Параметр2** определяет фактические параметры, передаваемые серверному сценарию **MyScript**. Сервер IIS определяет, что поступивший запрос предназначен для обработки сценарием, после чего запускает программу сценария, передает ей параметры и выполняет передачу результатов запроса клиенту.

Кроме протокола CGI, для работы со сценариями используются технологии ASP (Active Server Pages - Активные страницы сервера) и ISAPI (Internet Server Programming Interface - Программный интерфейс сервера Интернет). В технологии ASP вызов сценариев выполняется такой строкой запроса:

**http://www.anysite.com/scripts/MyScripts?Параметр1=Значение1&Параметр2=Значение2**

В результате исполняется сценарий **MyScript.asp**, который, как правило, генерирует новую страницу HTML. Интерфейс ISAPI предоставляет возможность удаленного вызова функций, хранимых в библиотеках ISAPI. Вызов этих функций выполняется по такому запросу HTTP:

**http://www.anysite.com/isapi.dll?Переменная1&Переменная2**

# Переполнение буфера IIS

Атаки на переполнение буфера — это "серебрянная пуля" для хакеров. При удачном расположении планет атака этого типа может позволить получить контроль над удаленной системой с помощью одного нажатия на кнопке. Служба 1IS всегда была одной из основных служб систем семейства Windows NT, которые доступны по Internet. Поэтому IIS являлась и является одной из главных целей для атак на переполнение буфера.

Переполнение буфера происходит, когда программа не выполняет проверку длины вводимых данных. Таким образом, любые неожидаемые данные ввода попадают в непредназначенную для них область стека исполнения процессора. Программист может так подобрать вводимые данные, чтобы в результате их исполнения был запущен его собственный код. Самое главное при использовании этого метода— создать так называемый код командного интерпретатора (shellcode) и разместить его в том месте, где буфер переполнится и "вылезет" в стек исполнения.

# HTTP Hacking

Протокол HTTP позволяет хакерам достичь много, поскольку его поддержка сервером IIS не отличается надежной защитой от попыток несанкционированного доступа. В ранних версиях IIS 2.0 достаточно было ввести такой адрес:

**http://www.anysite.com/../../../../../winnt/secret.file**

чтобы загрузить с Web-сервера информацию, содержащуюся в файле **secret.txt**. Это - пример ошибки в реализации системы защиты Windows, хранящей разрешения на доступ к информационным ресурсам в списках ACL. В более новых версиях IIS эта ошибка исправлена, но ее можно найти у Web-серверов других производителей. А взамен описанной уязвимости в последних версиях IIS имеются другие, и их список непрерывно пополняется, что можно видеть по сообщениям на сайтах, посвященных информационной безопасности.

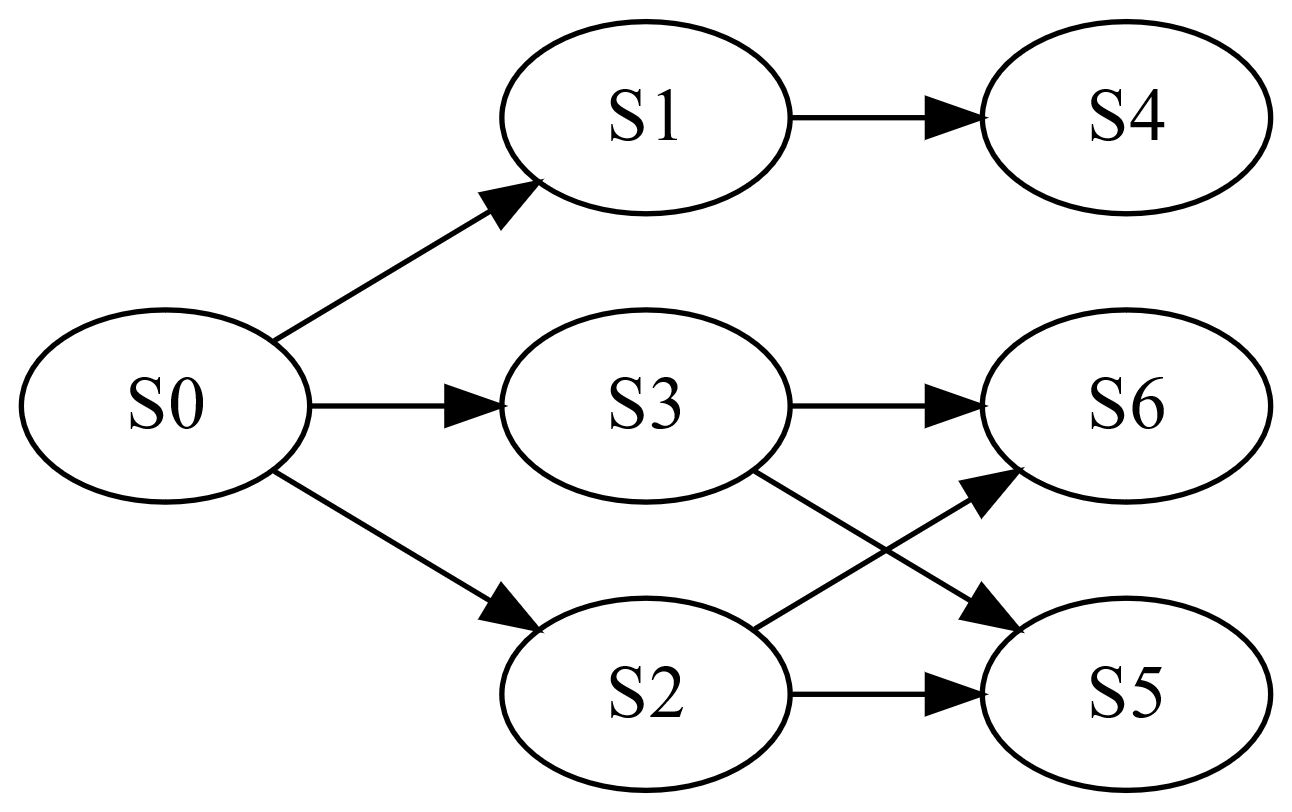
# Уязвимые сценарии

Одной из основных уязвимостей Web-серверов, в том числе сервера IIS — это плохое программирование сценариев, используемых в интерактивных Web-страницах. Дело в том, что для обмена информацией со сценариями Web-серверов используется протокол CGI (Common Gateway Interface - Общий шлюзовой интерфейс), который вообще не обеспечивает никакой защиты, а всего лишь регламентирует передачу параметров от клиента Web серверному сценарию. Получив запрос к сценарию CGI, сервер просто передает полученные параметры сценарию, запущенному на сервере. Причем права сценария на доступ к ресурсам серверного компьютера определяются контекстом безопасности Web-сервера, т. е., применительно к серверу IIS, с правами учетной записи System, обеспечивающей практически полный доступ к ресурсам системы.

То, что происходит с переданными CGI-сценарию параметрами, определяется программой, а программы пишут программисты. И каждый, кто хоть когда-либо писал программы, знает, насколько трудно и утомительно согласовать типы фактических и формальных параметров программы, и насколько мешает творческой фантазии необходимость скрупулезно проверять корректность передаваемых параметрами данных. Поэтому часто эта задача оставляется на потом, или вообще отбрасывается - и программа становится полностью зависимой от внешней среды.

Так что если, к примеру, в сценарий Perl, выполняемый в режиме интерпретации, т.е, шаг за шагом, по мере считывания кода программы, передать вместо, скажем, числового значения некий программный код, то не исключено, что вместо аварийного завершения сценарий сможет исполнить переданный код. И это - самые настоящие парадные двери для хакера, поскольку плохо написанных сценариев - хоть пруд пруди, и, немного поискав по сайтам Web, где-нибудь да наткнешься на открытые двери.

# Орграф



# Состояния

|  |  |
| --- | --- |
| Состояние | Описание |
| S0 | корректное состояние системы |
| S1 | вычисление доступных файлов |
| S2 | перебор доступных CGI/ ASP |
| S3 | ввод данных, которые переполнят буфер |
| S4 | доступ к файлам |
| S5 | исполнение кода с правами учетной записи |
| S6 | отказ обслуживания |