Международный союз электросвязи

МСЭ-Т X.1211

(09/2014)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность в киберпространстве –
Кибербезопасность

Методы предотвращения атак на базе веб-сети

Рекомендация МСЭ-Т X.1211

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1211

Методы предотвращения атак на базе веб-сети

Резюме

В Рекомендации МСЭ-Т X.1211 описываются методы, которыми можно смягчить последствия атак на базе веб-сети, происходящих, когда используются уязвимости хостов веб-сайтов и внедряется вредоносный код, который может заразить компьютер пользователя. В нескольких дополнениях показано, как происходят атаки, а также какие меры по устранению можно предпринять.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1211	26.09.2014 г.	17-я	11.1002/1000/12154

Ключевые слова

Предотвращение, внедрение SQL, шпионское ПО, подозрительный контент, уязвимость, атака на базе веб-сети.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1211

Методы предотвращения атак на базе веб-сети

1 Сфера применения

В настоящей Рекомендации представлены методы предотвращения атак на базе веб-сети. Описываются сценарии использования для распространения вредоносного кода через веб-сеть, а также функциональные методы и функции для предотвращения атак на базе веб-сети.

2 Справочные документы

Отсутствуют.

3 Термины и определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 ресурс (asset) [b-ISO/IEC 27000]: Все, что представляет ценность для организации.

ПРИМЕЧАНИЕ. – Существует большое число типов ресурсов, в том числе:

a) информация;

b) программное обеспечение, например компьютерная программа;

c) физические ресурсы, например компьютер;

d) услуги;

e) люди, а также их квалификация, навыки и опыт; и

f) нематериальные активы, например репутация и престиж.

3.1.2 случай атаки (attack instance) [b-ITU-T X.1544]: Конкретная подробно описанная атака против приложения или системы, целью которой являются уязвимые или слабые места в этой системе.

3.1.3 схема атаки (attack pattern) [b-ITU-T X.1544]: Обобщение общих подходов в случае атаки, наблюдаемой в неконтролируемых ситуациях в отношении приложений или систем (например, введение запроса SQL, атака через посредника, перехват сеанса связи и т. д.).

ПРИМЕЧАНИЕ. – С одной схемой атаки могут быть связаны множество различных случаев атаки.

3.1.4 язык описания гипертекстовых документов (hyperext markup language, HTML) [b-ITU-T M.3030]: Система информации кодирования из широкого диапазона областей (например, текст, графика, результаты запросов к базам данных) для отображения браузерами всемирной "паутины". В документ вставляются специальные коды, называемые тегами, для того чтобы иметь возможность сообщить браузеру, каким образом представлять информацию.

3.1.5 вредоносное программное обеспечение (malware) [b-ISO/IEC 27033-1]: Вредоносное программное обеспечение, созданное специально для нанесения ущерба или разрушения системы путем осуществления атак, направленных на нарушение конфиденциальности, целостности и/или доступности.

3.1.6 метод запутывания (obfuscation technique) [b-NIST SP 800-83]: Способ создания вируса с целью усложнения его обнаружения.

3.1.7 информация, позволяющая установить личность (personally identifiable information, PII) [b-ITU-T X.1252]: Любая информация: a) которая идентифицирует или может использоваться для идентификации, обращения или установления местоположения лица, к которому такая информация относится; b) на основе которой может быть получена информация идентификации или контактная информация частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

3.1.8 угроза (threat) [b-ITU-T X.800]: Потенциальное нарушение безопасности.

3.1.9 домен безопасности (security domain) [b-ITU-T T.411]: Набор ресурсов, в отношении которых действует одна стратегия безопасности.

3.1.10 орган домена безопасности (security domain authority) [b-ITU-T X.810]: Орган безопасности, ответственный за реализацию стратегии безопасности в отношении какого-либо домена безопасности.

3.1.11 стратегия безопасности (security policy) [b-ITU-T T.411]: Набор правил, которые определяют процедуры и услуги, требуемые для поддержания заданного уровня безопасности набора ресурсов.

3.1.12 сигнатура (signature) [b-NIST SP 800-83]: Набор характеристик известных экземпляров вредоносного кода, который может использоваться для выявления известного вредоносного кода и некоторых новых вариантов известного вредоносного кода.

3.1.13 шпионское ПО (spyware) [b-NIST SP 800-83]: Вредоносный код, предназначенный для нарушения конфиденциальности пользователя.

3.1.14 плагин веб-браузера [b-NIST SP 800-83]: Механизм для отображения или выполнения определенных типов контента через веб-браузер.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 аномалия (anomaly): Последовательность в данных, которая не соответствует ожидаемому поведению.

3.2.2 атаки "теневая загрузка" (drive-by-download attacks): Схема атаки на базе веб-сети, предпринимаемой при посещении пользователем веб-сайта, которая использует уязвимости браузера и запускает автоматическую загрузку и установку вредоносного кода без ведома или разрешения этого пользователя.

3.2.3 атака на базе веб-сети (web-based attack): Схема атак, при которой злоумышленники нарушают безопасность законных веб-сайтов, в результате чего в приложение внедряется вредоносный код, который, в свою очередь, может использоваться для заражения компьютера пользователя, посещающего эти веб-сайты, или использовать уязвимости веб-сайтов для инициирования атак на компьютерные системы пользователя, посещающего эти веб-сайты, что происходит без применения вредоносного программного обеспечения.

3.2.4 система защиты от атак на базе веб-сети (web-based attack protection system): Комплекс систем, которые обнаруживают уязвимости, вредоносное программное обеспечение или вредоносные коды, внедренные в законный веб-сайт, и сообщают администратору веб-сети о результатах обнаружения, что неизбежно ведет к их удалению.

ПРИМЕЧАНИЕ. – Мероприятия по обнаружению можно планировать как выполняемые по графику или как инициируемые событиями в сети или запросами от других систем.

3.2.8 компьютер-зомби (zombie computer): Компьютер, безопасность которого была нарушена злоумышленником, получившим контроль над этим компьютером и установившем на него вредоносные коды, такие как компьютерные вирусы, троян или ботнет, которые могут использоваться для осуществления злонамеренных действий, например распространения спама по электронной почте и атак типа "отказ в обслуживании".

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

CAPEC	Common Attack Pattern Enumeration and Classification	Перечень и классификация общеизвестных схем атак
CSRF	Cross-Site Request Forgery	Подделка межсайтовых запросов
CWE	Common Weakness Enumeration	Перечень общеизвестных слабых мест
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DOM	Document Object Model	Объектная модель документа

HTML	HyperText Markup Language		Язык описания гипертекстовых документов
HTTP	HyperText Transfer Protocol		Протокол передачи гипертекста
ID	Identity		Идентичность
IODEF	Incident Object Description Exchange Format		Формат обмена описаниями инцидентов как объектов
LDAP	Lightweight Directory Access Protocol		Упрощенный каталог доступа к каталогам
MITM	Man-in-the-Middle		Посредник
OS	Operating System	ОС	Операционная система
OWASP	Open Web Applications Security Project		Открытый проект обеспечения безопасности веб-приложений
PC	Personal Computer	ПК	Персональный компьютер
PII	Personally Identifiable Information		Информация, позволяющая установить личность
PUI	Program under Inspection		Программа под контролем
SNS	Social Network Service		Сервис социальной сети
SQL	Structured Query Language		Язык структурированных запросов
SSRF	Server-Side Request Forgery		Подделка серверного запроса
S/W	Software	ПО	Программное обеспечение
URI	Uniform Resource Identifier		Универсальный идентификатор ресурса
URL	Uniform Resource Locator		Универсальный указатель ресурса
XSPA	Cross-site Port Attack		Межсайтовая атака портов
XSS	Cross-Site Scripting		Межсайтовая атака с внедрением сценария

5 Условные обозначения

Отсутствуют.

6 Общий обзор

Вредоносное программное обеспечение, которое используется для нарушения безопасности информационных ресурсов, определяется как программное обеспечение, созданное специально для нанесения ущерба или разрушения системы путем осуществления атак, направленных на нарушение конфиденциальности, целостности и/или доступности.

Атаки на базе веб-сети – это атаки, при которой злоумышленники пытаются нарушить безопасность законных веб-сайтов, используя их уязвимости, в результате чего на эти веб-сайты внедряется вредоносный код, который, в свою очередь, может использоваться для заражения компьютера пользователя, посещающего эти веб-сайты. Вредоносный код может принимать различные формы: это может быть невидимый тег встроенного фрейма, направляющий пользователя посетить атакуемый сайт, или это может быть вредоносное приложение, написанное на языке компьютерной программы (например, сценарий или программный компонент). Типичными примерами уязвимостей, используемых при атаках на базе веб-сети, является внедрение SQL и подделка межсайтовых запросов.

Схема атаки на основе подделки межсайтовых запросов [b-CAPEC-62] представляет собой тип атаки на базе веб-сети, при которой передаются несанкционированные команды для выполнения или запрашивается выполнение нежелательных действий на доверенном веб-сайте без ведома пользователя, когда этот пользователь подключен к доверенному веб-сайту. Внедрение языка структурированных запросов (SQL) является еще одним типом атаки на базе веб-сети на управляемый базой данных веб-сайт, при которой злоумышленник добавляет код языка структурированных запросов (SQL) в поле ввода веб-формы для получения доступа к ресурсам или внесения изменений в данные. Эта атака используется для хищения информации из базы данных, из которой данные обычно

недоступны, и/или для получения доступа к главным компьютерам организации через компьютер, на котором размещена эта база данных. Встроенный фрейм, известный также как тег iframe [b-iframe], используется для встраивания невидимого документа в текущий документ на языке описания гипертекстовых документов (HTML), обманом побуждая пользователя щелкнуть по невидимому документу посредством кликджекинга (clickjacking) [b-CAPEC-103].

В последнее время уровень атак на базе веб-сети существенно возрастает в результате роста объема использования вычислительных устройств конечного пользователя и увеличения числа веб-сайтов, содержащих вредоносное программное обеспечение.

Так, антивирусные методы могут применяться на стороне сервера и могут внедряться брандмауэры веб-приложений на прокси-серверах для экономически эффективного применения этих методов.

При осуществлении атак на базе веб-сети администраторы веб-сайтов могут не знать о том, что веб-сайты взломаны, в них внедрены вредоносные коды и они используются для распространения вредоносных кодов. Кроме того, пользователи тоже не знают о том, что их компьютеры могут заражаться вредоносными кодами с сайтов, которые они посещают. Ряд инцидентов может быть предотвращен путем установки антивирусного программного обеспечения (ПО), однако это не обеспечивает оптимального решения.

Рост объема атак на базе веб-сети обусловливается следующими причинами:

- возрастает объем атак в форме теневых загрузок с общедоступных веб-сайтов;
- атаки в значительной степени скрыты и изменяются в динамическом режиме, делая неэффективными традиционные средства обнаружение вредоносных кодов и предотвращения их распространения;
- атаки направлены на плагины веб-браузеров конечных пользователей;
- атаки, направленные на внедрение SQL, используются для заражения общедоступных веб-сайтов;
- содержащие вредоносные коды рекламные объявления перенаправляют пользователей на вредоносные веб-сайты; и
- бурный рост уникальных и целевых образцов вредоносного программного обеспечения.

7 Методы системы защиты от атак на базе веб-сети

7.1 Общие методы

Методы системы защиты от атак на базе веб-сети характеризуются следующим:

- в силу проектного решения они масштабируемы, устойчивы и надежны;
- они эксплуатируются в рамках нескольких доменов безопасности, каждый из которых управляется ответственным за безопасность администратором; и
- они осуществляют обмен информацией об уязвимостях веб-сайтов, веб-сайтах или о зараженных вредоносным программным обеспечением веб-сайтах (то есть о веб-сайтах с невидимым встроенным тегом, перенаправляющим пользователей на зараженный вредоносным программным обеспечением веб-сайт) [b-CAPEC-103].

ПРИМЕЧАНИЕ. – Существующий формат обмена описаниями инцидентов как объектов (IODEF) [b-ITU-T X.1541] может использоваться для обмена информацией.

- они применяются в модели развертывания одного из двух типов: централизованная модель и распределенная модель. В централизованной модели вся информация о зараженных вредоносным программным обеспечением веб-сайтах и типах вредоносного программного обеспечения должна сообщаться, сопровождаться и управляться централизованным сервером. В распределенной модели каждый домен безопасности должен создавать ответственного агента, и должен осуществляться обмен информацией о зараженных вредоносным программным обеспечением веб-сайтах и типах вредоносного программного обеспечения между ответственными агентами, которые существуют в распределенном местоположении.
- они конфигурируются иерархическим образом для упрощения масштабируемой работы.

7.2 Функциональные методы

Функциональные методы системы защиты от атак на базе веб-сети характеризуются следующим:

- они выявляют известное вредоносное программное обеспечение в законном веб-контенте и предупреждают установку вредоносного программного обеспечения на веб-сайты;
- они обнаруживают невидимый встроенный тег, перенаправляющий пользователя на другие веб-сайты, которые устанавливают вредоносное программное обеспечение;
- они обнаруживают уязвимости, которые могут использоваться для типовых атак на базе веб-сети, таких как внедрение SQL, межсайтовые ссылки и т. д., как это описано в Дополнении IV;
- они осуществляют анализ на основе сигнатур или аналогичный анализ для обнаружения известного вредоносного программного обеспечения на веб-сайте;
- они осуществляют анализ на основе поведения для определения неизвестного вредоносного программного обеспечения;
- они сообщают администратору веб-сайта о заражении вредоносным программным обеспечением для удаления вредоносного программного обеспечения с сайтов;
- они обнаруживают скрытое вредоносное программное обеспечение, использующее дробление строки, кодирование строки, кодирование пользовательской строки, изменение поведения сценария, запутывающие функции изменения объектной модели документа (DOM), скрытые за общедоступными услугами ссылки и перенаправление страниц на веб-сайте;
- они обнаруживают вредоносное программное обеспечение, которое может использоваться для атак типа "подделка межсайтовых ссылок" на веб-сайтах;
- они анализируют поведение подозрительного вредоносного программного обеспечения на веб-сайтах;
- они информируют пользователей о зараженных веб-сайтах, в случае если пользователь посещает эти зараженные веб-сайты;
- они сообщают администратору безопасности о том, что этот веб-сайт, зараженный вредоносным кодом, может в перспективе использоваться для атаки на базе веб-сети, если система защиты от атак на базе веб-сети обнаруживает вредоносное программное обеспечение на веб-сайте;
- они осуществляют обмен информацией о черных списках вредоносных веб-сайтов; и
- они определяют уязвимости веб-сайтов, в том числе внедрение SQL и межсайтовое внедрение сценария, и сообщать администратору этих веб-сайтов об их обнаруженных уязвимостях.

7.3 Методы управления

Методы управления системы защиты от атак на базе веб-сети характеризуются следующим:

- они обеспечивают управление безопасностью на основе стратегий безопасности при использовании в разных доменах безопасности;
- они имеют унифицированный интерфейс в целях поддержки управления для системы централизованного управления;
- они поддерживают управление доверием и принимать данные о событиях, связанных с атаками, только от доверенных доменов безопасности;
- они поддерживают управление ресурсами системы и защищать систему от перегрузки; и
- они поддерживают управление эксплуатацией и техническим обслуживанием, включая управление конфигурацией системы, управление журналами регистрации, мониторинг состояния систем и т. д.

7.4 Методы обеспечения безопасности и конфиденциальности

Методы обеспечения безопасности и конфиденциальности системы защиты от атак на базе веб-сети характеризуются следующим:

- конфиденциальность, аутентификация источника данных и целостность информации, которой обмениваются через интерфейс связи домены безопасности;

- предотвращение утечки информации, позволяющей установить личность (PII), которую обрабатывает веб-система предотвращения;
- обеспечивают устойчивость к различным сетевым атакам, например атакам DDoS; и
- обеспечивают функции проведения аудита, которые могут отследить неправомерное использование собранной для системы защиты от атак на базе веб-сети информации и злоупотребление такой информацией неавторизованными объектами.

8 Функции системы защиты от атак на базе веб-сети

Система защиты от атак на базе веб-сети должна обеспечивать, как минимум, следующие функции, не ограничиваясь ими:

- обнаружение всех известных уязвимостей на веб-сайтах;
- обнаружение веб-сайтов, содержащих вредоносное программное обеспечение, используемое для распространения вредоносного программного обеспечения;
- оповещение администратора веб-сайтов, содержащих вредоносное программное обеспечение и имеющих известные уязвимости, которые могут использоваться злоумышленниками;
- сбор необходимой информации об уязвимостях веб-сайтов и о вредоносном программном обеспечении, которое они содержат;
- совместное использование информации о зараженных вредоносным программным обеспечением веб-сайтах и о веб-сайтах, которые используются для распространения вредоносного программного обеспечения между доверенными объектами в домене безопасности и между несколькими доменами;
- реализация стратегии безопасности системы защиты на базе веб-сети в домене; и
- защита системы защиты от атак на базе веб-сети от любых атак.

9 Формат обмена информацией

Следует наращивать совместное использование информации об обмене информацией по результатам анализа вредоносного программного обеспечения (например, перечень и характеристики атрибутов вредоносного программного обеспечения). При применении настоящей Рекомендации можно использовать [b-ITU-T X.1546] для обмена информацией по результатам анализа вредоносного программного обеспечения.

Дополнение I

Сценарии атак на базе веб-сети

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Сценарий заражения вредоносным программным обеспечением

На рисунке I.1 показан типовой сценарий атак на базе веб-сети.

1 Злоумышленники нарушают безопасность законного веб-сайта, имеющего уязвимости, и затем устанавливают вредоносное программное обеспечение или сценарий, которые используются для осуществления атаки на компьютер пользователя, или устанавливают теги для перенаправления доступа пользователя на веб-сайт, содержащий вредоносное программное обеспечение, для атаки на компьютер пользователя, который посетил этот веб-сайт.

2 Когда пользователь-жертва посещает веб-сайт, безопасность которого была нарушена злоумышленниками, на компьютер этого пользователя совершает атаку внедренное вредоносное программное обеспечение или этот пользователь перенаправляется на другой веб-сайт, который содержит вредоносное программное обеспечение для атаки на компьютер пользователя.

3 Если в компьютере пользователя имеются уязвимости браузера, которые могут быть использованы определенным вредоносным программным обеспечением, это вредоносное программное обеспечение осуществляет установку на компьютер пользователя, и он становится компьютером, зараженным вредоносным программным обеспечением без ведома или разрешения пользователя.

4 Установленное на компьютер пользователя вредоносное программное обеспечение может использоваться для осуществления массированных атак типа "распределенный отказ в обслуживании" (DDoS) или для хищения личной информации, такой как идентичность (ID) и пароль, и передачи ее злоумышленникам.

Рисунок I.1 – Типовой сценарий атак на базе веб-сети

I.2 Подделка межсайтовых запросов (CAPEC-62)

Подделка межсайтовых запросов (CSRF) может стать причиной того, что жертва неосознанно сделает один или несколько запросов на основе протокола передачи гипертекста (HTTP) к уязвимому веб-сайту, которому пользователь доверяет. Типовая атака типа "подделка межсайтовых запросов" может нарушить соответственно целостность данных и обеспечить злоумышленнику возможность изменить информацию, которую хранит уязвимый веб-сайт.

Когда веб-сайт запрашивает аутентификацию пользователя, он, как правило, не требует от пользователя ввода своего пароля для каждого запроса HTTP. Вместо этого веб-сайт определяет состояние аутентификации пользователя между несколькими запросами HTTP с помощью жетонов, таких как куки сеанса или заголовок авторизации HTTP. Именно в этом заключается проблема: веб-браузеры запоминают жетон, связанный с универсальным указателем ресурса (URL), и автоматически прикрепляют жетон, когда веб-сайту выдается новый запрос HTTP, даже если этот запрос был задуман не пользователем. CSRF использует поведение браузера. В случае CSRF пользователю достаточно лишь посетить веб-сайт с вредоносным кодом, который может содержать логику JavaScript, которая выдает (вероятно скрытые) запросы HTTP другим веб-сайтам (например, банку пользователя), и эти запросы HTTP могут быть авторизованы этим веб-сайтом в силу наличия жетонов. CSRF позволяет осуществить различные виды вирусных атак, такие как отправка электронной почты с почтовых веб-сервисов, размещение комментария в блоге от имени пользователя, изменение списка друзей пользователя в сервисе социальной сети (SNS) или изменение установок в домашнем маршрутизаторе.

I.3 Межсайтовые атаки портов/подделки серверного запроса

Межсайтовые атаки портов/подделка серверного запроса (XSPA/SSRF) – это метод злоупотребления веб-приложениями, при котором обрабатываются URL, поступающие со входа веб-браузера. Типовая атака XSPA/SSRF направлена на внутреннюю сеть через уязвимое приложение. Атака может вызывать сканирование портов, нарушение конфиденциальности данных, вести к выполнению неразрешенной программы и использованию уязвимых ресурсов внутренней сети.

Приложение считается уязвимым к XSPA/SSRF, если оно не проверяет ответы, полученные от удаленных серверов, и входные данные, обеспечиваемые конечным пользователем. Например, приложение, которое загружает изображение с предоставленного пользователем URL, может получить доступ к ресурсу внутренней сети, если пользователь объявляет URL как "http://localhost/secret.txt". В некоторых случаях могут использоваться специальные универсальные идентификаторы ресурсов (URI), для того чтобы уязвимое приложение направляло запрос к конкретным сервисам, таким как "https", "gopher", "ftp", "ldap". Могут также использоваться определяемые языком средства, такие как "php://fd", "php://memory".

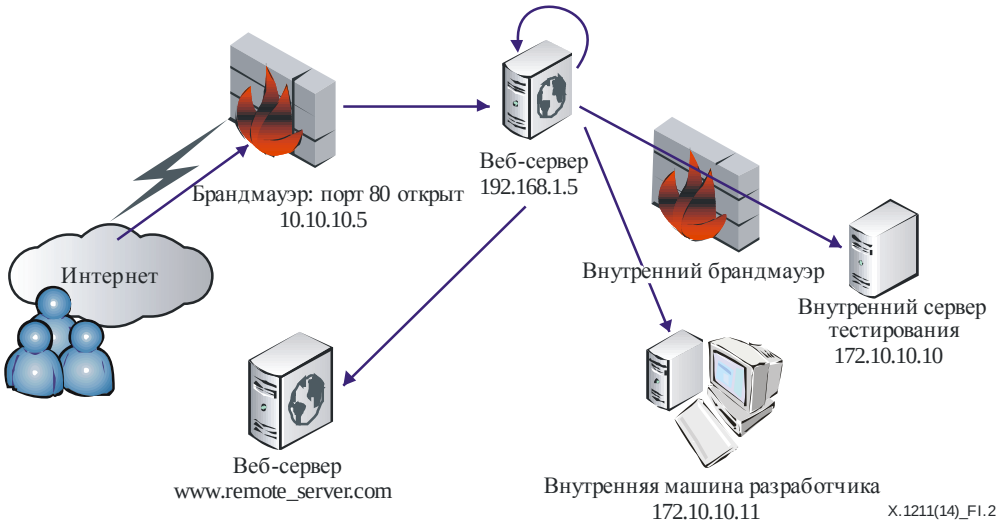

Рисунок I.2 – Типовой сценарий атак типа "межсайтовые атаки портов/ подделки серверного запроса"

I.4 Внедрение SQL (CAPEC-66)

Типовой сценарий внедрения SQL [b-CAPEC-66] основан на неудовлетворительной логической проверке входных данных веб-приложений. Каналами ввода могут служит запросы GET и POST HTTP, cookie-файлы браузера, полезная нагрузка на базе XML, входные файлы и другие.

Затем целевые входные данные внедряются в запрос SQL. Вот базовый пример внедрения SQL в параметр HTTP "GET":

- Первоначальный запрос – "SELECT title, content FROM table1 WHERE id = %d",

где "id" – целевой параметр.

При обычных условиях "id" – какое-либо натуральное число. Но ввиду отсутствия логической проверки вместо числа злоумышленник может вставить следующие входные данные:

- %d = "1 UNION SELECT user, password FROM secret_table".

Это приведет к несанкционированному доступу к секретной таблице ("secret_table"), следствием чего станет раскрытие конфиденциальных данных непосредственно в выходных данных браузера.

В зависимости от реализации базы данных SQL такая атака может привести к:

- раскрытию конфиденциальных данных из базы данных или файловой системы;
- потере/изменению данных;
- внедрению "черных ходов" и увеличению привилегий; и
- развертыванию вредоносного программного обеспечения у конечных пользователей, посещающих этот сайт.

I.5 Обнаружение вредоносного программного обеспечения на веб-сайтах

Методы, используемые для обнаружения вредоносного программного обеспечения, могут быть сгруппированы по двум категориям: обнаружение по аномалиям и обнаружение по сигнатурам [b-NA].

Для метода обнаружения по аномалиям критерием определения вредоносности находящейся под контролем программы являются составляющие штатного поведения. Конкретный тип обнаружения по аномалиям называется обнаружением на основе спецификаций. Методы обнаружения на основе спецификаций используют некоторые спецификации или наборы правил допустимого поведения, с тем чтобы принять решение о вредоносности находящейся под контролем программы. Программы, нарушающие набор правил или спецификацию, считаются вредоносными.

В случае обнаружения по сигнатурам критерием определения вредоносности находящейся под контролем программы являются характеристики того, что известно, как вредоносный код. Характеристики или сигнатура поведения вредоносного кода являются ключом эффективности метода обнаружения по сигнатурам.

Для каждого метода обнаружения может использоваться один из трех различных подходов: статический, динамический или смешанный. Конкретный подход или анализ метода на основе аномалий или сигнатур определяется тем, как этот метод осуществляет сбор информации для обнаружения вредоносного программного обеспечения. В статическом анализе для определения вредоносности используются синтаксические или структурные свойства программы (статический)/процесса (динамический), находящихся под контролем (PUI). Например, при статическом подходе к обнаружению по сигнатурам для определения вредоносности будет использоваться только структурная информация (например, последовательность байтов), а при динамическом подходе будет использоваться информация о времени работы (например, системы, встречающиеся в стеках для переменных программы) PUI.

В целом статический подход заключается в попытке обнаружения вредоносного программного обеспечения до выполнения программы, находящейся под контролем. Динамический подход, напротив, заключается в попытке определения вредоносного поведения в процессе выполнения программы или после выполнения программы.

Существуют смешанные методы, сочетающие эти два подхода. В таком случае для обнаружения вредоносного программного обеспечения используется статическая и динамическая информация.

Существует несколько методов обнаружения вредоносного программного обеспечения на веб-сайтах; эти методы описаны в Дополнении III.

Дополнение II

Метод заражения компьютера пользователя вредоносным программным обеспечением

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Настоящее дополнение предназначено для описания типовых сценариев, которые могут использовать злоумышленники, в помощь администраторам для понимания этих сценариев.

Первый шаг атаки на базе веб-сети заключается в установке и запуске вредоносных кодов вирусов на компьютере пользователя. Эти коды могут содержать регистраторы клавиатуры и руткиты (которые могут превратить компьютер пользователя в компьютер-зомби или направить конфиденциальную информацию пользователя злоумышленникам).

Цель атаки может достигаться либо путем использования ряда известных уязвимостей различных компонентов программного обеспечения, доступных с помощью браузера (например, компоненты операционной системы, доступные с помощью браузера через ActiveX и т. д.), или применяя методы атаки с использованием психологических приемов, заставляющих пользователя установить и запустить на своей системе вредоносное программное обеспечение. Кроме того, во время этих атак предпринимаются попытки хищения учетных данных пользователя, для чего применяется фишинг или атаки типа "межсайтовая атака с внедрением сценария", запускаемые в скрытом встроенном фрейме.

Существует ряд способов, которые используются для заражения компьютера пользователя вредоносным программным обеспечением: использование компонента ActiveX, методы психологической атаки, пропущенный кодек, инструментальные средства удаления вредоносного программного обеспечения и атаки типа "подделка межсайтовых запросов". Подробная информация содержится в [b-NTobjectives]. Кроме того, существует список общих шаблонов атак и полный перечень и классификация схем в [b-ITU-T X.1544].

Дополнение III

Типовые примеры метода запутывания

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Зараженный вредоносным кодом контент использует метод запутывания, с тем чтобы скрыть вредоносное программное обеспечение как от человека, так и от программного обеспечения обнаружения уязвимостей [b-ITU-T X.1520]. Методы запутывания достаточно эффективны в силу следующих причин:

- большое число администраторов веб-сайтов настороженно относятся к удалению кодов сценариев, которых они не понимают;
- администраторы баз данных затрудняются при проведении чистки зараженных баз данных, не зная, какие шаблоны искать;
- большое число методов обнаружения основываются на часто используемых формах или других методах, связанных с поиском строки, вследствие чего усложняется обнаружение запутанного HTML.

Существует несколько методов запутывания: дробление строки, кодирование строки, кодирование пользовательской строки, изменение поведения сценария, запутывающие функции изменения DOM, скрытые за общедоступными услугами ссылки и перенаправление страниц. Подробная информация содержится в [b-NTobjectives].

Дополнение IV

Методы предотвращения атак на базе веб-сети

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Настоящее дополнение предназначено для представления ряда методов обнаружения вредоносного программного обеспечения на веб-сайтах [b-NTobjectives]. Вредоносный контент может быть обнаружен путем сопоставления сигнатур контента, внесения в черный список сайтов атак или анализ контента на предмет подозрительного поведения с помощью проприетарных механизмов.

IV.1 Удаление уязвимостей веб-сайта

Простейший способ заключается в удалении уязвимостей веб-сайта, включая внедрение SQL и межсайтовые атаки с внедрением сценария. Если злоумышленник не сможет вставить в веб-сайт вредоносный контент, то браузер клиента не будет выполнять вредоносное программное обеспечение, вставленное в веб-сайт. Следовательно, наиболее эффективным способом предотвращения атак на базе веб-сети является устранения с веб-сайта всех уязвимостей.

IV.2 Сопоставление сигнатур

Учитывая, что существует большое число методов запутывания и автоматических инструментов запутывания вредоносного программного обеспечения, в практическом плане нецелесообразно обнаруживать на веб-сайте содержащий вредоносное программное обеспечение контент, используя метод обнаружения по сигнатурам. Широко известно, что злоумышленники могут автоматически кодировать вредоносный контент с помощью нового ключа для каждого веб-сайта, в результате чего для каждого веб-сайта создается иная сигнатура вредоносного программного обеспечения.

Вместе с тем контент с открытым вредоносным программным обеспечением не изменяется часто, и, следовательно, вредоносное программное обеспечение на веб-сайте может быть обнаружено с помощью сигнатуры. Если контент с открытым вредоносным программным обеспечением получен путем декодирования кодированного вредоносного программного обеспечения, а сигнатура открытого вредоносного программного обеспечения рассчитывается на основании открытого вредоносного программного обеспечения, то с помощью этого метода может быть обнаружено вредоносное программное обеспечение путем сравнения рассчитанной сигнатуры вредоносного программного обеспечения с ранее составленным перечнем всех сигнатур контента с вредоносным программным обеспечением, известными заранее.

IV.3 Внесение сайта в черный список

Внесение сайтов атак в черный список относится к наиболее ценным методам обнаружения. При том что вредоносный контент может быть полностью размещен на хорошем веб-сайте (без потребности в автоматической загрузке каких-либо сценариев или встроенных фреймов с сайта атаки, что скрывает их связь с сайтом атаки), для завершения предпринятой атаки необходим обмен определенными данными с сайтом атаки. Этот необходимый обмен данными может принимать разные формы: сценарий атаки должен загрузить вредоносное программное обеспечение с сайта атаки или отправить собранные личные данные из системы пользователя на сайт злоумышленника, или нечто подобное. В любом случае для сценария атаки необходимо установление соединения с сайтом атаки.

Если существует алгоритм обнаружения для внешних ресурсов к перечню занесенных в черный список сайтов, может возникнуть подозрение, что этот веб-сайт содержит вредоносное программное обеспечение. Следовательно, любые удары, направленные на занесенные в черный список сайты, будут свидетельствовать о присутствии вредоносного контента на анализируемой странице.

IV.4 Обнаружение методов запутывания

Если веб-сайт содержит контент страницы, закодированный с применением методов запутывания, это может стать обоснованным указателем на то, что этот веб-сайт имеет вредоносное намерение. Например, если веб-сайт содержит контент с длинной кодированной строкой, то это может быть вредоносный контент. Вместе с тем, хотя длинная строка вызывает подозрение, нельзя всегда предполагать, что этот веб-сайт содержит вредоносный контент, до тех пор пока не будет выполнено его декодирование и анализ его действий.

IV.5 Оценка поведения подозрительного контента

Наиболее эффективным способом является анализ поведения подозрительного контента. Если деятельность контента вызывает подозрение, это может указывать на вредоносное намерение. Типичное поведение, которое может рассматривать как вредоносное, включает доступ к локальному жесткому диску, создание объекта оболочки приложения и загрузку (доступ) внешнего исполняемого контента.

Дополнение V

Типовые примеры рисков безопасности приложений OWASP

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Открытый проект обеспечения безопасности веб-приложений (OWASP) – сотрудничество на основе открытых кодов по созданию базирующихся на веб-сети инструментов, технологий и методик обеспечения безопасности, объединяющее лидеров отрасли, образовательные организации и отдельных лиц со всего мира, опубликовал список OWASP топ-10 успешных атак на базе веб-сети [b-OWASP] и CWE [b-ITU-T X.1524] CWE-928: слабые места в топ-10 успешных атак на базе веб-сети OWASP [b-CWE], которые представлены в таблице V.1.

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-1 – Внедрение	Любое лицо, имеющее возможность направить системе недоверенные данные, включая внешних пользователей, внутренних пользователей и администраторов.	Злоумышленники предпринимают простые атаки на базе текста, которые используют синтаксис целевого интерпретатора. Практически любой источник данных может стать вектором внедрения, в том числе внутренний источник.	Бреши внедрения возникают, когда приложение направляет недоверенные данные интерпретатору. Бреши внедрения весьма распространены, особенно в унаследованном ПО, часто обнаруживаются в запросах SQL, запросах LDAP, запросах XPath, командах ОС, программных аргументах и т. д. Бреши внедрения легко обнаруживаются при анализе ПО, но значительно сложнее – при тестировании. Помочь злоумышленникам обнаружить их могут сканеры и фазеры.	Внедрение может привести к потере или искажению данных, отсутствию подотчетности или отказу в доступе. Внедрение может иногда привести к полному захвату главной машины.	Рассмотрите коммерческую ценность затронутых данных и платформы, на которой работает интерпретатор. Все данные могут быть похищены, изменены или уничтожены. Может ли пострадать ваша репутация?	CWE-77, CWE-78, CWE-89, CWE-90, CWE-91, CWE-929
A-2 – Нарушение аутентификации и управления сеансом	Рассмотрите анонимных внешних злоумышленников, а также пользователей с собственными учетными записями, которые могут предпринять попытку хищения учетных записей других пользователей. Рассмотрите также внутренних сотрудников, которые стремятся замаскировать свои действия.	Злоумышленник использует утечки или бреши в функциях аутентификации или управлении сеансом (например, незащищенные учетные записи, пароли ID сеансов) для имитации пользователей.	Разработчики часто создают клиентские схемы аутентификации и управления сеансом, однако сложно создать эти схемы корректно. Вследствие этого в таких клиентских схемах зачастую имеются бреши в таких областях, как выход из системы, управление паролями, таймауты, функция запоминания пользователя, секретный вопрос, обновление учетной записи и т. д. Поиск таких брешей может оказаться затруднительным в силу уникальности каждой реализации.	Такие бреши могут открыть возможность атаки на некоторые или все учетные записи. Добившись успеха, злоумышленник может делать все, что может делать жертва. Часто целями атак становятся привилегированные учетные записи.	Рассмотрите коммерческую ценность затронутых данных или функций приложений. Рассмотрите также коммерческие последствия того, что об уязвимости станет известно широкой общественности.	CWE-256, CWE-287, CWE-384, CWE-311, CWE-319, CWE-522, CWE-523, CWE-613, CWE-620, CWE-640, CWE-930

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-3 – Межсайтовая атака с внедрением сценария (XSS)	Рассмотрите каждого, кто может направить системе недоверенные данные, включая внешних пользователей, внутренних пользователей и администраторов.	Злоумышленник направляет сценарии атаки на базе текста, которые используют интерпретатор в браузере. Практически любой источник данных может стать вектором атаки, в том числе внутренний источник, например данные из базы данных.	Наиболее распространенной брешью в безопасности веб-приложений является XSS. Бреши XSS возникают, когда приложение содержит поставляемые пользователем данные на странице, направленной браузеру без надлежащей проверки или выхода из этого контента. Существуют три известных типа брешей XSS: 1) хранимый XSS; 2) отображенный XSS; и 3) XSS, основанный на DOM. Обнаружение большинства брешей XSS довольно просто осуществляется с помощью тестирования или анализа кода.	Злоумышленники могут выполнять сценарии на браузере жертвы, для того чтобы похищать сеансы пользователя, искажать веб-сайты, вставлять агрессивный контент, перенаправлять пользователей, похищать браузеры пользователя, используя вредоносное программное обеспечение, и т. д.	Рассмотрите коммерческую ценность затронутой системы и всех данных, которые она обрабатывает. Рассмотрите также коммерческие последствия того, что об уязвимости станет известно широкой общественности.	CWE-79, CWE-931
A-4 – Небезопасные прямые ссылки на объекты	Рассмотрите типы пользователей вашей системы. Имеют ли какие-либо пользователи только частичный доступ к определенным типам системных данных?	Злоумышленник, являющийся авторизованным пользователем системы, просто изменяет значение параметра, который содержит прямую ссылку на системный объект, на другой объект, для которого этот пользователь не авторизован. Предоставляется ли доступ?	Генерируя веб-страницы, приложения часто используют подлинное имя или ключ объекта. Приложения не всегда проверяют, авторизован ли пользователь для целевого объекта. Результатом этого является брешь, которую составляет небезопасная прямая ссылка на объект. Для обнаружения таких брешей осуществляющие тестирование лица могут легко изменить значения параметра. Анализ кода быстро покажет, проверена ли надлежащим образом авторизация.	Такие бреши могут нарушить все данные, на которые может содержать ссылку такой параметр. Если ссылки на объекты не являются непредсказуемыми, злоумышленник может легко получить доступ ко всем имеющимся данным этого типа.	Рассмотрите коммерческую ценность раскрытых данных. Рассмотрите также коммерческие последствия того, что об уязвимости станет известно широкой общественности.	CWE-22, CWE-99, CWE-639, CWE-932

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-5 – Небезопасная конфигурация	Рассмотрите анонимных внешних злоумышленников, а также пользователей с собственными учетными записями, которые могут предпринять попытку нарушения системы. Рассмотрите также внутренних сотрудников, которые стремятся замаскировать свои действия.	Злоумышленник осуществляет доступ к стандартным учетным записям, неиспользуемым страницам, через незакрытые бреши, к незащищенным файлам и директориям и т. д., для того чтобы получить неразрешенный доступ к системе или собрать сведения о системе.	Небезопасная конфигурация может возникнуть на любом уровне прикладного стека, включая платформу, веб-сервер, сервер приложений, базу данных, структуру и пользовательский код. Разработчикам и системным администраторам необходимо взаимодействовать для обеспечения надлежащей конфигурации всего стека. Для обнаружения недостающих корректирующих вставок, ненадлежащей конфигурации, использования стандартных учетных записей, излишних услуг и т. д. полезны автоматические сканеры.	Система может быть полностью нарушена без вашего ведома. Все ваши данные могут быть похищены или медленно изменяться с течением времени. На восстановление могут потребоваться значительные затраты.	Система может быть полностью нарушена без вашего ведома. Все ваши данные могут быть похищены или медленно изменяться с течением времени. На восстановление могут потребоваться значительные затраты.	CWE-2, CWE-16, CWE-209, CWE-215, CWE-548, CWE-933

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-6 – Раскрытие конфиденциальных данных	Рассмотрите, кто может получить доступ к вашим конфиденциальным данным и любым копиям этих данных. Это включает данные в местах хранения, в процессе передачи и даже в браузерах ваших клиентов. Сюда относятся внешние и внутренние угрозы.	Злоумышленники, как правило, не нарушают криптозащиту напрямую. Они осуществляют взлом каким-то иным способом, например похищают ключи, предпринимают атаки через посредника или похищают данные в виде незашифрованного текста с сервера, в процессе передачи или с браузера пользователя.	Наиболее распространенной брешью является невыполнение шифрования конфиденциальных данных. При использовании криптозащиты распространенным дефектом является генерация слабых ключей и управление слабыми ключами, распространено использование слабых алгоритмов, в частности методов хеширования с использованием слабых паролей. Слабости браузеров весьма распространены и легко обнаруживаются, однако их сложно использовать широкомасштабно. Внешним злоумышленникам трудно обнаруживать бреши на стороне сервера из-за ограниченного доступа, и, как правило, их также сложно использовать.	Результатом сбоя является, как правило, вскрытие всех данных, которые подлежат защите. Обычно эта информация включает конфиденциальные данные, такие как истории болезни, учетные данные, личные данные, кредитные карты и т. д.	Рассмотрите коммерческую ценность утраченных данных и последствия для вашей репутации. Какова ваша юридическая ответственность в случае раскрытия этих данных? Рассмотрите также ущерб для своей репутации.	CWE-310, CWE 311, CWE-312, CWE-319, CWE-325, CWE-326, CWE-934

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-7 – Контроль доступа к функциональ-ному уровню	Любое лицо, имеющее доступ к сети, может направить запрос вашему приложению. Могут ли получить доступ анонимные пользователи к индивидуальным функциям или обычные пользователи к привилегированным функциям?	Злоумышленник, являющийся авторизованным пользователем системы, просто изменяет URL или параметр доступа к привилегированной функции. Предоставляется ли доступ? Анонимные пользователи могут получить доступ к индивидуальным функциям, которые не защищены.	Приложения не всегда надлежащим образом защищают прикладные функции. Иногда защита функционального уровня управляется через конфигурацию, и возникает нарушение конфигурации системы. Разработчики должны в ряде случаев предусматривать проверки надлежащего кода, о чем они забывают. Обнаружить такие бреши просто. Самым сложным является определение того, какие существуют страницы (URL) или функции в качестве целей атак.	Такие бреши открывают перед злоумышленниками возможность доступа к функциям, для которых они не авторизованы. Основными целями атак такого типа являются функции администратора.	Рассмотрите коммерческую ценность раскрытых функций и данных, которые они обрабатывают. Рассмотрите также последствия для вашей репутации в случае, если об этой уязвимости станет известно широкой общественности.	CWE 285, CWE-287, CWE-935

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-8 – Подделка межсайтовых запросов (CSRF)	Рассмотрите всех, кто может загружать контент в браузеры ваших пользователей и, следовательно, вынудить их направить запрос на ваш веб-сайт. Для этого может использоваться любая линия на веб-сайт или иной HTML, к которым осуществляют доступ ваши пользователи.	Злоумышленник создает поддельные запросы HTTP и вынуждает жертву направить их через теги изображений, XSS или с помощью иных многочисленных способов. Если пользователь аутентифицирован, атака будет успешной.	CSRF использует то, что большинство веб-приложений дают злоумышленникам возможность прогнозировать все детали конкретного действия. Поскольку браузеры отправляют учетные данные как сеансовые куки автоматически, злоумышленники могут создавать вредоносные веб-страницы, которые генерируют поддельные запросы, неотличимые от законных. Бреши CSRF достаточно просто обнаруживаются путем тестирования на возможность проникновения или анализа кода.	Злоумышленники могут вынудить жертвы осуществить любую операцию по изменению состояния, на выполнение которой жертва имеет разрешение, например обновление учетных данных, осуществление покупок, выход из системы и даже регистрация в системе.	Рассмотрите коммерческую ценность затронутых данных или функций приложения. Представьте, что вы не уверены, намеревались ли пользователи предпринять эти действия. Рассмотрите последствия для своей репутации.	CWE-346, CWE-352, CWE-441, CWE-642, CWE-935
A-9 – Использование компонентов с известными уязвимостями	Некоторые уязвимые компоненты (например, каркасные библиотеки) могут определяться и использоваться с помощью автоматизированных средств, что расширяет набор факторов угроз, включая не только целевых злоумышленников, но и несистематизированных участников.	Злоумышленник определяет слабый компонент путем сканирования или ручного анализа. Он представляет проникновение как необходимое и осуществляет атаку. Если используемый компонент находится глубоко в приложении, это повышает сложность.	Практически любому приложению присущи эти проблемы, поскольку большинство групп разработчиков не уделяют достаточно внимания обеспечению обновления своих компонентов/ библиотек. Зачастую разработчики даже не знают всех компонентов, которые они используют, и не интересуются их версией. Зависимости компонентов ухудшают ситуацию.	Возможен полный диапазон уязвимостей, включая внедрение, нарушение управления доступом, XSS и т. д. Результатом может стать захват главной машины, от минимального до полного, и нарушение данных.	Рассмотрите возможное значение каждой уязвимости для коммерческого предприятия, управляемого затронутым приложением. Оно может быть тривиальным или может означать полное нарушение.	CWE-937

Таблица V.1 – Список OWASP Топ-10 рисков безопасности приложений

Тип атаки	Фактор угрозы	Направленность атаки	Слабое место в системе безопасности	Технические последствия	Коммерческие последствия	Ссылки
A-10 – Непроверенные перенаправления или пересылки	Рассмотрите всех, кто может вынудить ваших пользователей направить на ваш веб-сайт запрос. Для этого может использоваться любая линия на веб-сайт или иной HTML, которые используют ваши пользователи.	Злоумышленник устанавливает гиперссылку на непроверенное перенаправление и вынуждает жертву щелкнуть по этой ссылке. Как правило, жертвы щелкают по ссылке, поскольку эта ссылка находится на законном сайте. Злоумышленник использует небезопасную пересылку для обхода проверок системы безопасности.	Приложения часто перенаправляют пользователей на другие страницы или используют аналогичным образом внутренние пересылки. Иногда целевая страница определяется в непроверенном параметре, позволяя злоумышленнику выбирать страницу назначения. Обнаружить непроверенные перенаправления просто. Найдите перенаправления, в которых вы можете установить полный URL. Непроверенные пересылки обнаружить сложнее, поскольку их целью являются внутренние страницы.	При таких перенаправлениях может предприниматься попытка установки вредоносного программного обеспечения или жертву могут вынудить раскрыть пароль или иную конфиденциальную информацию. Небезопасные пересылки позволяют обходить контроль доступа.	Рассмотрите коммерческую ценность сохранения доверия своих пользователей. Что если их захватит вредоносное программное обеспечение? Что если злоумышленники имеют доступ только к внутренним функциям.	CWE-601, CWE-938

Библиография

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications Markup Language (tML) framework.*

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993) | ISO/IEC 8613-1:1994, *Information technology − Open Document Architecture (ODA) and interchange format: Introduction and general principles.*

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology − Open Systems Interconnection − Security frameworks for open systems: Overview*.

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

[b-ITU-T X.1520] Рекомендация МСЭ-Т X.1520 (2014 г.), *Общеизвестные уязвимости и незащищенность.*

[b-ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 г.), *Перечень общеизвестных слабых мест*.

[b-ITU-T X.1541] Рекомендация МСЭ-Т X.1541 (2012 г.), *Формат обмена описаниями инцидентов как объектов.*

[b-ITU-T X.1544] Рекомендация МСЭ-Т X.1544 (2013 г.) *Перечень и классификация общеизвестных схем атак.*

[b-ITU-T X.1546] Recommendation ITU-T X.1546 (2014), *Malware attribute enumeration and characterization.*

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-CAPEC-62] CAPEC-62: *Cross Site Request Forgery (aka Session Riding).*
https://capec.mitre.org/data/definitions/62.html

[b-CAPEC-66] CAPEC-66: *SQL Injection*.
https://capec.mitre.org/data/definitions/66.html

[b-CAPEC-103] CAPEC-103: *Clickjacking.*
https://capec.mitre.org/data/definitions/103.html

[b-CWE] CWE-928: *Weaknesses in OWASP Top Ten (2013).*
http://cwe.mitre.org/data/graphs/928.html

[b-iframe] W3C (2014), *HTML <iframe> Tag*.
http://www.w3schools.com/tags/tag_iframe.asp

[b-NA] Idika, Nwokedi, and Mathur, Aditya P. (2007), *A Survey of Malware Detection Techniques*, Department of Computer Science, Purdue University, 2 February.
http://www.serc.net/system/files/SERC-TR-286.pdf

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling.*

[b-NTobjectives] Kuykendall, Dan (2009), *Is Your Website Already Infected? Analyzing and Detecting Malicious Content*, 20 March.
http://www.manvswebapp.com/is-your-website-already-infected

[b-OWASP] OWASP (2013), *OWASP Top 10 application security risks*.
https://www.owasp.org/index.php/Top_10_2013-Top_10

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2015 г.