

Ризики для безпеки веб сервісів та їх мінімізація

Львівський національний університет імені Івана
Франка

Кафедра радіоелектронного матеріалознавства

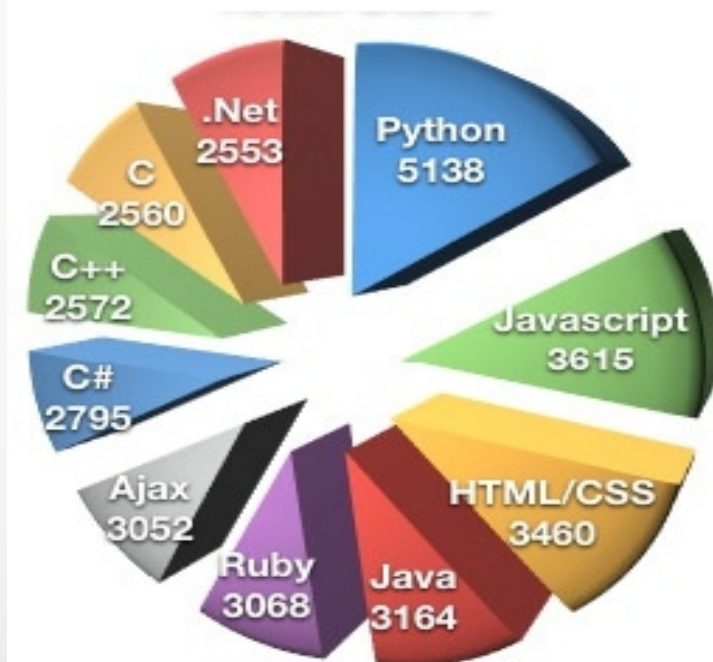
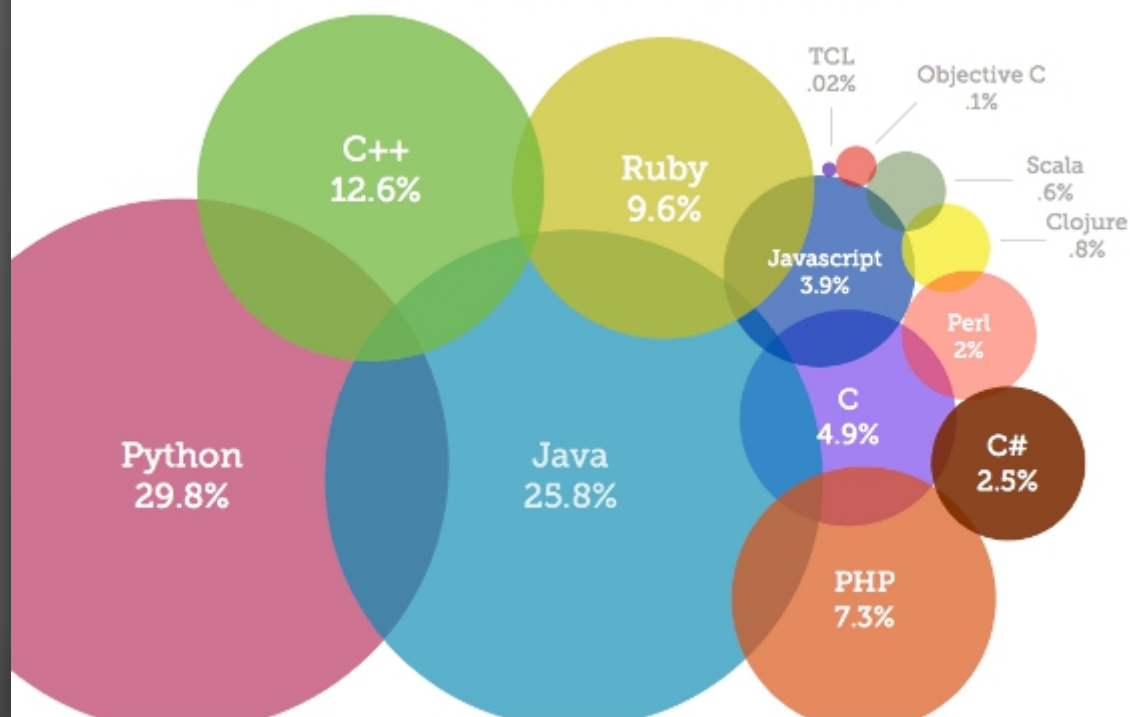
Підготувала студентка групи ФЕІ - 41 Литвин В.

Безпека веб-сервісів.

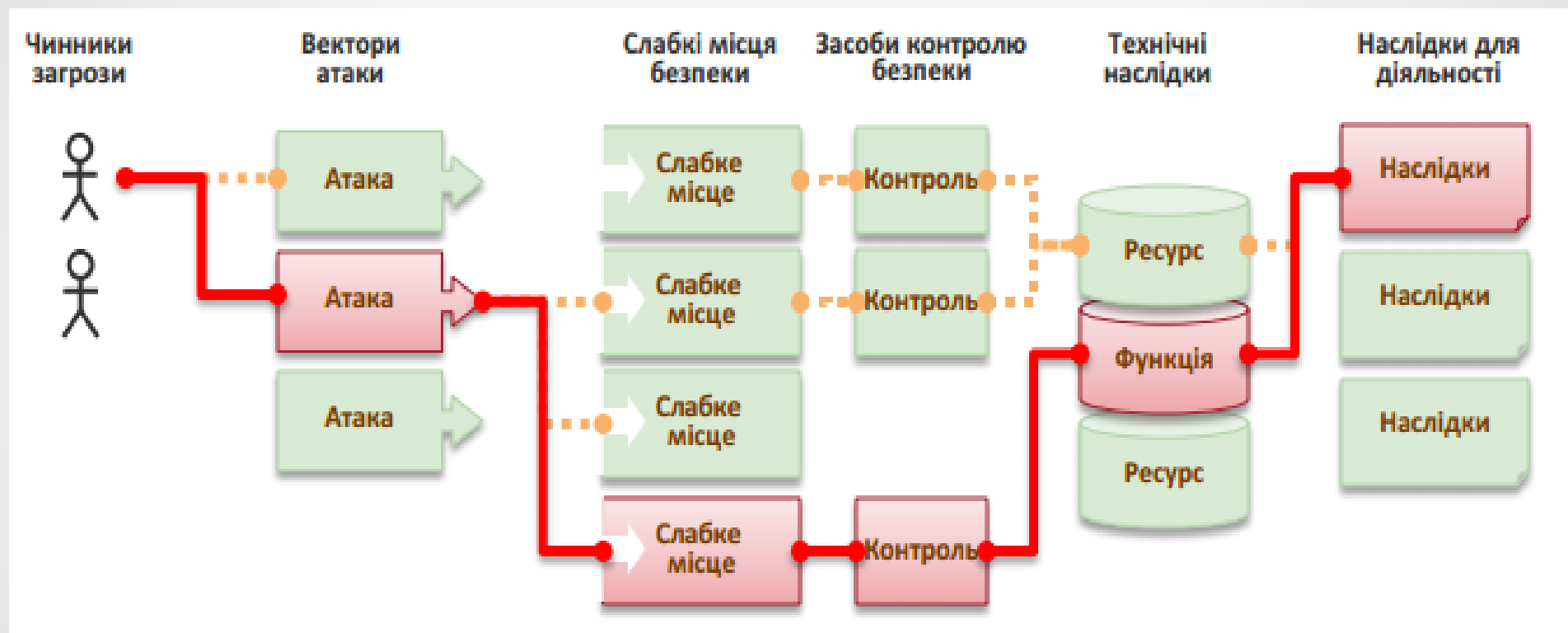


Безпека - це такий стан складної системи, коли дія зовнішніх і внутрішніх факторів не призводить до погіршення системи або до неможливості її функціонування і розвитку.

Most Popular Coding Languages of 2013



Ризики для безпеки.




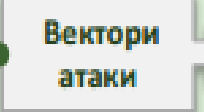
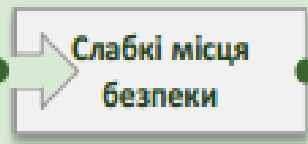
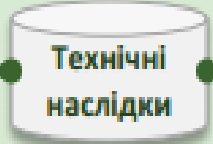
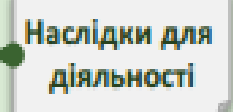
Вставка інструкцій.

Злам типу «Вставка інструкцій», наприклад вставка інструкцій SQL, ОС та LDAP, відбувається, коли ненадійні дані відправляються на інтерпретатор даних як частина команди або запиту. Ворожі дані зломисника можуть призвести до того, що інтерпретатор почне виконувати довільні команди, або зломисник отримає доступ до даних без належної авторизації.

Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність ЗВИЧАЙНА	Можливість виявлення СЕРЕДНЯ	Наслідки ТЯЖКІ	Специфічні для додатка / діяльності
Зважайте на всіх, хто може надіслати сумнівні дані, включаючи зовнішніх користувачів, внутрішніх користувачів та адміністраторів.	Зломисники надсилають прості тексти, в яких використовується синтаксис цільового інтерпретатора. Майже будь-яке джерело даних може бути вектором вставки інструкцій, включаючи внутрішні джерела.	Злам типу «Вставка інструкцій» відбувається, коли додаток відправляє ненадійні дані в інтерпретатор. Вставки інструкцій дуже розповсюджені, особливо в успадкованому коді. Їх можна часто знайти у запитах SQL, LDAP, Xpath або NoSQL; командах ОС; синтаксичних аналізаторах XML; заголовках SMTP, програмних аргументах тощо. Вставки інструкцій легко виявити під час перевірки коду, однак їх часто важко виявити шляхом тестування. Сканери та технологія тестування «Fuzzing» можуть допомогти зломисникам знайти вставки інструкцій.		Вставка інструкцій може призвести до втрати або ушкодження даних, неналежної звітності або до відмови у доступі. Інколи вставка інструкцій може призвести до повної підміни хосту.	Зважайте на цінність уражених даних та на платформу, на якій працює інтерпретатор. Всі дані можуть бути вкрадені, змінені або видалені. Чи може постраждати ваша репутація?

Некоректна аутентифікація та управління сеансами

Функції додатка, пов'язані з аутентифікацією та управлінням сеансами, часто некоректно впроваджені, що дозволяє зломисникам обходити паролі, ключі або сеансові ідентифікатори, або використовувати інші типи зламів для отримання інших ідентифікаторів користувачів.

 <p>Чинники загрози</p>	 <p>Вектори атаки</p>	 <p>Слабкі місця безпеки</p>		 <p>Технічні наслідки</p>	 <p>Наслідки для діяльності</p>
<p>Специфічні для додатка</p>	<p>Можливість зламу СЕРЕДНЯ</p>	<p>Поширеність ПОШИРЕНА</p>	<p>Можливість виявлення СЕРЕДНЯ</p>	<p>Наслідки ТЯЖКІ</p>	<p>Специфічні для додатка / діяльності</p>
<p>Зважайте на анонімних зовнішніх зломисників, а також на користувачів з власними обліковими записами, які можуть спробувати викрасти чужий обліковий запис. Також зважайте на членів організації, які хочуть приховати свої дії.</p>	<p>Зломисник використовує витік даних або недоробки у механізмі аутентифікації або управлінням сесіями (наприклад, незахищені облікові записи, паролі, ІД сесій), щоб видати себе за користувача.</p>	<p>Розробники часто створюють механізми аутентифікації та управління сесіями, однак створити їх правильно досить складно. Як результат, такі механізми мають дефекти щодо реєстрації, управління паролем, часу очікування, запам'ятовування, секретних питань, оновлення облікових записів тощо. Інколи виявити такі дефекти важко, оскільки кожне впровадження є унікальним.</p>		<p>Такі злами дають можливість атакувати деякі або навіть <u>всі</u> облікові записи. Після успішного зламу зломисник може робити все, що може робити жертва. Часто злами націлені на облікові записи з привілеями.</p>	<p>Зважайте на цінність уражених даних для діяльності або функцій додатка.</p> <p>Крім того, зважайте на наслідки з розкриття уразливості на діяльність.</p>

Міжсайтове виконання сценаріїв (XSS)

Атаки XSS відбуваються, коли додаток отримує ворожі дані та відправляє їх до веб-браузера без належної перевірки. Атаки XSS дозволяють зловмисникам виконувати сценарії у браузері жертви, в результаті яких вони можуть перехоплювати сеанси користувача, видозмінювати веб-сайти або перенаправляти користувачів на інші шкідливі сайти.

Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність ДУЖЕ ПОШИРЕНА	Можливість виявлення ЛЕГКА	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
Зважайте на всіх, хто може надіслати сумнівні дані, включаючи зовнішніх користувачів, внутрішніх користувачів та адміністраторів.	Зловмисник надсилає простий текстовий сценарій атаки, який уражає інтерпретатор браузера. Майже будь-яке джерело даних може бути вектором атаки, включаючи внутрішні джерела, такі як елементи баз даних.	<u>XSS</u> є найбільш розповсюдженою атакою на веб-додатки. Атаки XSS виникають, коли додаток включає дані, що надаються користувачем, у сторінку, яка відправляється в браузер без належної перевірки або фільтрування змісту. Існує три відомих типи атак XSS: 1) <u>Збережені</u> , 2) <u>Відображені</u> , та 3) <u>Атаки XSS, основані на об'єктній моделі документу (DOM)</u> . Виявити більшість атак XSS досить легко за допомогою тестування або аналізу коду.		Зловмисники можуть виконати сценарії в браузері жертви для перехоплення сеансу користувача, спотворити веб-сторінку, вставити шкідливі дані, переадресувати користувача, перехопити браузер користувача за допомогою шкідливих програмних засобів тощо.	Зважайте на цінність ураженої системи для діяльності та всіх даних, які вона обробляє. Крім того, зважайте на наслідки з розкриття уразливості на діяльність.


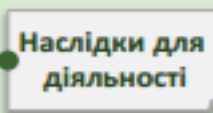
Небезпечні прямі посилання на об'єкти

Пряме посилання на об'єкт відбувається, коли розробник залишає незахищеним посилання на внутрішній об'єкт додатку, такий як файл, каталог або ключ до бази даних. Без перевірки прав доступу або іншого захисту зломисники можуть маніпулювати такими посиланнями з метою несанкціонованого доступу до даних.

 <p>Чинники загрози</p>	<p>Вектори атаки</p>	 <p>Слабкі місця безпеки</p>		<p>Технічні наслідки</p>	<p>Наслідки для діяльності</p>
<p>Специфічні для додатка</p>	<p>Можливість зламу ЛЕГКА</p>	<p>Поширеність ЗВИЧАЙНА</p>	<p>Можливість виявлення ЛЕГКА</p>	<p>Наслідки ПОМІРНІ</p>	<p>Специфічні для додатка / діяльності</p>
<p>Зважайте на типи користувачів вашої системи. Чи мають користувачі лише частковий доступ до певних типів системних даних?</p>	<p>Зловмисник, який є авторизованим користувачем системи, просто змінює значення параметра, яке використовується для прямого посилання на об'єкт, для посилання на інший об'єкт, прав доступу до якого немає у користувача. Чи отримає він доступ?</p>	<p>Під час запитів до веб-сторінок додатки часто використовують реальні імена або ключі об'єкта. Додатки не завжди перевіряють, чи має користувач право доступу до цільового об'єкта. Це призводить до виникнення недоліків у вигляді небезпечного прямого посилання на об'єкти. Тестувальники можуть легко маніпулювати значеннями параметрів для виявлення таких недоліків. Аналіз коду швидко показує, чи належним чином були перевірені права доступу.</p>		<p>Такі злами можуть поставити під загрозу всі дані, на які посилається параметр. За виключенням випадків, коли посилання на об'єкти є непередбачуваними, зловмисник легко отримає доступ до всіх наявних даних такого типу.</p>	<p>Зважайте на цінність уражених даних для подальшої діяльності. Крім того, зважайте на наслідки з розкриття уразливості для діяльності.</p>

Небезпечна конфігурація оточення

Належна безпека вимагає визначення та використання безпечної конфігурації для додатків, середовища розробки, сервера додатка, веб-сервера, сервера бази даних та платформи. Необхідно визначати, впроваджувати та підтримувати безпечні налаштування, оскільки типові налаштування є, як правило, небезпечними. Крім того, програмне забезпечення повинно бути оновленим.

 Чинники загрози	 Вектори атаки	 Слабкі місця безпеки		 Технічні наслідки	 Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність ЗВИЧАЙНА	Можливість виявлення ЛЕГКА	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
Зважайте на анонімних зовнішніх зловмисників, а також на користувачів з власними обліковими записами, які можуть поставити під загрозу систему. Також зважайте на членів організації, які хочуть приховати свої дії.	Зловмисник отримує доступ до стандартних облікових записів, невикористаних сторінок, невиправлених недоліків, незахищених файлів та каталогів тощо, щоб отримати несанкціонований доступ до системи або інформацію про неї.	Небезпечна конфігурація може виникнути на будь-якому рівні архітектури додатка, включаючи платформу, веб-сервер, сервер додатка, базу даних, середовище розробки та частину програми. Розробники та системні адміністратори повинні разом працювати над тим, щоб забезпечити належну конфігурацію всієї архітектури. Автоматичні сканери сприяють виявленню відсутніх виправлень, неправильних конфігурацій, випадків використання стандартних облікових записів, непотрібних сервісів тощо.		Такі недоліки нерідко дають зловмисникам доступ до певних системних даних або функцій. Інколи такі недоліки ставлять під загрозу всю систему.	Система може бути повністю захоплена без вашого відома. Всі ваші дані можуть бути викрадені або змінені з часом. Витрати на відновлення можуть бути суттєвими.

Витік критичних даних

Багато веб-додатків неналежним чином захищають такі критичні дані як дані кредитних карток, індивідуальні податкові номери та облікові дані для перевірки автентичності. Зловмисники можуть вкрати або змінити такі слабо захищені дані та здійснити шахрайські операції з кредитними картками, вкрати особисті дані або вчинити інші кримінальні правопорушення.

Критичні дані слід додатково захищати шляхом шифрування під час збереження або передачі, а також необхідно дотримуватися певних застережень під час обміну такими даними з браузером.

Специфічні для додатка	Можливість зламу ВАЖКА	Поширеність РІДКІСНА	Можливість виявлення СЕРЕДНЯ	Наслідки ТЯЖКІ	Специфічні для додатка / діяльності
Зважайте на те, хто може отримати доступ до критичних даних вашого додатка та будь-яких резервних копій таких даних. Такі дані містять дані, що зберігаються, дані, що передаються, та навіть дані у браузерах користувачів. Звертайте увагу як на зовнішні, так і на внутрішні загрози.	Як правило, зловмисники не ламають безпосередньо шифровані дані. Вони ламають щось інше, наприклад, крадуть ключі, здійснюють атаки через посередника або крадуть чисті текстові дані з сервера під час передачі або з браузера користувача.	Найпоширеніший недолік – відсутність шифрування конфіденційних даних. При використанні алгоритмів шифрування, як правило, слабкими залишаються такі функції як створення та управління ключами, використовуються слабкі алгоритми, а також слабкі методи хешування паролів. Слабкі місця браузерів дуже поширені, і їх легко виявити, однак важко впровадити у великих масштабах. Зовнішні зловмисники стикаються з труднощами під час виявлення недоліків з боку сервера через обмежений доступ, тому їх також важко використовувати.		Збір часто розкриває всі дані, що мають бути захищені. Як правило, така інформація включає в себе такі критичні дані як медичні картки, ідентифікаційні дані, особисті дані, дані кредитних карток тощо.	Зважайте на цінність втрачених даних для діяльності, а також наслідки для вашої репутації. Яку правову відповідальність ви понесете у разі розголошення таких даних? Також зважайте на шкоду вашій репутації.

Відсутність контролю доступу до функціонального рівня

Більшість веб-додатків перевіряють права доступу до функціонального рівня перед тим, як відображати відповідну функцію в інтерфейсі користувача. Однак додаткам необхідно виконувати аналогічні перевірки контролю доступу на сервері, коли здійснюється доступ до кожної функції. Якщо запити не перевіряються, зломисники можуть підробляти їх для доступу до функцій без відповідної авторизації.

 Чинники загрози	 Вектори атаки	 Слабкі місця безпеки		 Технічні наслідки	 Наслідки для діяльності
Специфічні для додатка	Можливість зламу ЛЕГКА	Поширеність ЗВИЧАЙНА	Можливість виявлення СЕРЕДНЯ	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
Будь-хто з доступом до мережі може відправити запит до вашого додатка. Чи можуть анонімні користувачі отримати доступ до приватних функцій або звичайні користувачі – до привілейованих функцій?	Зловмисник, який є авторизованим користувачем системи, просто змінює URL або параметр привілейованої функції. Чи надається доступ? Анонімні користувачі можуть отримати доступ до приватних функцій, що не захищені.	Додатки не завжди належним чином захищають свої функції. Інколи захист на функціональному рівні здійснюється за рахунок конфігурації, а система налаштована невірно. Інколи розробники повинні включати належні перевірки коду, а вони забувають. Виявити такі недоліки легко. Найважче визначити, які саме сторінки (URL) або функції можуть бути атаковані.		Такі недоліки дають зловмисникам можливість отримати доступ до незахищених функцій. Для такого типу атаки ключовими цілями є адміністративні функції.	Зважайте на значення розкритих функцій та даних, що ними оброблюються, для діяльності. Крім того, зважайте на наслідки для вашої репутації у випадку розкриття таких уразливостей.


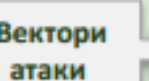
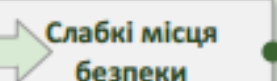
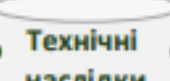
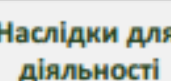
Підробка міжсайтових запитів (CSRF)

Атака CSRF змушує підключений до системи браузер жертви автоматично відправляти підроблені запити HTTP, включаючи фрагмент даних (кукіз) сеансу жертви та іншу інформацію щодо аутентифікації, до уразливого веб-додатка. Це дає зломисникам змогу змусити браузер жертви створювати запити, які уразливий додаток вважає правомірними запитами жертви.

 Чинники загрози	 Вектори атаки	 Слабкі місця безпеки		 Технічні наслідки	 Наслідки для діяльності
Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність ЗВИЧАЙНА	Можливість виявлення ЛЕГКА	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
Зважайте на всіх, хто може завантажити інформацію в браузери ваших користувачів та, відповідно, примусити їх подати запит до вашого веб-сайта. Будь-який веб-сайт або початковий код HTML, до яких має доступ ваш користувач, можуть зробити це.	Зловмисник створює примусовий HTTP запит та змушує жертву передати його через теги зображень, XSS або іншими, численними способами. <u>Якщо користувач аутентифікований</u> , атака матиме успіх.	<u>CSRF</u> користується тим, що більшість веб-додатків дають зловмисникам можливість передбачити всі деталі конкретної дії. Оскільки браузери відправляють такі ідентифікаційні дані як фрагменти даних (кукіз) сеансів автоматично, зловмисники можуть створити шкідливі веб-сторінки, що будуть створювати примусові запити, які неможливо буде відрізнити від дозволених. Виявлення недоліків CSRF досить легке: за допомогою тестування на проникнення або аналізу коду.		Зловмисники можуть обманути жертв та змусити їх виконати будь-які дії щодо зміни стану, на які жертви мають право, наприклад, оновити дані облікового запису, здійснити покупку, вийти з облікового запису або навіть увійти до нього.	Зважайте на цінність уражених даних або функцій додатка для вашої діяльності. Уявіть ситуацію, коли ви не впевнені, чи дісно користувачі намагалися здійснити цю операцію або виконати ці дії. Зважайте на наслідки для вашої репутації.

Використання компонентів з відомими уразливостями

Такі компоненти як бібліотеки, середовища розробки та інші модулі програмного забезпечення майже завжди працюють з повними привілеями. Якщо використовується уразливий компонент, така атака може сприяти втраті критичних даних або підміні сервера. Додатки, що використовують компоненти з відомими уразливостями, можуть знизити рівень захисту та сприяти різноманітним атакам та наслідкам.


 Чинники загрози	 Вектори атаки	 Слабкі місця безпеки		 Технічні наслідки	 Наслідки для діяльності
Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність ПОШИРЕНА	Можливість виявлення ВАЖКА	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
Деякі уразливі компоненти (наприклад, система бібліотек) можна ідентифікувати та використовувати з автоматизованими інструментами, розширюючи діапазон чинників загрози шляхом включення хаотичних злоумисників.	Зловмисник виявляє слабкі компоненти шляхом сканування або ручного аналізу. Він підбирає втручання та здійснює атаку. Це ускладнюється, якщо компоненти, що використовуються, знаходяться глибоко у додатку.	Віртуально, кожний додаток має такі проблеми, оскільки команди розробників не звертають увагу на забезпечення оновлення своїх компонентів/бібліотек. У багатьох випадках розробники навіть не знають всіх компонентів, що вони використовують, і ніколи не замислюються над їх версіями. Залежності компонентів ще більше ускладнюють ситуацію.		Можливий весь діапазон слабких місць, включаючи вставку інструкцій, некоректний контроль доступу, XSS тощо. Наслідки можуть сягати від мінімальних до перехоплення всього вузла та розкриття даних.	Зважайте на значення кожної уразливості для діяльності, яка контролюється ураженням додатком. Вона може бути незначною або призвести до повного розкриття даних.

Небезпечні переадресування

Веб-додатки часто перенаправляють користувачів на інші сторінки та веб-сайти, а також використовують сумнівні дані для визначення цільової сторінки. Без належної перевірки зловмисники можуть перенаправляти жертв до фальшивих або шкідливих сайтів або використовувати переадресування для доступу до несанкціонованих сторінок.

 Чинники загрози	 Вектори атаки	 Слабкі місця безпеки		 Технічні наслідки	 Наслідки для діяльності
Специфічні для додатка	Можливість зламу СЕРЕДНЯ	Поширеність РІДКІСНА	Можливість виявлення ЛЕГКА	Наслідки ПОМІРНІ	Специфічні для додатка / діяльності
<p>Зважайте на всіх, хто може обманути ваших користувачів та змусити їх подати запит до вашого веб-сайта. Будь-який веб-сайт або механізм HTML, що використовуються вашими користувачами, можуть зробити це.</p>	<p>Зловмисник створює посилання на недозволену адресу та змушує жертву перейти по ньому. Жертви відкривають посилання, оскільки воно виглядає як посилання на дозволений сайт. Зловмисник направляє небезпечне переадресування в обхід перевірки безпеки.</p>	<p>Додатки часто переадресовують користувачів на інші сторінки або аналогічно використовують внутрішні застереження. Інколи цільова сторінка вказана у неперевіреному параметрі, що дає зловмисникам можливість вибрати сторінку призначення.</p> <p>Виявити неперевірені переадресування легко. Знайдіть переадресування, де ви можете вказати весь URL. Неперевірені пересилання важчі, оскільки їх ціллю є внутрішні сторінки.</p>		<p>Такі переадресування можуть призвести до спроби встановити шкідливе програмне забезпечення або змусити жертву розкрити пароль або іншу критичну інформацію. Небезпечні пересилання можуть дозволити обійти контроль доступу.</p>	<p>Зважайте на цінність довіри користувачів для діяльності.</p> <p>Що буде, якщо їх перехопить шкідливе програмне забезпечення?</p> <p>Що буде, якщо зловмисники зможуть отримати доступ тільки до внутрішніх функцій?</p>

Резюме факторів Топ 10 ризиків

РИЗИК	 Чинники загрози				Наслідки для діяльності	
		Можливість зламу	Поширеність	Можливість виявлення		
A1-Вставка інструкцій	Специфічні для додатка	ЛЕГКА	ЗВИЧАЙНА	СЕРЕДНЯ	ТЯЖКІ	Специфічні для додатка
A2-Аутентифікація	Специфічні для додатка	СЕРЕДНЯ	ПОШИРЕНА	СЕРЕДНЯ	ТЯЖКІ	Специфічні для додатка
A3-Міжсайтове виконання сценаріїв (XSS)	Специфічні для додатка	СЕРЕДНЯ	ДУЖЕ ПОШИРЕНА	ЛЕГКА	ПОМІРНІ	Специфічні для додатка
A4-Небезпечні ППО	Специфічні для додатка	ЛЕГКА	ЗВИЧАЙНА	ЛЕГКА	ПОМІРНІ	Специфічні для додатка
A5-Небезпечна конфігурація	Специфічні для додатка	ЛЕГКА	ЗВИЧАЙНА	ЛЕГКА	ПОМІРНІ	Специфічні для додатка
A6-Критичні дані	Специфічні для додатка	ВАЖКА	РІДКІСНА	СЕРЕДНЯ	ТЯЖКІ	Специфічні для додатка
A7-Доступ до функціонального рівня	Специфічні для додатка	ЛЕГКА	ЗВИЧАЙНА	СЕРЕДНЯ	ПОМІРНІ	Специфічні для додатка
A8- CSRF	Специфічні для додатка	СЕРЕДНЯ	ЗВИЧАЙНА	ЛЕГКА	ПОМІРНІ	Специфічні для додатка
A9-Компоненти	Специфічні для додатка	СЕРЕДНЯ	ПОШИРЕНА	ВАЖКА	ПОМІРНІ	Специфічні для додатка
A10-Переадресування	Специфічні для додатка	СЕРЕДНЯ	РІДКІСНА	ЛЕГКА	ПОМІРНІ	Специфічні для додатка

Загальні заходи безпеки в мережі

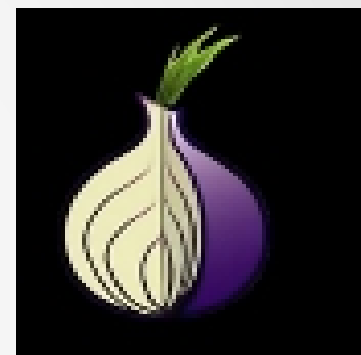
- Ввімкніть приватний перегляд



- Не забувайте виловуватись



- Приховайте свою IP-адресу



- Остерігайтеся відкритих Wi-Fi точок доступу



Дякую за увагу.

