**1.Що таке Cross-Site Scripting (XSS)? -**

**(XSS)?** remains one of the most common security vulnerabilities currently found in web-applications.

**Cross-Site Scripting (XSS**) залишається однією з найпоширеніших вразливостей для безпеки, які наразі знаходяться в веб-програмах. Межсайтовый скриптинг (XSS) – это уязвимость, которая заключается во внедрении кода, исполняемого на стороне клиента (JavaScript) в веб-страницу, которую просматривают другие пользователи.

1. **Sources of Untrusted Input (Джерела ненадійного вводу)**

It is important that you do not overlook potential sources of untrusted input, as doing so may mean you overlook a potential problem. Keep in mind that:

All input sources must be examined, including:

Query parameters within the submitted URL and any other URLs coming in as data

Post parameters in they body of the request

HTTP Headers

Structured data formats such as JSON, XML, etc.

Encoded data

AJAX submissions are not immune from XSS vulnerabilities, depending on the circumstances

Web Services may be an “enabling technology” when it comes to XSS vulnerabilities, since they are largely designed without consideration of how information is displayed

**Джерела ненадійного вводу**

Майте на увазі, що:

**Всі джерела інформації повинні бути перевірені, включаючи:**

**Параметри запиту в поданій URL-адресі та будь-які інші URL-адреси, що надходять як дані**

**Параметри публікації в тілі запиту**

**Заголовки HTTP**

**Формати структурованих даних, такі як JSON, XML тощо.**

**Закодовані дані**

**Заявки AJAX** не захищені від вразливостей XSS, залежно від обставин

Веб-сервіси можуть бути "технологією, що дозволяє", коли мова йде про вразливості XSS, оскільки вони в значній мірі розробляються без урахування того, як відображається інформація

3. Чим провіряти?

**3.1 <script>alert('aa');</script>**

Если на сайте много форм, то лучше вего воспользоваться программой для поиска уязвимостей. Одним из самых продвинутых считается Acunetix Web Security Scanner, его сможете найти на торентах.

Самые лучшие цели – это разнообразные самописные движки и скрипты.

В качестве полезной нагрузки для вставки можно выбрать

**<script>alert(1)</script>**

Наша полезная нагрузка попадёт туда, где сейчас слово «наволочка». Т.е. превратиться в значение тэга **input**. Мы можем этого избежать – закроем двойную кавычку, а затем и сам тэг с помощью **"/>**

**"/><script>alert(1)</script>**

**3.2 HTML**

Если сказать совсем просто, то злонамеренный код «обычных» непостоянных XSS мы можем увидеть, если откроем HTML код. Например, ссылка сформирована подобным образом:

|  |  |
| --- | --- |
| 1 | http://example.com/search.php?q="/><script>alert(1)</script> |

А при открытии исходного **HTML** кода мы видим что-то вроде такого:

<https://hackware.ru/?p=1174>

**4.** Имеются также **специализированные инструменты для сканирования на XSS уязвимости**. Среди них особенно можно выделить:

* [XSSer](https://kali.tools/?p=1758) – это не только мощный сканер, который умеет использовать разные методы внедрения и обхода фильтрации, это также автоматизированный инструмент по поиску уязвимых к XSS сайтов (по доркам). Для сайтов с найденными уязвимостями умеет внедрять полезную нагрузку для реальной атаки;
* [XssPy](https://kali.tools/?p=1755) – тоже достаточно самостоятельный инструмент, который умеет находить все страницы сайта (в том числе и на субдоменах) и проверять все элементы ввода на этих страницах;
* [BruteXSS](https://kali.tools/?p=1752) – положительной особенностью этого инструмента является полное исключение ложных срабатываний.

**5. Провірка вірусів**

### **VirusTotal**

VirusTotal — самый популярный сервис проверки файлов и сайтов на вирусы, использующий в работе сразу 6 десятков антивирусов.

1. Зайдите на сайт [https://www.virustotal.com](https://www.virustotal.com/) и откройте вкладку «URL».
2. Вставьте в поле адрес сайта или страницы и нажмите Enter (или по иконке поиска).

<https://remontka.pro/scan-website-for-viruses/>

https://2ip.ru/site-virus-scaner/