MỤC LỤC

Easy challenge: Uncle Arnold's Local Band Review

a. Mục tiêu

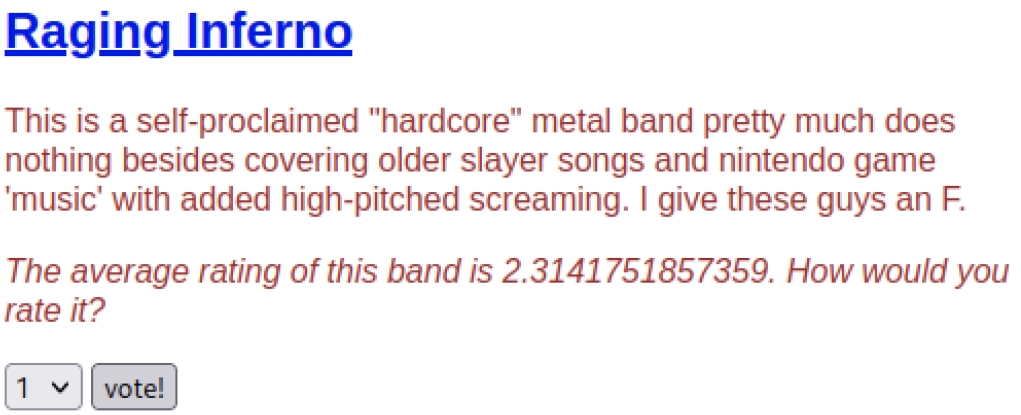
From: HeavyMetalRyan

Message: Hey man, I need a big favour from you. Remember that website I showed you once before? Uncle Arnold's Band Review Page? Well, a long time ago I made a $500 bet with a friend that my band would be at the top of the list by the end of the year. Well, as you already know, two of my band members have died in a horrendous car accident... but this ass hole still insists that the bet is on!
I know you're good with computers and stuff, so I was wondering, is there any way for you to hack this website and make my band on the top of the list? My band is Raging Inferno. Thanks a lot, man!

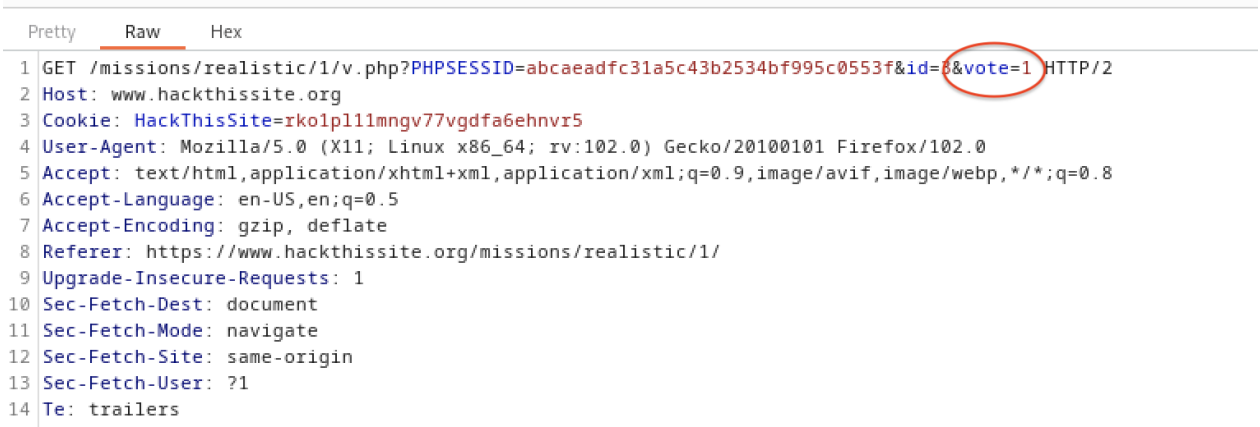
Đưa ban nhạc của Raging Inferno lên đầu danh sách.

b. Phương pháp

Tại ban nhạc Raging Inferno chọn số bất kỳ và bấm `vote!`.



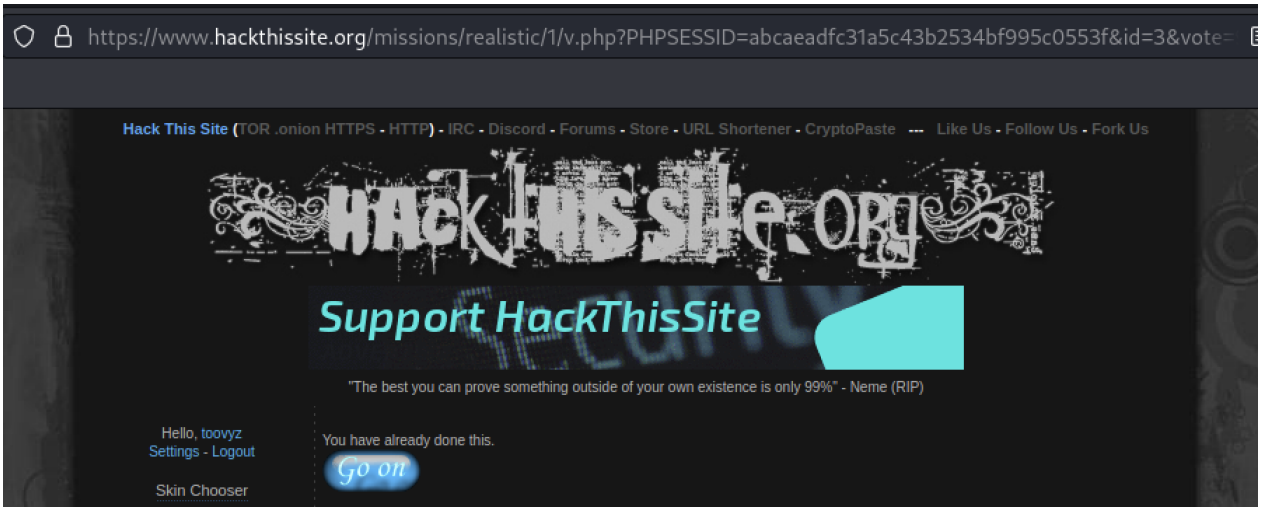
Dùng công cụ Burp Suite bắt request thấy tham số `vote` truyền đi với giá trị được chọn.



Sửa thành giá trị của `vote` thành `9999999999`, và forward.

```
Pretty  Raw  Hex
1  GET /missions/realistic/1/v.php?PHPSESSID=abcaeadfc31a5c43b2534bf995c0553f&id=3&vote=9999999999 HTTP/2
2  Host: www.hackthissite.org
3  Cookie: HackThisSite=rko1pl11mngv77vgdfa6ehnvr5
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Referer: https://www.hackthissite.org/missions/realistic/1/
9  Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
```

c. Kết quả

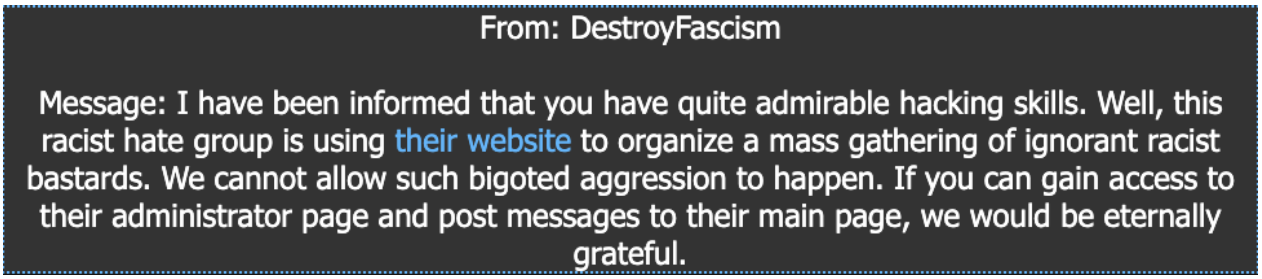


d. Kỹ thuật sử dụng

- Lỗi giả mạo tham số (Parameter manipulation)
- Mô tả: Giả mạo hoặc thay đổi một số tham số trên URL hay web form.

Easy challenge: Chicago American Nazi Party

a. Mục tiêu



Truy cập vào trang quản trị viên và đăng tin lên trang chính.

b. Phương pháp

Chuột phải → `View Page Source`.

Ta thấy có dòng cuối có `font color` cùng màu với background, thử mở file `update.php`.

Thấy có 1 form login, thử với payload sql injection đơn giản và nhấn `Submit Query`.

enter your username and password, white brother!

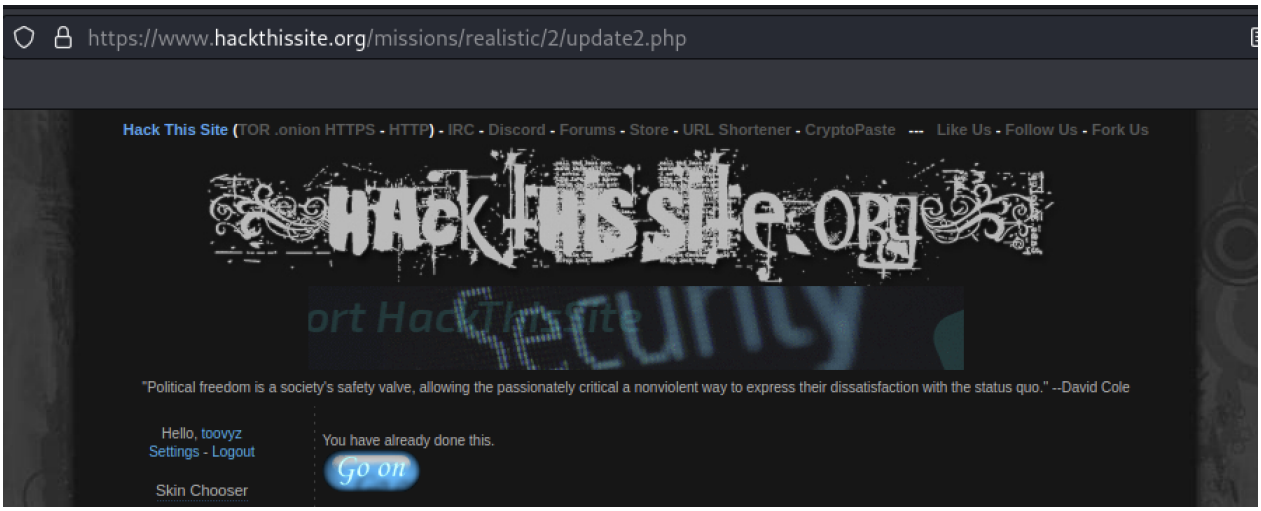
username

toovy ' or 1=1 --

password

Submit Query

c. Kết quả



d. Kỹ thuật sử dụng

- SQL injection.
- Mô tả: Lợi dụng lỗ hổng kiểm tra đầu vào, truyền các truy vấn sql độc hại thông qua web input.

Moderate: Peace Poetry: HACKED

a. Mục tiêu

From: PeacePoetry

Message: I run this website where people can read and submit peace-related poetry. I am doing this out of good will towards others, and I don't see why I would be making enemies out of this, but some real ass hole hacked my website posting a bunch of ignorant aggressive propaganda on the front page. And I made that website a while ago, and I no longer have access to it. Do you think you can hack in and change it back? Please? Oh, and bonus points if you message me the name of the bastard who did this!
My website can be found here.

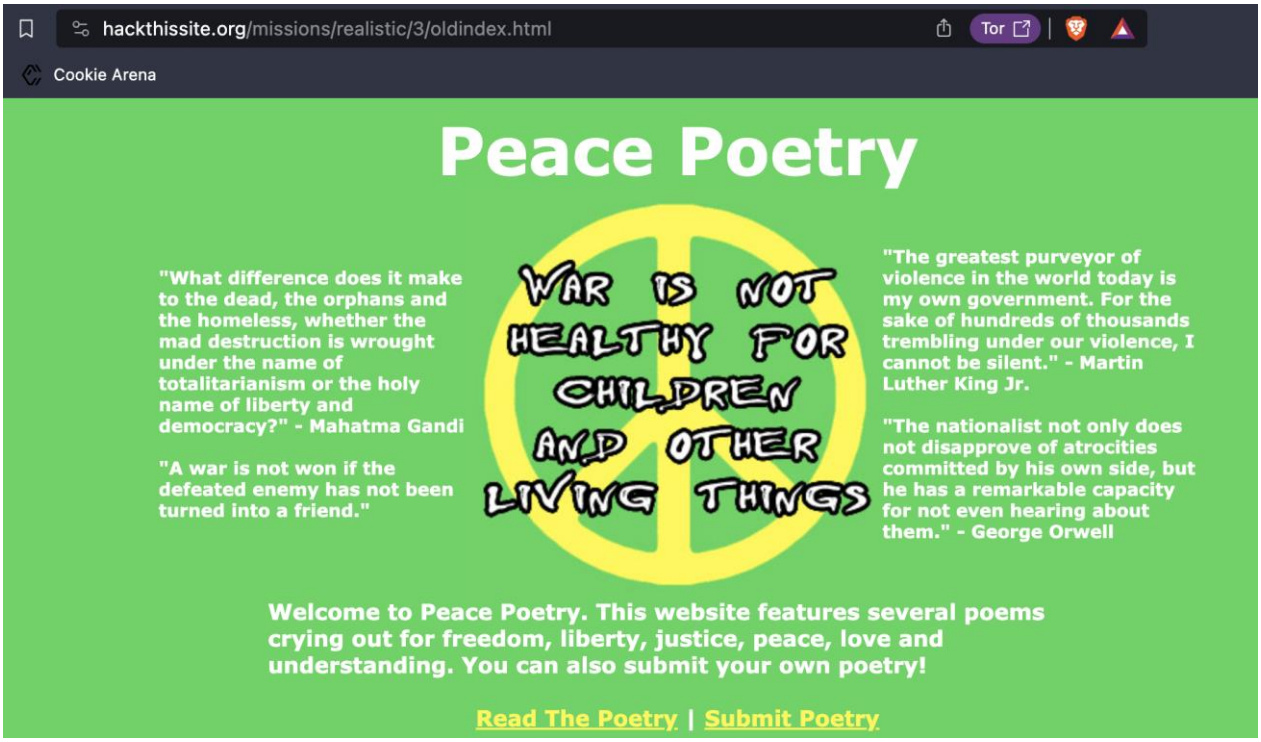
Thay đổi frontpage của website như cũ.

b. Phương pháp

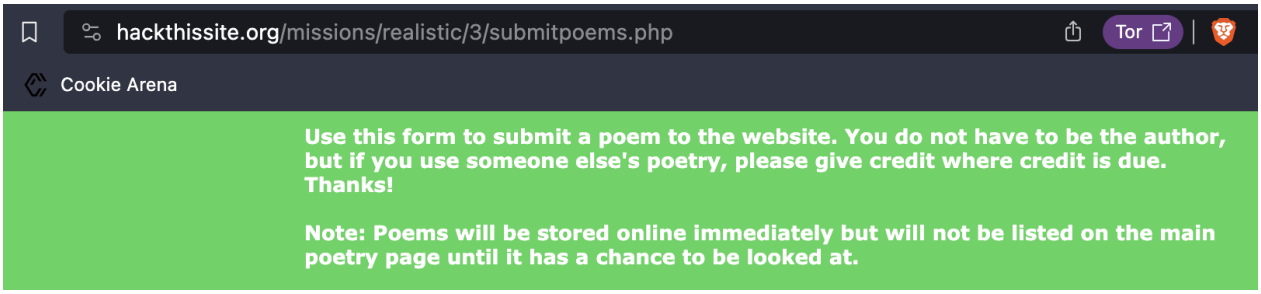
Vào website, View Page Source. Attacker có tâm để lại note:

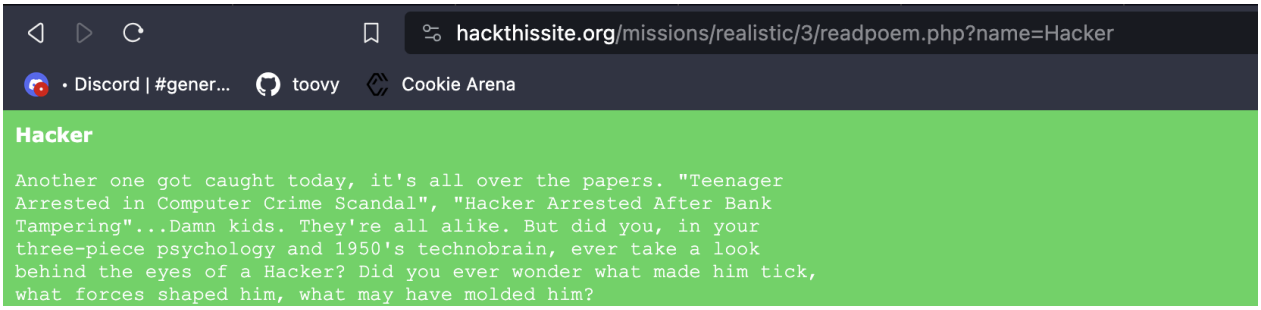
<!--Note to the webmasterThis website has been hacked, but not totally destroyed. The old website is still up. I simply copied the old index.html file to oldindex.html and remade this one. Sorry about the inconvenience.-->

Biết được website cũ vẫn còn và đổi tên thành `oldindex.html`. Tiến hành mở file này.



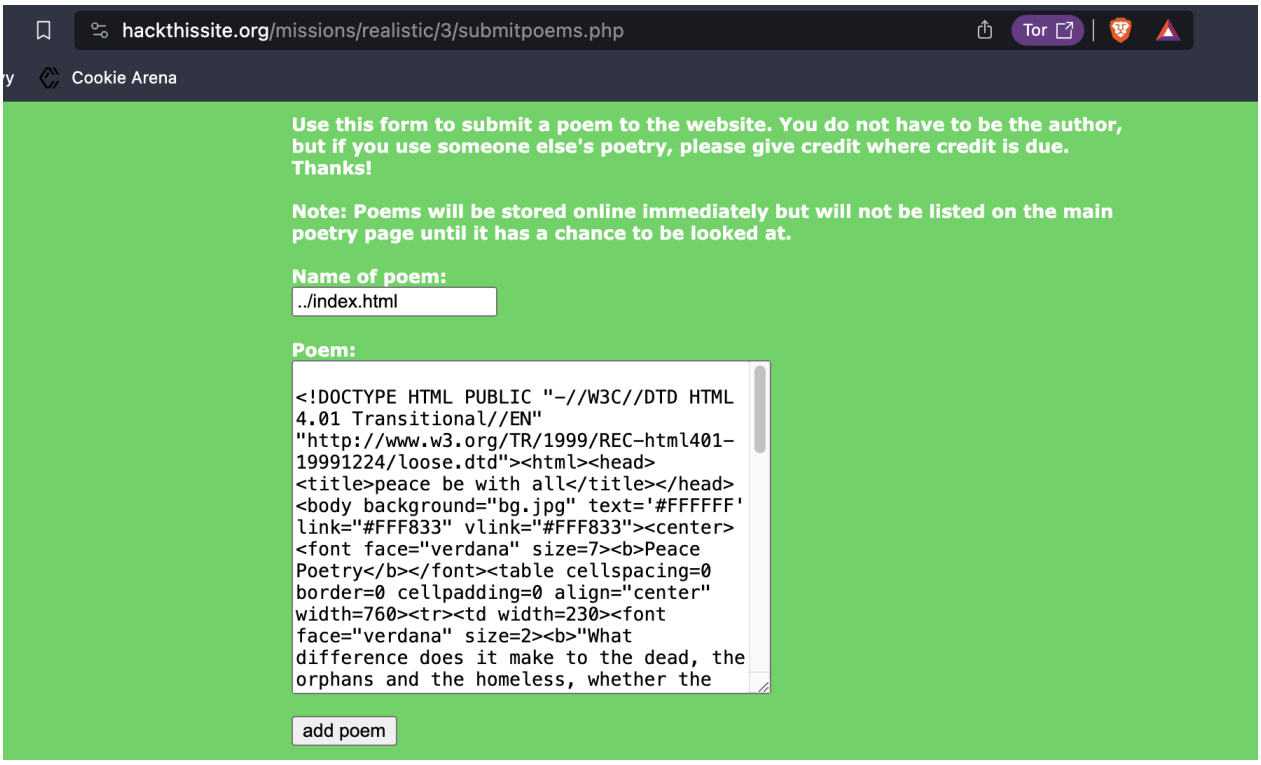
Vào `Submit Poetry` và `Read The Poetry`.



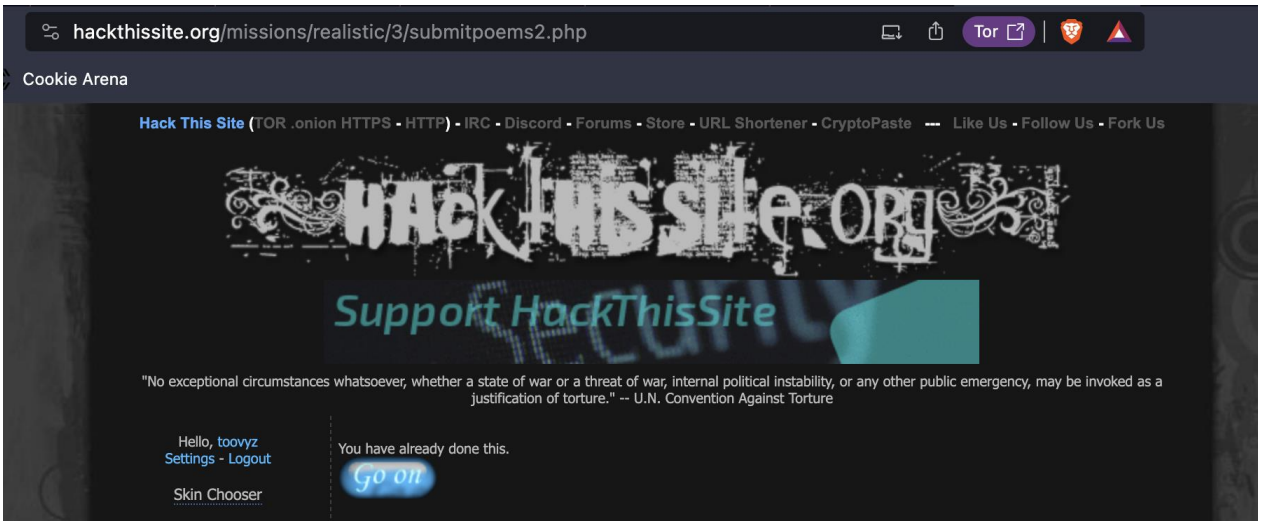


Khi gửi thơ lên, website sẽ lưu trữ online, với tên file là tên của bài thơ.

Quay lại `Submit Poetry`, gửi lên file `../index.html` với nội dung là source code của `oldindex.html` và bấm `add poem`.



c. Kết quả



d. Kỹ thuật sử dụng

- Remote Code Execution.
- Mô tả: Khiến website thực thi các lệnh trong input.

Moderate: Fischer's Animal Products

a. Mục tiêu

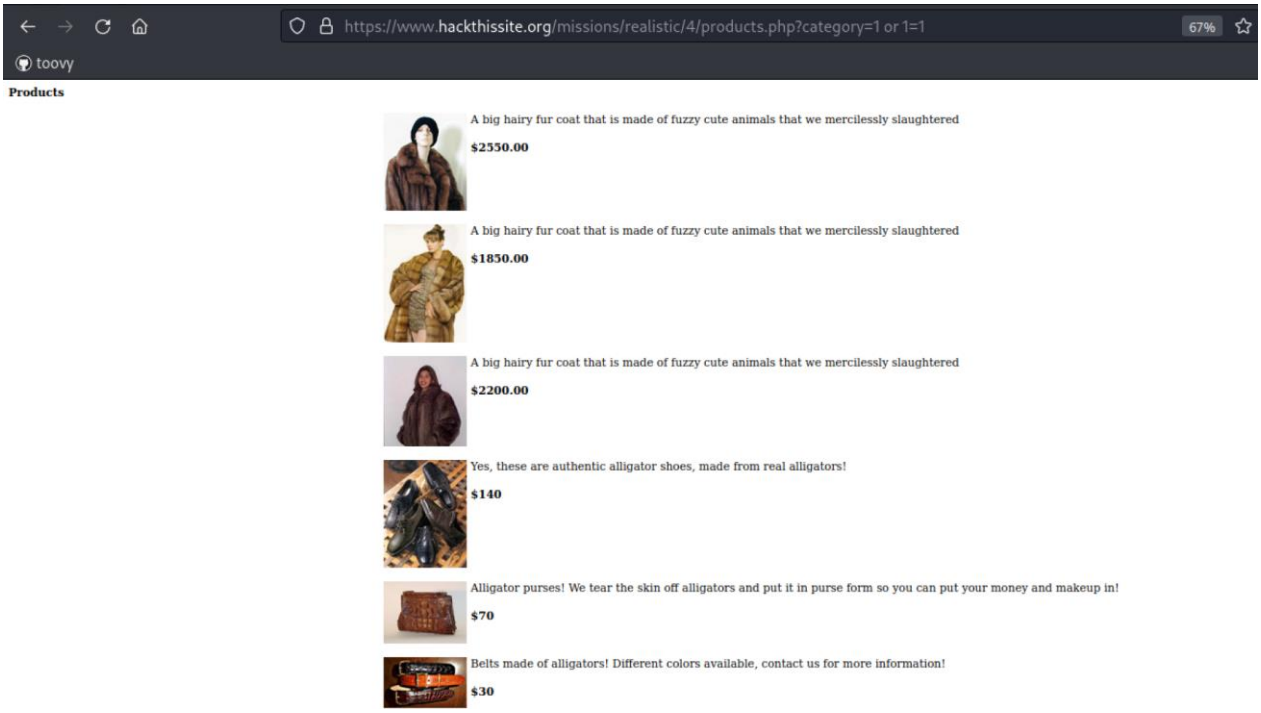
Trả lời thư này kèm theo danh sách các địa chỉ email trong website.

b. Phương pháp

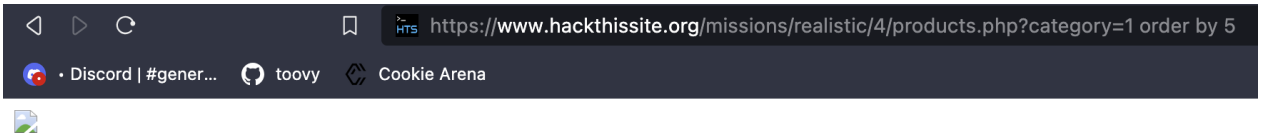
Điền `'` vào ô Mailing List, thì hiện lỗi sau. Biết được nhiệm vụ là lấy được danh sách email trong bảng `email`.

Error inserting into table "email"! Email not valid! Please contact an administrator of Fischer's

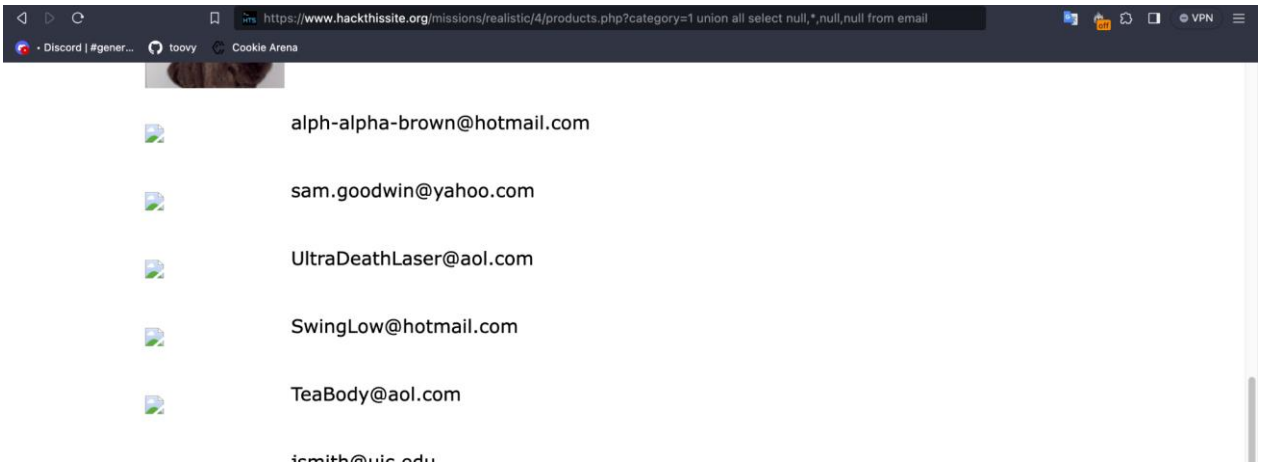
Quay lại trang đầu, chọn `Fur Coats!`. Sau đó điền thử với query `or 1=1`, trang web hiển thị tất cả sản phẩm → dùng UNION attack để lấy dữ liệu.



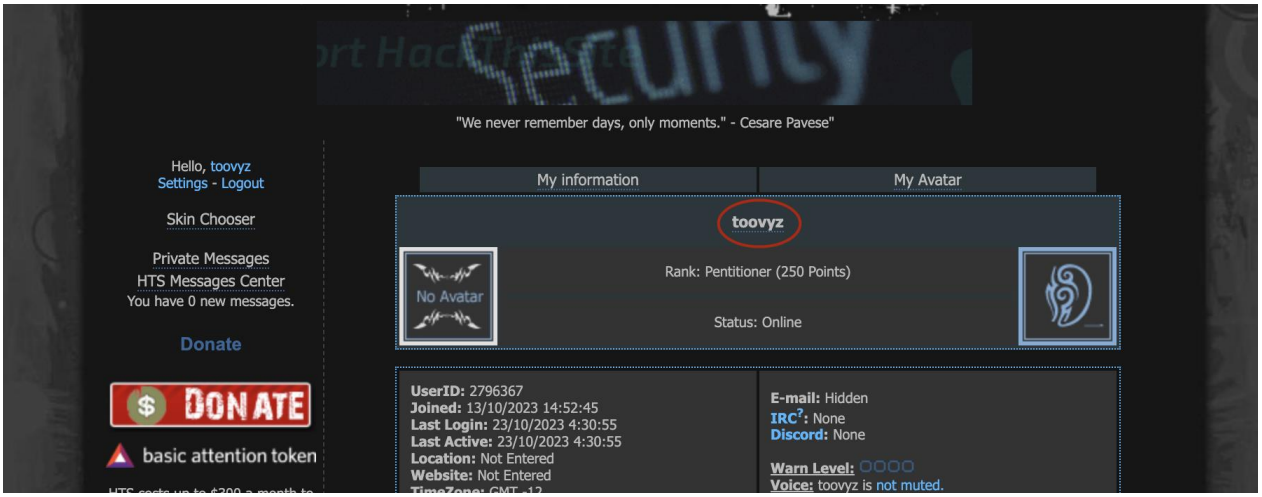
Dùng mệnh đề ORDER BY để tìm ra số cột trong bảng product → 4 cột.



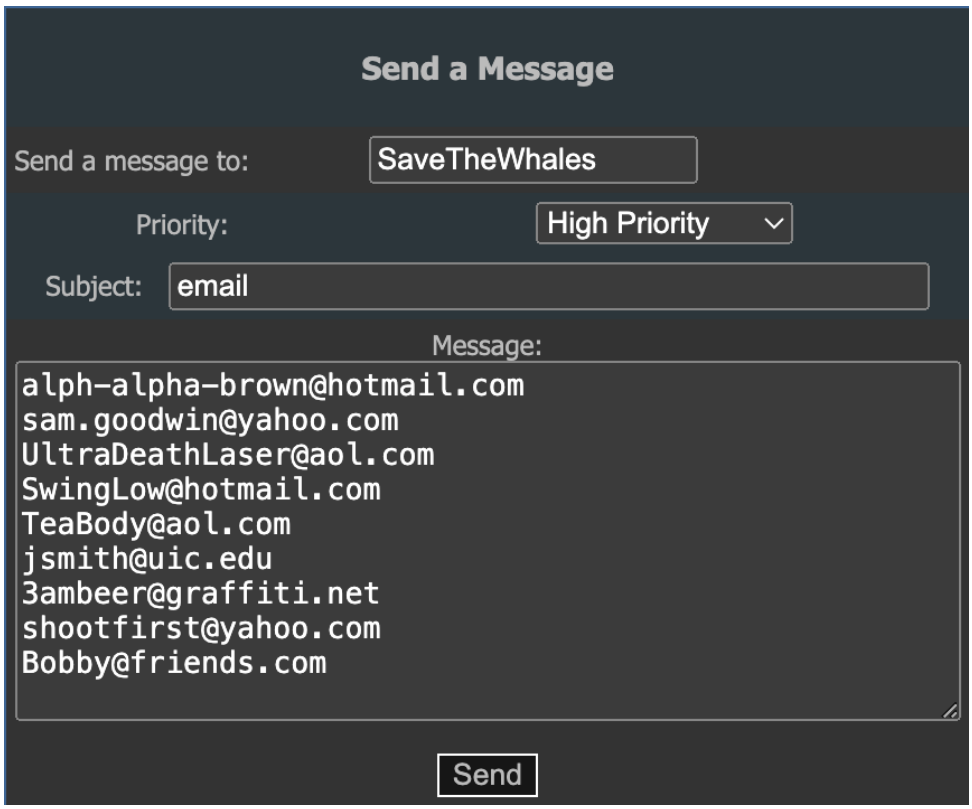
Chèn `union all select null,*,null,null from email`.



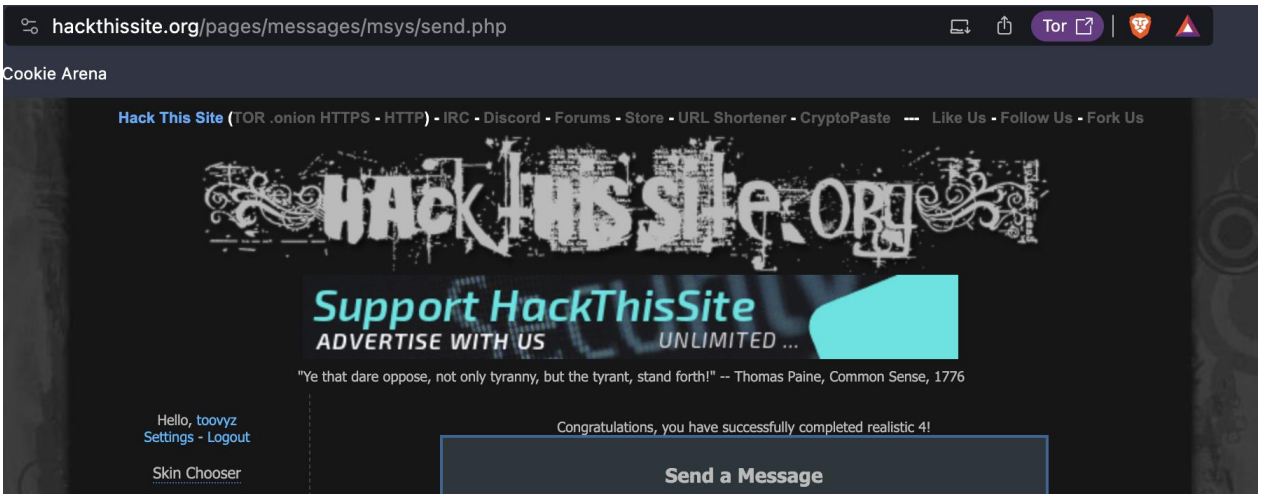
Nhận được danh sách các email. Sau đó vào profile của mình, bấm vào username.



Soạn email với list các email thu được, người nhận là tác giả của challenge - SaveTheWhales, bấm `send`.



c. Kết quả



d. Kỹ thuật sử dụng

- SQL injection: UNION attack.
- Mô tả: Dùng UNION để lấy dữ liệu từ bảng khác trong cơ sở dữ liệu.

Moderate: Damn Telemarketers!

a. Mục tiêu

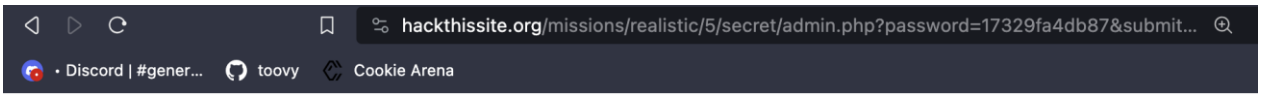
From: spiffomatic64

Message: Yo! This is Spiffomatic64 from Hackthissite.org! I'm a bit of a hacker myself as you can see, but I recently came upon a problem I couldn't resolve.....
Lately I've been getting calls day and night from the telemarketing place. I've gone to their website and hacked it once deleting all of their phone numbers so they wouldn't call me anymore. That was a temporary fix but they put their database back up, this time with an encrypted password. When I hacked them I noticed everything they used was 10 years out of date and the new password seems to be a 'message digest'. I have done some research and I think it could be something like a so-called hash value. I think you could somehow reverse engineer it or brute force it. I also think it would be a good idea to look around the server for anything that may help you.

Tìm được hash value và reverse nó.

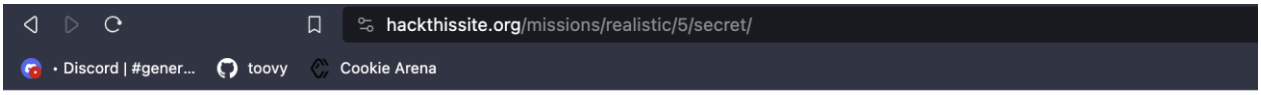
b. Phương pháp

Kiểm tra xung quanh, biết được chỉ có admin mới có thể access được database. Vào database, submit password ngẫu nhiên. Website direct tới `secret/admin.php?=.`



Invalid Password

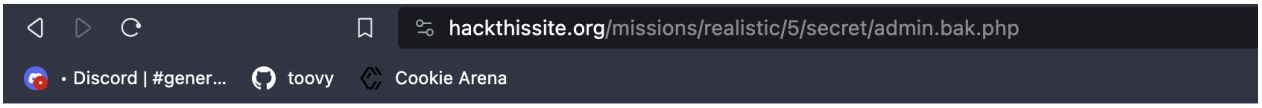
Mở thư mục `secret`.



Index of /missions/realistic/5/secret

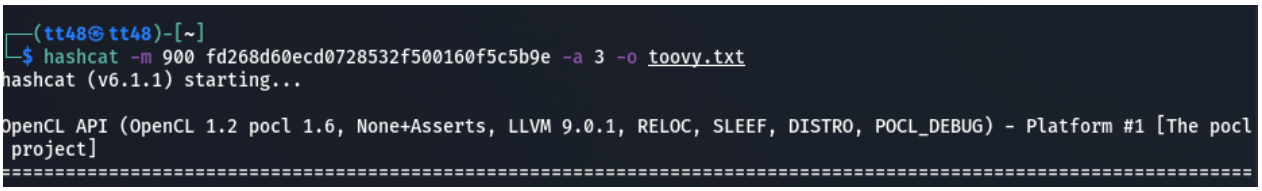
Name	Last modified	Size	Description
Parent Directory		-	
admin.bak.php	2013-12-30 05:28	230	
admin.php	2013-12-30 05:28	621	

Mở tiếp tệp `admin.bak.php`.

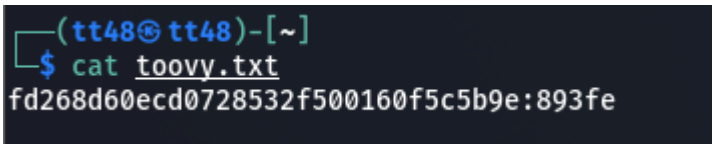


error matching hash fd268d60ecd0728532f500160f5c5b9e

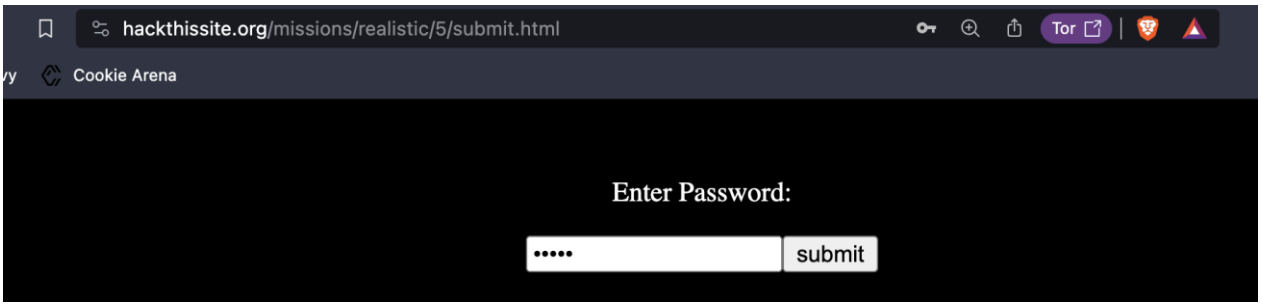
Dùng hashcat để crack: `hashcat -m 900 fd268d60ecd0728532f500160f5c5b9e -a 3 -o toovy.txt`.



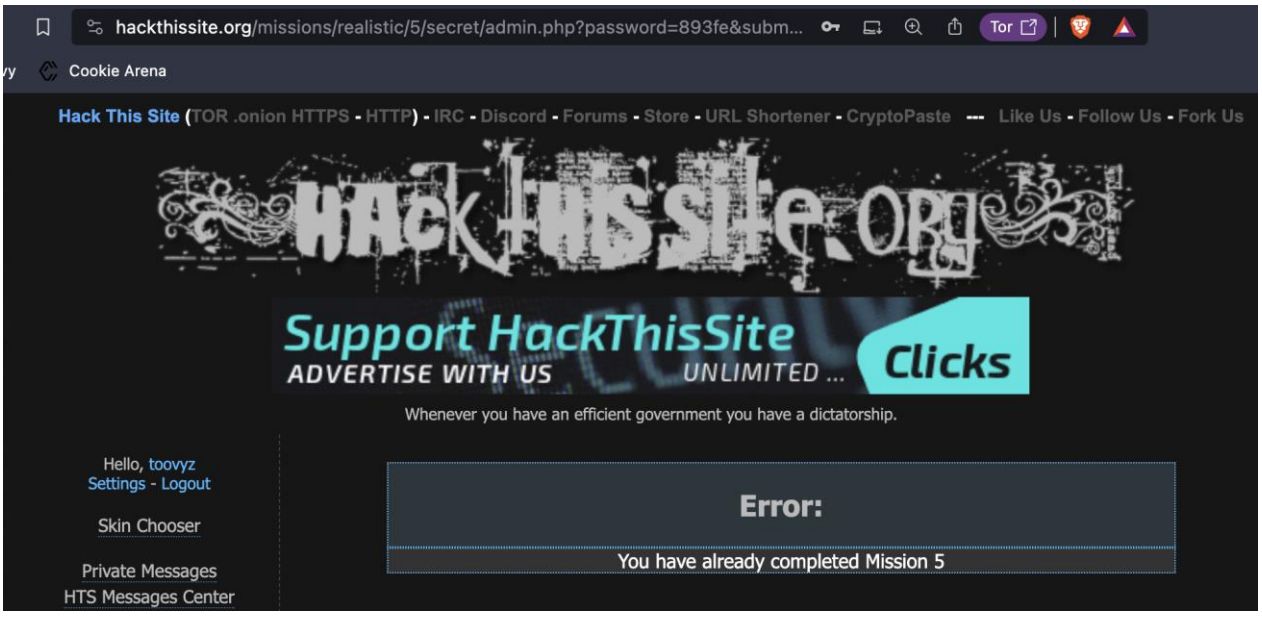
Plain text thu được: `893fe`.



Dùng mật khẩu mới brute force được đăng nhập vào database.



c. Kết quả



d. Kỹ thuật sử dụng

- Path Traversal và Hash Cracking.
- Mô tả: Path traversal hay còn gọi là Directory Traversal là một lỗ hổng bảo mật cho phép kẻ tấn công đọc các file tùy ý trên server. Nó dẫn đến việc bị lộ thông tin nhạy cảm của ứng dụng web như thông tin đăng nhập, một số file hoặc thư mục hệ điều hành.

Moderate: What's Right For America

a. Mục tiêu

From: FreedomOfChoice

Message: Friend of freedom and liberty, I invite you to take a look at the hate speech being spewed over the web at http://www.hackthissite.org/missions/realistic/7/. It's so funny that conservatives keep saying they want to protect the values of America - freedom, tolerance, and democracy - but when it comes to personal choices like private marijuana use or same-sex marriages, they damn them to burn in eternal hell and send them to jail. This is a personal freedom issue. No one else is hurt if two consenting adults decide to marry. But people who claim to have the moral high ground decide to ruin it for everyone else and discriminate against same-sex couples. To think that they are talking about making a constitutional amendment to STOP OUR FREEDOM TO MARRY is ludicrous. This injustice must be stopped.
There is an admin section on that website somewhere, perhaps hidden among their directory structure. It would be a great fight against moral tyranny and a victory for freedom if you could somehow hack into their website. Thank you.

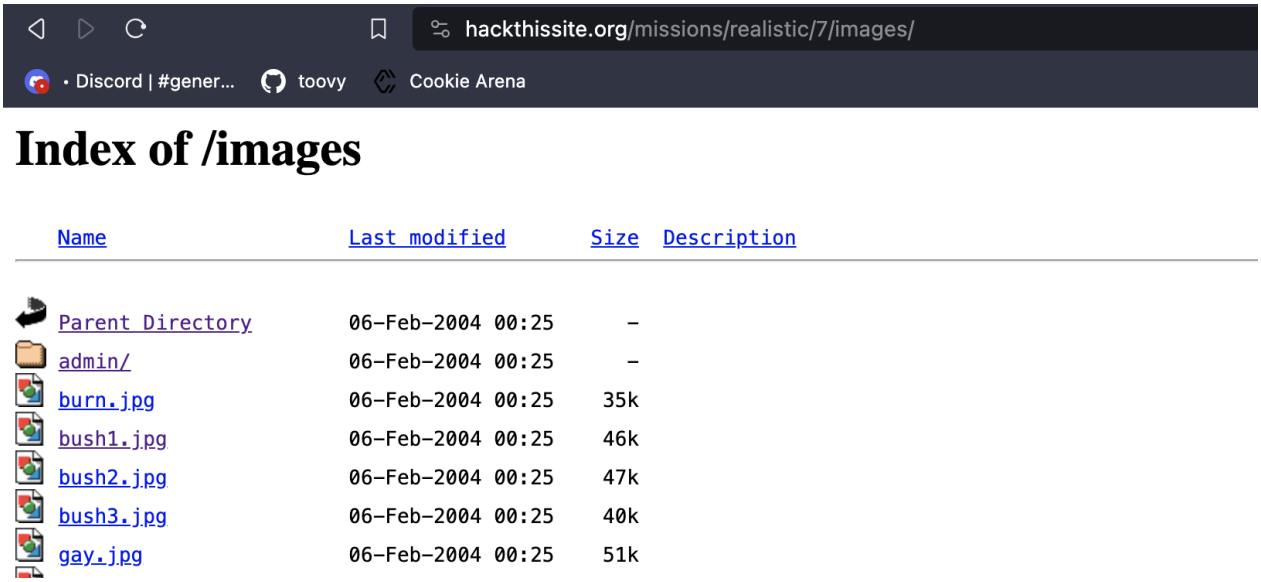
Xâm nhập vào admin section.

b. Phương pháp

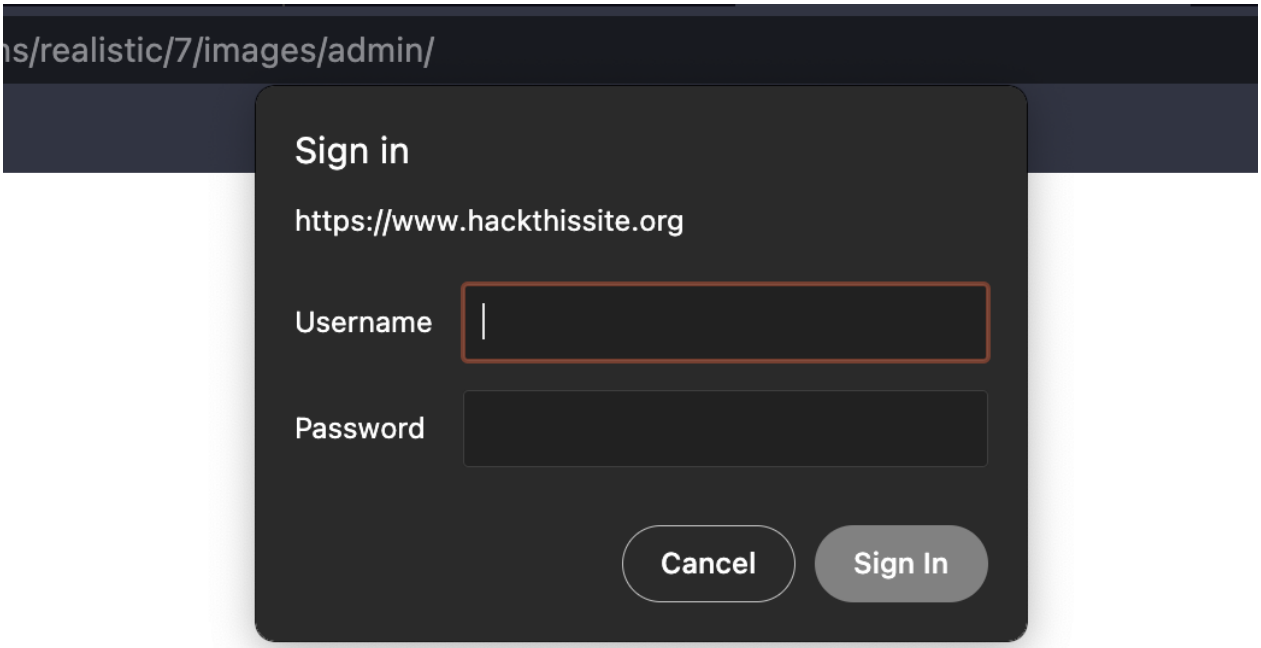
Vào trang `Patriotism` → View Page Source.

```
<center><img src="images/logo.jpg" width=500 height=49 border=0>
<br /><b>The Right is taking back America... and you love it!</b></center><Br>

<center><b>Spread the Word!</b></center>

Help spread conservative action by downloading and printing these posters. Here are some tips: post

<center>
<a href="showimages.php?file=patriot.txt">Patriotism</a> | <a href="showimages.php?file=bush.txt">L
</center>
<br />



<center><a href="images/patriot1.jpg
"><img src="images/patriot1.jpg
" width=100></a> <a href="images/patriot2.jpg
"><img src="images/patriot2.jpg
" width=100></a> <a href="images/patriot3.jpg
"><img src="images/patriot3.jpg
" width=100></a> <a href="images/patriot4.jpg
"><img src="images/patriot4.jpg
" width=100></a> <a href="images/patriot5.jpg
"><img src="images/patriot5.jpg
" width=100></a> <a href=""><img src="" width=100></a> </center></font>
</td></tr></table>
```

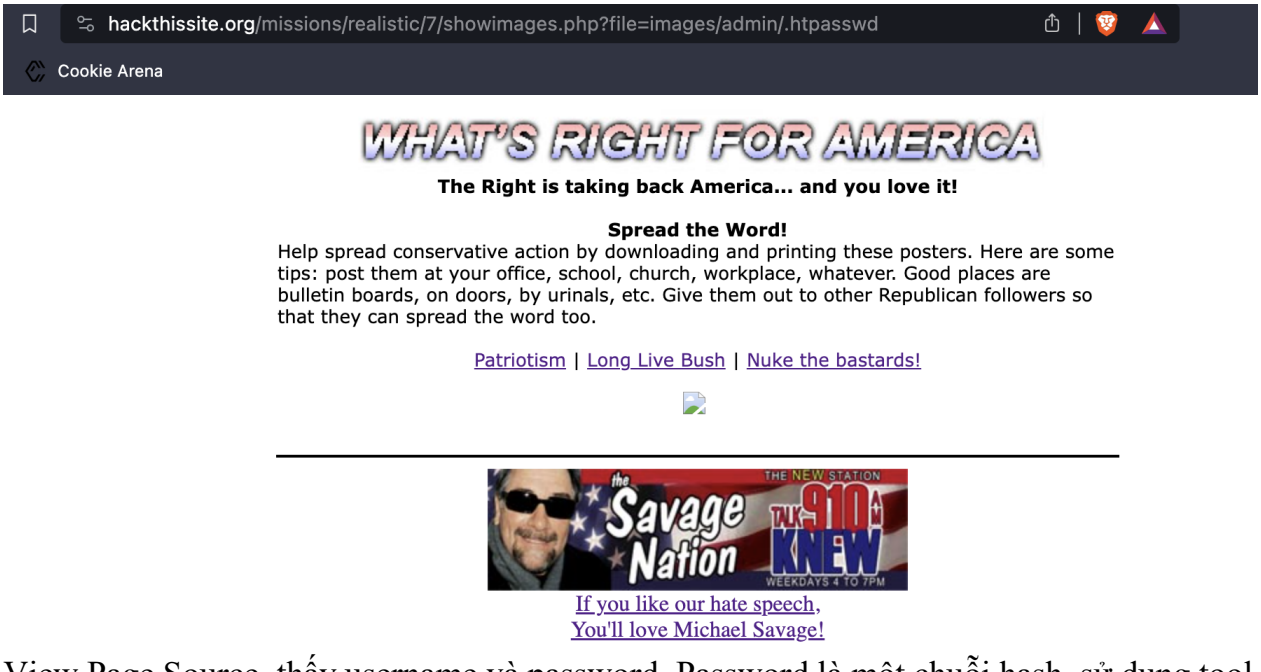
Thấy các hình ảnh trong trang này và trang chủ đều nằm trong thư mục `images`, mở file `images`.



Mở tiếp thư mục `admin/`.



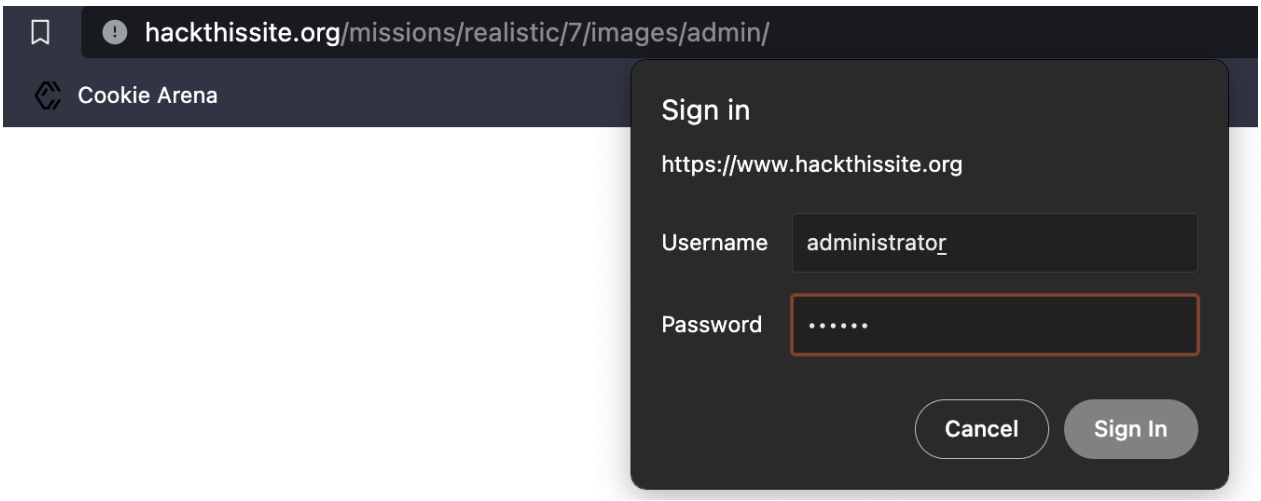
Thử mở file `.htpasswd` - tệp mà Apache sử dụng để xác thực, trong thư mục admin: `?file=images/admin/.htpasswd`.



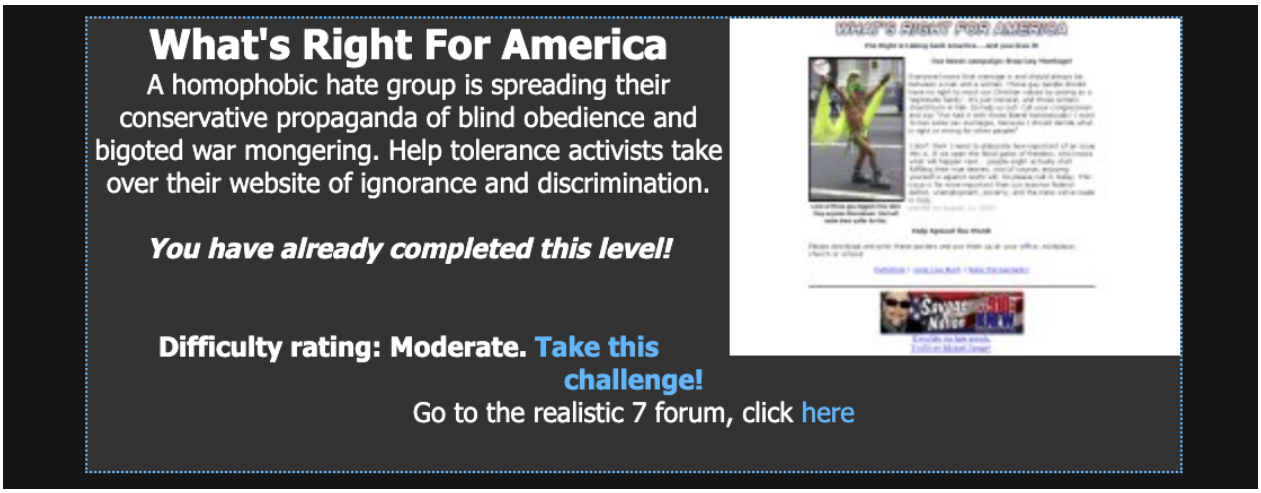
View Page Source, thấy username và password. Password là một chuỗi hash, sử dụng tool crack hash như John the Ripper, Hashcat …

```
26
27 <center><a href="administrator:$1$AAODv...$gXPqGkIO3Cu6dnclE/sok1
28 "><img src="administrator:$1$AAODv...$gXPqGkIO3Cu6dnclE/sok1
29 " width=100></a> <a href=""><img src="" width=100></a> </center></font>
30 </td></tr></table>
31
```

Đăng nhập bằng username và password.



c. Kết quả



d. Kỹ thuật sử dụng

- Path traversal.
- Mô tả: Truy cập đến các file nằm ngoài thư mục root của website.

Hard: ToxiCo Industrial Chemicals

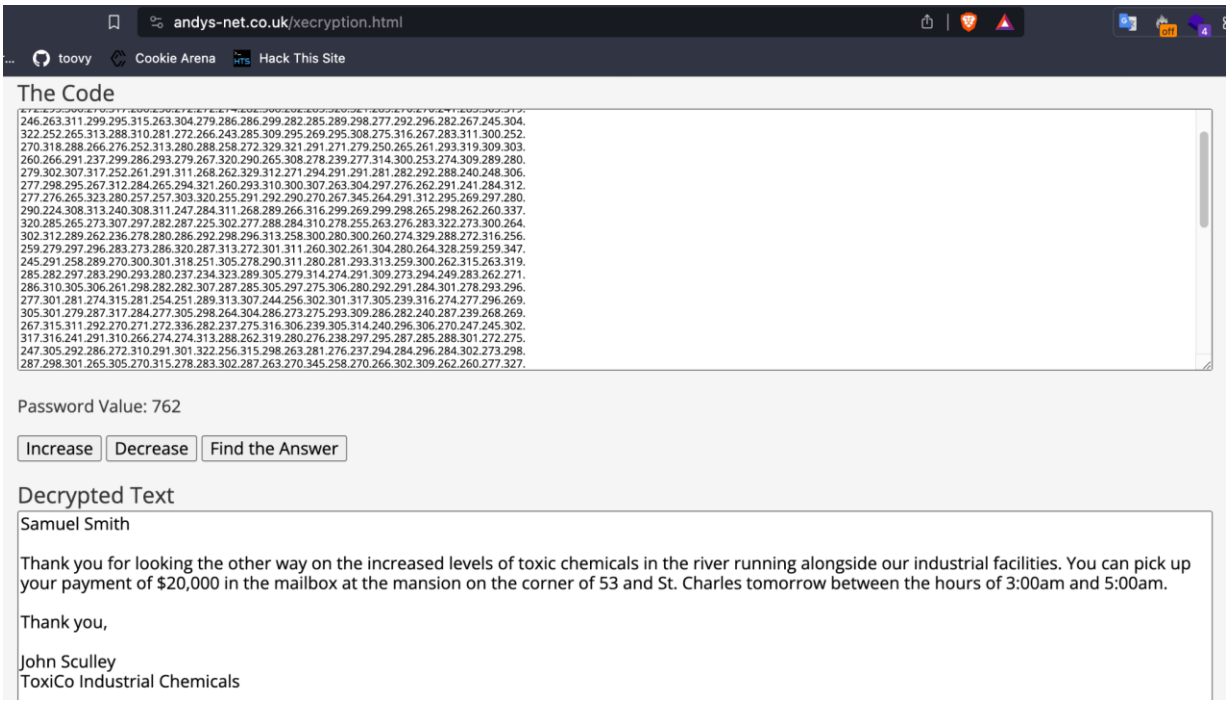
a. Mục tiêu

From: ToxiCo_Watch

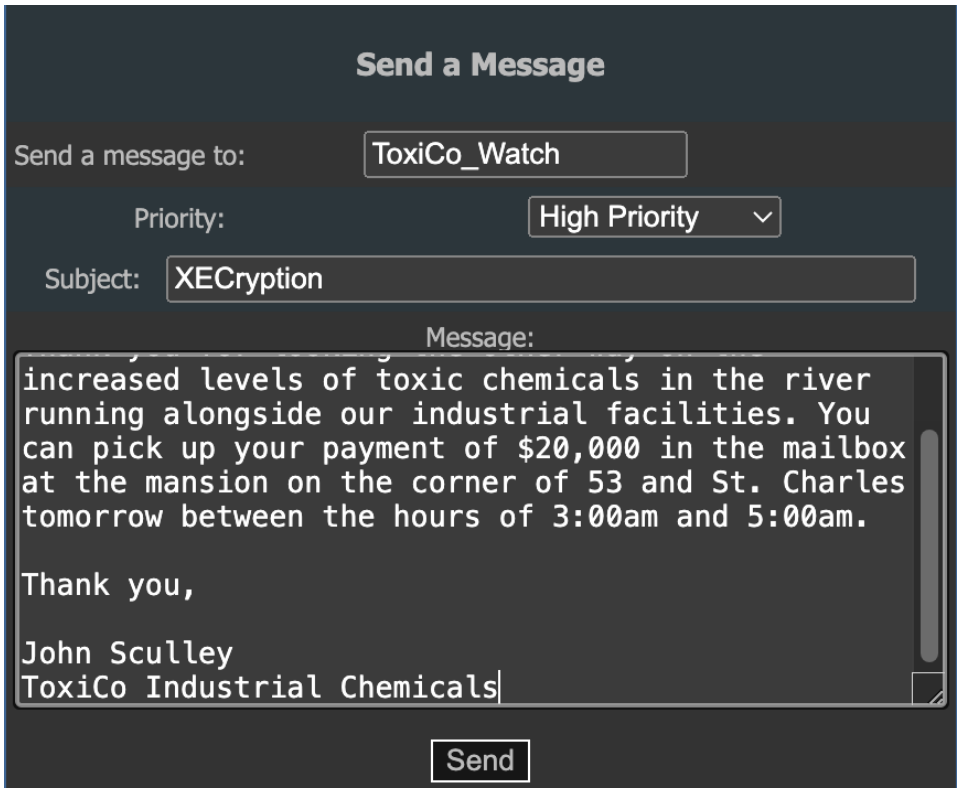
Message: Hello esteemed hacker, I hope you have some decent cryptography skills. I have some text I need decrypted.
I work for this company called ToxiCo Industrial Chemicals, which has recently come under fire because of the toxic chemicals we are dumping into the river nearby. Ecological inspectors have reported no problems, but it is widely speculated that they were paid off by ToxiCo management because the water pollution near the ToxiCo factory has always been a serious and widely publicized issue.
I have done some packet sniffing on my network and I have recovered this email that was sent from the CEO of the company to Chief Ecological Inspector Samuel Smith. However, it is encrypted and I cannot seem to decode it using any of my basic decryption tools. I have narrowed it down to the algorithm used to encrypt it, but it is beyond my scope. I was hoping you can take a look at it.
Please check it out,
more details are on the page. If you can unscramble it and reply to this message with the original text, it would be much appreciated. Thank you.

b. Phương pháp

Vào trang copy đoạn mã. Google search `XECryption decrypt`, paste đoạn mã vào trang decrypt online bất kỳ.



Copy plain text và gửi cho ToxiCo_Watch.



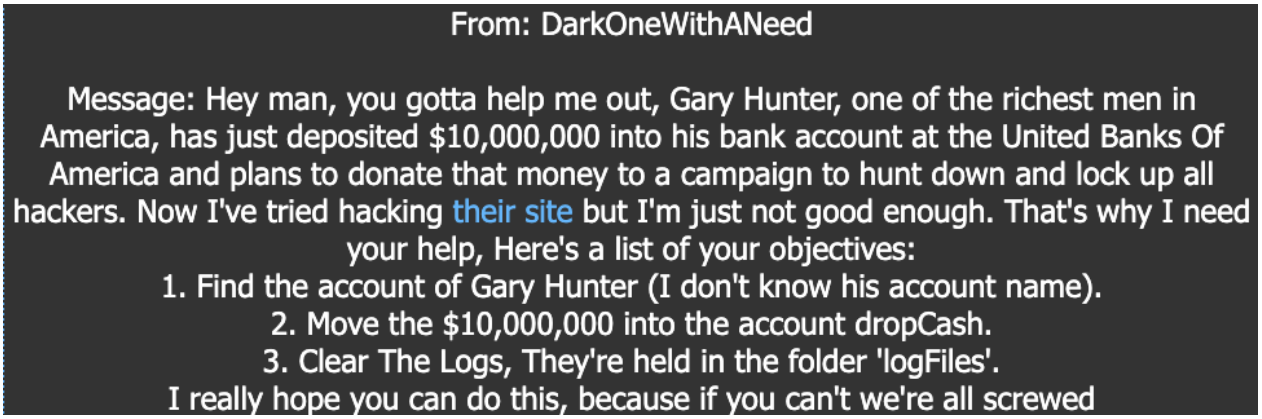
c. Kết quả

d. Kỹ thuật sử dụng

- XECryption decode.

Hard: United Banks Of America

a. Mục tiêu



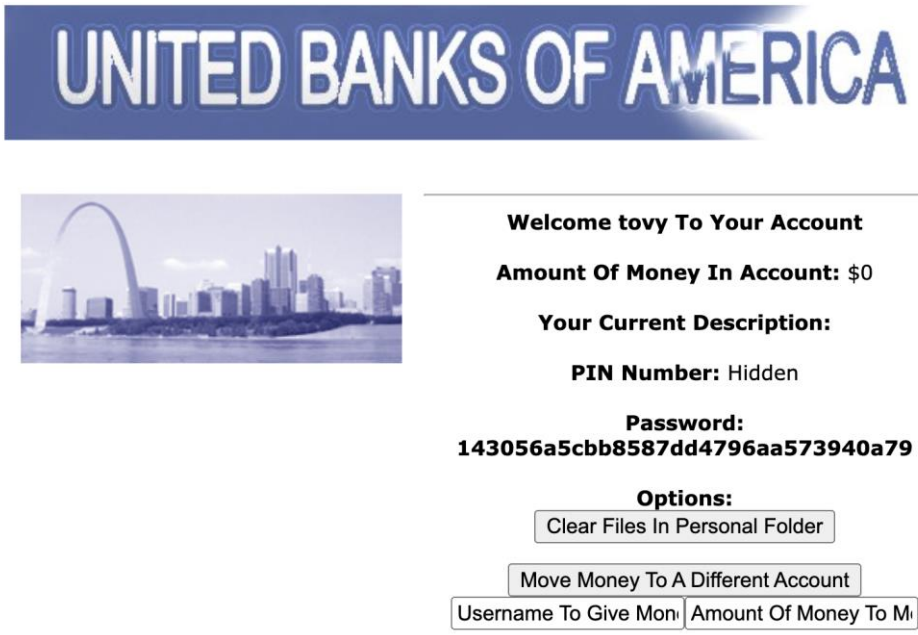
Tìm account của Gary Hunter, chuyển $10,000,000 sang dropCash và cuối cùng xóa `logFiles`.

b. Phương pháp

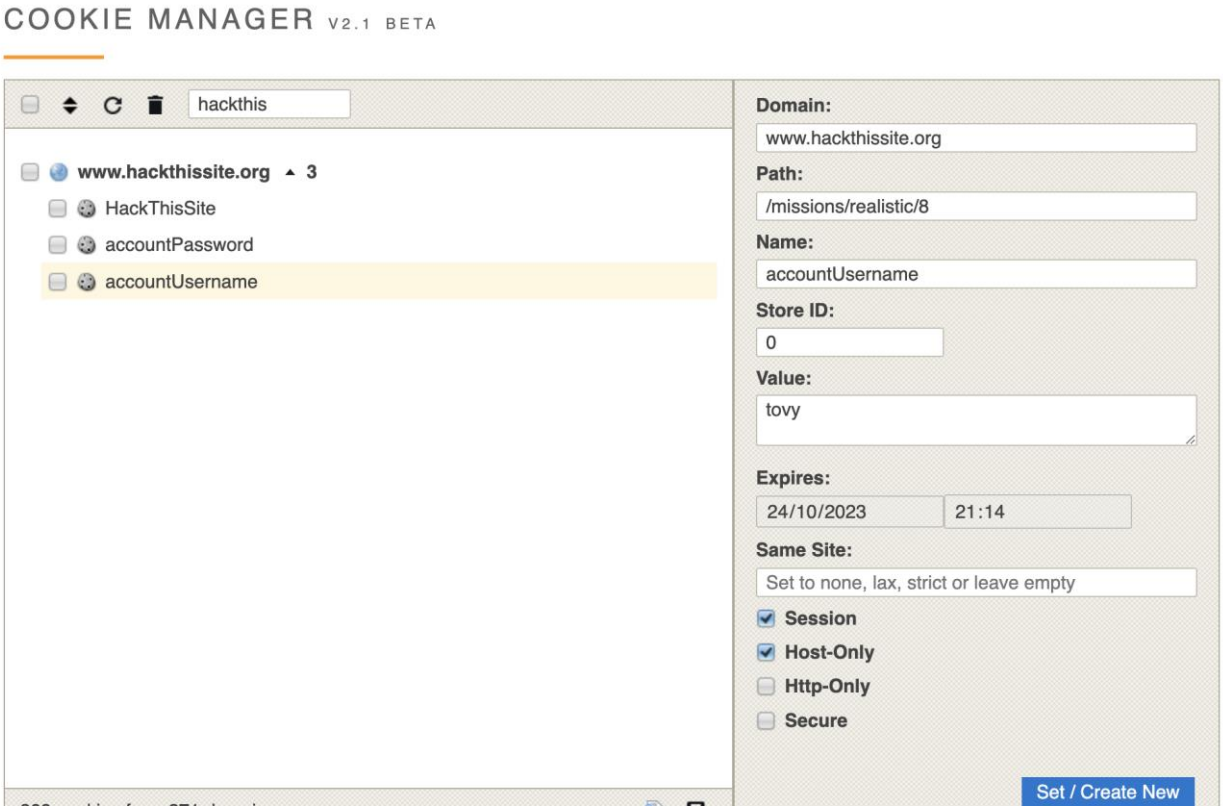
Vào từng tab Home, Login, Register, Help, User Info để kiểm tra. Cuối cùng ở User Info có lỗ hổng SQL injection. Inject `' or 1=1 --` , nó hiển thị thông tin tất cả user.

Search Gary thì thấy account sau:

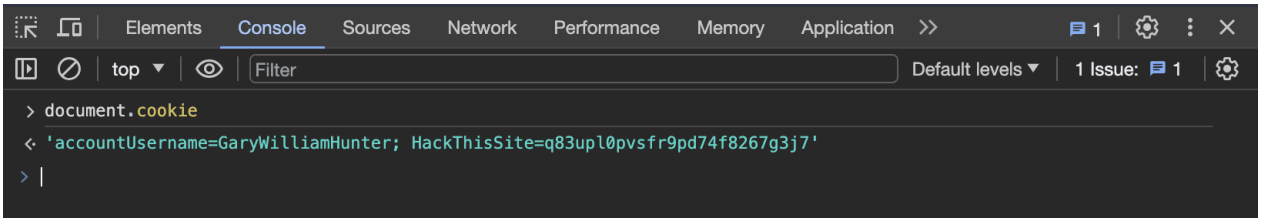
Tiếp theo, đăng ký account sau đó đăng nhập bằng account mới vừa đăng kí.



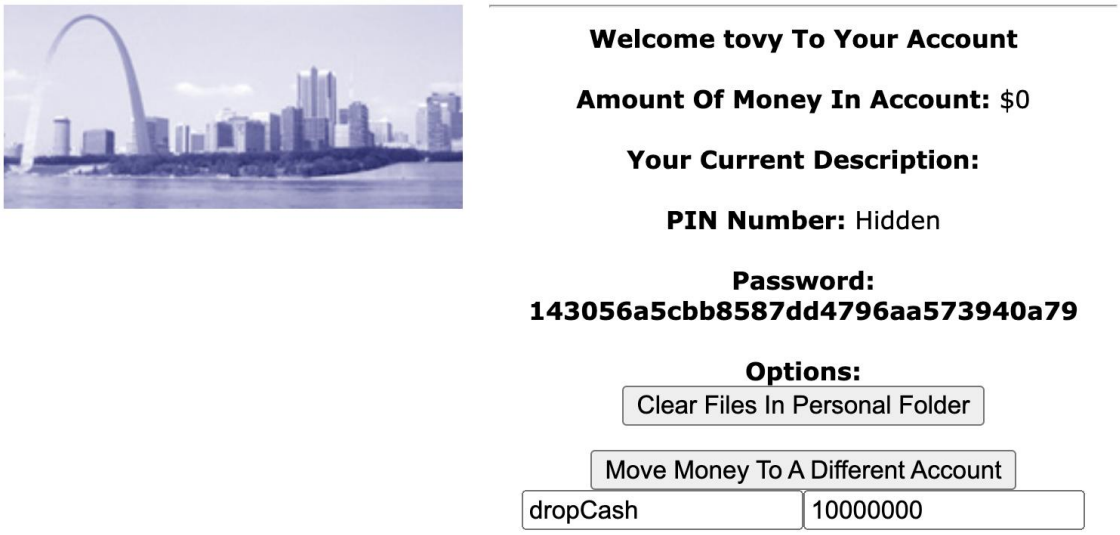
Xem xét cookie, thấy có `accountUsername` và `accountPassword` với giá trị là username và password mà user dùng để đăng nhập.



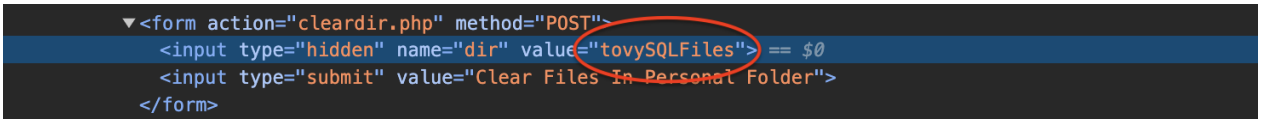
Đổi `value` của `accountUsername` thành GaryWilliamHunter và xóa cookie `accountPassword`. Sau đó quay lại trang login, chuột phải → Inspect → Console → gõ `document.cookie` để check lại.



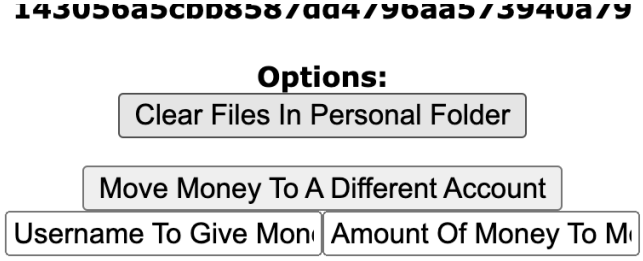
Sau chuyển `10000000` cho `dropCash`.



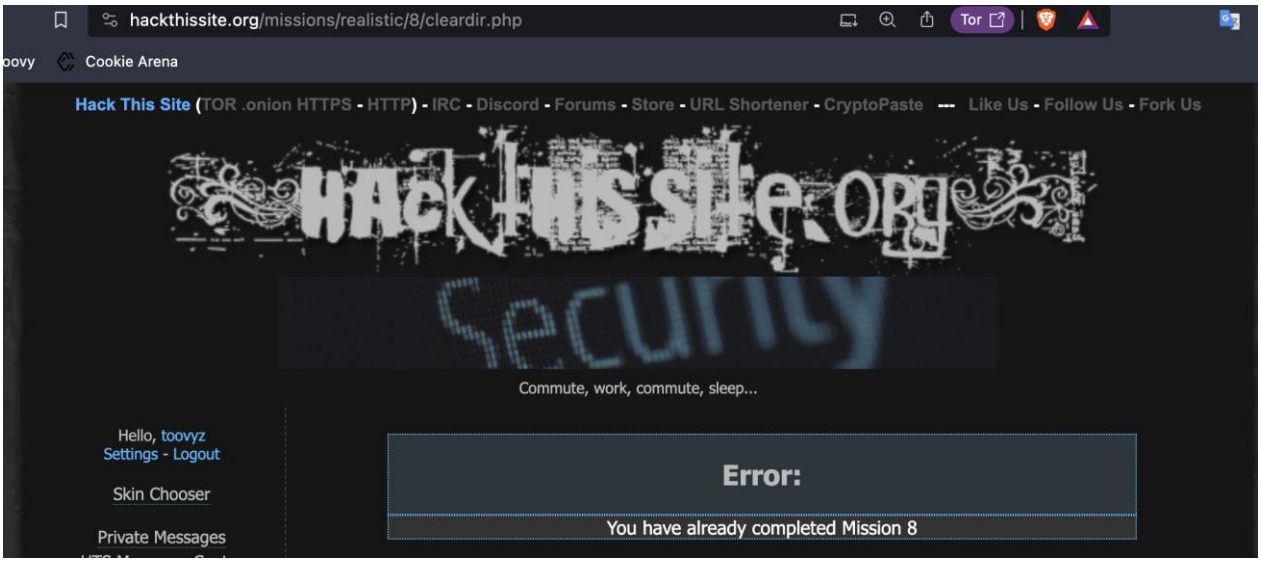
Thành công chuyển tiền, việc còn lại là xóa thư mục `logFiles`. Đăng nhập lại với account `tovy`, chuột phải → Inspect. Sửa `tovySQLFiles` thành `logFiles`.



Sau đó click chọn ô `Clear Files In Personal Folder`.



c. Kết quả



d. Kỹ thuật sử dụng

- SQL injection, Session Hijacking.
- Mô tả: attacker kiểm soát phiên duyệt web của user để có quyền truy cập vào thông tin nhạy cảm, hoặc giả danh để thực hiện các hành động không mong muốn.