

MỤC LỤC

Easy challenge: Uncle Arnold's Local Band Review	2
a. Mục tiêu	2
b. Phương pháp	2
c. Kết quả	3
d. Kỹ thuật sử dụng.....	3
Easy challenge: Chicago American Nazi Party	4
a. Mục tiêu	4
b. Phương pháp	4
c. Kết quả	5
d. Kỹ thuật sử dụng.....	5
Moderate: Peace Poetry: HACKED.....	6
a. Mục tiêu	6
b. Phương pháp	6
c. Kết quả	8
d. Kỹ thuật sử dụng.....	8
Moderate: Fischer's Animal Products.....	9
a. Mục tiêu	9
b. Phương pháp	9
c. Kết quả	12
d. Kỹ thuật sử dụng.....	12
Moderate: Damn Telemarketers!	13
a. Mục tiêu	13
b. Phương pháp	13
c. Kết quả	14
d. Kỹ thuật sử dụng.....	15
Moderate: What's Right For America	16
a. Mục tiêu	16
b. Phương pháp	16
c. Kết quả	19
d. Kỹ thuật sử dụng.....	19
Hard: ToxiCo Industrial Chemicals.....	20
a. Mục tiêu	20
b. Phương pháp	20
c. Kết quả	21
d. Kỹ thuật sử dụng.....	21
Hard: United Banks Of America	22
a. Mục tiêu	22
b. Phương pháp	22
c. Kết quả	25
d. Kỹ thuật sử dụng.....	25

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!

Dưa ban nhạc của Raging Inferno lên đầu danh sách.

b. Phương pháp

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

[Raging Inferno](#)

This is a self-proclaimed "hardcore" metal band pretty much does nothing besides covering older slayer songs and nintendo game 'music' with added high-pitched screaming. I give these guys an F.

The average rating of this band is 2.3141751857359. How would you rate it?

1 ▾

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

Pretty	Raw	Hex
1 GET /missions/realistic/1/v.php?PHPSESSID=abcaeafc31a5c43b2534bf995c0553f&id=8& 2 Host: www.hackthissite.org 3 Cookie: HackThisSite=rko1p111mngv77vgdfa6ehnvr5 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	GET /missions/realistic/1/v.php?PHPSESSID=abcaeafc31a5c43b2534bf995c0553f&id=8&vote=1 HTTP/2 Host: www.hackthissite.org Cookie: HackThisSite=rko1p111mngv77vgdfa6ehnvr5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://www.hackthissite.org/missions/realistic/1/ Upgrade-Insecure-Requests: 1 Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: same-origin Sec-Fetch-User: ?1 Te: trailers	

Sửa thành giá trị của vote thành 999999999, và forward.

Pretty	Raw	Hex
1 GET /missions/realistic/1/v.php?PHPSESSID=abcaeafc31a5c43b2534bf995c0553f&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

From: DestroyFascism

Message: I have been informed that you have quite admirable hacking skills. Well, this racist hate group is using [their website](#) to organize a mass gathering of ignorant racist bastards. We cannot allow such bigoted aggression to happen. If you can gain access to their administrator page and post messages to their main page, we would be eternally grateful.

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

b. Phương pháp

Chuột phải → View Page Source.



The screenshot shows a dark-themed web browser. On the left is the website content, which includes a red header with a white swastika logo and the words "WHITE POWER". Below this is a banner with the text "JOIN THE AMERICAN NAZI PARTY FIGHT FOR WHITE POWER". Under the banner are two event posts: "Meeting July 18th" by "WhiteKing" and "RALLY AT INS BUILDING" by "Jones". On the right is a context menu with several options: "Save Page As...", "Save Page to Pocket", "Select All", "Take Screenshot", "View Page Source" (which is highlighted in blue), "Inspect Accessibility Properties", and "Inspect (Q)". At the bottom of the menu is a "Translate this page" button.

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

```
23 <center><a href="/missions/realistic/2/update.php"><font color="#000000">update</font></a></center><br />
24
25 </body>
26 </html>
```

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

The screenshot shows a web browser window with the URL <https://www.hackthissite.org/missions/realistic/2/update2.php>. The page displays a banner for "Hack This Site" with various links like "Hack This Site (TOR .onion HTTPS - HTTP) - IRC - Discord - Forums - Store - URL Shortener - CryptoPaste - Like Us - Follow Us - Fork Us". Below the banner is a large, stylized "HACK THIS SITE ORG" logo. A quote at the bottom left reads: "'Political freedom is a society's safety valve, allowing the passionately critical a nonviolent way to express their dissatisfaction with the status quo.' --David Cole". On the left side, there's a sidebar with user information: "Hello, toowyz" and "Settings - Logout". On the right side, a message says "You have already done this." with a blue "Go on" button. The overall theme is dark with some light-colored text and graphics.

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 đê 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.

The screenshot shows a browser window with the URL <http://hackthissite.org/missions/realistic/3/oldindex.html>. The page content is as follows:

Peace Poetry

"What difference does it make to the dead, the orphans and the homeless, whether the mad destruction is wrought under the name of totalitarianism or the holy name of liberty and democracy?" - Mahatma Gandhi

"A war is not won if the defeated enemy has not been turned into a friend."

WAR IS NOT HEALTHY FOR CHILDREN AND OTHER LIVING THINGS

"The greatest purveyor of violence in the world today is my own government. For the sake of hundreds of thousands trembling under our violence, I cannot be silent." - Martin Luther King Jr.

"The nationalist not only does not disapprove of atrocities committed by his own side, but he has a remarkable capacity for not even hearing about them." - George Orwell

Welcome to Peace Poetry. This website features several poems crying out for freedom, liberty, justice, peace, love and understanding. You can also submit your own poetry!

[Read The Poetry](#) | [Submit Poetry](#)

Vào Submit Poetry và Read The Poetry.

Use this form to submit a poem to the website. You do not have to be the author, but if you use someone else's poetry, please give credit where credit is due. Thanks!

Note: Poems will be stored online immediately but will not be listed on the main poetry page until it has a chance to be looked at.

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.

Use this form to submit a poem to the website. You do not have to be the author, but if you use someone else's poetry, please give credit where credit is due. Thanks!

Note: Poems will be stored online immediately but will not be listed on the main poetry page until it has a chance to be looked at.

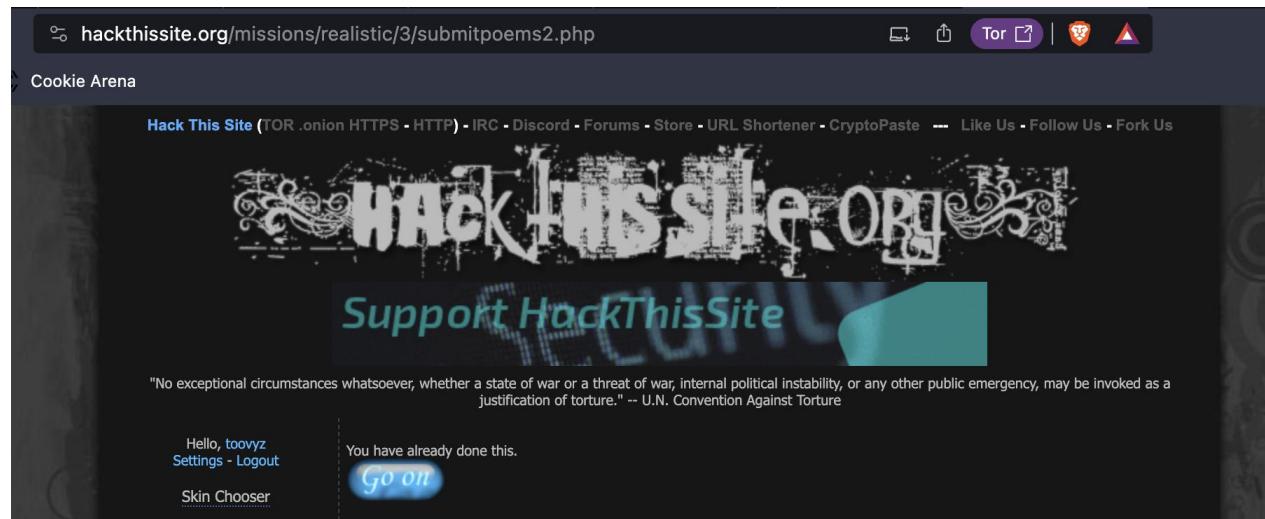
Name of poem:
./index.html

Poem:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd"><html><head>
<title>peace be with all</title></head>
<body background="bg.jpg" text="#FFFFFF" link="#FFF833" vlink="#FFF833"><center>
<font face="verdana" size=7><b>Peace
Poetry</b></font><table cellspacing=0 border=0 cellpadding=0 align="center" width=760><tr><td width=230><font face="verdana" size=2><b>What
difference does it make to the dead, the
orphans and the homeless, whether the
```

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

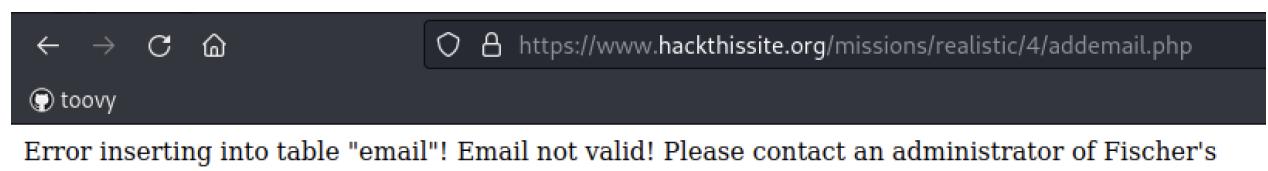
From: SaveTheWhales

Message: Hello, I was referred to you by a friend who says you know how to hack into computers and web sites - well I was wondering if you could help me out here. There's this local store who is killing hundreds of animals a day exclusively for the purpose of selling jackets and purses etc out of their skin! I have been to their website and they have an email list for their customers. I was wondering if you could somehow hack in and send me every email address on that list? I want to send them a message letting them know of the murder they are wearing. Just reply to this message with a list of the email addresses. Please? Their website is at <http://www.hackthissite.org/missions/realistic/4/>. Thanks so much!!

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.



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.

A big hairy fur coat that is made of fuzzy cute animals that we mercilessly slaughtered
\$2550.00

A big hairy fur coat that is made of fuzzy cute animals that we mercilessly slaughtered
\$1850.00

A big hairy fur coat that is made of fuzzy cute animals that we mercilessly slaughtered
\$2200.00

Yes, these are authentic alligator shoes, made from real alligators!
\$140

Alligator purses! We tear the skin off alligators and put it in purse form so you can put your money and makeup in!
\$70

Belts made of alligators! Different colors available, contact us for more information!
\$30

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

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

alph-alpha-brown@hotmail.com

sam.goodwin@yahoo.com

UltraDeathLaser@aol.com

SwingLow@hotmail.com

TeaBody@aol.com

ismith@uic.edu

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

The screenshot shows a user profile page for 'toovyz'. At the top, there's a banner with the text 'Port Hack The Security' and a quote: "'We never remember days, only moments.' - Cesare Pavese". Below the banner, the user's name 'Hello, toovyz' and 'Settings - Logout' are displayed. A 'Skin Chooser' link is also present. On the left, there are links for 'Private Messages' (0 new messages), 'Donate' (with a button for 'basic attention token'), and a 'HTC costs up to €200 a month to...' link. The main area shows 'My information' and 'My Avatar' tabs. The 'My information' tab is active, showing the user's rank as 'Pentitioner (250 Points)', status as 'Online', and various account details like UserID, Joined date, Last Login, Last Active, Location, Website, and Timezone. The 'My Avatar' tab shows a placeholder 'No Avatar' and a custom profile picture of an ear.

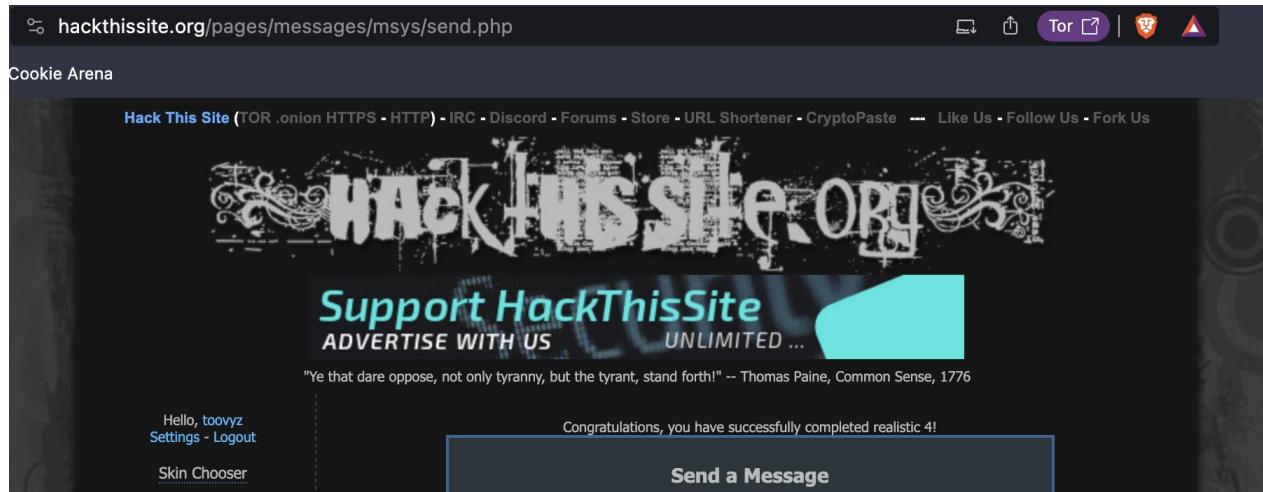
Soạn email với list các email thu được, người nhận là tác giả của challenge - SaveTheWhales, bấm send.

The screenshot shows a 'Send a Message' form. The recipient field is filled with 'SaveTheWhales'. The priority is set to 'High Priority'. The subject is 'email'. In the message body, there is a list of email addresses:

```
alph-alpha-brown@hotmail.com
sam.goodwin@yahoo.com
UltraDeathLaser@aol.com
SwingLow@hotmail.com
TeaBody@aol.com
jsmith@uic.edu
3ambeer@graffiti.net
shootfirst@yahoo.com
Bobby@friends.com
```

At the bottom right of the message body is a 'Send' button.

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

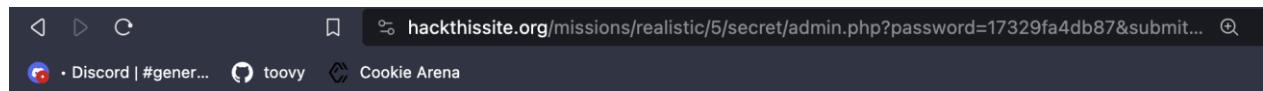
From: spiffomatic64

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.

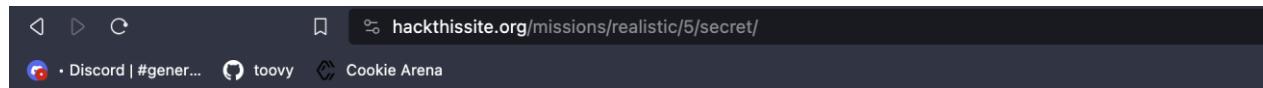
b. Phương pháp

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.

Discord | #gener... toovy Cookie Arena

hackthissite.org/missions/realistic/5/secret/admin.bak.php

error matching hash fd268d60ecd0728532f500160f5c5b9e

Dùng hashcat để crack: hashcat -m 900

fd268d60ecd0728532f500160f5c5b9e -a 3 -o toovy.txt.

```
(tt48@tt48)-[~]
$ hashcat -m 900 fd268d60ecd0728532f500160f5c5b9e -a 3 -o toovy.txt
hashcat (v6.1.1) starting...
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
```

Plain text thu được: 893fe.

```
(tt48@tt48)-[~]
$ cat toovy.txt
fd268d60ecd0728532f500160f5c5b9e:893fe
```

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

hackthissite.org/missions/realistic/5/submit.html

Cookie Arena

Enter Password:

..... submit

c. Kết quả

hackthissite.org/missions/realistic/5/secret/admin.php?password=893fe&subm...

Cookie Arena

Hack This Site (TOR .onion HTTPS - HTTP) - IRC - Discord - Forums - Store - URL Shortener - CryptoPaste --- Like Us - Follow Us - Fork Us

HACK THIS SITE ORG

Support HackThisSite
ADVERTISE WITH US UNLIMITED ... Clicks

Whenever you have an efficient government you have a dictatorship.

Hello, toovy
Settings - Logout

Skin Chooser

Private Messages

HTS Messages Center

Error:

You have already completed Mission 5

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.

```
12 <center>
13 <br /><b>The Right is taking back America... and you love it!</b></center><br>
14
15 <center><b>Spread the Word!</b></center>
16
17 Help spread conservative action by downloading and printing these posters. Here are some tips: post
18 <center>
19 <a href="showimages.php?file=patriot.txt">Patriotism</a> | <a href="showimages.php?file=bush.txt">L
20 </center>
21 <br />
22
23
24
25
26 <center><a href="images/patriot1.jpg
27 "></a> <a href="images/patriot2.jpg
29 "></a> <a href="images/patriot3.jpg
31 "></a> <a href="images/patriot4.jpg
33 "></a> <a href="images/patriot5.jpg
35 "></a> <a href=""><img src="" width=100></a> </center></font>
37 </td></tr></table>
```

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

hackthissite.org/missions/realistic/7/images/

Discord | #gener... toovy Cookie Arena

Index of /images

Name	Last modified	Size	Description
Parent Directory	06-Feb-2004 00:25	-	
admin/	06-Feb-2004 00:25	-	
burn.jpg	06-Feb-2004 00:25	35k	
bush1.jpg	06-Feb-2004 00:25	46k	
bush2.jpg	06-Feb-2004 00:25	47k	
bush3.jpg	06-Feb-2004 00:25	40k	
gay.jpg	06-Feb-2004 00:25	51k	

Mở tiếp thư mục admin/.

ns/realistic/7/images/admin/

Sign in

https://www.hackthissite.org

Username |

Password

Cancel Sign In

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

hackthissite.org/missions/realistic/7/showimages.php?file=images/admin/.htpasswd

Cookie Arena

WHAT'S RIGHT FOR AMERICA

The Right is taking back America... and you love it!

Spread the Word!

Help spread conservative action by downloading and printing these posters. Here are some tips: post them at your office, school, church, workplace, whatever. Good places are bulletin boards, on doors, by urinals, etc. Give them out to other Republican followers so that they can spread the word too.

[Patriotism](#) | [Long Live Bush](#) | [Nuke the bastards!](#)



If you like our hate speech,
You'll love Michael Savage!

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

```
26 <center><a href="administrator:$1$AA0Dv...$gXPqGkI03Cu6dnclE/sok1
27 "></a> <a href=""><img src="" width=100></a> </center></font>
29 </td></tr></table>
30
31
```

Đăng nhập bằng username và password.

hackthissite.org/missions/realistic/7/images/admin/

Cookie Arena

Sign in

https://www.hackthissite.org

Username	<input type="text" value="administrator_"/>
Password	<input type="password" value="....."/>

[Cancel](#) [Sign In](#)

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.

The screenshot shows a browser window with the URL andys-net.co.uk/xecryption.html. The page title is "The Code". The main content area contains a large block of encrypted text, which is the captured email message from the ToxiCo Watch. Below the text, there is a "Password Value:" input field containing "762", and three buttons: "Increase", "Decrease", and "Find the Answer".

Password Value: 762

Decrypted Text

Samuel Smith

Thank you for looking the other way on the increased levels of toxic chemicals in the river running alongside our industrial facilities. You can pick up your payment of \$20,000 in the mailbox at the mansion on the corner of 53 and St. Charles tomorrow between the hours of 3:00am and 5:00am.

Thank you,

John Sculley
ToxiCo Industrial Chemicals

Copy plain text và gửi cho ToxiCo_Watch.

Send a Message

Send a message to: **ToxiCo_Watch**

Priority: **High Priority**

Subject: **XECryption**

Message:

```
increased levels of toxic chemicals in the river  
running alongside our industrial facilities. You  
can pick up your payment of $20,000 in the mailbox  
at the mansion on the corner of 53 and St. Charles  
tomorrow between the hours of 3:00am and 5:00am.  
  
Thank you,  
  
John Sculley  
ToxiCo Industrial Chemicals
```

Send

c. Kết quả

The screenshot shows a completed challenge on the HackThisSite.org platform. The URL in the address bar is `hackthissite.org/pages/messages/msys/send.php`. The page title is "Hack This Site". The main content area displays a message from "John Sculley" to "ToxiCo_Watch" containing a threat about toxic chemicals and a payment of \$20,000. Below the message is a "Send" button. The footer of the site includes links for "Cookie Arena", "Hack This Site", "Hack This Site (TOR .onion HTTPS - HTTP)", "IRC", "Discord", "Forums", "Store", "URL Shortener", "CryptoPaste", "Like Us", "Follow Us", and "Fork Us". A large watermark for "HACK THIS SITE.ORG" is visible across the center. A blue banner at the bottom encourages "Support HackThisSite" and "ADVERTISE WITH US". The status bar at the bottom right says "Congratulations, you have successfully completed realistic 6!".

d. Kỹ thuật sử dụng

- XECryption decode.

Hard: United Banks Of America

a. Mục tiêu

From: DarkOneWithANeed

Message: Hey man, you gotta help me out, Gary Hunter, one of the richest men in America, has just deposited \$10,000,000 into his bank account at the United Banks Of America and plans to donate that money to a campaign to hunt down and lock up all hackers. Now I've tried hacking [their site](#) but I'm just not good enough. That's why I need your help, Here's a list of your objectives:

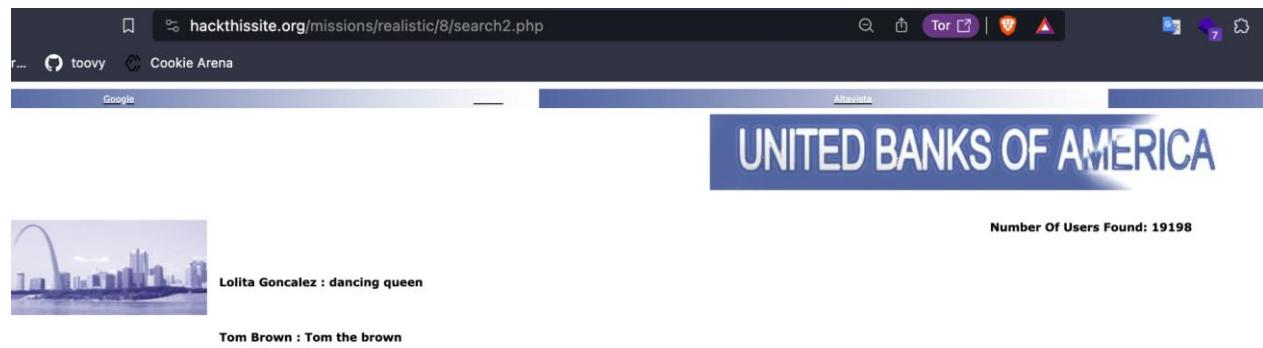
1. Find the account of Gary Hunter (I don't know his account name).
2. Move the \$10,000,000 into the account dropCash.
3. Clear The Logs, They're held in the folder 'logFiles'.

I really hope you can do this, because if you can't we're all screwed

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:



Karen Oldfield :

GaryWilliamHunter : -- \$\$\$\$\$ --

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

UNITED BANKS OF AMERICA



Welcome tovyy To Your Account

Amount Of Money In Account: \$0

Your Current Description:

PIN Number: Hidden

Password:

143056a5cbb8587dd4796aa573940a79

Options:

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

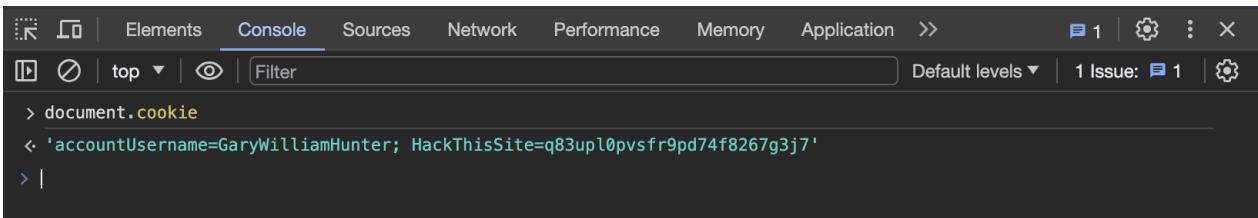
COOKIE MANAGER v2.1 BETA

The screenshot shows a cookie manager interface with a sidebar and a main panel. The sidebar lists cookies for 'www.hackthissite.org': 'HackThisSite', 'accountPassword', and 'accountUsername'. The 'accountUsername' cookie is selected and highlighted with a yellow background. The main panel displays the following details for the selected cookie:

Domain:	www.hackthissite.org
Path:	/missions/realistic/8
Name:	accountUsername
Store ID:	0
Value:	tovy
Expires:	24/10/2023 21:14
Same Site:	Set to none, lax, strict or leave empty
<input checked="" type="checkbox"/> Session	
<input checked="" type="checkbox"/> Host-Only	
<input type="checkbox"/> Http-Only	
<input type="checkbox"/> Secure	

Set / Create New

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.



```
> document.cookie
<- 'accountUsername=GaryWilliamHunter; HackThisSite=q83upl0pvsfr9pd74f8267g3j7'
```

Sau chuyển 10000000 cho dropCash.



Welcome tovy To Your Account

Amount Of Money In Account: \$0

Your Current Description:

PIN Number: Hidden

Password:
143056a5cbb8587dd4796aa573940a79

Options:

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.

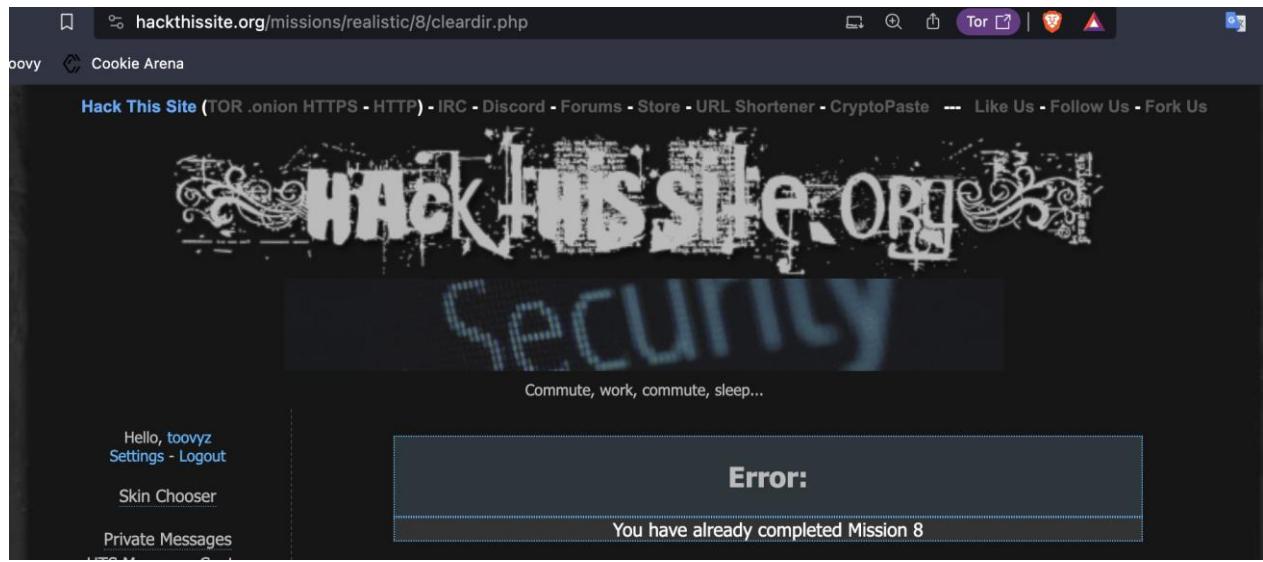
```
▼<form action="cleardir.php" method="POST">
  <input type="hidden" name="dir" value="tovySQLFiles"> == $0
  <input type="submit" value="Clear Files In Personal Folder">
</form>
```

Sau đó click chọn ô Clear Files In Personal Folder.

143056a5cbb8587dd4796aa573940a79

Options:

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.