

## Forum:[Hack Forums](#)

Thread: [\[CHALLENGE\] Cryptography+Website takeover \[easy/medium\]](#)

**Viktory** - April 11, 2015, 5:10 am

I haven't seen many challenges like this before, so I decided I'll make one! This is also my first challenge. If yall like it I'll make more in the future!

This challenge doesn't require of you to be an 3li1e h@ck3r. All you need is basic website security knowledge, and your brain.

Just remember to check Case-Sensitive in your notepad or use a piece of paper. ;)

The objective

- Decipher the image
- Get website
- Shell website
- Edit your name into a certain "solvers.html" page.
- PM me when all is done

It's not that simple though! But you will understand when you get there ;)

ReadMe

- No tools will help you here!
- Hints are everywhere, it's up to you to use them :D
- Feel free to PM me if you're stuck somewhere, you will not directly receive the solution though.
- Feel free to collaborate with other members and share your findings with one another in this thread. Please do not give others the solution directly though, let them attempt it too.
- There are 4 checkpoints, last one being the end of the challenge.
- Please DO NOT HARM THE WEBSITES!
- Finally, if you chose to share your findings with other members, enclose them in spoiler tags.

Right, with that out of the way, let's fall into the rabbit hole!

Solvers!

- Cross Marian
- The Cybercriminal
- The Judge
- Twerl
- Your name here!

The challenge will end in a week from now (18th of April, 12pm IST) or whenever I feel like waking up around that time. I'll post the solution in last page as I won't be able to edit op anymore at that time.

**Cross Marian** - April 11, 2015, 6:24 am

I solved it :) Thanks for challenge , i don't have enough posts so i can't pm you :(

**Viktory** - April 11, 2015, 6:44 am

(Apr 11, 2015 06:24 AM)Cross Marian Wrote: [\[CITE\]](#) I solved it :) Thanks for challenge , i don't have

enough posts so i can't pm you :(  
Great job! Nice to see new people around here who aren't idiots :D

**The Cybercriminal** - April 11, 2015, 6:47 am

I solved it, added my name to the list and showed you on Skype! :)

**Pseudonymous** - April 11, 2015, 7:13 am

Stuck on the cryptography lol. Any more hints?

**Cross Marian** - April 11, 2015, 7:46 am

(Apr 11, 2015 07:13 AM)Pseudonymous Wrote: [\[CITE\]](#) Stuck on the cryptography lol. Any more hints?

Spoiler [\(Click to View\)](#)

Stuck on the cryptography lol. Any more hints?

-Pseudonymous

**The Judge** - April 11, 2015, 9:01 am

Solved it thanks 4 the shits and giggles

**Twerl** - April 11, 2015, 10:38 am

Solved it, that was fun.

Thanks and stuff! <3

**Viktory** - April 11, 2015, 11:55 pm

(Apr 11, 2015 07:13 AM)Pseudonymous Wrote: [\[CITE\]](#) Stuck on the cryptography lol. Any more hints? Spoiler [\(Click to View\)](#) Think.

Each letter is "Pseudonymous" too :p

We know that there is a URL in the image. What does a URL begin with? Substitute those in.

(Apr 11, 2015 09:01 AM)The Judge Wrote: [\[CITE\]](#) Solved it thanks 4 the shits and giggles (Apr 11, 2015 10:38 AM)Twerl Wrote: [\[CITE\]](#) Solved it, that was fun.

Thanks and stuff! <3

Good job to both of you!

**Pseudonymous** - April 12, 2015, 6:27 am

(Apr 11, 2015 11:55 PM)Viktory Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#) Think.

Each letter is "Pseudonymous" too :p

We know that there is a URL in the image. What does a URL begin with? Substitute those in.

Good job to both of you! Yes I got some of the letters man ?

**Viktory** - April 12, 2015, 6:34 am

(Apr 12, 2015 06:27 AM)Pseudonymous Wrote: [\[CITE\]](#) Yes I got some of the letters Please remove the hint from your post or put it in spoilers!

Clear your PM box too.

EDIT: I cannot edit OP anymore as I'm an unupgraded plebeian. I'll put your name in new posts and release the solvers.html when the challenge ends though <3

**z8sr2dx024** - April 13, 2015, 5:09 pm

ah. cool another puzzle. keep doing them!!!

Viktory - April 14, 2015, 7:21 am

==CHALLENGE ENDED==

As of Apr 14, the webadmin of Site 1 removed all backdoors and somewhat fixed their security (can't write to other dirs anymore, but the sqli vuln is still there and we still have file\_priv lol) so I'll have to close the challenge.

I will post the solution for you guys who have been unable to complete the challenge though.

Step 1: Decipher the Image.

Tried to make this one easy for you guys. It is based on the same principle as Caesar shift, but the actual substitutions are random.

All you had to do here was look at the image, find words that you are certain are correct (for example, UWWY is HTTP), then replace all Us, Ws and Ys with their respective substitutes, and so on.

Doing that, we get the following message

"HTTP://TINYURL.COM

GOOD LUCK AND HAVE FUN

/SHELLMEE

-VIKTORY".

Step 2: Acquire website url, shell website (CHECKPOINT 1)

I slipped up on this originally. I meant to close all admin and login areas, but forgot to close the /login dir so one or two people were able to shell through there (thanks rmsg0d!).

My original plan here was to have you guys get your shell uploaded using INTO OUTFILE query to get a makeshift uploader written to the website. FPDs, and file privs were also conveniently provided at the point of injection.

I had replaced /admin and /login directories with the message "Not that easy! Perhaps you can use an 0x55504c4f41444552?"

That may have given you guys a clue saying you had to inject a PHP uploader script into the SQL query, like Code select 1,0xUPLOADHEX,3 INTO OUTFILE "FPD/UPLOADER.PHP"--

Now just open up that and get your shell up.

Step 3: Put your name into the /solvers.html file! Or should we? (CHECKPOINT 2)

Once you opened up that file, you would be greeted with another crypto message. It said:

"Thank you Mario! But our challenge ends in another website.

Perhaps it ends in /FEJY/FFF/TACEAH-CAXZ?

<!--CHALLENGE DOES NOT END YET DONT PUT UR NAME HERE SILLY-->"

Deciphering that message using the same scheme as above, we get

"/wamp/www/zilair-live"

Step 4: Almost there! (Checkpoint 3)

Googling "Zilair" gives us the website on the first link. Opening it up gives us the checkpoint in an alert box.

Now, putting the above deciphered text into the webshell's navigator puts us in the directory for Zilair's website, with all privileges.

Step 5: Aaand we're done! (Checkpoint 4, finish)

Navigating to <http://zilair.com/solvers.html> we get greeted by a Congratulations message.

All you have to do now is put your name on there through the shell and feel good about yourself =]

Thanks for playing! I'll make more in the future.

chris\_serge - April 15, 2015, 9:22 pm

(Apr 14, 2015 07:21 AM)Viktory Wrote: [\[CITE\]](#) ==CHALLENGE ENDED==

As of Apr 14, the webadmin of Site 1 removed all backdoors and somewhat fixed their security (can't write to other dirs anymore, but the sqli vuln is still there and we still have file\_priv lol) so I'll have to close the challenge.

I will post the solution for you guys who have been unable to complete the challenge though.

Step 1: Decipher the Image.

Tried to make this one easy for you guys. It is based on the same principle as Caesar shift, but the actual substitutions are random.

All you had to do here was look at the image, find words that you are certain are correct (for example, UWWY is HTTP), then replace all Us, Ws and Ys with their respective substitutes, and so on.

Doing that, we get the following message

"HTTP://spam.COM

GOOD LUCK AND HAVE FUN

/SHELLMEE

-VIKTORY".

Step 2: Acquire website url, shell website (CHECKPOINT 1)

I slipped up on this originally. I meant to close all admin and login areas, but forgot to close the /login dir so one or two people were able to shell through there (thanks rmsg0d!).

My original plan here was to have you guys get your shell uploaded using INTO OUTFILE query to get a makeshift uploader written to the website. FPDs, and file privs were also conveniently provided at the point of injection.

I had replaced /admin and /login directories with the message "Not that easy! Perhaps you can use an 0x55504c4f41444552?"

That may have given you guys a clue saying you had to inject a PHP uploader script into the SQL query, like Code select 1,0xUPLOADHEX,3 INTO OUTFILE "FPD/UPLOADER.PHP"--

Now just open up that and get your shell up.

Step 3: Put your name into the /solvers.html file! Or should we? (CHECKPOINT 2)

Once you opened up that file, you would be greeted with another crypto message. It said:

"Thank you Mario! But our challenge ends in another website.

Perhaps it ends in /FEJY/FFF/TACEAH-CAXZ?

<!--CHALLENGE DOES NOT END YET DONT PUT UR NAME HERE SILLY-->"

Deciphering that message using the same scheme as above, we get

"/wamp/www/zilair-live"

Step 4: Almost there! (Checkpoint 3)

Googling "Zilair" gives us the website on the first link. Opening it up gives us the checkpoint in an alert box.

Now, putting the above deciphered text into the webshell's navigator puts us in the directory for Zilair's website, with all privileges.

Step 5: Aaand we're done! (Checkpoint 4, finish)

Navigating to <http://zilair.com/solvers.html> we get greeted by a Congratulations message.

All you have to do now is put your name on there through the shell and feel good about yourself =]

Thanks for playing! I'll make more in the future.

Thanks for share the solution, i was lost, i have to work with more imagination.