

Forum:[Hack Forums](#)

Thread: [Hacking/cracking websites.](#)

BluexXxKalishnikov - June 15, 2010, 1:12 am

Website hacking;

A lot of people have been asking here about how to hack websites and such, so I figured I'd make a short(hopefully short enough to not bore you all) thread explaining a few methods. First of all understand there won't be a magic program that'll 'hack' these websites for you. There are some SQLi programs that'll do most of the work for you, but you won't learn a thing, so just take the time to learn it on your own and actually benefit from the knowledge. I won't be explaining HOW everything is done but rather what CAN be done, and will link you to helpful tutorials/places to look at the end of this post.

SQL injection:

Wikipedia Wrote:SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

SQL injection, SQLi, or Structured Query Language injection is when you're exploiting a vulnerability in the SQL coding of a website, basically. Preventing this from happening to you is simple, stay up to date with arising vulnerabilities, take time to ensure everything is written properly, just use common sense and be careful, best advice someone can give you.

'Types' of SQLi:

There are really two main types of SQLi; targeting a site, and blind SQL injection. Targeting a site would be someone knows a site they want hacked, and searches for a vulnerability to exploit. When targeting a site the attacker may wait long periods of time, through site upgrades, for a vulnerability to open up. The more popular of the two, blind SQLi, is when someone usually Googles 'dorks'. Dorks are what you see at the end of a URL. Searching for dorks, someone clicks and checks each one to see if they are or are not vulnerable/exploitable.

XSS:

Wikipedia Wrote:Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007.[1] Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site's owner.

There's the basics of XSS, cross-site scripting. As I've never experimented a lot with it, I can't tell you much, but it seems less effective than SQLi in ways. The basic idea I've got of it is you're generally just stealing cookies.

Non-persistent

Without going too far into it, non-persistent XSS is when you use malicious code to steal the session cookie of a user.

Persistent

Persistent cross-site scripting, however, is executed through malicious code that is saved onto the sites server. Being saved on the server and showing up actually on the website, it's being exposed to more users, and can leave the owner/admin of said website open to the exploit as well.

Remote File Inclusion:

Wikipedia Wrote:Remote File Inclusion (RFI) is a type of vulnerability most often found on websites, it allows an attacker to include a remote file usually through a script on the web server. The vulnerability occurs due to the use of user supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

- Code execution on the web server

- Code execution on the client-side such as Javascript which can lead to other attacks such as cross site scripting (XSS).

- Denial of Service (DoS)

- Data Theft/ManipulationI'm not going to lie, I don't understand this very much. I'm working on learning this so when I can afford ub3r I will edit this to include a more in-depth description of RFI attacks.

End to this thread;

I'm hoping this thread is well appreciated by you all and it's helped you in some way. I would've gone further into this but there's too much to be said about each technique, while tutorials on each can be found, this is just to let you know what some methods are.

Helpful links:

Tutorials

[Detailed Basic and Full SQL Injection Tutorial](#) by [dan1el](#).

[\[TUT\] SQL Injection Tutorial for Beginners](#) by [Known as KraZi](#).

[\[Tutorial\] Stealing Cookies With XSS](#) by [Skittles-](#).

[XSS Tutorial - Cross Scripting Attacks](#) by [FeAR Being](#).

[Simple RFI Tutorial](#) by [MajorDeath](#).

Wikipedia links

[SQL Injection Wiki](#).

[XSS Wiki](#).

[RFI Wiki](#).

Thank you for reading,

Thank you for reading this thread, and hopefully showing appreciation. IF this has helped you in any way, please post in this thread to help me keep this alive. It's in the beginner hacking section because this is where most questions are asked before the person is asked/told to go to the website/forum hacking section, [here](#).

-BluexXxKalishnikov

m0n - June 15, 2010, 1:14 am

Looks real nice. :)

Very informative, great guide for newbies!

Maybe change the subheading colours to a lighter colour?

Reading it like that is kinda hard, sorry if it kinda conflicts with your name :D

BluexXxKalishnikov - June 15, 2010, 1:16 am

(Jun 15, 2010 01:14 AM)m0n Wrote: [\[CITE\]](#) Looks real nice. :)

Very informative, great guide for newbies!

Maybe change the subheading colours to a lighter colour?

Reading it like that is kinda hard, sorry if it kinda conflicts with your name :D

Ah, yeah, I was going to go with a lighter blue but I thought this would turn out light enough. I'll be changing it shortly, any suggestions for a different color? :)

m0n - June 15, 2010, 1:16 am

(Jun 15, 2010 01:16 AM)BluexXxKalishnikov Wrote: [\[CITE\]](#) Ah, yeah, I was going to go with a lighter blue but I thought this would turn out light enough. I'll be changing it shortly, any suggestions for a different color? :)

Perhaps a lighter blue/yellow/green?

Whichever you think looks best. :)

BluexXxKalishnikov - June 15, 2010, 3:31 am

Made it light blue. Am I missing anything important I should add to this before the thread can't be edited?

xcode5 - June 15, 2010, 4:20 am

Thanks this is really usefull for noobs.

BluexXxKalishnikov - June 15, 2010, 5:20 pm

(Jun 15, 2010 04:20 AM)xcode5 Wrote: [\[CITE\]](#) Thanks this is really usefull for noobs.

Thanks, I hope it helps everyone out at least a little. :)

JPistofast - June 15, 2010, 7:17 pm

Bumped because I liked your thread, and this will help out some users who are confused.

R8Z - June 15, 2010, 9:16 pm

second bump here. Your thread help alot users. Very useful!!

BluexXxKalishnikov - June 16, 2010, 3:25 am

(Jun 15, 2010 07:17 PM)jpistofast Wrote: [\[CITE\]](#) Bumped because I liked your thread, and this will help out some users who are confused.

I'm glad you like it :) Pass it around when people ask about this sort of thing, if possible.

(Jun 15, 2010 09:16 PM)634848 Wrote: [\[CITE\]](#) second bump here. Your thread help alot users. Very useful!!

I hope it helped ya out some bro! :D

Abseven - June 17, 2010, 5:19 am

I really liked this thread as a newbie, I think its put me on the right track.

BluexXxKalishnikov - June 20, 2010, 5:14 am

Sorry for taking so long to reply, but thanks for using your first post in my thread! :)

BluexXxKalishnikov - July 3, 2010, 4:51 pm

People are asking questions about website hacking, so I'm bumping this up rather than linking to it :)

FuKing - July 3, 2010, 5:38 pm

Do you know anyone who is pro at RFI? I need to know if it works on big servers or if you have to link it to XSS and do the cookie business. SQL injecting is just so easy and gives you so much information.... UGH torn between what to try.

Humanoid - July 3, 2010, 5:40 pm

Really good thread, it will help many people out...

BluexXxKalishnikov - August 12, 2010, 10:35 am

(Jul 3, 2010 05:38 PM)FuKing Wrote: [\[CITE\]](#) Do you know anyone who is pro at RFI? I need to know if it works on big servers or if you have to link it to XSS and do the cookie business. SQL injecting is just so easy and gives you so much information.... UGH torn between what to try.

Lol aren't you the one who wanted to hack Brazzers? How'd that work out for ya?

(Jul 3, 2010 05:40 PM)Humanoid Wrote: [\[CITE\]](#) Really good thread, it will help many people out... Thanks, I hope it does. :)

balkis0n - January 28, 2011, 4:33 pm

Nice Tutorial , good job!

BluexXxKalishnikov - March 9, 2011, 4:02 am

(Jan 28, 2011 05:33 PM)balkis0n Wrote: [\[CITE\]](#) Nice Tutorial , good job!

Thank you! ? I haven't been checkin my threads often so sorry for the late reply, but I always love seeing posts like this on one of them.