

Forum:[Hack Forums](#)

Thread: [\[XSS\] Google Vuln - Curious fact READ \[XSS\]](#)

Pr3nK - March 9, 2012, 4:27 pm

Hi guys, i think i've found a XSS vulnerability on Google.com, but strangely the popup appear without writing any XSS vector, but simply searching a particular word. I wanna know if i can see how the vector automatically start and make the popup appears.

Can we call it XSS vuln? Should I report the problem to Google?

Judge for yourself

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

1337B345T3R - March 9, 2012, 4:28 pm

Yeah you should. People who have reported XSS's to google have gotten paid in excess of \$500! Do it bro. Oh and give me 75% of the money lol.

Pr3nK - March 9, 2012, 4:29 pm

(Mar 9, 2012 05:28 PM)1337B345T3R Wrote: [\[CITE\]](#) Yeah you should. People who have reported XSS's to google have gotten paid in excess of \$500! Do it bro. Oh and give me 75% of the money lol.

How I said in my previous post, it doesn't appear with any XSS vector ?

FastFive - March 9, 2012, 4:32 pm

the only way this happened IMO is that an advertisement, or search result contained an xss vector. can you please view the source, find the code which triggered this event by search for "alert(/1/)" and post the surrounding area of code so we can tell what the hell happened? this sounds interesting

Pr3nK - March 9, 2012, 4:35 pm

(Mar 9, 2012 05:32 PM)FastFive Wrote: [\[CITE\]](#) the only way this happened IMO is that an advertisement, or search result contained an xss vector. can you please view the source, find the code which triggered this event by search for "alert(/1/)" and post the surrounding area of code so we can tell what the hell happened? this sounds interesting

In the source code there isn't any trace of any kind of vector. This is very strange....

FastFive - March 9, 2012, 4:44 pm

the only thing i can think of that could explain this is that one of the page previews/iframes that google has for every site contained code in it, and it was triggered
or you missed something in the source code... i would double check if i were you...

010100111001 - March 9, 2012, 4:46 pm

If you send me the link I will look into what is causing this for you and get back to you.

Testing 123 Testing 123 Testing 123 Testing 123

Pr3nK - March 9, 2012, 4:49 pm

(Mar 9, 2012 05:44 PM)FastFive Wrote: [\[CITE\]](#) the only thing i can think of that could explain this is that one of the page previews/iframes that google has for every site contained code in it, and it was

triggered

or you missed something in the source code... i would double check if i were you...Among the results of my search there are some vectors, but if i input one of them the popup doesn't appear. So I'm undecided whether or not to report it...

(Mar 9, 2012 05:46 PM)010100111001 Wrote: [\[CITE\]](#) If you send me the link I will look into what is causing this for you and get back to you. Sorry mate, but i prefer not to send you the syntax because it maybe is an important vuln. If you can give me some advice you're welcome

FastFive - March 9, 2012, 5:28 pm

look man idk, if you trust me send me the link and ill look at it. your right, it could be something big, it looks like persistant xss originated from another site, however if this is being caused by an outside source as i suspect you are not the creator or finder of this, and chances are a large amount of people know of it already

email the page to security@google.com, then post the link here. they only reward the fist sender.

Pr3nK - March 10, 2012, 2:10 am

I sent the email to GoogleSec about a hour ago. I heard they don't answer on the weekend, means that wait

RebornX - March 10, 2012, 3:15 am

They will respond , make sure you used correct format.

cheatson - March 10, 2012, 3:21 am

Cool, very odd indeed. Let's hope the bug is exploitable- a popup alone isn't a security risk but it's a shame you couldn't find the source of the problem to show that it is exploitable, I am sure they would fix it in any case as they would with any annoying bug like that, but not so sure they would investigate it to the point to prove its exploitable for your benefit. Figners crossed for you. And don't worry about the 'format' of your emal, it doesn't actually matter.

MaXoNe - March 10, 2012, 3:26 am

Use burp suite and try to intercept you request and if it is inside get request try to change it . If it works you'll be \$500 dollars richer :)

?Razor - March 10, 2012, 3:34 am

Dont share this to anyone,
Otherwise they will report it and they will get paid.

Nice found man keep going!

Sanch0 - March 10, 2012, 4:34 am

congrats man, as umut said, dont give it out otherwise ppl will steal it. :s

Pr3nK - March 12, 2012, 2:56 am

Today the Google Security Team answers me, this is the email:

Spoiler ([Click to View](#))

[img]http://img141.imageshack.us/img141/4850/schermata20120312a10501.jpg[/img]

No money and no HoF? XD

HaxOr? - March 12, 2012, 2:59 am

They are looking into it.

Calm down.

Pr3nK - March 13, 2012, 6:13 pm

Finally they answer me: I win a reward of \$500 :D Thanks to the community
[img]http://img14.imageshack.us/img14/2231/googlehy.jpg[/img]

zer0pwn - March 13, 2012, 6:27 pm

Well, there is one page that detects "alert". It's the page where you report a vulnerability.

EDIT:

Didn't see any of the comments, nice work man :D

Pr3nK - March 13, 2012, 6:39 pm

(Mar 13, 2012 06:27 PM)Zer0Pwn Wrote: [\[CITE\]](#) Well, there is one page that detects "alert". It's the page where you report a vulnerability.

EDIT:

Didn't see any of the comments, nice work man :DThank you mate, i really appreciate a comment from a great HF member like you ?

xx 0x0 xx - March 13, 2012, 7:01 pm

nice work dude :) keep going i hope i find one someday XD

Pr3nK - March 13, 2012, 7:05 pm

(Mar 13, 2012 07:01 PM)mats0o0o0 Wrote: [\[CITE\]](#) nice work dude :) keep going i hope i find one someday XD

Thanks dude, we have to keep on studying and working harder ?

games-lol-owned - March 13, 2012, 7:09 pm

lol so when they fix this i defo wanna know what you searched lmfao

Kirk_sv - March 13, 2012, 10:10 pm

Nice work man, I have reported two similar and just put me in the honorable mention xD

What extension of firefox is that it says: sql, xss... etc?

jnat0r - March 14, 2012, 1:10 am

(Mar 13, 2012 10:10 PM)Kirk_sv Wrote: [\[CITE\]](#) What extension of firefox is that it says: sql, xss... etc?

I don't know exactly what that program is but acunetix is good one too. ?

Pr3nK - March 14, 2012, 2:37 am

(Mar 13, 2012 10:10 PM)Kirk_sv Wrote: [\[CITE\]](#) Nice work man, I have reported two similar and just put me in the honorable mention xD

What extension of firefox is that it says: sql, xss... etc?

It's HackBar, very handy and useful ?

worldwideweb - March 14, 2012, 2:54 am

Nice found Pr3nK,

Congratzz ?

VirusTotal - March 14, 2012, 4:14 am

Congratz for the reward ;)
Enjoy your \$ 500

Jesse Pinkman™ - March 14, 2012, 5:22 am

Nice work dude and big congrats on the \$500! You've definitely earned it.

Keep up the good work!

??¢??? - March 14, 2012, 7:20 am

If you want any help with it , feel free to Pm me :) . If you deserve award from google i'll help you get one .

In Gold We Trust - March 14, 2012, 10:04 am

Wow i am jelly :)
Have fun with your \$500!

Pr3nK - March 14, 2012, 10:37 am

(Mar 14, 2012 05:22 AM)Demon 2 Wrote: [\[CITE\]](#) Nice work dude and big congrats on the \$500!
You've definitely earned it.

Keep up the good work!

(Mar 14, 2012 10:04 AM)iJoris Wrote: [\[CITE\]](#) Wow i am jelly :)
Have fun with your \$500!
Thank you guys! Really appreciate it ?

(Mar 14, 2012 07:20 AM)??¢??? Wrote: [\[CITE\]](#) If you want any help with it , feel free to Pm me :) . If you deserve award from google i'll help you get one .They answered me yesterday, and they judged the vulnerability is eligible to 500\$. Thank you anyway

powerbk2 - March 14, 2012, 11:20 am

THIS IS MEH FRIEND IN MEH TEAM :D good find mate ;)

Xr1ghtXss - March 14, 2012, 12:00 pm

This is an awesome find man! Good job!
~ Team Ultimatum!

b0lt - March 14, 2012, 1:18 pm

Good job! Keep up the good work! :)

FastFive - March 14, 2012, 2:15 pm

so what caused it, did you ever find out?

NuffSaid - March 15, 2012, 5:25 am

Nice find , bruh. Congrats! Enjoy the \$\$\$ lol.

imAnoobLOL - May 14, 2012, 2:54 pm

\$500! Very nice bro, I hope I become like you one day.

krazy - October 21, 2013, 12:33 pm

Yea pr3nk that was really awesome! But you never mentioned what you searched that caused it? We sure wanna know..

kamasattu - October 22, 2013, 9:34 am

so wait for there reply try to work on that ... once you success... then inform them

?Alexander - October 22, 2013, 10:34 am

This thread is from 2012. Stop gravedigging this shit.

Sundae - October 22, 2013, 10:39 am

(Oct 22, 2013 10:34 AM)Jess Aarons Wrote: [\[CITE\]](#) This thread is from 2012. Stop gravedigging this shit.

Says stop gravedigging, posts on the thread anyway.

/logic

SIM-1241186 - October 22, 2013, 10:44 am

(Oct 22, 2013 10:39 AM)Sundae Wrote: [\[CITE\]](#) Says stop gravedigging, posts on the thread anyway.

/logic

Arrogant response implying posting on gravedug thread is illogical, posts on the thread commenting so.

/WhereAreYouGoingWithThis

/JoinTheParty

/WaitAreWeStartingANewTrendWithBackslashesOnForums

/Negative3sIncoming

/ThisIsFunny

-3?? - October 22, 2013, 10:46 am

(Oct 22, 2013 10:44 AM)hackforumspang Wrote: [\[CITE\]](#) Arrogant response implying posting on gravedug thread is illogical, posts on the thread commenting so.

/whereareyougoingwiththisDoing exactly the same as the first guy did

/Willthereeverbeanendofthis?

Dogelan - March 2, 2014, 3:54 am

Stop gravedigging you fucking retards.

/thread

/yolosawg

VipVince - March 2, 2014, 5:23 am

/partofthegang.

/actuallyclosednow.