

sla.ckers.org web application security forum :: Full Disclosure :: Widespread XSS for Google Search Appliance

sla.ckers.org web application security forum :: Full Disclosure :: Widespread XSS for Google Search Appliance - maluc, sla.ckers.org.

- Published: date not stated
- Original: <<http://sla.ckers.org/forum/read.php?3,3109,3124>>
- Preserved from: <http://sla.ckers.org/forum/read.php?3,3109,3124> (stored) on 2026-08-11
- Capture timestamp: 20070829072149
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

sla.ckers.org web application security forum :: Full Disclosure :: Widespread XSS for Google Search Appliance

[[image: image]](<http://www.webappsec.org/>) Paid Advertising

[SLA.CKERS.ORG HA.CKERS SLACKING](#) [[image: sla.ckers.org web application security lab forums]] (<http://sla.ckers.org/forum/>)

Where you should disclose your vulnerabilities. Go read [RFPolicy](#) if you want to do responsible disclosure, and go here for when all else fails.

Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 17, 2006 01:20PM

So i fell asleep last night and didn't finish the encoding script as i assumed i would. But finally finished (pain in the ass to write btw)

The topic is plenty descriptive - it's an XSS in most sites that uses the google search API with it's generic results template. The api allows any encoding method to be used for output, and doesn't sanitize until after the page has been converted. (Google.com uses the same API but it's unaffected because it santizes in UTF8 before converting to the output encoding)

GoogleDorks: [www.google.com] [www.google.com]

Did i confuse you yet? - Just add the parameter oe=UTF-7 to any site using google's search API and the query q=<script>alert("XSS")</script> converted to UTF-7 using [\[maluc.sitesled.com\]](http://maluc.sitesled.com) .. Which translates to:

```
+ADw-script+AD4-alert(+ACI-XSS+ACI-)+ADw-/script+AD4-
```

Don't forget that all + have to be %2B in GET strings

```
%2BADw-script%2BAD4-alert%281%29%2BADw-/script%2BAD4-
```

Examples: [\[ask.stanford.edu\]](http://ask.stanford.edu) [\[google2.fda.gov\]](http://google2.fda.gov) [\[search.unc.edu\]](http://search.unc.edu) [\[search.nhl.com\]](http://search.nhl.com) [\[search.mo.gov\]](http://search.mo.gov) [\[search.nces.ed.gov\]](http://search.nces.ed.gov) [\[externalsearch.nist.gov\]](http://externalsearch.nist.gov) [\[gb-server-1.mit.edu%2BADw-/SCRIPT%2BAD4-%2BADw-x\]](http://gb-server-1.mit.edu%2BADw-/SCRIPT%2BAD4-%2BADw-x)

You can also sometimes append any parameter like apple=">[Injection] to the search string: [\[externalsearch.nist.gov%2BADw-/SCRIPT%2BAD4-%2BADw-x\]](http://externalsearch.nist.gov%2BADw-/SCRIPT%2BAD4-%2BADw-x)

One problem though: any site with embedded script like for(i=0;i<10;i++) gets changed to for(i=0;i<10;i) .. which is an infinite loop. you'll have to overwrite that when exploiting..

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [WhiteAcid](#) (IP Logged)

Date: November 17, 2006 05:01PM

Awesome, simply awesome.

Quote:

One problem though: any site with embedded script like for(i=0;i<10;i++) gets changed to for(i=0;i<10;i) .. which is an infinite loop. you'll have to overwrite that when exploiting..

Why's that?

Don't forget our IRC: irc://irc.irchighway.net/#slackers -[WhiteAcid](#) - your friendly, very lazy, web developer

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 17, 2006 05:38PM

because of how UTF7 encoding works.. any special characters - i.e. not a-z A-Z 0-9 or ' () , - . / : ? .. get encoded. And the format has the start character of + and optional end character of -. like < to +ADw-

So ++ gets interpreted as an invalid encoding and erased. An annoying side-effect if that infinite for() loop comes before the injection and thus can't be overwritten fast enough :/ .. luckily, most seem to be afterwards so they can be fixed during exploit

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [br0ken](#) (IP Logged)

Date: November 17, 2006 07:09PM

Bows to maluc You my friend are one smart cookie ;) Me on the other hand ... not so much. My first try I added oe=UTF-7 as said ... but never noticed oe=UTF-8 in front :(*head down in shame *

It processes the first parameter you enter&oe=UTF-8&oe=UTF-7&... == the smrtest thing I have ever done !

So yeah great find ;) You have brought much humility to my simple life.

hehe ./br0ken

//edit BtW this infinite loop seems to freeze ie6 about 75% for me ?

Edited 2 time(s). Last edit at 11/17/2006 07:14PM by br0ken.

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 17, 2006 07:43PM

ya, it froze ie7 once or twice for me as well.. theres alot of ways to freeze a browser with javascript if you intentionally wanna - especially IE.

and while i always appreciate people paying homage to me ^^ .. don't be so hards on yourself. we all make those mistakes often particularly around 3-5am for me

i just tend to hide my retardedness in PMs, which RSnake can attest to -.-

and btw, it works on any site that ends up showing this in the source

```
<meta http-equiv="content-type" content="text/html; charset=UTF-7">
```

and none that don't (like most custom pages using the google api directly)

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [jungsonn](#) (IP Logged)

Date: November 18, 2006 05:41AM

Though, excellent find! wish i had more time on my hands to look at it more closely.

Re: Widespread XSS for Google Search Appliance

Posted by: [ChristPuncher](#) (IP Logged)

Date: November 20, 2006 10:44AM

Nevermind

Edited 1 time(s). Last edit at 12/12/2006 06:14AM by ChristPuncher.

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: November 20, 2006 11:49AM

Over the last few hours alone 11 Google employees have read the article, Maluc:

65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.0" 200 8080 "-" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.0" 200 8080 "-" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.0" 200 8080 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.0" 200 8080 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.8) Gecko/20061108 Fedora/1.5.0.8-1.fc5 Firefox/1.5.0.8" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.0.6) Gecko/20060728 Firefox/1.5.0.6" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "http://www.google.com/url?sa=D&q=http%3A%2F%2Fha.ckers.org%2Fblog%2F20061118%2Fwidespread-xss-for-google-search-appliance%2F" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1) Gecko/20061010 Firefox/2.0" 65.57.245.11 - - "GET /blog/20061118/widespread-xss-for-google-search-appliance/ HTTP/1.1" 200 8080 "-" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.13) Gecko/20060724 Firefox/1.0.8 (Ubuntu package 1.0.8)"

As id pointed out, "Google should really learn how to use caching proxies."

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [ChristPuncher](#) (IP Logged)

Date: November 20, 2006 01:24PM

Fixed.

Edited 1 time(s). Last edit at 12/12/2006 06:15AM by ChristPuncher.

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 20, 2006 02:41PM

wow, probably got put on some google memo.. i'm interested to see how quickly they can patch atleast the majority of their clients

that's good to know christpuncher.. never was a fan of sloppy seconds ^^ welcome to the forums - you may have permanently put yourself on an FBI watchlist though :x

sadly though, this one disclosed by unsticky has been live for almost 2 months: [\[www.fbi.gov\]](http://www.fbi.gov) (wait four seconds.)

-maluc

Edited 1 time(s). Last edit at 11/29/2006 05:50AM by maluc.

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: November 28, 2006 09:11AM

[\[www.nist.org\]](http://www.nist.org)

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: November 28, 2006 09:12AM

[\[news.zdnet.com\]](http://news.zdnet.com) We weren't mentioned in the article, however Google has issued a patch in their next version. Until everyone patches up, holes abound.

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: November 28, 2006 09:43AM

[\[news.com.com\]](http://news.com.com) Again, we weren't mentioned here. But I like the moral of the story. Google introduces holes into your machines (web accelerator toolbar spyware) and onto your network (search appliance).

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 28, 2006 03:10PM

lol, i like how nist links to a random mortgage agent [\[ha.ckers.com\]](http://ha.ckers.com)

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: **id** (IP Logged)

Date: November 28, 2006 04:35PM

Next time I'm in vegas I should call DARIN FERRARO, set up an appointment to see a home and politely ask for the ckers.com domain...

-id

Re: Widespread XSS for Google Search Appliance

Posted by: **maluc** (IP Logged)

Date: November 28, 2006 05:11PM

lol, you should.. would be a probably inexpensive way to get it it's not like "ckers" is related in any way to his business or name

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: **digi7al64** (IP Logged)

Date: November 28, 2006 05:43PM

I did pm some with this but they haven't replied and its been enough time. perhaps you might have better luck then i have it getting it to fire.

[www.google.com;+ADw-+AC8-SCRIPT+AD4]]

'Just because you got the bacon, lettuce, and tomato don't mean I'm gonna give you my toast.'

Re: Widespread XSS for Google Search Appliance

Posted by: **maluc** (IP Logged)

Date: November 28, 2006 07:53PM

as i said in the first post.. google.com is not affected because they sanitize all input in UTF-8 (whereas their Search Appliance product sanitizes it in the output encoding of choice)

so if your input encoding is set to UTF-8 (or anything that's not UTF-7), and your output to UTF-7 query= +ADw- : it sanitizes, but nothing is dangerous. then it converts the +ADw- to UTF-7, +-ADw- .. which is the correct way to encode a +

if you set the input to UTF-7 .. and output to UTF-7 query= +ADw- : it first converts the +ADw- to UTF-8, or < .. then it santizes that - changing it to %22. then it converts that back to UTF-7, +ACU-22 .. which is the correct way to encode %22

Since google always sanitizes in UTF-8 .. there's no way around it. If there was, i never would've disclosed it >:)

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: **digi7al64** (IP Logged)

Date: November 28, 2006 09:27PM

hmmm,

I follow with what you are saying, but somewhere something got changed.

When i compare the results from last week to this week using the same links i can confidently say that they have changed the parser function within the last week. This i know because i could break of out the search input field and today i can't. The problem i originally had was that i couldn't figure out the correct way to submit the search value and get it to xss.

Furthermore today's results compared against last week show that they have removed the + signs altogether from the search field which was causing the breakout (when used with utf-7).

'Just because you got the bacon, lettuce, and tomato don't mean I'm gonna give you my toast.'

Edited 1 time(s). Last edit at 11/28/2006 09:37PM by digi7al64.

Re: Widespread XSS for Google Search Appliance

Posted by: [jungsonn](#) (IP Logged)

Date: November 29, 2006 05:05AM

Maluc, is there a way to circumvent this in "normal" sites? i can image by just tamper the header to read UTF-7 instead of UTF-8. Or is this idea too wild? i'm not completely absored by your UTF-7 info, so any explanation is welcome.

Like: sending a form, and in the same time changing the UTF-8 > UTF-7 ?

Edited 2 time(s). Last edit at 11/29/2006 05:08AM by jungsonn.

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: November 29, 2006 07:09AM

Well each browser will have it's default encoding set in its Options. So if it's not explicitly said otherwise, it uses the default. I don't think you'll find many users with UTF-7 or US-ASCII as default. And i can only think of two ways to define it explicitly in an HTML page:

the Response header.. Content-Type: text/html; charset=utf-7

the meta tag.. <meta http-equiv="Content-Type" content="text/html; charset=utf-7">

the Search Appliance works because it sets the meta charset to whatever oe= in the GET. That's the main way i find it on random sites. Except more than 50% of the time, i find it as an Advanced Search feature that's there but never even used normally. So keep an eye on the View Source and GET string.

the second way that i'm not sure if it's possible.. is to use Flash to send a raw Request to the page and include the header Accept-Charset: UTF-7 it may not be as simple as that though, and may

require something more like Accept-Charset: UTF-7;q=0,ISO-8859-1 or UTF-8 if that's the website's default. q=0 means that charset is not allowed. Again, i haven't tried this out yet..

the quality value (q=0) is kinda confusing to explain so i'll point ya to the [RFC2616 section 14.2](#). And i can't really think of any other way right now. That might be because it's 9am and i haven't slept yet ^^;

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [jungsonn](#) (IP Logged)

Date: November 29, 2006 12:11PM

Thanx maluc, that's much info to read.

Re: Widespread XSS for Google Search Appliance

Posted by: [Ghozt](#) (IP Logged)

Date: December 01, 2006 04:13PM

[\[www.us-cert.gov\]](#) [\[digg.com\]](#)

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: December 03, 2006 07:48PM

Interesting... I guess CERT didn't feel like mentioning your name Maluc. Maybe you shouldn't find vulnerabilities in them anymore. ;) Some one is mad.

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [jungsonn](#) (IP Logged)

Date: December 04, 2006 12:19AM

they are "aware"

:)

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: December 04, 2006 11:36AM

lol.. well it seems like anything short of arbitrary code execution isn't enough to make it into CERT's database. And no pentesters were credited on that summary page - so i'm happy enough to see them mention it ^^

That said, i stumbled upon that announcement right after they made it.. and was the reason i stopped to test their site more thoroughly. but i promise i'm not bitter >.>

i was really hoping their search engine would be vulnerable to the same issue since it has a charset=blah .. but i came up empty when i tried it last week :/

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: December 05, 2006 05:29PM

John Herron sent this over: [www.kb.cert.org]

You finally got your credit, Maluc!

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [rsnake](#) (IP Logged)

Date: December 05, 2006 05:31PM

And here: [secunia.com]

- RSnake

Gotta love it. <http://ha.ckers.org>

Re: Widespread XSS for Google Search Appliance

Posted by: [maluc](#) (IP Logged)

Date: December 05, 2006 05:43PM

woot, my first entry into cert :3

how nice

-maluc

Re: Widespread XSS for Google Search Appliance

Posted by: [unsticky](#) (IP Logged)

Date: December 09, 2006 09:01AM

Edit: Nevermind, my idea didn't work as I thought it did.

Edited 1 time(s). Last edit at 12/09/2006 09:03AM by unsticky.

Sorry, only registered users may post in this forum.