About arbitrary HTML on Smash Boards

Cathy J. Fitzpatrick

December 18, 2010

Note: This paper is intended for non-technical readers who do not have a security, programming, or computer science background. As such, it describes the security issues on a very basic, expository/introductory level.

Abstract

Arbitrary HTML can be used to impersonate any user who views any post by a moderator. This includes making posts and sending PMs as the compromised user, as well as reading all of the user's PMs. It also includes deleting posts the user would not otherwise be able to moderate. Another attack would allow a moderator to gain many users' emails and passwords, which could be used to login at other sites, such as PayPal, with grave consequences to the affected users. Smash Boards has too many moderators to entrust them all with this power. Even a single disgruntled and technically inclined moderator could do extremely major and irreparable damage to the community. A technically naive moderator could easily be lulled to post something on behalf of an attacker, with the same results. The use of HTML in posts on Smash Boards should be disabled.

1 Introduction

It is common knowledge that moderators on Smash Boards are able to embed arbitrary HTML in their posts. The security implications of this have been known to me since I started using Smash Boards in 2008. I am not sure whether these implications are common knowledge, but if so, evidently they are not considered important, since moderators are still allowed to use arbitrary HTML as of the time of writing.

On December 18th, 2010, I visited the Smash Boards forum index for the first time in several months. The newest thread in the User Blogs forum[1] was by SuSa, a well known user and moderator. The title of the thread was something

[1] See `http://www.smashboards.com/forumdisplay.php?f=198`.

along the lines of a "A guide on how to get HELLBANNED"[2]. Out of curiosity, I viewed this thread, and was shocked and disturbed by the highly offensive images it contained. The thread has since been deleted and SuSa demodded.

I have no idea of the circumstances behind his posting that thread, but it's apparent he was disgruntled and considered himself done with Smash Boards. Thus, he was fully prepared to do something egregious to do whatever damage he could to the community on his way out. However, the brief shock[3] he no doubt inflicted upon a relatively small collection users, including myself, is nothing compared to what he could have done if he were more clever. Indeed, his attack was cleaned up by other moderators quite quickly. His attack was also easily detectable: simply by viewing the thread, it was obvious he was up to no good, and thus he limited the exposure of the material. As a result, SuSa did not manage to inflict significant damage to the site or community.

However, if SuSa had made use of his ability to post arbitrary HTML on account of being a moderator, he would have been able to inflict a far more damaging attack, which would have resisted detection for likely a significant amount of time, and generally caused a large amount of hardship to innocent Smash Boards users.

In this document, I will explore several possible attacks that could be deployed by embedding arbitrary HTML in a moderator's post. I will also explore the reasons why these attacks should be taken seriously, even though Smash Boards has never had a problem with one of them in the past (as far as I know). Finally, I will offer some recommendations both to users of Smash Boards and the administration.

2 Using arbitrary HTML to take over users' accounts temporarily

The most obvious attack possible with arbitrary HTML is also one of the most dangerous. If it is possible for an attacker to make arbitrary HTTP requests as somebody, the attacker can do anything with the victim's browser that the victim can, including making posts or private messages as the victim, using the victim's forum permissions (such as moderator abilities beyond the attacker's), viewing the victim's private messages, and more.

Normally, it is safe to visit arbitrary web pages without worrying about the web page taking over your browser and making arbitrary HTTP requests. The main security mechanism that prevents this is known as the same origin policy[4]. Bowsers that implement this policy, which includes all popular browsers, prevent a web page from making an HTTP request to a server other than the server that the web page is running on. This prevents web pages from carrying out actions as you without your permission.

[2]The thread has since been deleted and I did not save the title.

[3]Although I personally closed the thread quickly, we can imagine that some users may have long-lasting discomfort as a result of viewing this thread.

[4]See `http://en.wikipedia.org/wiki/Same_origin_policy`.

However, a moderator on Smash Boards can embed in her post a JavaScript script which will make use of the XMLHttpRequest object[5] to make client-side HTTP requests on the victim's (anybody who views the post containing the script) computer. Since these requests originate from Smash Boards, they can make arbitrary requests to Smash Boards, as the victim.

Simply viewing a malicious post by a moderator allows the moderator to make any post as you. This imposter post will be indistinguishable from a real post by you. For example, it will appear to be posted from your IP address, not the moderator's. The moderator could also send a PM as you, and then delete your copy of the PM from your sent box, so you aren't even aware it was sent. Perhaps worse still, a moderator can retrieve all of your PMs, and then send the results back to herself as a PM from you, and then delete your copy of that PM. The moderator can also read information in your User CP, such as your email address, which is useful in conjunction with the attack descriped in the next section.

This attack cannot be used to gain access to the modcp or admincp, because those portions of the forums require re-entering your password, which this attack does not normally allow the attacker to obtain. This attack also cannot be used to permanently hijack a victim's account, because changing a user's password or email requires entering the user's old password.

This is still an extremely powerful attack. It allows moderators to do dangerous things that they could not normally do, and any use of the attack would go undetected for some time.

The only thing users of Smash Boards can do to avoid this attack is to disable JavaScript in their browsers, which also cripples many other features of the forum software, making it an unattractive option.

3 Using arbitrary HTML to obtain users' passwords

A different attack can be used to trick many users into divulging their passwords. Unlike the previous attack, which essentially always works, this attack has a social element to it and will not work against every user. However, it is likely to work against many users. Indeed, this attack has been used many times successfully in the past against large web sites with arbitrary HTML vulnerabilities[6].

In this attack, a moderator embeds a JavaScript script in his post that uses the DOM methods to replace the entire content of the page by a fake login page. The fake login page will look 100% identical to a real Smash Boards login page. The only difference will be the URL displayed in the address bar. Users are used to having to re-enter their password from time to time for various reasons and

[5] See `http://www.w3.org/TR/XMLHttpRequest/`.

[6] For example, in 2006, attackers used this attack against MySpace to collect the user names and passwords of at least 34,000 users. See `http://www.schneier.com/blog/archives/2006/12/realworld_passw.html`.

many of them will not think anything is unusual and will consequently enter in their user name and password. In fact, if you use password saving in your browser, it may even fill in the fields for you, adding further legitimacy to the form and encouraging you to submit it[7].

After the user submits the fake login form, her user name and password are sent to the attacker, who adds them to a database. At this point, the attacker can programatically permanently hijack the user's attack by changing their password, and then doing anything that they could do with the attack described in the previous section, and more. For example, this attack allows the attacker to make use of the admincp and engage in various malicious behaviours.

Alternatively, the attacker may choose a far more subtle use of the credentials. The attacker may simply use the credentials to obtain your email address from your User CP and then try your email and password at various other web sites, such as PayPal. Since many people use the same password on more than one site, there is a good chance that at least some users will have PayPal accounts with their Smash Boards email and password. At this point, the attacker can steal the user's entire PayPal balance and max out their credit cards.

This attack is extraordinarily dangerous and allows the attacker access to information that she would not even be able to get easily if she had stolen Smash Board's entire SQL database[8].

4 Risk assessment

Since moderators are supposed to be "trusted users", it may appear that these attacks are unlikely to be put to use, and thus that they are not cause for concern. Several observations come into play here.

First of all, it doesn't make sense to allow moderators to do indirectly what they cannot do directly. Both of the attacks described in this document, and other attacks, allow for privilege escalation, rendering differential permissions pointless (i.e. having some people with different permissions from other people). This alone is a serious problem. If a moderator does not need a permission, there is no reason why he should even have access to it. Smash Boards already attempts to adhere to this philosophy, with only some moderators being super moderators or administrators.

Second, Smash Boards has a very large number of moderators, with moderators coming and going on a regular basis. At the time of writing, there are approximately 125 moderators[9]. Although we can assume all of these moderators have been carefully vetted, it is just too many people to entrust with the extremely dangerous powers described above. If even a single moderator at any time becomes disgruntled with the site, she can leave by executing one of these

[7] See `http://news.cnet.com/2100-1002_3-6137844.html`.

[8] For example, VBulletin stores each user's password as a salt and a hash, making it computationally expensive to obtain passwords from the database, unlike this attack, which is cheap and efficient.

[9] See `http://www.smashboards.com/showgroups.php` for the exact list.

attacks on the way out. This hasn't happened yet[10], but if it ever happened — even once — the damage would be very great.

Third, everybody who becomes a moderator was apparently well-meaning, enthusiastic to help the site, and eager to participate. Most of these people will jump at the chance to help other people solve a problem. And although all of these people are computer-wise to the extent that they use the Internet on a daily basis and play Super Smash Brothers, the majority of moderators are not as technically inclined as a skilled attacker.

It is easy to imagine a scheme an attacker could use to post his attack. He would simply produce some JavaScript-powered Brawl-related tool, including the attack as a hidden component[11]. Then he would write to a moderator expressing his frustration at not being able to post his useful tool. Being a good samaritan, the moderator may post the tool on the user's behalf. Thus, the attack has been unleashed. Since the attack includes legitimate Brawl-related content, detection would not be immediate.

This particular scheme could be avoided with directions to moderators. However, there are many variations on it that could work. And considering there are so many moderators, even with well documented policies, at least one of them may ignore or not be familiar with the policies.

I conclude the risk posed by allowing moderators to use arbitrary HTML in posts is very great.

5 Recommendations

Having concluded that the status quo presents an unacceptable risk, we need to consider the solution to the problem.

In light of the dangerous possibilities described in this document, the administrators of Smash Boards should immediately disable the use of HTML in posts and announcements by moderators.

Arbitrary HTML is currently used to provide some useful features, such as embedding YouTube videos in posts. This feature can be preserved by introducing a new [youtube] BB Code tag using the Custom BB Code feature of VBulletin[12]. An additional advantage of this scheme is that it allows all users to embed YouTube videos, not just moderators.

Until the administrators of Smash Boards fix this issue, Smash Boards users may want to use a tool like NoScript[13] to disable JavaScript on Smash Boards, even though this also disables many useful forum features, such as inline editing. Users are also advised to change their Smash Boards password to a password they do not use on any other site.

This will protect users from both attacks described in this document.

[10] The number of moderators on Smash Boards has increased dramatically since Brawl's release and especially in the last year. Having fewer moderators in the past may also explain the lack of any attacks.

[11] This could be very well obfuscated with eval() and decode(), for example.

[12] See `http://www.vbulletin.com/docs/html/bb_code`.

[13] See `http://noscript.net/`.