Worst security hole you've seen? [closed]

Asked 15 years, 3 months ago Modified 13 years, 1 month ago

Viewed 78k times

413

votes

As it currently stands, this question is not a good fit for our Q&A format. We expect answers to be supported by facts, references, or expertise, but this question will likely solicit debate, arguments, polling, or extended discussion. If you feel that this question can be improved and possibly reopened, visit the help center for guidance.

Closed 13 years ago.

Locked. This question and its answers are locked because the question is off-topic but has historical significance. It is not currently accepting new answers or interactions.

What is the worst security hole you've ever seen? It is probably a good idea to keep details limited to protect the guilty.

For what it's worth, here's a question about what to do if you find a security hole, and another with some useful answers if a company doesn't (seem to) respond.

security

Share

edited May 23, 2017 at 12:03

community wiki
14 revs, 7 users 47%
si618

47 Should be community wiki imo... – ChristopheD Sep 24, 2009 at 5:38

15 the 60 answers and 28 upvotes would seem to outweigh the 5 votes to close (that took all day to accumulate, AFAIK). but I will refrain from voting to reopen until this has been discussed. – rmeador Sep 24, 2009 at 22:57

Huh? Why was this closed? Shouldn't we also close: stackoverflow.com/questions/325862/… or stackoverflow.com/questions/1705/… – si618 Sep 24, 2009 at 23:30

Or a more generalised version of stackoverflow.com/questions/23102/… – si618 Sep 24, 2009 at 23:44

7 Even if your question has been community wiki for hours, the comment is still a good comment to upvote, as it reminds people that *questions similar to this one should be community wiki*. That's what I think. – Joren Sep 25, 2009 at 19:44

Comments disabled on deleted / locked posts / reviews |

163 Answers

Sorted by: Highest score (default)

1 2 3 4 5 6 Next

644 votes

From early days of online stores:

Getting a 90% discount by entering .1 in the quantity field of the shopping cart. The software properly calculated the total cost as .1 * cost, and the human packing the order simply glossed over the odd "." in front of the quantity to pack :)

Share

answered Sep 24, 2009 at 9:25

community wiki
John Stauffer

75 This is definitely an argument in favor of using a strongly typed system. – Powerlord Sep 24, 2009 at 14:00

54 What's the site? I want a 90% discount!!! – amischiefr Sep 24, 2009 at 14:27

58 Maybe you should have requested a .10 percent quanity instead. ;) – MiffTheFox Sep 26, 2009 at 3:08

81 Jeff Bezos mentioned that in the very early days of Amazon, you could have a negative quantity of books and Amazon would credit your account (and presumably wait for you to ship it to them). See 0:47 at youtube.com/watch?v=-hxX_Q5CnaA – Jeff Moser Sep 29, 2009 at 20:18

10 Would have loved to see the face of the customer who actually got delivered the .1 harddrives he paid for. – relet Jul

16, 2010 at 12:47

575

votes

The least forgivable security hole, and unfortunately a very common and easy to find one at that, is Google hacking. Case in point:

http://www.google.com/search?q=inurl%3Aselect+inurl%3A%2520+inurl%3Afrom+inurl%3Awhere

It's amazing how many pages on the Internet, government sites in particular, pass an SQL query through the query string. It's the worst form of SQL injection, and it takes no effort at all to find vulnerable sites.

With minor tweaks, I've been able to find unprotected installations of phpMyAdmin, unprotected installations of MySQL, query strings containing usernames and passwords, etc.

Share

edited Oct 30, 2010 at 10:57

community wiki
3 revs, 3 users 67%
Juliet

25 johnny.ihackstuff.com/ghdb – ykaganovich Sep 25, 2009 at 3:11

6 Oh dear God, how inconceivably stupid. That would be me marching that developer to HR with a box in hand.

– squillman Oct 2, 2009 at 16:18

95 little Bobby tables strikes again... xkcd.com/327 – gbjbaanb Oct 7, 2009 at 12:21

86 OMFG ... next time I have a bad day, I go drop some tables – Michael Niemand Oct 15, 2009 at 16:17

11 What I really like about this example is that the first result is from an Oracle blog. – Ravi Wallau Mar 13, 2010 at 2:57

398 votes

Social Engineering:

```
<Cthon98> hey, if you type in your pw, it will
show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
<AzureDiamond> you can go hunter2 my hunter2-ing
hunter2
<AzureDiamond> haha, does that look funny to you?
<Cthon98> lol, yes. See, when YOU type hunter2, it
shows to us as *******
<AzureDiamond> thats neat, I didnt know IRC did
that
<Cthon98> yep, no matter how many times you type
hunter2, it will show to us as *******
<AzureDiamond> awesome!
<AzureDiamond> wait, how do you know my pw?
<Cthon98> er, I just copy pasted YOUR ******'s and
it appears to YOU as hunter2 cause its your pw
<AzureDiamond> oh, ok.
```

From bash.org

Share

answered Sep 30, 2009 at 22:44

community wiki
Bob Aman

2 Used to happen all the time on Runescape. – EvilTeach Mar 13, 2010 at 3:42

7 This particular exchange is highly unlikely to have actually happened (who would type "er" when they're trying to cover something up?), but funny nonetheless. – Michael Myers ♦ Mar 15, 2010 at 16:06 ✎

1 mmyers: it's also highly unlikely someone is stupid enough to get rm -rf'd, but that definitely happens. I've seen it myself :) – Matthew Iselin Mar 29, 2010 at 6:53

25 There is nothing more insecure than the idiots brain – Earlz Jun 23, 2010 at 20:38

1 @EvilTeach they actually implemented that on RuneScape. Not even kidding! – corsiKa Dec 9, 2011 at 22:56

339 votes

True story from my early days at Microsoft.

You haven't known fear until the day you wake up and see the headline on ZDNet.com that morning is "**Worst Internet Explorer Security Hole Ever Has Been Discovered In 'Blah'**" where 'Blah' is code you wrote yourself six months previously.

Immediately upon getting to work I checked the change logs and discovered that someone on another team --

someone we trusted to make changes to the product -- had checked out my code, changed a bunch of the security registry key settings for no good reason, checked it back in, and never got a code review or told anyone about it. To this day I have no idea what on earth he thought he was doing; he left the company shortly thereafter. (Of his own accord.)

(UPDATE: A few responses to issues raised in the comments:

First, note that I choose to take the charitable position that the security key changes were unintentional and based on carelessness or unfamiliarity, rather than malice. I have no evidence one way or the other, and believe that it is wise to attribute mistakes to human fallibility.

Second, our checkin systems are much, much stronger now than they were twelve years ago. For example, it is now not possible to check in code without the checkin system emailing the change list to interested parties. In particular, changes made late in the ship cycle have a lot of "process" around them which ensures that the right changes are being made to ensure the stability and security of the product.)

Anyway, the bug was that an object which was NOT safe to be used from Internet Explorer had been accidentally released as being marked "safe for scripting". The object was capable of writing binary files -- OLE Automation type libraries, in fact -- to arbitrary disk locations. This meant that an attacker could craft a type library that contained certain strings of hostile code, save it to a path that was a known executable location, give it the extension of something that would cause a script to run, and hope that somehow the user would accidentally run the code. I do not know of any successful "real world" attacks that used this vulnerability, but it was possible to craft a working exploit with it.

We shipped a patch pretty darn quickly for that one, let me tell you.

I caused and subsequently fixed many more security holes in JScript, but none of them ever got anywhere near the publicity that one did.

Share

edited Sep 26, 2009 at 3:06

community wiki
3 revs, 2 users 96%
Eric Lippert

81 Arguably, this is actually 2 security exploits; the other one being how to get code onto a production build server without anyone noticing / approving the change ;-p – Marc Gravell Sep 24, 2009 at 11:30

8 "had checked out my code, changed a bunch of the security registry key settings for no good reason, checked it back in, and never got a code review or told anyone about it" -- doesn't sound like incompetence to me, it sounds like malicious intent from someone knew *exactly* what they were doing. – Juliet Sep 24, 2009 at 13:57

80 "Never attribute to malice that which can be adequately explained by stupidity." -- Hanlon's Razor – David R Tribble Sep 24, 2009 at 22:27

15 There is no one source control system mandated for use across Microsoft. Most teams these days either use Source Depot or Team Foundation. Unsurprisingly, the Visual Studio product teams generally use Team Foundation. Eat your own dogfood, you know. – Eric Lippert Oct 10, 2009 at 21:11

40 Who checks ZDNet before going to work? – Neil N Jan 7, 2010 at 7:05

274 votes

I hope you can spot what's wrong here. (Terribly wrong, in fact):

```
String emailBody = "";

for (int i = 0; i < subscribers.Count; i++)
{
    emailBody += "Hello " +
subscribers[i].FirstName + ",";
    emailBody += "this is a reminder with your
account information: \n\n:";
    emailBody += "Your username: " +
subscribers[i].Username + "\n";
    emailBody += "Your password: " +
subscribers[i].Password + "\n";
    emailBody += "Have a great day!";


emailDispatcher.Send(subscribers[i].EmailAddress,
emailBody);
}
```

The last recipient was the happiest ;)

Share

edited Jan 17, 2010 at 22:18

community wiki
2 revs, 2 users 90%
Alex

226 Are you talking about the fact that you store plain-text passwords or the fact that the emailBody is never cleared? I'm not even sure which is worse. – Kristof Provost Sep 24, 2009 at 10:38

208 You mean not using StringBuilder? :D (Just kidding.) – ShdNx Sep 24, 2009 at 10:42

58 @Kristof - I'm guessing he means the fact that the last user gets a list of ALL the users and passwords. :) – Don Branson Sep 24, 2009 at 10:51

141 I absolutely *loathe* systems that email me back my password as part of the registration process. This has two flaws: 1. They're storing my plaintext password somewhere within their system. If not their permanent user database, definitely their registration processing system. 2. It was sent via EMAIL, either plain text or HTML, SMTPing its way through mail relays across the internet. There's a number of men-in-the-middle which could intercept this. At the very least, if you feel the need to send me emails with secure information, let me specify my public PGP key to you to encrypt it! – Jesse C. Slicer Sep 24, 2009 at 15:06

16 I used MD5 hashes to protect the passwords in a database once. But after I ran the results though a rainbow table and matched about 50% of the passwords... I figured it was a good time to add a salt. – Matthew Whited Sep 24, 2009 at 18:30

206

votes

The old IBM System 36 dumb terminals had a keyboard combination that started the recording of a macro. So when a terminal was not logged in, you could start the recording of a macro and leave it in that position. Next time someone logged in, the keystrokes would be recorded in the macro and the recording would end automatically when maximum allowed keys was recorded. Just come back later and replay the macro to autolog-in.

Share

edited Feb 8, 2017 at 14:15

community wiki

2 revs

Stefan

204

votes

The worst security hole I've ever seen was actually coded by yours truly and caused the Google Bot to delete my entire database.

Back when I was first learning Classic ASP, I coded my own basic blog application. The directory with all the admin scripts was protected by NTLM on IIS. One day I moved to a new server and forgot to re-protect the directory in IIS (oops).

The blog home page had a link to the main admin screen, and the main admin screen had a DELETE LINK for each record (with no confirmation).

One day I found every record in the database deleted (hundreds of personal entries). I thought some reader had broke into the site and maliciously deleted every record.

I came to find out from the logs: The Google Bot had crawled the site, followed the admin link, and the proceeded to follow all the DELETE LINKS, thereby deleting every record in the database. I felt I deserved the Dumbass of the Year award getting inadvertently compromised by the Google Bot.

Thankfully I had backups.

Share

edited Oct 30, 2010 at 11:09

community wiki

2 revs, 2 users 96%
Matias Nino

13 Guess it shows how common a mistake it is. – si618 Sep 25, 2009 at 0:27

96 That's why you should always POST for changing actions. – recursive Sep 30, 2009 at 22:22

7 @recursive: true, but if the directory is not password-protected, it doesn't stop a human deleting everything. – DisgruntledGoat Jan 18, 2010 at 0:39

2 I've had this problem with browser plugins that prefetch links. I once worked for a blogging site, and we were puzzled for days when one user reported that all comments on her blog would mysteriously vanish. – Matthew Mar 13, 2010 at 2:47

7 No, you didn't deserve that award. You would have deserved it if this had happened and you *didn't* have backups. – Ryan Lundy Dec 22, 2010 at 23:16

187
votes

The worst hole I've ever seen was a bug in a web application where giving an empty user name and password would log you in as administrator :)

Share

edited Oct 30, 2010 at 10:59

community wiki
2 revs, 2 users 50%
Kaitsu

144 A bug or a feature for lazy developers? :) – si618 Sep 24, 2009 at 5:47

9 I've seen such code. That is usually because the user lookup use a LIKE, as in "SELECT * FROM [User] Where UserName LIKE '%" + userName + "%'". And since the administrator is typically the first user in the database, it return that user. – Pierre-Alain Vigeant Sep 24, 2009 at 17:34

11 why would you do a LIKE with a username?... so I could be admin by typing adm when I ment to type Adam – Matthew Whited Sep 24, 2009 at 18:27

20 Most companies give you three attempts to log in under a given user-ID before they lock out the account. So it's trivially easy to lock out someone *elses* account with three bad passwords. – David R Tribble Sep 24, 2009 at 22:38

3 I've seen this in a lot of corporate webapps that authenticate against an LDAP directory. In LDAP, an empty password results in a *successful anonymous* login. The anonymous user can't do much, but the webapps using this mechanism don't go as far as to check - they just assume "success = correct password"! – SimonJ Oct 23, 2010 at 20:42

174 votes

Once noticed this on the URL of a web-site.

```
http://www.somewebsite.com/mypage.asp?
param1=x&param2=y&admin=0
```

Changing the last parameter to admin=1 gave me admin privileges. If you are going to blindly trust user input at least don't telegraph that you are doing it!

Share

edited Sep 26, 2009 at 6:10

community wiki
2 revs, 2 users 92%
JohnFx

19 It's a handy feature ;) Haven't you seen WarGames? Something like "every good developer adds a backdoor to their system" hehe. – alex Jan 17, 2010 at 23:37

38 So maybe they should have used &admin=JOSHUA – JohnFx Jan 18, 2010 at 15:39

164 votes

I saw this one in The Daily WTF.

```
<script language="javascript">
<!--//
/*This Script allows people to enter by using a
form that asks for a
UserID and Password*/
function pasuser(form) {
    if (form.id.value=="buyers") {
        if (form.pass.value=="gov1996") {

location="http://officers.federalsuppliers.com/agents
        } else {
            alert("Invalid Password")
        }
    } else {
        alert("Invalid UserID")
    }
}
//-->
</script>
```

Nothing can beat this IMHO.

Share

edited Oct 2, 2009 at 15:47

community wiki
2 revs, 2 users 82%
Konamiman

21 I think this may be not as stupid as you think. This trivial password might work like the button "yes, I am from the federal governemnt" with the difference that a person who tries to misuse it, if caught, can also be prosecuted for "providing false credentials" (or how they call it?) – ilya n. Sep 24, 2009 at 10:20

29 ilya : It's Javascript, so it's visible to the user. After seeing that, you can just go to officers.federalsuppliers.com/agents.html, bypassing any kind of control. – Alsciende Sep 24, 2009 at 12:04

68 Don't worry, as long as the web site is copyrighted, the DMCA provides 100% protection. You're not allowed to "circumvent" the Javascript. – Steve Hanov Sep 24, 2009 at 13:33

13 @Steve Hanov: You have an interesting definition of "circumvent" If I type that url into my browser... or even copy/paste it... I'm not bypassing anything, I'm just using my browser to go to an address I put in my address bar. Which is one of the intended purposes of a web browser. – Powerlord Sep 24, 2009 at 13:39

46 congrats, you're innocent, too bad it costs 300k to convince a jury that – Dustin Getz Sep 24, 2009 at 13:59

141

votes

At a university no less, which will remain nameless, they had all their action queries being passed through the URL instead of form posted.

The thing worked a treat until Google Bot came along and ran through all of their URLs and wiped their database.

Share

answered Sep 24, 2009 at 11:19

community wiki
Evernoob

18 Good old SQL Injection by Design. I've worked with reporting functionality that has had that "feature" built in. – ICodeForCoffee Sep 24, 2009 at 13:27

18 @ICodeForCoffee: where's the SQL injection here? This is just confusing the purposes of GET vs POST. It's a fairly common mistake by novice web devs. I recall reading a Daily WTF article about this exact problem. – rmeador Sep 24, 2009 at 15:24

Didn't an very early version if Wikipedia have this problem? They had links which would revert edits or something. – DisgruntledGoat Oct 13, 2009 at 13:57

14 The real problem here is the Googlebot could wipe the database without ever authenticating. – MiffTheFox Nov 30, 2009 at 14:57

34 Hope they were able to retrieve them from google cache. – fastcodejava Jun 6, 2010 at 5:03

136
votes

Surprised no one has brought up social engineering, but I got a kick out of this article.

Summary: malicious users can buy a few dozen flash drives, load them with an auto-run virus or trojan, then sprinkle said flash drives in a company's parking lot late at night. Next day, everyone shows up to work, stumble on the shiny, candy-shaped, irresistable hardware and say to themselves "oh wow, free flash drive, I wonder what's on it!" -- 20 minutes later the entire company's network is hosed.

Share

answered Sep 24, 2009 at 14:15

community wiki
Juliet

69 Autorun is evil. – Mark Ransom Sep 24, 2009 at 16:16

22 **@mmyers:** banning flash drives is not the good approach. Break the autorun/autoplay. – Jay Sep 25, 2009 at 12:54

10 Read some time ago, another approach (from the floppy disk times). Live a boot infected floppy disk labeled "Accounting data - confidential" in a corridor of the office and wait 5 minutes. Irresistible! – Rodrigo Sep 25, 2009 at 15:03

13 Fortunately, I can always boot up from a Linux Live CD and examine the flash drive from there. – David Thornley Oct 2, 2009 at 17:28

6 @Jay - Unfortunately, how many people would look at the files and then double click on them "to see what they do"?

Banning is a necessity many of times because people don't think. – JasCav Mar 15, 2010 at 16:09

130

votes

"Pedo mellon a minno", "Speak friend and enter", on the gates of Moria.

Share

answered Oct 2, 2009 at 15:49

community wiki
Adriano Varoli Piazza

13 As if anyone who speaks Elvish can't be trusted! – Artelius Nov 5, 2009 at 8:21

6 xkcd.com/424 – lily Aug 29, 2010 at 15:49

103

votes

Microsoft Bob
(Credit: Dan's 20th Century Abandonware)

If you enter your password incorrectly a third time, you are asked if you have forgotten your password.

http://img132.yfrog.com/img132/8397/msbob10asignin15.gif

But instead of having security, like continuing to prompt for the correct password until it's entered or locking you out after a number of incorrect attempts, you can enter any new password and it will replace the original one! Anyone can do this with any password "protected" Microsoft Bob account.

There is no prior authentication required. his means User1 could change their own password just by mistyping their password three times then entering a new password the fourth time -- never having to use "change password."

It also means that User1 could change the passwords of User2, User3... in exactly the same way. Any user can change any other user's password just by mistyping it three times then entering a new password when prompted -- and then they can access the account.

http://img132.yfrog.com/img132/9851/msbob10asignin16.gif

Share

edited Oct 1, 2009 at 22:29

community wiki
3 revs
JohnFx

7 This is the same behavior as Windows itself when a computer is not administered by a domain. Even on Windows Vista Ultimate, you can reset a password at any time. I am guessing that denial-of-service is considered a bigger threat than unauthorized access; especially since you can get most stuff just by re-mounting the drive elsewhere anyway. I believe the purpose of the password in this case is for intrusion *detection* rather than prevention. – Jeffrey L Whitledge Nov 4, 2009 at 8:57

1 @Jeffrey: Thing is, once the black hat has physical access, it's pretty much "game over". If you want to protect against that, you need serious encryption (as well as ways to scan for hardware and software keyloggers, etc.). – David Thornley Apr 9, 2010 at 17:27

8 Someone wiser than me pointed out this is just good threat modeling. 'Bob' was for home use in an non-networked era and you were FAR more likely to suffer an attempted DOS from your little sister or a hangover than from some burglar. Bob let you know that your account had been accessed (because your old password no longer worked) but didn't try to do more. – bgiles May 3, 2010 at 16:51

20 My wife just saw me looking at this... Her:"Oh my gosh! What program is that?!" Me:"...Microsoft Bob?" Her:"I *loved* Microsoft Bob!" *Sigh*... – Tim Goodman Jul 16, 2010 at 16:35

10 @ChristianWimmer - Sounds kind of like giving people a backpack marked "Parachute" so they get used to the feel of one on their back, but without telling them there is no parachute in there. – JohnFx Oct 25, 2010 at 21:21

102
votes

I had Joe X's former home address, and needed to know his newer current address in the same city, but had no way to contact him. I figured he was receiving the usual daily pile of mail order catalogs, so I arbitrarily called the 800 number for See's Candies (as opposed to Victoria's Secret, or Swiss Colony, or any other big mailer):

Me: "Hi, I'm Joe X. I think you've got me on your mailing list twice, at both my old address and my new address.

Does your computer show me at [old address] or at [fake address]?"

Operator: "No, we show you at [new address]."

Share

answered Jun 3, 2010 at 6:55

community wiki
joe snyder

36 Ah, gotta love social engineering. The human aspect of security is usually the weakest. – EMP Jun 3, 2010 at 23:02

In the UK you've admitted to a criminal offense - "Knowingly or recklessly obtaining or disclosing personal data or information without the consent of the data controller" – Flexo - Save the data dump ♦ Aug 24, 2011 at 18:30

95 votes

Giving **1=1** in a textbox **lists all the users** in the system.

Share

answered Sep 24, 2009 at 5:48

community wiki
rahul

325 Greetings from Bobby Tables. – Gumbo Sep 24, 2009 at 5:50

4 how can @Gumbo's comment is upvoted 4 times as much as the answer? – Lie Ryan Oct 29, 2010 at 20:47

12 Simply, 4 times the amount of people that voted the question up had voted his comment :/ – RobertPitt Oct 30, 2010 at 11:58

4 Would one of the 221 up-voters of the Bobby Tables comment tell the rest of us what the hell Bobby Tables is? – kirk.burleson Oct 30, 2010 at 12:00

15 @kirk.burleson: xkcd.com/327 – gspr Oct 30, 2010 at 15:21

76
votes

Being an application security consultant for a living there are lots of common issues that let you get admin on a website via something. But the really cool part is when you can buy a million dollars worth of socks.

It was a friend of mine working on this gig but the jist of it was that prices for items in a certain now very popular online book (and everything else) shop were stored in the HTML itself as a hidden field. Back in the early days this bug bit a lot of online stores, they were just starting to figure out the web. Very little security awareness, I mean really who is going to download the HTML, edit the hidden field and resubmit the order?

Naturally we changed the price to 0 and ordered 1 million pairs of socks. You could also change the price to negative but doing this made some part of their backend billing software buffer overflow ending the transaction.

If I could choose another it would be path canonicalization issues in web applications. It's wonderful to be able to do foo.com?file=../../../../etc/passwd

Share

edited Sep 24, 2009 at 10:50

community wiki
2 revs, 2 users 75%
Collin

9 Awesome, you'd never have a missing left sock ever again! – si618 Sep 24, 2009 at 6:30

75 Did you ever get the socks? – Alex Barrett Sep 24, 2009 at 9:55

32 The order went through and the fulfillment system alerted the warehouse. We realized it probably worked and told our point of contact that they should stop the order. Apparently a bit later a warehouse manager called in asking about the order to be sure it was real. He was wisely of the mind that it was a software error. – Collin Sep 24, 2009 at 21:06

27 @StuperUser, On your feet, of course. – strager Sep 1, 2010 at 3:30

12 No problem with storage, just hack the Ikea website to order 100,000 sets of drawers to put them in, – Neil Aitken Sep 28, 2010 at 8:46

63 votes

Committing the database root password to source control by accident. It was pretty bad, because it was source control on Sourceforge.

Needless to say the password got changed very quickly.

Share

answered Sep 24, 2009 at 5:59

community wiki
Matthew Iselin

144 OK, the password got changed very quickly... but by *whom*? – Eamon Nerbonne Sep 24, 2009 at 13:58

1 Been down this road. Many systems (like django, for example) practically encourage this, since they ask you to put your DB password into the settings file, which naturally, is very easy to check in. – mlissner Apr 18, 2011 at 3:46

56
votes

Not changing admin passwords when key IT employees leave the company.

Share

answered Sep 24, 2009 at 10:27

community wiki
Max

1 or leaving the factory defaults like admin/admin (as well or especially in the hardware)... – Gnark Sep 24, 2009 at 11:29

47 I've got one worse -- I left a university after having been strung along, with the directory telling me they were creating a higher grade job for me after I had graduated, but I later found out he told my manager they were *not* to promote me. Needless to say, I wasn't happy about it. I specifically told my manager to change *every* password I had access to. The week after I left, I get an e-mail from my manager with the root password, 'just in case I needed it'. I contacted the sysadmin to make sure it was

changed again, as I didn't want to take the fall if something went wrong. – Joe Sep 24, 2009 at 13:53

10 @Sophomore: I recall in Feynman's biography him commenting that many of the giant, ultra-secure safes housing the Manhattan project secrets were left in the default combinations. – Brian Sep 24, 2009 at 19:48

12 I can just imagine a USSR spy getting to the safe and trying everything he can think of to crack the safe, "Damn! I can't crack it. Wouldn't it be funny if I could just...wow, score one for Mother Russia!" – Eric Sep 30, 2009 at 23:09

3 Can't smile while reading this, I was working as an IT technician a summer at a very well known swedish company, and when I returned several years later to work as an engineer, I had some problem installing some software. Out of blue I remebered the old admin password, and voila! it worked =) – Viktor Sehr Apr 9, 2010 at 16:05

50 votes

Though this is not the worst security hole I’ve ever seen. But this is at least the worst I’ve discovered myself:

A pretty successful online shop for audiobooks used a cookie to store the identification information of the current user after successful authentication. But you could easily change the user ID in the cookie and access other accounts and purchase on them.

Share

edited Sep 25, 2009 at 12:29

community wiki

2 revs
Gumbo

Wow ...I had the exact thing happen to me on an ASP code I inherited. – Radu094 Nov 1, 2009 at 22:36

I maintain an app that has this exact issue. It's high up on the fix list, to be sure. Thankfully, it isn't an ecommerce site. – quentin-starin Aug 31, 2010 at 18:55

12 This happens for more often than most people realize. – ChrisLively Oct 22, 2010 at 20:47

47
votes

Right at the start of the .com era, I was working for a large retailer overseas. We watched with great interest as our competitors launched an online store months before us. Of course, we went to try it out... and quickly realized that our shopping carts were getting mixed up. After playing with the query string a bit, we realized we could hijack each other's sessions. With good timing, you could change the delivery address but leave the payment method alone... all that after having filled the cart with your favorite items.

Share

answered Sep 24, 2009 at 5:49

community wiki
Eric J.

Of course, this means that you've maliciously done something to get them to send merchandise to you fraudulently if you actually do this, and told "them" your address. – David Thornley Nov 25, 2009 at 20:25

6 Yes, that's what makes it a major security hole. We did not actually pressed the buy button, but we could have. And, based on news reports, some people did. – Eric J. Nov 30, 2009 at 17:37

45 votes

When I first joined the company I currently work at, my boss was looking over the existing e-commerce web site of a prospective new client. This was in the fairly early days of both IIS and e-commerce, and security was, shall we say, less than stringent.

To cut a long story short, he altered a URL (just out of curiosity), and realised that directory browsing wasn't turned off, so you could just cut the page name off the end of the URL and see all the files on the web server.

We ended up browsing a folder containing an Access database, which we downloaded. It was the entire e-commerce customer/order database, replete with several thousand unencrypted credit card numbers.

Share

edited Oct 7, 2009 at 17:42

community wiki
2 revs, 2 users 89%
Mark Bell

1 This was nearly twelve years ago, when data-driven web sites were a cutting-edge novelty; many sites ran against Access or similar, because no-one wanted to invest in a SQL Server license for something that was seen as an 'aside' to their core business. How things have changed! – Mark Bell Jan 18, 2012 at 9:28

45 votes

[People posting their passwords on public websites...]

Share

answered Sep 1, 2010 at 3:15

community wiki
Longpoke

17 Nice touch making the `...` a link as well :p – invert Oct 14, 2010 at 7:36

"2811A Console password: PrincessLeia" This was my favorite. – MrZander Feb 2, 2012 at 23:23

44 votes

When I was 13 years old my school opened a social network for the students. Unfortunately for them I found a security bug where you could change the URI to another userID like "?userID=123" and become logged in for that user. Obviously I told my friends, and in the end the schools social network was filled with porn.

Wouldn't recommend it though.

Share

answered Sep 24, 2009 at 5:43

community wiki
hannson

3 why wouldn't u recommend this? what happened?
– Simon_Weaver Jan 7, 2010 at 5:30

55 @Simon_Weaver: I guess 13-years-olds don't usually have a good taste for porn. – slacker Aug 30, 2010 at 0:12

@slacker +1 to put you at 1000 rep! except i don't think rating comments gives you rep :-(– Simon_Weaver Sep 2, 2010 at 3:07

2 "good taste for porn" - there's an oxymoron. – Zann Anderson Feb 18, 2011 at 6:58

43 votes

I think the blank username / password field for superuser access is by far the worst. But one I have seen myself was

```
if (password.equals(requestpassword) ||
username.equals(requestusername))
{
    login = true;
}
```

Too bad one operator makes such a big difference.

Share

edited Sep 30, 2009 at 22:03

community wiki
2 revs, 2 users 78%
Stefan Ernst

10 wow, i naturally have a compulsion to fix it – wag2639 Jun 23, 2010 at 17:02

The fact that a real password is used instead of a hash is actually also rather bad ... – Peter Kriens Jan 24, 2012 at 13:51

First I was "what's wrong?", and then I was "AAAAaaaaaaaAAAA! OMG" – Bojan Kogoj Feb 14, 2012 at 13:40

42
votes

Mine would be for a bank I was a customer of. I wasn't able to log on, so I called customer service. They asked me for my user name and nothing else - didn't ask any security questions or try to verify my identity. Then instead of sending a password reset to the email address they had on file, they asked me what email address to send it to. I gave them an address different than what I had on file, and was able to reset my password.

So essentially, all a hacker would need is my user name, and he could then access my account. This was for a major bank that at least 90% of people in the United States would have heard of. This happened about two years ago. I don't know if it was a poorly trained customer service rep or if that was standard procedure.

Share

answered Sep 24, 2009 at 6:29

community wiki
Sean

22 and what bank is it, please? – TigerTiger Sep 24, 2009 at 9:16

5 @Si: it writes 'I WAS a customer of...'. I think that answers the question. :) – ShdNx Sep 24, 2009 at 10:53

8 This was Washington Mutual, which was seized by the FDIC and sold to Chase early this year. They also had strange error messages. When I tried to set my password from the temp one I kept getting a "Passwords don't match" error, even though they were the same and I even copy/pasted. I realized that if I put "invalid characters" like a forward slash, instead of saying invalid characters, it would give me that other message. – Sean Sep 24, 2009 at 19:44

11 @Elizabeth: Uhm... you realize that's to prevent phishing right? If someone tries to copy or mimic the bank website it can look exactly the same, but presumably they don't have access to the database, so they can't pull up the right security picture. That's why that's there. Not all users are smart enough to check the cert (which might be similarly bluffed) – mpen Sep 26, 2009 at 2:20

13 Protecting your financial accounts is overkill? ... – Joe Phillips Sep 27, 2009 at 15:57

36 votes

I'll share one I created. Kind of.

Years and years and years ago the company I was working for wanted indexing on their ASP web site. So off I went and set up Index Server, excluded a few admin directories and all was good.

However unknown to me someone had given a sales person ftp access to the web server so he could work from home, this was the days of dialup and it was the easiest way for him to swap files.... and he started uploading things, including documents detailing the markup on our services.... which index server indexed and starting serving up when people searched for "Costs".

Remember kids, whitelists not blacklists.

Share

answered Sep 24, 2009 at 9:18

community wiki
blowdart

76 I think "whitelists not blacklists", while often good advice, is not the correct lesson to learn here. The correct lesson is "don't put private data on a public server". Also, "don't let sales people access the server". – rmeador Sep 24, 2009 at 15:23

7 Oh, the harmony between the answer and the avatar. – Çağdaş Tekin Oct 6, 2009 at 15:24

35 votes

One of the simplest, yet really cost worthy is:

Payment systems that use engines such as PayPal can be flawed because the response back from PayPal after payment was successful is not checked as it should be.

For example:

I can go on to some CD purchase website and add some content to the cart, then during the checkout stages there's usually a form on the page that has been populated with fields for paypal, and a submit button to "Pay"..

Using a DOM Editor I can go into the form "live" and change the value from `£899.00` to `£0.01` and then click submit...

When I'm on the PayPal side of things I can see that the amount is 1 penny, so I pay that and PayPal redirects some parameters to the initial purchase site, who only validates parameters such as `payment_status=1`, etc., etc. and do not validate the amount paid.

This can be costly if they do not have sufficient logging in place or products are automatically dispatched.

The worst kind of sites are sites who deliver applications, software, music, etc.

Share

edited Oct 30, 2010 at 10:40

community wiki
3 revs, 2 users 80%
RobertPitt

12 +1 Agreed. In the hosted payment page situation the originating website should not allow the user to drive values to

be posted; instead the page should post back to itself upon user click and then the server formulate and send a post op to the payment "gateway" directly with appropriate values. It all depends on what the gateway expects and how interactions can be made with it, but I cannot see any gateway worth its salt not having a more secure scenario than what you described. Maybe I'm wrong though. – John K Oct 23, 2010 at 20:29

you can mimic post request's via server side so sending the data that way you can make sure that the data being sent to the gateway is exactly that, and then redirect them with the location header. – RobertPitt Nov 4, 2010 at 11:20

PayPal has an encryption option that lets site prevents this. The site posts-back the data to itself first, encrypts the order data server-side with a key known only to them and PayPal, and then sends that data to PayPal who decrypt it. Unencrypted order data is never sent in form fields that way. It's only an option though, so not every site using PayPal does it that way. They should though! – Michael Low Dec 28, 2010 at 18:13

35

votes

How about an online document manager, which allowed to set every security permission you could remember...

That is until you got to the download page... download.aspx?documentId=12345

Yes, the documentId was the database ID (auto-increment) and you could loop every single number and anyone could get all the company documents.

When alerted for this problem the project manager response was: Ok, thanks. But nobody has noticed this before, so let's keep it as it is.

Share

edited Nov 15, 2011 at 9:56

community wiki
3 revs, 3 users 75%
Sergio

56 I really hate that attitude, been getting it a few times. Makes me want to let others do it just to teach 'em a lesson. – syaz Sep 24, 2009 at 10:47

I finally got the go-ahead to fill a hole like this at my last job... after months of complaining about it. – eyelidlessness Sep 26, 2009 at 2:33

It's not that uncommon to find websites that let you do this. You'll see a directory of recent or archived articles, but can't go back farther in the list than a page or two without having to log in. Just open the first article, and change the right parameter in the url to any post number you want to see any article. – bob-the-destroyer Oct 21, 2010 at 1:16

2 Here's a great example of this. In this NY Times article: nytimes.com/2009/01/14/dining/14power.html?_r=1&ref=dining the picture shown is a replacement for the much more hilarious original version, still available here:graphics8.nytimes.com/images/2009/01/14/dining/14power2_650.jpg – Jamie Treworgy Oct 21, 2010 at 17:51

34
votes

A Norwegian pizza delivery had a security hole where you could order *negative* amounts of pizzas at their new and shiny internet portal and get them for free.

Share

edited Sep 24, 2009 at 16:55

community wiki
2 revs
user110763

42 The other security hole is the employees, right? "Well sir, the computer says you get 15 pizzas for free, so... here you go!... do I get a tip?" – Nathan Long Sep 24, 2009 at 18:55

6 ...your pizza place gives out DVDs too? O.o – mpen Sep 26, 2009 at 2:23

5 As a former pizza driver... no, we didn't give a rats ass about that kind of stuff. And neither did our managers. – eyelidlessness Sep 26, 2009 at 2:29

48 Wouldn't the delivery guy come by to *collect* the pizzas you're *selling* them? – Jon B Oct 2, 2009 at 17:34

7 Wow.. and the delivery guy had to give you the tip? =)) – Andrei Rînea Oct 13, 2010 at 20:05

1 2 3 4 5 6 Next