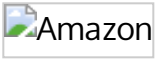
(/)
I build great experiences. Currently available for hire (https://burke.services). More about me (/about)

“Invalid Username or Password”: a useless security measure

Posted on December 1, 2014 (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/)

Login attempts fail because computer users can't remember their email or didn't input the right password. Most websites on the Internet won't tell you which one is actually incorrect.

Amazon:



Shoprunner:

Hacker News:

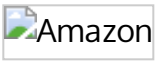
If you tell an attacker the email address is wrong, they'll try a different one. If you tell them the password is wrong, then an attacker knows that the username is correct, and can go on to try a bunch of passwords for that username until they hit the right one. So sites won't tell you which one is wrong, to try and avoid the information disclosure.

Unfortunately **this assumes that there's no other way for an attacker to discover whether a username/email address is registered for a service**. This assumption is incorrect.

99.9% of websites on the Internet will only let you create one account for each email address. So if you want to see if an email address has an account, **try signing up for a new account with the same email address.**

Here are all of the websites above, confirming that an account exists with my email address/username:

Amazon:



Shoprunner:

Hacker News:

So what we've done by promoting "Invalid username or password" is made our login form UX much, much worse, without increasing the security of our product.

If people don't log in to your site every day (every site on the web except Facebook or Google), not remembering credentials is a huge barrier to accessing your site. Don't make it harder by adding a vague error message that doesn't increase your site's security at all.

But there's a tradeoff there between security and UX, I hear you say. I am trying to show you there is no tradeoff, as presented above; you are choosing between a better user experience and a worse user experience.

What should I do instead?

Here is an actual UX/security tradeoff: you *can* make the signup process email based. When someone attempts to sign up with an email address, you send them an email to complete the registration process. If they don't control the email inbox, they can't see whether the email address has an account already. This is much more arduous and requires two context switches (go into your email, avoid distraction, wait for email to arrive, click link in email, remember what you were doing on site). I don't recommend this, because of the context switches, though you *can* implement it.

Otherwise, accept that your login page and your signup pages are targets for malicious behavior, and design appropriately.

- Rate limiting can go a fair way to preventing brute force attacks. To find email addresses, an attacker is going to need to try a lot of email addresses and/or a lot of passwords, and get a lot of them wrong. Consider throttling invalid login attempts by IP address or subnet. Check submitted passwords against a dictionary of common passwords (123456, monkey, etc) and ban that traffic extra hard. Exponential backoff (forcing attackers to try again after 1, 2, 4, 8, 16.. seconds) is useful.

- Give guidance to users about creating strong passwords. Allow easy integration with LastPass or 1Password.
- Add a 2-factor auth option to your website. Encourage users to use it.
- Warn users about malicious behavior ("someone is trying to snoop your password") and contact them about suspicious logins.

Liked what you read? I am available for hire. (https://burke.services)
Posted in Usability (https://kevin.burke.dev/category/usability-2/).

36 thoughts on ""Invalid Username or Password": a useless security measure"

1. 
   Hugo Osvaldo Barrera (https://hugo.barrera.io)
   December 1, 2014 at 11:15 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57779)

   Gmail does it too, but you can send and email and see if it bounces to check if an account exists.

   The assumption that usernames should be secret is stupid and senseless. Passwords are meant to be secret. Emails and usernames are not.
   Heck, emails would be public, were it not for spam issues.

   Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57779#respond) ↓

   1. 
      Jonathan
      December 2, 2014 at 10:16 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-59340)

      Interesting read about the topic…. I know it introduces the distraction factor, but I think that the concept of password itself is just wrong… And this article says it better than I would:

      https://medium.com/@ninjudd/passwords-are-obsolete-9ed56d483eb (https://medium.com/@ninjudd/passwords-are-obsolete-9ed56d483eb)

      Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=59340#respond) ↓

      1. 
         Michael Ekoka (http://brazen.ca)
         December 3, 2014 at 8:11 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-60521)

         @Jonathan: I believe the approach advocated in that article is what Mozilla Passwordless is about (https://hacks.mozilla.org/2014/10/passwordless-authentication-secure-simple-and-fast-to-deploy/ (https://hacks.mozilla.org/2014/10/passwordless-authentication-secure-simple-and-fast-to-deploy/)). I also remember that at the time they announced it, someone on Hacker News claimed to have used the approach for years in their company, and that users

hated it. As a result they were going back to a more traditional login. Have a read, it's the top comment in the thread https://news.ycombinator.com/item?id=8458039 (https://news.ycombinator.com/item?id=8458039) . It's an interesting discussion.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=60521#respond) ↓

2. 

Havvy

December 1, 2014 at 12:17 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57833)

Yep, doubly so if you have a non-form submission way of checking user existence, e.g. /user/:user/ as a route.

Thanks for correcting that misinformation in my mind.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57833#respond) ↓

3. 

Frans Lytzen (http://blog.lytzen.name)

December 1, 2014 at 12:28 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57842)

Heh, after an independent security review we are being forced to take this even further;
We lock people out for five minutes after three invalid login attempts. We are no longer allowed to tell users they have been locked out. So, even if they do remember their password (or even does a reset) we just have to tell them their uid/pwd is wrong when they try to log in. And for "forgot password"? Just tell the user "we have sent you an email – IF we recognised the email you put in".

As for rate limiting; Doing it well can be a fair bit of work. I simply put an artifical one second delay into any response where the uid or password was wrong. Short enough to not annoy real users, long enough to effectively prevent brute force attacks. And even if someone did try brute force, monitoring would pick that up long before they tried a meaningful number of combinations.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57842#respond) ↓

1. 

Nigel (http://www.safeplaces.co.uk)

December 1, 2014 at 1:48 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57921)

Interesting point. It is this info leakage that lets me as a human recover site passwords when I've forgotten them.

However, there are ways to ensure that this attack can't be used against you. For one, if you have your own mail server you can use a unique email address for each site. This kills this exploit, because the attacker has to guess from a near infinite range of possible username emails.

Also, since the attacker would have to write custom scripts to attack a website where it requires a different route to determine the username, it stops a huge range of automated attack scripts. Stopping drive-by script kiddies removes a huge risk.

What we could do with is a different route. Perhaps simply emailing the account holder a reset after 5 failed attempts, in addition to rate limiting, etc. Of course this also gets annoying when the script kiddies are running a botnet against your log in page. I've had 44 emails alerting me to auto-blocked IPs of hackers in the last 5 days. With a huge site with thousands of users, that would in itself become a DDoS of the email servers!

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57921#respond) ↓

2. **James (http://knowthen.com)**
December 1, 2014 at 7:37 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58313)

Conventional wisdom shattered… Nice article!

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58313#respond) ↓

4. **Charles Feduke (http://www.deploymentzone.com)**
December 1, 2014 at 12:58 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57870)

I was just having this discussion with a co-worker recently and neither of us thought of the fact that the sign up process bleeds this information anyway!

I disagree with adding two factor authentication as a general recommendation outside of very sensitive data. (On the flip side, its appalling that none of the banks or financial institutions I've worked with won't even permit two factor authentication.)

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57870#respond) ↓

5. **Vic Metcalfe**
December 1, 2014 at 2:30 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57972)

I've implemented this as you suggest by sending the email either way and not disclosing the existence of the account. For me it was a privacy issue as this was for a job board, and we wanted to be sensitive to job seeker's privacy.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57972#respond) ↓

6. **Conan**
December 1, 2014 at 2:34 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57978)

On top of the concerns about exposing sensitive email addresses for signups to services that might have larger repercussions (hey, person@gmail.com (mailto:person@gmail.com) just signed up for a subversive website!), the other thing is that you shouldn't allow people to sign up for an account without confirming that account – I shouldn't be able to sign you up for fascists weekly without confirmation that I actually own your email address.

Emails are public individually, but correlation between emails and accounts on certain websites can be sensitive information. For example, some people would be very interested in the email addresses associated with underground marketplaces.

So don't leak email addresses unless you're comfortable with making a choice for your users on the security tradeoffs of known users of your service in a larger scale, and expect that your users that have shared passwords between sites are going to be ok with their accounts being trivially compromisable on a short basis. (AKA, anytime someone decrypts/discovers a password, expect a pass of trying that password anywhere that username is confirmed is going to take place). If you're storing any sort of sensitive information, or information that could be used to compromise other accounts, best not to affiliate those usernames with your service. See Mat Honen's stream of service compromises to lead to ownage of his twitter account.

The goal isn't to be un-ownable, it's to increase the cost of attack, and making sure that attackers cannot identify who your users are increases that cost.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57978#respond) ↓

7. **Alex Smith (https://alexsmith.io/)**
   December 1, 2014 at 2:35 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-57981)

Honeypots are also very useful in detecting malicious behavior and have very few repercussions on real users.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=57981#respond) ↓

8. **Amber**
   December 1, 2014 at 4:37 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58134)

Note that if you do go the rate-limiting path, be careful not to implement it in such a way that a malicious individual can easily lock the rightful owner of the account out by spamming login attempts.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58134#respond) ↓

9. **Michael Chermside (http://mcherm.com/)**
   December 1, 2014 at 5:07 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58177)

It is not useless if you have different rate-limiting and security monitoring for login and new user registration.

The bank I work at is an excellent example. Creating an account is a heavyweight process with several controls, and we do NOT want to leak information about what accounts exist to everyone capable of attempting logins.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58177#respond) ↓

10. **Justin Koreska**
    December 1, 2014 at 7:35 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58311)

Dude, thanks for posting this and "correcting that misinformation in [our] minds".

I chuckle at how widely held this reasoning is among developers who think they know what they're doing (like me, having made this argument to clients and UX people) and yet they never thought twice about the signup page!

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58311#respond) ↓

11. **James (http://knowthen.com)**
    December 1, 2014 at 7:39 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58314)

Conventional wisdom shattered… Nice article!

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58314#respond) ↓

12. **Brian Rue (https://rollbar.com)**
    December 1, 2014 at 8:17 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58343)

Great post – agree in full. Question: any tips on how to "allow easy integration with LastPass or 1Password"?

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58343#respond) ↓

1. **kevin** Post author
   December 1, 2014 at 8:48 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58373)

   Nope haha but something they should really think about

   Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58373#respond) ↓

3. **Brendan Ashworth (http://blog.ashworth.in)**
   December 1, 2014 at 8:26 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58353)

Great article! I had given thought to this previously but never really followed through, I'll be sure to fix it up in my applications. It is funny / ironic how something as commonplace as this would go so unnoticed, right?

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58353#respond) ↓

4. **Eric Wilson**
   December 1, 2014 at 8:29 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58356)

This depends on the system though, there are plenty of smaller systems that still do manual account creation. I often build internet apps that validate to active directory and we most certainly do not have a self serve approach to creating domain users. I also would not disclose/advertise if email address is acceptable in the username field.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58356#respond) ↓

5. **Marten**
   December 2, 2014 at 11:10 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-58873)

Let's assume the user inserted a wrong username, this username is registered, though. User gets an error message stating that the password is wrong:
User is left confused.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=58873#respond) ↓

6. **Markus Unterwaditzer (https://unterwaditzer.net)**
   December 2, 2014 at 1:48 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-59008)

I think a detail you might be missing for some services is that Captchas block automated queries for used emails well enough, while nobody would dare putting a captcha on a login page.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=59008#respond) ↓

1. **FooCap**
   December 17, 2014 at 9:32 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-71733)

I've seen at least 2 sites which do have captchas on the login page.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=71733#respond) ↓

7. **Šime Vidas (http://webplatformdaily.org)**
December 2, 2014 at 3:38 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-59098)

What are your thoughts on passwordless authentication? (Meaning, no sign up, no password. User enters their email address. Site sends an URL with an one-time token via email. User follows that URL. Site confirms user's identity and uses token in URL to set user's session cookie. User is permanently signed in – unless they manually sign out, of course.)

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=59098#respond) ↓

1. **Marco Barbosa**
December 5, 2014 at 6:44 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-62277)

I would be also interested to know the authors opinion on passwordless authentication.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=62277#respond) ↓

8. **Benjamin (http://twitter.com/benjaminnetter)**
December 5, 2014 at 5:44 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-62244)

I don't think you understand why most services say "Wrong e-mail or password". It's not because it's more secure, it's because on the back-end side, you don't really know which one is wrong.

If you ever implemented authentication, you know how it works. You get an e-mail and a password, and you do a find on your database with both values as email='your@email.com' and password='thep4ssword'. You either have a user, or you don't. But you don't know if it's because the user doesn't exist or if the password is wrong.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=62244#respond) ↓

1. **kevin** Post author
December 5, 2014 at 1:15 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-62701)

I don't get it. Why don't you fetch the account record by email and then compare passwords in code?

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=62701#respond) ↓

2. **Markus Unterwaditzer (https://unterwaditzer.net)**
December 6, 2014 at 9:46 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-63596)

That's not how password checking should ever be implemented at all, since passwords should not be stored on the server.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=63596#respond) ↓

1. **Gabriel**

December 9, 2014 at 5:57 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-66574)

> You mean passwords should not be stored in clear text on the server – the hashed passwords must be stored somewhere. And what kevin meant was selecting by email and then comparing the hashed password from the login form with the hashed password from the user record instead of selecting for the existence of a given email/hash combination.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=66574#respond) ↓

9. **Blaine Cook (https://poetica.com)**
December 5, 2014 at 6:39 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-62264)

Glad to see others talking about this stuff. We do a similar thing with some added magic at Poetica. I wrote up a post a little over a year ago on how we approach the problem: http://blog.romeda.org/2013/06/thoughts-on-signin.html (http://blog.romeda.org/2013/06/thoughts-on-signin.html)

Our thinking has evolved in subtle ways that make things easier for our users; I encourage you to try the Poetica sign in to get a feel for it!

We'd love to release it as a service (or, better, open source) once we have some spare cycles, but in the meantime encourage anyone building sign in systems to consider using the approach.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=62264#respond) ↓

10. Pingback: Why you should care about e-mail verification | Snake Eyes Software (http://snakeeyessoftware.com/site/why-you-should-care-about-e-mail-verification/)

11. **Kirk Hadley**
December 9, 2014 at 8:23 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-67063)

Somewhat related: here's an excellent example of a site using the "forgot password" tool, without explicitly revealing if the email is indeed registered w/ the site: https://arxiv.org/user/lost_password (https://arxiv.org/user/lost_password)

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=67063#respond) ↓

12. **wumin**
December 10, 2014 at 8:46 pm (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-67563)

I wonder how the system tell the different between "wrong password" and "wrong username".If the username is exist and the password is wrong,perhaps user typed the wrong password,perhaps user accidently typed other's account.it can go both way.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=67563#respond) ↓

13. Pingback: What is Brute Force? | Malware Clean (http://www.malwareclean.net/2014/11/what-is-brute-force/)

14. Pingback: How Strong Are Your Passwords? | Malware Clean (http://www.malwareclean.net/2014/11/how-strong-are-your-passwords/)

5. **alech**
December 24, 2014 at 3:12 am (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/#comment-77003)

Also, even if not explicitly checkable in the sign-up form, it is quite hard to build a login system that is not suspectible to timing side-channel attacks (i.e. in almost all systems, an “invalid user” error is shown a tad quicker than an “invalid password” error). Probably not worth the effort to even try.

Reply (https://kevin.burke.dev/kevin/invalid-username-or-password-useless/?replytocom=77003#respond) ↓

6. Pingback: Декабрьская лента: лучшее за месяц | Сообщество Аналитиков UML2.ru (http://timglu.ru/?p=147)

View the source code (https://github.com/kevinburke/2013)