Schneier on Security

Home > Blog

Why I Hate Password Rules

The other day, I was creating a new account on the web. It was financial in nature, which means it gets one of my most secure passwords. I used Password Safe to generate this 16-character alphanumeric password:

```
:s^Twd.J;3hzg=Q~
```

Which was rejected by the site, because it didn't meet its password security rules.

It took me a minute to figure out what was wrong with it. The site wanted at least two numbers.

Sheesh.

Okay, that's not really why I don't like password rules. I don't like them because they're all different. Even if someone has a strong password generation system, it is likely that whatever they come up with won't pass somebody's ruleset.

Tags: Password Safe, passwords

Posted on November 16, 2021 at 5:33 AM • 82 Comments

Comments

Jason • November 16, 2021 6:07 AM

Aren't long passwords better than short ones (https://xkcd.com/936/)?

I usually use

pwgen -ync 40

to create password. But there's quite a few sites/services that don't want such long passwords or reject special chars.

Jörn Franke • November 16, 2021 6:16 AM

It would be nice if all password managers would standardize password generation options. Then the website could say: please instruct your password manager to use option x,y,z to generate the password – and that is it.
It may also boost usage of password managers and strong passwords.

Ulrich Boche • November 16, 2021 6:21 AM

Fortunately, PasswordSafe allows you to specify custom password rules if needed. Especially idiotic are custom sets of special characters for a website. Fortunately some tell you what they allow and you can copy the set into the custom rule.

I agree wholeheartedly that custom password rules are a nuisance, as well as the requirement to change the password at regular intervals.

Clive Robinson • November 16, 2021 6:31 AM

@ Bruce, ALL,

> If someone has a strong password generation system, it is likely that whatever they come up with won't pass somebody's ruleset.

Whilst true and expected, it is actually also desirable that it should be so.

If you invert the argument you get,

"All password rules should be the same"

Is perilously close to,

"All eggs in one basket"

Failings, or as others might put it,

"Lacks hybid vigour"

And that's important.

As I and others have been discussing[1] there is a great deal of importance in,

"It you build something and it works you learn nothing you did not know already, if it fails and you fix it you learn something new, success is built on failure not success."

So logically a multiplicity of rule sets gives us,

1, Hybrid vigour.
2, Oportunities to learn.

Both are desirable.

[1] https://www.schneier.com/blog/archives/2021/11/friday-squid-blogging-squid-game-cryptocurrency-was-a-scam.html/#comment-393414

Ted • November 16, 2021 6:34 AM

Oh wow! I just tried to generate a password in PasswordSafe and the first one gave me at least 2 numbers. I won't disclose it here, because it is my first test and it is in use.

But here is another example: Lj]B*U7dm)P1

Further tests show that the default password generation policy doesn't necessarily have a rule for a minimum of two numbers. But then I realized you could change the policy settings in the generator to give more numeric digits and check this out: 04(882SRj=B7

Oh my yay! Fun, fun, fun! ☺

Clive Robinson • November 16, 2021 6:37 AM

@ ALL,

With regards password managers on various devices, there is a conversation over on the Friday Squid about reasons to use or not use one and why,

https://www.schneier.com/blog/archives/2021/11/securing-your-smartphone.html/#comment-393432

So not one but to cases of synchronicity in one place at the same time…

Does that mean "Enemy action"?

Eric Hacker • November 16, 2021 6:40 AM

Passwords will never go away.

NIST should sponsor a contest to develop better password complexity scoring algorithms the same as they do for cryptographic standards.

Snarki, child of Loki • November 16, 2021 6:53 AM

The variations on "which special characters are okay" is annoying, but I guess Little Bobby Tables, AKA Robert'); DROP TABLE STUDENTS ;– might be to blame.

No, what bugs me is the pages that won't let you copy/paste from your password manager to the password box, PLUS lookalike characters if you forget to check the 'avoid similar-looking characters' box when generating the password.

0O001I11I0O1

Which is *FINE* if you see it in a decent font, but not all webpages do that.

Bill • November 16, 2021 8:34 AM

The NIST has already advised on passwords, and issued guidelines a couple of years ago — recommending LESS COMPLEX passwords (no rules) in favor of longer passwords.
They cite research indicating that complex passwords are not harder to crack, and are much harder to remember (which is why people write them down, or now use password managers). Longer passwords, on the other hand, can be easy to remember as phrases or strings of words, etc. Longer passwords are harder to crack.

Frederi • November 16, 2021 8:36 AM

The worst i have met are websites that force you to follow password rules, but prevent you from copying/pasting passwords…

Scott Raun • November 16, 2021 8:38 AM

The reason I hate everyone's password complexity requirements is because practically no one tells you what they are until you haven't met them!

Joe Schumacher • November 16, 2021 8:46 AM

Would all sites having the same standard only help adversaries with better formulating their brute force attack?

Joe • November 16, 2021 8:48 AM

Would all sites having the same standard only help adversaries with better formulating their brute force attack?

Paul • November 16, 2021 8:53 AM

I've found that most financial sites have very short limits on password lengths and often get confused by any punctuation. It seems they may be passing the input directly to their 20 yr old MVS system or they only want to support passwords someone with a touch phone can enter?

In my head, I know that a completely random, 15 character password should be fine, but something tells me that a 33, 44, 55, 66 completely random character password is better.
It isn't like I'll ever remember these or ever actually type them in, so if I must have a password at all, why not allow 15-4K as the length boundaries and disable complexity mandates after 30 characters?

Hopefully, everyone here is using a password manager, perhaps a U2F token for 2FA. My bank sent out a branded RSA key when I ask years ago for free, but they have never made it mandatory to use, if you have one. That seems foolish to me. Allowing people to use less secure methods should only be allowed if they call in and speak with a bank employee trained on anti-phishing conversations.

Remember at one bank, they asked me for a few answers to the security questions when I called them to report a login failure bug. Seems she could see those. I always use random answers for all their “security questions” … and told her that. She was convinced I was me when I said the last 4 characters for my dog’s name was $9rP and it was about 30 random characters.

The entire “site image” stuff is a joke.

Laurent • **November 16, 2021 9:04 AM**

My personal way to accommodate the rules is:
– create a long secure password with letters only
ex: lqpkdfanptnolofhtji
– Add the requested constrains:
ex: lqpkdfanptnolofhtji.1A

The security of the final password is the security of the initial one (20 alphabetical characters should be fine).

The only problem is when the constrain is to make the password shorter. If the length limit is 12 characters, my final password has the secirity of only 9 alphabetical characters.

Chelloveck • **November 16, 2021 9:22 AM**

@Scott Raun: Or tell you what they are, but in vague terms. “One or more special characters like ! @ #” and then reject things like ‘<' or ';'. Even better is the login page I saw that listed the section sign (U+00A7, §) among the examples of acceptable symbols. Right, like I'm going to trust that your coders can stick to a consistent codepage or Unicode normalization.

And then there are the sites which silently mangle passwords on the password change form, but *don't* apply the same mangling rules on the login page.

William Entriken • **November 16, 2021 9:27 AM**

NIST has published guidelines on what types of passwords should be accepted for login systems. We should promote and share solutions to the problem.

https://pages.nist.gov/800-63-3/sp800-63b.html

Specifically the relevant recommendation here is: Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.

Aaron • **November 16, 2021 10:23 AM**

I’ve been befuddled before by a financial website when it rejected my password which was auto generated from a password manager. First, my password was to long; seemed their limit was 10 digits. Second it wasn’t that they didn’t want special characters, it was that they only wanted one special character. Then I had to make sure my digit was not at the beginning of the password. After I finally made a successfully adjusted password and logged in… I wrote the bank customer service and righteously gave them hell for actually making password security weaker with such nonsense. I no longer have to deal with the site but they are now at least incorporating two factor authentication; wondering if I got through to them or they had a security breach.

---

zenon • November 16, 2021 10:34 AM

@jason Re: XKCD scheme

Although longer passwords are better than shorter passwords, if you click through on the "Sheesh" link that Bruce provided, that resolves to https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html . In that article, he explicitly notes:

"This is why the oft-cited XKCD scheme for generating passwords — string together individual words like "correcthorsebatterystaple" — is no longer good advice. The password crackers are on to this trick."

I won't try to expand further on Bruce's excellent explanation (and good follow-up comments), but it is noteworthy that that post was made in March of 2014 .

Tim • November 16, 2021 10:42 AM

@clive

> Whilst true and expected, it is actually also desirable that it should be so.

rolls eyes

Usability has a huge impact on how people interact with systems. If you purposely make the experiance different from site to site – users will take shortcuts including making weaker passwords. A common "password standard" would benefit everyone greatly and reduce risk over all.

Iain • November 16, 2021 10:56 AM

Personally, I don't necessarily mind the differing rulesets for passwords across different sites. What really annoys me are those sites that don't provide the full ruleset, and also don't correctly check the provided password against the mystery ruleset, which then allows the password creation/change but then doesn't accept the password upon login. This tends to happen mainly with backslashes, not sure why.

Aaron Toponce • November 16, 2021 10:59 AM

I'm personally a fan of Apple's Keychain password generator. You're guaranteed 1 uppercase, 1 digit, 1 nonalphanumeric, and the rest lowercase. The security margin is about 72 bits.

Granted, this wouldn't meet Bruce's bank's requirements in that they need 2 digits, but in most cases, this never fails.

Some examples:

1ojwih-himgar-zyGbuq
xyvka9-nAnwov-wodqub
hizri4-vagqec-wIxnav
vynwa7-nigtah-jYjpom
ziqzag-5ikQes-tehcaf

Len • November 16, 2021 11:06 AM

I've used a system that rejected passwords that didn't meet the rules but didn't tell you what the rules were! I just had to keep trying until I came up with something that worked.

Clive Robinson • November 16, 2021 11:36 AM

@ Tim,

> Usability has a huge impact on how people interact with systems.

sad shake of head

Then why after the biblical lifetime are we still using a system that we have known from day one is broken?

Seventy years ago when people first started thinking about passwords for computer security, computer resources were so expensive in terms of storage that passwords made sense. Also the only human interface other than switches and light bulbs were old fashioned teleprinters going back fourty or fifty years before then.

We have kind of moved on, bio-metrics has come and more or less been found to be wanting in much the same way four digit PINs are.

We've even tried moving the PIN onto a token that produces a TAN or equivalent.

The simple fact is user authentication sucks, either it is insecure or not fit for purpose.

Arguably passwords need to be up in the 100-200bit equivalent, the human mind can do maybe 24bits of random digits and depending on who you talk to less with random alphas.

So we try using words from a list which have betwen 8 and 12 bits depending on the list size, but again only as random, humans will try to rearange the word order to make it more memeroble, then depending on other measures those words could be as few as 4bits each.

Pass phrases tend to get selected from common sources such as songs, poems, dialog and have as little as 2bit per word…

So you are back to a random password for security…

Passwords that have any kind of human determination in them are weak, a lot weaker than people think, and length realy has little to do with it.

To see why, guess the last two letters of,

“TheCatSatOnTheM”

Or,

“L1v3L0ngAndPr0sp”

Or a whole bunch more.

Andrew MacCormack • November 16, 2021 11:40 AM

Some kind of easy machine-readable standard encoding of password rules, a bit like a geek code?

L8-16 1-Cap 1-Low 1-Num 0Special 0Unicode (8-16 chars allowed, 1 or more caps, 1 or more lower case, 1 or more number, 0 special chars, 0 unicode)
L12-32 2-Cap 1-Low 1-Num 0-Special 0Unicode 0#; (12-32 chars, 2 or more caps, 1 or more lower case, 1 or more number, 0 or more special chars, 0 unicode, # and ; not allowed)
L16- 0-Cap 0-Low 0-Num 0-Special 0-Unicode 0Pwned (16 character or up, no enforced chars, checked against haveIbeenPwned database)

---

mrfox • November 16, 2021 11:47 AM

Many years ago, my bank – a major US financial institution – wouldn’t accept account passwords with characters other than [a-zA-Z0-9] or longer than 8 characters.

Their help pages mentioned “WILL1AM” as an example of a good password. Certainly no evil haxxor could figure out such clever spelling tricks! I am not making this up.

From what I can tell, things are mostly sane these days, and most sites will accept a secure password.

There is still the idiocy of disabling paste in password fields – who came up with that?? why?!? – but it seems to be falling out of favor, too, and a short snippet of javascript, stored as a bookmark, fixes the problem. There’s also a browser plugin for that IIRC.

Chris • November 16, 2021 11:53 AM

In addition to poorly defined password rules (given only after you’ve had one rejected), another poor practice is to require user names to be something common, often an email address. This makes it easy for hackers to target many of a person’s accounts, since breaking one usually leads to a cascade of other broken accounts. I prefer to generate user names using a random string generator like the one in PasswordSafe.

Oh yes – every password rule makes it easier to crack the password, by decreasing the possible entropy of the allowed choices. Other than reasonable hardware limits, there should be no rules.

Austin • November 16, 2021 11:55 AM

Still better than many banks that either truncate the password to only 6 or 8 characters or drop out all special characters.

I tested this on a small credit union and could put anything or nothing after the first six characters and it still authenticated. On another city government payment portal if you left out the special characters from your password it still would authenticate.

I'm sure it was a legacy unix setting to conserve storage or cup processing hash but still shocked it was still this way.

The bank responded and after a while it had been increased (not sure how many characters) but the government office never replied.

Guy • November 16, 2021 12:26 PM

Can't help but think that passwords, as A Thing, are the wrong abstraction here. We've gotten to the point where the work needed to use any given gizmo rivals the utility of the thing itself. Why can't everyone just send me an OTP on a side channel and be done with it?

Tom Rollins • November 16, 2021 12:26 PM

That is incredible.

It makes me want to create a website that uses a password rule that requires the use of all four characters 'l', '1', '0' and 'O' in the password.

After all, it's important to have a mix of lowercase and uppercase letters and numbers.

---

jamez • November 16, 2021 12:30 PM

@clive, you make good points, but don't let them be dragged down by poor ones. in the case of "TheCatSatOnTheM" and "L1v3L0ngAndPr0sp" while a human can easily finish those, a computer can't. plus (as we all know) when cracking a password it's all or nothing, not like in the movies where it gets decrypted one character at a time and the cracker could help by finishing the job manually.
but the latter password has decent entropy and would actually be pretty good–if it weren't just dictionary words with standard substitutions.

Gilbert Fernandes • November 16, 2021 12:54 PM

What annoys me the most is the length limitation. I like to use KeePass to store my passwords, and I like to use random.org to generate passwords, then mix them, and I wrote a python script that adds a random amount of UTF-8 asian + various characters at random so I get a very long and secure password.

They are so long and complex that I don’t even try to type them.

First problem I meet : websites that limit passwords to X characters. Sometimes with values as low as 8.

Second problem : websites that will let you enter a 64-character long passwords, but only record the first N chars from it. So when you come back next time, you paste the password and it doesn’t work and you have to guess how much you have to paste to enter, while avoiding an account lock.

Third problem : websites that are so badly programmed they can’t even apply their own rules. I have this at work currently : they want a password with numbers, lower case and upper case and symbols. I create a password that has several numbers, several upper, several lower, and several symbols and it FAILS to be accepted. This, being a developer myself, drives me absolutely nuts. Because they can’t even make a Regexp properly. And when you put your hand on the person that wrote that crap and see the code, they did not even use a Regexp but a series of .contains().

Passwords should be something like 128 or 256-chars wide. Full UTF-8 including any langage : egyptian glyphs, asian-langages symbols, old tongues from previous millenia. Perhaps a standard needs to be pushed for 256-char full UTF-8 range + a generator based on proper random source to generate such very-strong passwords. I don’t know.

Passwords might not be the future, but those limited to 8-chars are surely not.

Winter • November 16, 2021 1:03 PM

@jamez
“but the latter password has decent entropy and would actually be pretty good–if it weren’t just dictionary words with standard substitutions”

Not really. As you already mention, 1337 5p34k is a very simple substitution cipher. And any combination of characters found by Google search has a theoretical strength in the order of ~70 bits (very optimistic).

Any type of order, or trick, in your passphrase makes it predictable to a smaller, or more likely, larger extend. You lose password strength much faster than you think, whatever you think.

What helps a little is to increase the length. Many password crackers cannot handle very long strings well and will run out of memory. They will find a solution to this, eventually.

Jeff R • November 16, 2021 1:08 PM

We spend a lot of time talking about password complexity, length, and how random… but is that important?

What are we trying to protect against with all of these rules? What are the real threats to a password in 2021?

For many reasons, passwords should be

Not easily guessed

Unique

I protect passwords as a primary day-to-day responsibility for organizations of every size since 2010, yet I can only say that password cracking and brute forcing attacks are very uncommon. This is not because passwords got stronger.

Brute forcing and cracking were common in the past but are no longer valid concerns for most passwords because:

Login prompts no longer allow “guessing and bruting” attempts

It is best practice for applications to store passwords hashed using a strong cipher

For those limited number of systems, like Windows and legacy systems, there will be additional rules to enhance security. 95% of people don’t need 95% of their passwords to be long and complex.

They should have:

Authentication backed by a second factor

Systems that are not easily allowing an attacker to reset credentials

Please inform me if I’ve gone astray. Some of my most secure accounts are protected by a 5 character password (haven’t changed it since 2005) and I’m not afraid.

Dave • November 16, 2021 1:09 PM

It seems this could be mitigated quite a bit for websites, if there was another HTML INPUT tag attribute for the password input that describe the password rules, in such a way that a password generator could use it. If a browser could also parse it into human language, that would make it even better. It there were a set of standardized pre-defined rules, that could make this easier.

David Hess • November 16, 2021 1:26 PM

I have tried to use some sites where registration allows a longer password than the login, so once you are registered you are locked out if you used a longer password.

Anil • November 16, 2021 1:57 PM

There is an html attribute “passwordrules” which I think made it into Safari 12. Note sure if other browsers adopted it though. https://github.com/whatwg/html/issues/3518

Artur Sapek • November 16, 2021 2:22 PM

My favorite are ones where there’s a maximum length, implying they don’t even hash the password and store it in a varchar(x) db column

---

Me • November 16, 2021 2:37 PM

I agree that the worst “rule” is on password length.

Not only because it limits entropy, but because it implies that the backend storage is just plopping the password into a database, no hash, so salt and no pepper.

A1987dM • November 16, 2021 2:39 PM

My Google password is one of

GpOct*4OemGoldLists
}GoldOwe2OddsGbLid
#GallonOnOne2GpsLid
GotOOn}Ground1Lies
GodOilOem%GearLens6

> GivesOsOnGrant8Log
> [REDACTED]

easy to type and to remember, passes most password rules, and still has 40-odd bits of entropy.

---

doug • November 16, 2021 3:01 PM

Not a bad idea to include a couple odd characters at the end of whatever scheme you are using. like one of these. 【ஞ 〖ʻ

your password manager probably can accept those characters.

Clive Robinson • November 16, 2021 3:26 PM

@ Joe,

> Would all sites having the same standard only help adversaries with better formulating their brute force attack?

Yes… And it would net the attackers way more accounts because ot the incresed number od sites…

As it’s putting all the eggs in one basket.

Bart • November 16, 2021 3:43 PM

I use pass, the standard unix password manager.

pass generate sitename.com

usually passes the test on the first try (20 characters by default) though sometimes I have to pass the -n flag to disable special characters. Sometimes the site requires at least one special characters but you cannot include some special characters. At this point I usually give up.

Clive Robinson • November 16, 2021 3:48 PM

@ Laurent,

> Add the requested constrains: ex: Iqpkdfanptnolofhtji.1A

Has the advantage that you can use a simple rule for adding the constraints that would be easy to memorize, so not have to be stored with the actual password.

Thus gives you a little extra protection should your Password Manager contents become known to an adversary.

@ ALL,

It's a point that many miss, but a true random paswword concatonated or interleaved in some way with a site specific prefix, suffix or both that is far from random, and is easy to remember or work out means that you only store away incomplete passwords that are not of use to an attacker unless they have seen you type in a suffix etc AND can work out what the pattern/rule is you use.

They have to get the whole password right within three or for tries on a live system or grind through one heck of a lot of combinations on a password cracking system.

It not only strengthans your password, it also gives you a measure of extra protection should your password manager contents become known to an adversary.

However do remember that those random passwords do have to be different for every site otherwise you are in effect doing the equivalent of "reusing a OTP" thus alowing an easy attack in depth.

Paul • November 16, 2021 3:54 PM

Sites disallowing some special characters is the worst. "It's gonna lead to SQLi or OS injection". Well, what the heck are you doing with my password. It should go from request.POST("password") to scrypt (or something) to your database and not be used in cleartext anywhere.

To verify, scrypt.verify(request.POST("password"), value_from_the_database)

So to be clear, where is request.POST("password") being used ***IN_ANY_CONXEXT*** other than the storage or verification of my password?

Look at the rules for an AWS password. They are insane.

SpaceLifeForm • November 16, 2021 3:57 PM

@ mrfox

> There is still the idiocy of disabling paste in password fields – who came up with that??

There is actually some logic to that. The idea is to keep the password out of the cut and paste buffer, where it could possibly be exfiltrated, or accidently pasted later into another formbox.

Clive Robinson • November 16, 2021 4:03 PM

@ Iain,

> What really annoys me are those sites that don't provide the full ruleset, and also don't correctly check the provided password against the mystery ruleset,

The ones that "rattle my bars" as it were are the backend systems having one set of rules, but the front end web interface having a different set of rules.

So the backend system say only alows 8chars but the web interface alows more say 12chars in some frames but only 10 or 8 in others…

Where it goes horribly wrong is when it comes to changing passwords where the backend system wants you type them in twice, but the front end designer fails to handle it properly or worse trys to be cleaver by "comparing two web form entries" on the web interface rather than send it to the backend service "as is"…

---

lurker • November 16, 2021 5:05 PM

@doug. 【ஞ 〘'

your password manager probably can accept those characters.

Maybe my password manager can, but can some random website? I've had a couple recently who ought to know better but insisted (without saying so) on nothing outside a-z,A-Z,0-9. They didn't deserve my business…

Clive Robinson • November 16, 2021 5:26 PM

@ Jamesz,

> in the case of "TheCatSatOnTheM" and "L1v3L0ngAndPr0sp" while a human can easily finish those, a computer can't.

I think you missed my point

They are very common well known phrases which should “never be used” as password crackers have these in their databases.

All I’ve done is a little obfuscation by in the first case capitalising the initial letters of each word (so the last two are “at”). And in the second use “leet speak” substitution (so the last two should be “3r” not “er” as some might think).

The point is password crackers have these two obfuscation rules built in as standard, along with many others including different countries keyboard mappings.

So whilst the might make the search by a password cracker longer, those passwords will be searched for so found.

In effect the substitution is known.

So what effect does it have?

The base phrase “thecatsatonthemat” is 17 lower cas chars.

This makes the brut force search space 17^26 ~1e32 or ~2^107

But with upper case letters the brut force search space is now 17^52 ~1e64 or ~2^214.

But the phrase is just one of maybe a few thousand stock phrases, lets be generous and say 8192 or 2^13 which is a tiny search space.

Now with a “known rule” of capitalise each words initial letter it only doubles the search space or adds just 1bit to it…

With eight rules it only adds 3bits of increas to the search space, so each rule adds only 3/8ths or 0.375 of a bit… Each “known rule” adds a decreasing bit value to the search space…

So the difference between a 17 char random string and known string all in lower case is 2^107 -v- 2^13

But the nieve expectation of using capitals is the search space goes up to 2^214 not the reality of 2^14…

Hence many tend to think about some immense value in such rules, where as the reality is only fractions of a bit increase if the password cracker knows the base phrase and the obfuscation rule being used.

For some reason most do not see passwords the way the developers of password crackers do…

Martin Haeberli • November 16, 2021 6:07 PM

Re pasting passwords:

I have come across sites that:
-require (very) complex passwords (yes, easily generated with password managers
-don’t permit pasting
-don’t permit the password field to be unhidden for viewing while entering.

woe betide you if
-you have unseen typos in the entry field
AND
-you are locked out after only a few tries

Clive Robinson • November 16, 2021 6:20 PM

@ Dave,

> … if there was another HTML INPUT tag attribute for the password input that describe the password rules, in such a way that a password generator could use it.

Not realy a good idea.

Think about how you might exploit that with a “Man In The Middle”(MITM) attack.

You could force people to make the weakest passwords, not the strongest.

For instance if a rule was

“Password length 6-15 chars.”

A MITM Attack could tell you

“Password length 6-6 chars.”

The result would be a lot weaker but still be within the host system rule set.

Clive Robinson • November 16, 2021 6:25 PM

@ David Hess,

> I have tried to use some sites where registration allows a longer password than the login, so once you are registered you are locked out if you used a longer password.

Yes, I’ve come across that, and also with the “change password” window as well…

It can be “frustrating” to put it politely.

Clive Robinson • November 16, 2021 6:39 PM

@ SpaceLifeForm, MrFox,

> There is actually some logic to that. The idea is to keep the password out of the cut and paste buffer, where it could possibly be exfiltrated, or accidently pasted later into another formbox.

If I remember correctly, one “window system” made the Cut-n-Past Clipboard buffer available to all open windows and all background process… Ops.

Not as it should have been “Only” the user selected forground app, and “Only” when a user selected cut or paste.

Jibby • November 16, 2021 8:04 PM

The worst is when they want a shorter password than you’ve given them, but silently clip off the unwanted characters from end of string; but then your password manager doesn’t know it, and your password fails next time you try to log in.

Michael • November 16, 2021 8:32 PM

Creating a password generator that works for (theoretically) all rulesets would significantly reduce the search space for brute-forcing passwords.

The best ruleset is no ruleset* but only if you can trust your users to generate safe passwords.

*I will accept minimum length since short passwords are never secure

---

Dave • November 16, 2021 8:33 PM

> Clive Robinson • November 16, 2021 6:20 PM
>
> @ Dave,
>
> … if there was another HTML INPUT tag attribute for the password input that describe the password rules, in such a way that a password generator could use it.
>
> Not realy a good idea.
>
> Think about how you might exploit that with a “Man In The Middle”(MITM) attack.

If I think about what bad things an adversary might do if they have the ability to inject a MITM attack on the password registration web page, I cannot imagine why they would care about changing the password rules communicated to the user.

But, regardless, that MITM on the password rules is present even without this attribute. Usually the website describes the password rules in some form, which could still be intercepted. This just puts them in a common standardized place.

But, regardless, a password manager can mitigate this by detecting weak password rules and warning the user when the rules are weak.

Terence Bennett • November 16, 2021 11:42 PM

I like TeamPassword for this reason. When you generate a password through the Chrome extension, it lets you easily select what kind of characters and how many are needed. Great app. It saves me a ton of time.

Clive Robinson • November 16, 2021 11:56 PM

@ Dave,

> But, regardless, a password manager can mitigate this by detecting weak password rules and warning the user when the rules are weak.

It could, but will it?

The reason "Protocol Fall Back Attacks" have worked in the past and still work today is that,

"Software does not warn/tell the user what protocols are in use".

This appears to be standard behaviour in the software industry. A mentality of,

1, Make it work regardless.
2, Never worry the user.
3, Users will click through anyway.

The first two appear to be "branding" and "support cost" issues, the third typical marketing dept cynicism.

If you look at the hotel industry they alow all sorts of petty fraud to get by "just to keep the customer happy". But they "swallow the cost".

Credit Card companies likewise alowed offline transactions even though they could be used for fraud "just to keep the customer happy". But they would try to make the customer, merchant, or bank "swallow the cost"

Debit Card banks positively encorage low value fraud with NFC "tap-n-pay" systems "just to keep the,customer happy". But they try to force the customer, or merchant "swallow the cost"

We are not talking small sums of money here the Card Payment Industry tries to keep it "hidden" but at one point they indicated 4% of either transactions or turnover…

That is the power of "just to keep the customer happy"…

Brand names are even more important managment does not want a "user product" getting a bad name because some idiot site developer can not be bothered to secure things properly, so why worry the user with flashing red signs or popups? After all it's more likely to be some idiot news site, magazine or food blogger site than anything important.

Cory Doctorow has a piece over on his link site about getting attacked,

https://pluralistic.net/2021/11/13/opsec-soup-to-nuts/#secured

Note his software did not warn him about the link being potentially dodgy, and his after thoughts of,

> *"I'd created my Twitter account while standing in line for a Game Developer's Conference press pass, after Ev Williams sent me an invite to the beta. I didn't think I needed a good password for it, because it was a toy that sent you updates about other people's lunches over SMS. Half a decade later, I had tens of thousands of followers and the account was key to my professional life."*

What would Cory Dotorow's accounts be worth today?

SpaceLifeForm • November 17, 2021 1:27 AM

@ Clive

Not even 24 hours has passed

Timely. Password length, cleartext in Database.

https://twitter.com/tafs7/status/1460732419833802755

1406 Data too long for column 'telispire_password'

Daniel Cooper • November 17, 2021 1:34 AM

Actual exchange with an admin.

Me:
The password I'm trying to set is DIPq$22eXAcghjt9, but I get the following error message:
New password is not strong enough.

Admin:
One of the conditions for a password is that it cannot contain dictionary words. The password, below, has DIP in it. I guessing that is the issue.

Anonymous • November 17, 2021 2:28 AM

sheesh

love to read that

100% agree

Sam Lander • November 17, 2021 4:17 AM

Just received this gem:

> …
> 3. Mandatory special character. Please be advised that the only special character that system is accepting for now is a $ character.

I almost fell of the chair with giggles.

Matthias U • **November 17, 2021 4:50 AM**

Yeah, and then there are those that have no idea how to escape characters for their database and thus refuse to allow backslashes or quotes in passwords.

Wait, we no longer store plaintext passwords, and PHP has some sensible SQL escaping these days (assuming that you remember to actually use it, natch). No matter, we still reject those characters.

The most fun I had recently was with one that accepted UTF8 for registration, but I had to hack the HTTP:POST data encoding to LATIN1 in order to log in. Of course it worked on *their* system.

John • **November 17, 2021 8:10 AM**

This is an instance where rules don't make something more secure. This rule, for example, requiring at least two numbers reduces the possibilities within the same password character space and makes brute force attacks easier if the ruleset is known. A better rule would be to check for complexity (mixture of characters) rather than just checking for a minimum count.

Jonathan Rosenne • **November 17, 2021 11:30 AM**

When they say numbers they mean digits, specifically those Arabian digits commonly known as ASCII or Latin digits. Of course the Romans did not use them.

And they should follow NIST Special Publication 800-63B, especially allow non-Latin characters and long passwords. When it is allowed, for instance in PasswordSafe itself, I prefer to use a long and obscure sentence in Hebrew.

T R Valentine • **November 17, 2021 12:43 PM**

Just today, I went to login to a site and was told my complex 20 character password had 'expired' and had to be changed. My password manager had no notes about prohibited characters for a password and the given requirements (10 – 30 characters, at least one each of upper case, lower case, number, and special character) made no mention of forbidden characters. Through a process of elimination, I determined that **/.,~|;:”‘`?** were not allowed. What should have been a simple process turned into a fifteen minute ordeal.

TROY E HEDGEPETH • **November 17, 2021 1:51 PM**

You know what grinds my gears…
Sites that do not tell you their password rules until AFTER you have created and typed in a password that doesn’t meet those rules!
Geez, tell me BEFORE I create the password?

JChristensen • **November 17, 2021 2:47 PM**

Aside from being annoying, it’s always seemed to me that such rules (at least two digits, at least one capital letter, 8-16 characters, etc.) work in favor of someone trying to brute-force a password, as they reduce the search space.

SpaceLifeForm • **November 17, 2021 4:27 PM**

@ T R Valentine, Clive, Freezing_in_Brazil

```
Through a process of elimination, I determined that /.,~|;:”‘`? were not allowed
```

This tells me they are not hashing your password properly. This tells me that there is some unexpected scripting going on, probably Perl and/or Bash.

I’d guess Bash and use of eval.

I’ll bet you they will not allow a backslash either.

I’ll bet you did not try ampersand, parens, braces, or brackets. I’m sure they would be disallowed also.

Or, you did try those characters, but your post does not reflect that because the filters ate them.

Research shell forkbomb to get the gist of where I am coming from on this.

---

lurker • **November 17, 2021 5:20 PM**

I had to actually implement password “protected” login to a website, twice. The first time I used somebody else’s pre-rolled in php, but I wondered at the time why MySQL OTB had a window open to the world…

The second time I decided to throw the task upstream, but their IIS and ActiveDomain was not a happy marriage with my Apache on MacOS. Now I put only inconsequential stuff on a webserver, no login needed.

---

mexaly • **November 17, 2021 9:02 PM**

Hadn’t we all agreed that passwords are broken?

Miksa • **November 18, 2021 7:20 AM**

@ SpaceLifeForm

My personal policy is also never to copy-paste passwords because clipboards leak like a sieve, I always autotype or if that doesn't work I type manually.

I came to this conclusion when one time at my home computer I tried pasting something, and got a string I had copied earlier that in work, inside a Ubuntu virtual machine I used for my work duties. From there it had travelled through the VirtualBox console to the Ubuntu computer hosting the virtual machines. Then through another VirtualBox console into Win7 virtual machine, and finally through the RDP connection I had running from my home computer to that Win7. Four different computers and three different console connections were no hindrance.

I also like to use clipboard managers. It's immense quality of life improvement to a history of thousands of copy-pastes in immediate reach. Just ctrl-shift-v and type a few characters.

My preferred tool for password generation is "pwgen", it creates surprisingly memorable and easy to type passwords. Very useful when configuring something onsite and autotype isn't an option, type a random 16 character password a couple times and you just about remember it. I'm just always worried how much entropy they can have when they are that memorable.

Craig S. Cottingham • November 18, 2021 10:21 AM

My biggest pet peeve around this is not telling me what the requirements are in advance. I can't tell you how many times I've generated a 15-random word pass phrase and submitted it, only to get a validation error because I need to include digits. So I switch to a 100-random character password, only to get another validation error because it can't be longer than 20 characters.

Last night I encountered an even worse version of this. I reset my password on a doctor's patient portal system to a 100-random character password, and was told it was successful and was redirected to the login page. When I entered the new password, ONLY THEN did I get a validation error that my chosen password was too long.

Uthor • November 18, 2021 11:38 AM

My folks' bank has new owners and they needed to switch to the new website and the max password length is shorter than their old bank, so security on the new bank is going down.

I have had medical sites limit passwords to 8-12 characters, which is less than I use for stupid one-off sites that don't contain personal information (I think my default is 16 characters and I go up to 24-32 for banking and medical).

---

someone • November 18, 2021 12:48 PM

Yeah, I've run into the requirement the OP complains of, more than once. I do use PW Safe and I do have custom rules, but I frequently tweak the generated pw before submission, anyway. Sometimes I want to increase the length to make a pw more robust, so I will generate two or three strings nd concatentate them. Many times, I want a pw that, should I need to type it in manually, rather than copy & paste, won't take four tries and create a lot of frustration (been there) so I will change the generated pw string and substitute for characters that are difficult to read or to find on the keyboard in marginal lighting. Sometimes I combine the two approaches. I suppose all that tends to be a bit anal. While I don't use PW Safe as efficiently as possible, I do like having the random strings to improvise from.

Garabaldi • November 18, 2021 6:02 PM

@Snarki, child of Loki

> The variations on "which special characters are okay" is annoying, but I guess Little Bobby Tables, AKA Robert'); DROP TABLE STUDENTS ;– might be to blame.

Perhaps I should find a password that *hashes* to DROP TABLES or "!rm -rf *". Of course the hash should not be passed to an interpreter, but neither should the original password. And one should not be any harder to get right than the other so both bugs are probably out there.

Freezing_in_Brazil • November 18, 2021 9:20 PM

@ All

My password rules depend on the mission [I should say that I hate them too]. For non-critical tasks [e.g. signing up to a blog] anything like

openssl rand -base64 40

will do.

As you increase complexity there are still thousands of obscure non-literal languages to use to craft never-seen-before, memorable strings.

@ SFL

> This tells me they are not hashing your password properly. This tells me that there is some unexpected scripting going on, probably Perl and/or Bash.

Yes, I could agree with that.

Who? • November 19, 2021 9:35 AM

I HATE BIOS PASSWORDS!!!

There is no way to establish a common criteria amongst manufacturers. Some accept characters like !, #, ; or +, others not. Same about uppercase/lowercase letters, passwords lengths… I will end using only lowercase letters and numbers or just a word like "supersecret".

Ok, mostly unrelated to this thread, but I need to say it. I hate BIOS passwords because there is no way to establish a common criteria that can be applied to all our machines!

SpaceLifeForm • November 20, 2021 12:17 AM

@ Miksa

Out of VirtualBox, Ubuntu, Win7, and RDP, at least it is Win7.

I would avoid the others, but I'm sure it was not your call.

Tom S • November 21, 2021 9:32 AM

What REALLY jerks my chain are websites that disable the paste function. NIST.SP.800-63b Section 5 specifically states that the paste function should be allowed

"This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

I like using passwords that are the maximum length that a site will allow but it is really really hard to type long random sequences accurately twice especially when the characters are not being echoed.

I know of international banks that are guilty of this and they ignore my protestations.

Noel • November 22, 2021 7:22 AM

Hi,

I met an investment fund site that has a password rule and I used my password manager (KeePass) to generate one, something like this:
@QrQfnV4Z&Qh9FyiCm%'

Which met their rule except in their registration form that processes the submitted password, it miss-process the password failing to just treat ' as any other character rather than the beginning or ending of text string.

Removing the trailing ' or replacing it with something else was acceptable,

I submitted the report but possibly the company too embarrassing to admit to respond to my report.

Noel

Erica • November 22, 2021 11:45 AM

I recently noticed a new feature in 1Password. When creating an account and generating a password, one of my options is "Smart Password: 1Password will suggest a password that fits the requirements for this site." Much appreciated!

Subscribe to comments on this entry

Leave a comment

Login

Name

Email

URL:

□ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

Allowed HTML <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre> **Markdown Extra** syntax via https://michelf.ca/projects/php-markdown/extra/

Preview **Submit**

← Book Sale: *Click Here to Kill Everybody* and *Data and Goliath*

Wire Fraud Scam Upgraded with Bitcoin →