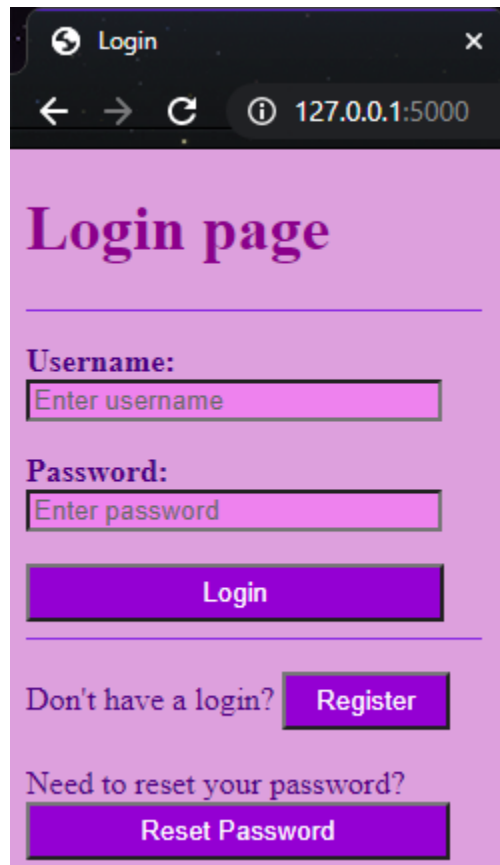


**Test case #1.** Showing new Login page and Password reset. Will try to reset password using credentials from last lab.

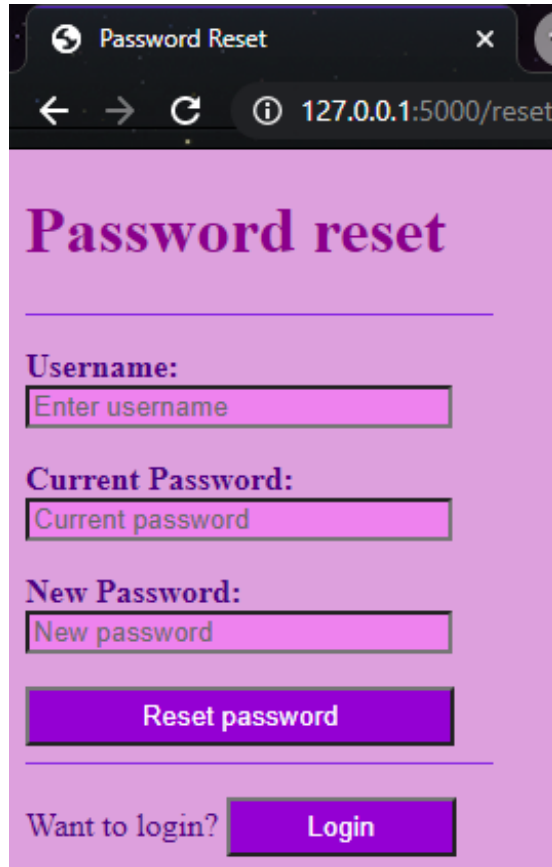
**Username:** TestForLab

**Password:** #1ComplexPassword



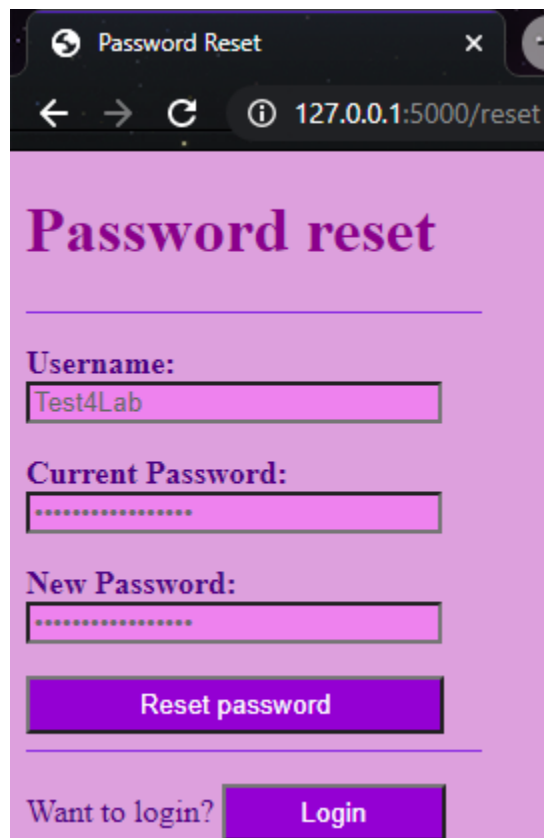
A screenshot of a web browser showing the 'Login' page. The browser's address bar displays '127.0.0.1:5000'. The page has a light blue header with the title 'Login'. Below the header, there are two input fields: 'Username:' with a placeholder 'Enter username' and 'Password:' with a placeholder 'Enter password'. A blue 'Login' button is positioned below the password field. At the bottom, there are two links: 'Don't have a login?' followed by a blue 'Register' button, and 'Need to reset your password?' followed by a blue 'Reset Password' button.

Figure 1. New Login Page



A screenshot of a web browser showing the 'Password Reset' page. The browser's address bar displays '127.0.0.1:5000/reset'. The page has a light blue header with the title 'Password reset'. Below the header, there are three input fields: 'Username:' with a placeholder 'Enter username', 'Current Password:' with a placeholder 'Current password', and 'New Password:' with a placeholder 'New password'. A blue 'Reset password' button is positioned below the 'New Password' field. At the bottom, there is a link 'Want to login?' followed by a blue 'Login' button.

Figure 2. Redirect to reset page from pressing button on login page.



A screenshot of a web browser showing the 'Password Reset' page. The browser's address bar displays '127.0.0.1:5000/reset'. The page has a light blue header with the title 'Password reset'. Below the header, there are three input fields: 'Username:' with the value 'Test4Lab', 'Current Password:' with masked characters, and 'New Password:' with masked characters. A blue 'Reset password' button is positioned below the 'New Password' field. At the bottom, there is a link 'Want to login?' followed by a blue 'Login' button.

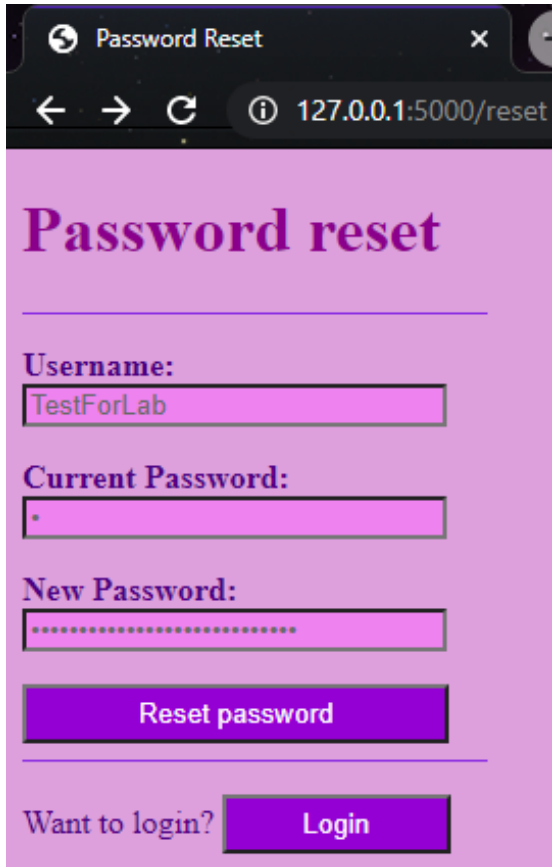
Figure 3. Trying to reset password with invalid user.



A screenshot of a web browser showing the 'Password Reset' page. The browser's address bar displays '127.0.0.1:5000/reset'. The page has a light blue header with the title 'Password reset'. Below the header, there is a red error message: 'Account with that username not found!'. Below the error message, there are three input fields: 'Username:' with a placeholder 'Enter username', 'Current Password:' with a placeholder 'Current password', and 'New Password:' with a placeholder 'New password'. A blue 'Reset password' button is positioned below the 'New Password' field. At the bottom, there is a link 'Want to login?' followed by a blue 'Login' button.

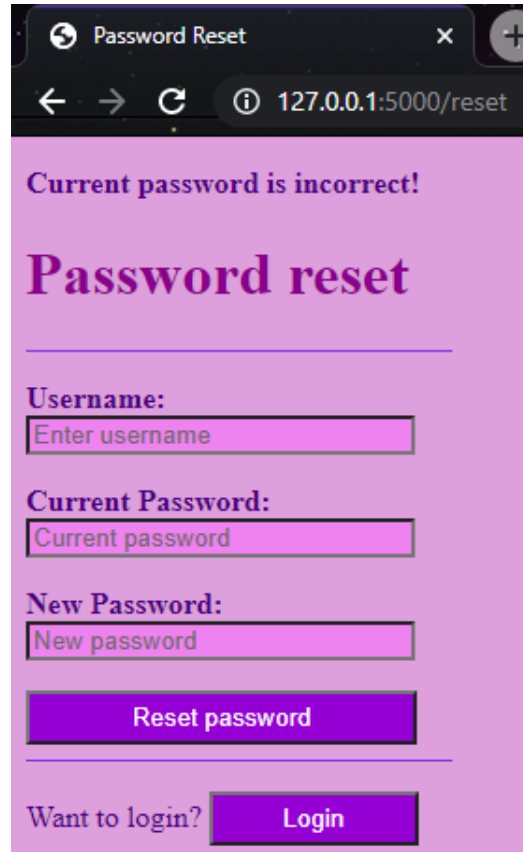
Figure 4. Flash from failed reset attempt.

**Test case #1 (cont).** Shows what happens when user tries to reset password with invalid login credentials or when new password is not complex enough.



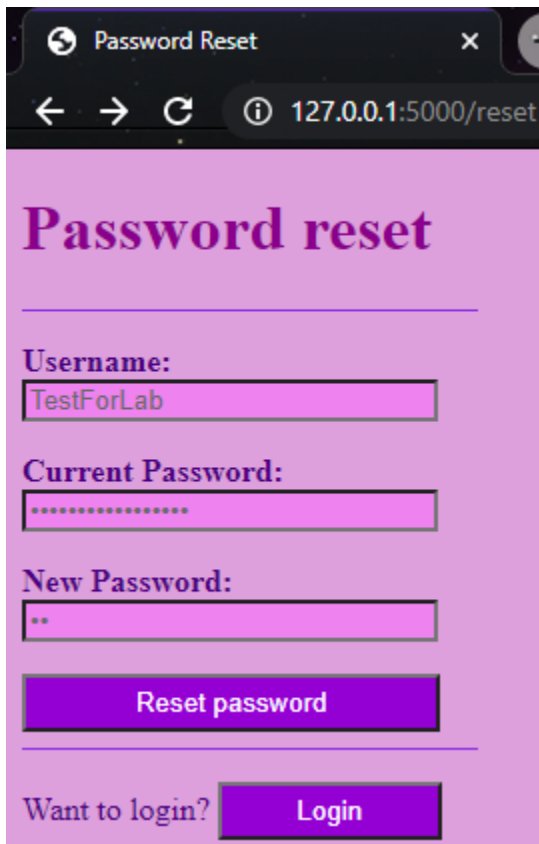
A screenshot of a web browser window titled "Password Reset" with the address bar showing "127.0.0.1:5000/reset". The page has a light blue background. At the top, the title "Password reset" is displayed in a large, bold, black font. Below the title, there are three input fields: "Username:" with the value "TestForLab", "Current Password:" with a single asterisk, and "New Password:" with a series of dots. A red "Reset password" button is positioned below the input fields. At the bottom, there is a "Want to login?" link and a "Login" button.

Figure 5. Password reset with mismatching user/pass.



A screenshot of the same "Password Reset" form, but with a red flash message at the top: "Current password is incorrect!". The input fields now contain placeholder text: "Enter username" for the Username field, "Current password" for the Current Password field, and "New password" for the New Password field. The "Reset password" button and the "Want to login? Login" link remain at the bottom.

Figure 6. Flash from failed reset attempt.



A screenshot of the "Password Reset" form, identical to Figure 5. The Username field contains "TestForLab", the Current Password field contains a single asterisk, and the New Password field contains a series of dots. The "Reset password" button is visible below the input fields.

Figure 7. Password reset with mismatching user/pass.



A screenshot of the "Password Reset" form with a red flash message at the top: "New password is not complex enough!". The input fields contain placeholder text: "Enter username", "Current password", and "New password". The "Reset password" button and the "Want to login? Login" link are at the bottom.

Figure 8. Flash from failed reset attempt.

**Test case #1 (cont).** Shows what happens when user makes a complex password with a common secret.

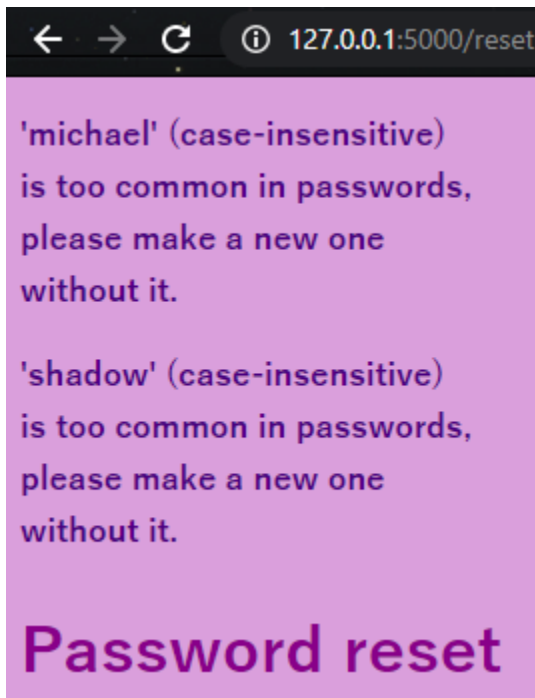


Figure 9. Reset attempt with Michaelshadow#1

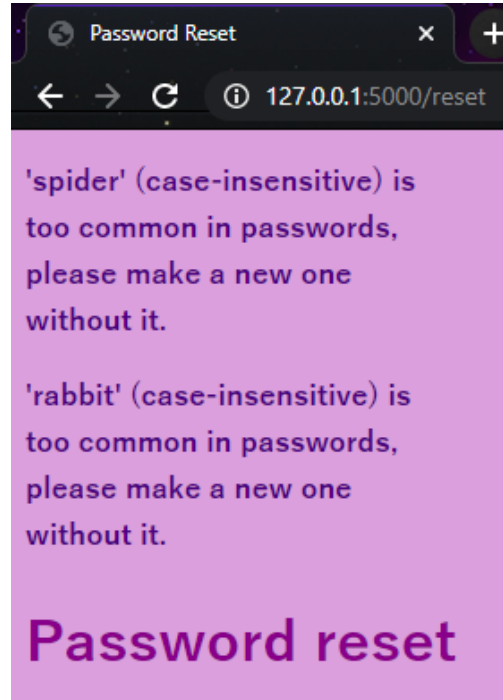


Figure 10. Reset attempt with RabbitSpider#1

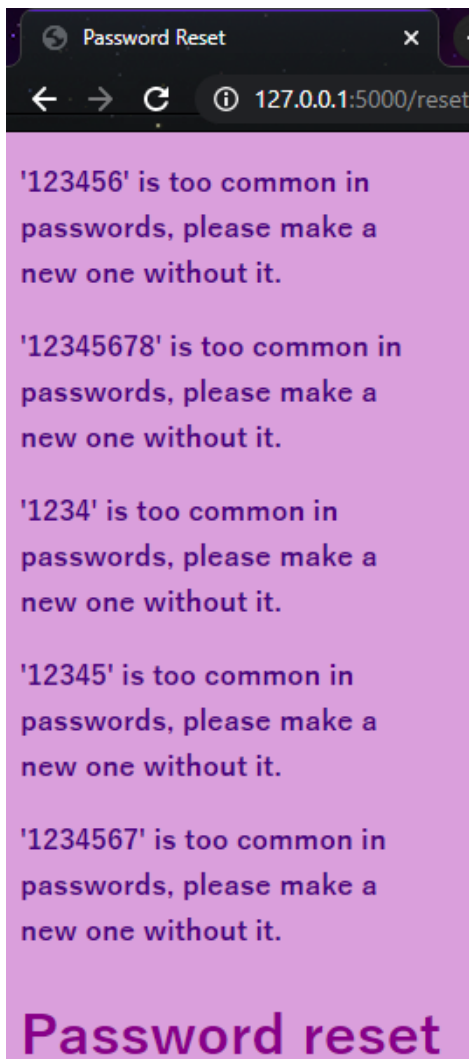


Figure 11. Reset attempt with woHEya12345678

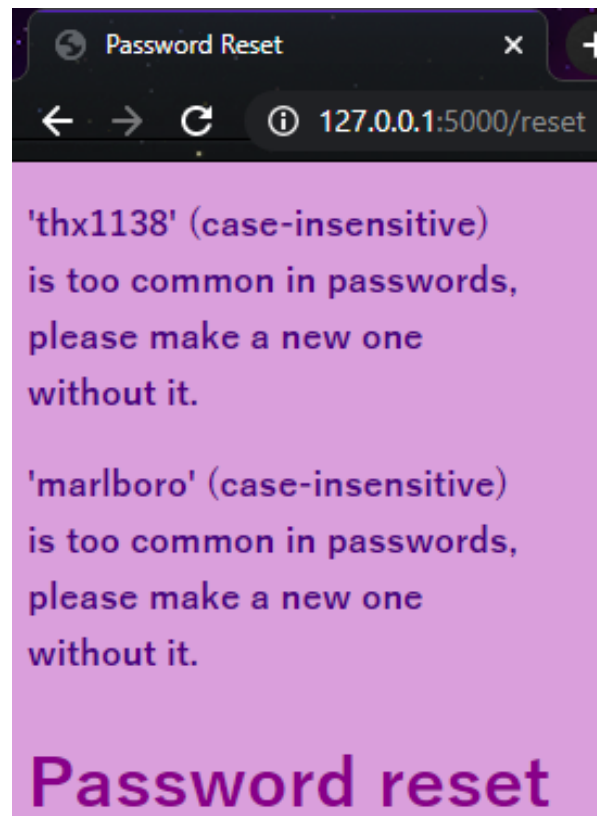


Figure 12. Reset attempt with @MarlboroHx1138

**Test case #2.** Showing what happens when a valid password reset occurs. New password: qFy^Kp78JZac@NKrPtAg



Figure 13. Successful password reset.



Figure 14. Redirect to login page and flash showing success.

```

1 TestForLab
2 $5$rounds=535000$qNM/uaA6WtfqTHp7$Jm.ML/YcijH8XNNCXiHNa.QGfj6Ybb6fmSyCk7wyK.4

```

Figure 15. Passfile before the password was reset.

```

1 TestForLab
2 $5$rounds=535000$4n04b.V6D4dhD3sA$1cTA4bLsv4TwfEdcda@nppPftdh8bwLH24laNTUdmvB

```

Figure 16. Passfile after a successful reset.

**Test case #3.** Logging in successfully with new password and showing failed log in attempts.

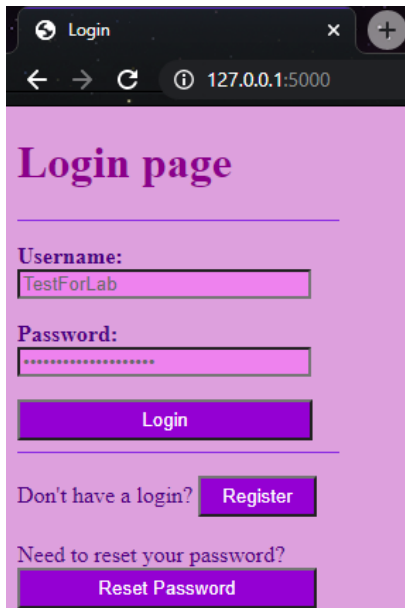


Figure 17. Logging in with new password.

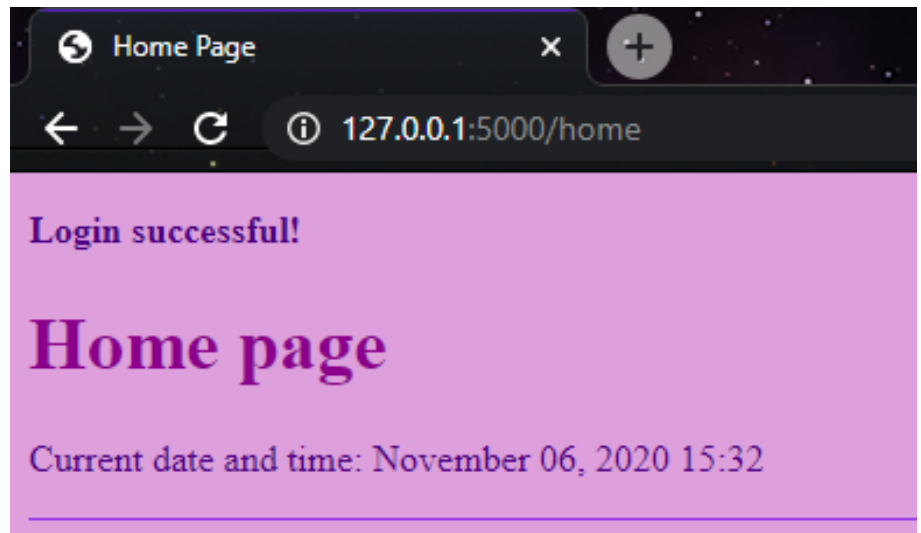


Figure 18. Login success with new password.



Figure 19. Logging in with incorrect password

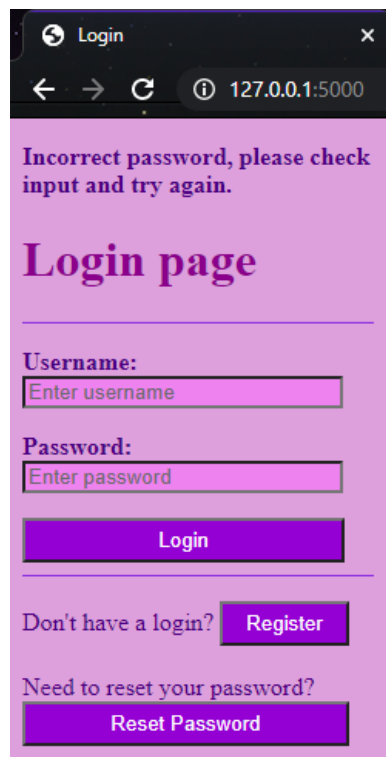


Figure 2. Login failure.

```

1 -----This file holds a log of all failed login attempts with their IP and the date/time-----
2 Failed login attempt for TestForLab from IP Address: 127.0.0.1| Date/time: November 06, 2020 15:33

```

Figure 21. Failed log in log file showing who tried to log in from what IP at what time.

#### Pylint results:

```

(venv) C:\Users\munki\PycharmProjects\lab8>pylint lab8.py

-----
Your code has been rated at 10.00/10 (previous run: 9.93/10, +0.07)

```

**How log file could be used:**

The log file can be used to detect trends in the user's log in location. If they repeatedly log in with the same IP, possibly same time(ish) of day too, then you can determine more about the user. If you use login time, you can try to figure out what time zone they are in/when they sleep. Though knowing when they sleep may seem creepy, it also means that if there is a login attempt when they should be sleeping, they could be getting hacked (or they could also be logging in at an irregular time and messing up their password). If they login with a different IP address, that isn't necessarily suspicious but it would be smart to have a verification system (2-factor authentication) to verify it is actually them. If someone with malicious intent were to access the log file, that would be problematic because they would learn usernames and IPs.

**Password Complexity:**

For the updated password complexity, all I did was check each password to see if it was in their password (regardless of case). If it showed up in their password, a message would flash showing the common secrets and tell the user to change their password.

**Decrypted messages:**

a) Morse code is easily recognizable, so it wasn't hard to crack the message:

**THIS SDEV 300 CLASS HAS SOME STRANGE REQUESTS.**

b) It took me a few tries (going down the rumkin index) to figure out how it was encoded. But then the message was instantly solved by the base64 decrypter. The message is: **So this is base64. Now I know.**

c) This one was pretty tricky, but rumkin's Cryptogram Solver made quick work of it, the message is:

---Begin Key---

**I am so clever. No one could ever possibly figure this out.**

---End Key---

I went back and solved it "manually" with this cypher:

A:	M	B:	N	C:	O	D:	P	E:	W	F:	R	G:	S	H:	T
I:	U	J:	V	K:	Q	L:	Z	M:	Y	N:	J	O:	A	P:	B
Q:	C	R:	D	S:	E	T:	F	U:	G	V:	H	W:	I	X:	X
Y:	K	Z:	L	0:	0	1:	1	2:	2	3:	3	4:	4	5:	5
6:	6	7:	7	8:	8	9:	9								