
iFruit Password Reset

EDINBURGH NAPIER UNIVERSITY

SOC09109 - GROUP PROJECT

JAKE S. SALT
40491309

Contents

1	Description	1
2	Step One	1
3	Step Two	2
4	Step Three	3
5	Step Four	4
6	Step Five	4
7	Step Six	6
8	Step Seven	7
9	Step Eight	8

1 Description

The aim of this attack is to gain control of an administrator account and steal password reset information, such as the user's email, reset token and selector in order to allow you to reset the passwords of other users and steal their data. This report will only detail how to reset another user's password, and not how to gain access to an admin account, nor elevate the access level a user has.

2 Step One

When you have access to an account with the appropriate privileges there will be a link on the navigation bar called '*Admin*'. If you do not see this link then your account does not have the correct level of privileges and will not be able to perform this task with ease (**Fig. 1**).



Figure 1:

3 Step Two

After opening the above link you will see a list of options, Users, Password Reset Data, and Bin 2 Hex will be among them (**Fig. 2**). We will start by opening the ‘*Users*’ link in order to find a user that we can target (**Fig. 3**). For this example we will be changing the password of “*Robert McGill*”, his Username is “*Bob*”, and his email is “*rmcgill@gmail.com*”. Let’s take a note of that for later.

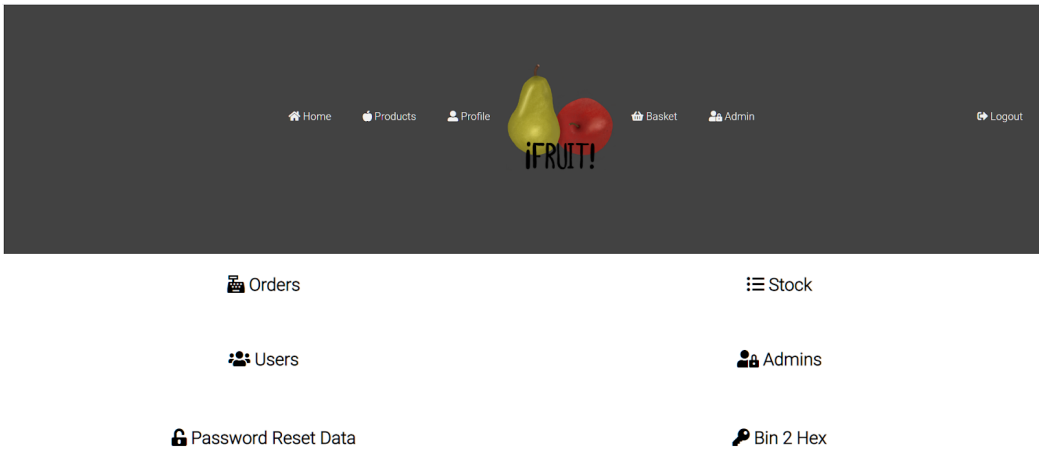


Figure 2:

Users:

User Id:	Username:	First Name:	Surname:	Email:	Profile:
1	Admin	Group	Project	email@domain.name	
2	Bob	Robert	McGill	rmcgill@gmail.com	
3	test	Test	User	test@user.com	

Figure 3:

4 Step Three

Now that we have an account to target we need to open a browser* and open up the same iFruit.com. We can then go to the login page and open the “Reset your password” link (**Fig. 4**). This will redirect you to a page where you can start the password reset process (**Fig. 6**). This is where you will need the user’s email address.

***Note:** You will need to open a new browser otherwise you will be automatically logged in, I recommend using a completely different one, i.e. Firefox and Google Chrome.

Login:

Username:

Password:

☐ Show Password

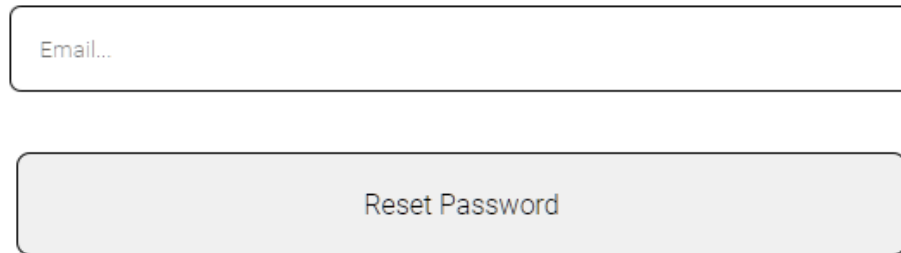
[Reset your password here.](#)

[Create an Account here.](#)

Figure 4:

Password Reset

An email containing instructions on how to reset your password will be sent to your account.

A screenshot of a web form for password reset. It features a text input field with the placeholder text "Email..." and a light gray button labeled "Reset Password" below it.

Reset Password

Figure 5:

5 Step Four

After entering the email address in the field on the “*Password Reset*,” press the “*Reset Password*” button, the page will issue a success message (**Fig. ??**). The page has successfully sent an email to the user with that account containing a “*Validator*” and “*Selector*” variable, which will allow us to change the password. To do this we need to log back into the admin account and open up the “*Password Reset*” link on the admin page (Follow steps One[2] Two[3]). This page will detail password resets for all users, we will be interested in the one for Robert McGill’s account (**Fig. ??**).

6 Step Five

Now that we are looking at the password reset data from the “*Password reset*” page, we can use it to change a user’s password. This system compiles an email that contains a link, that when pressed takes the user to a page where they can reset their password, this link is completely custom to each reset attempt and each user, making it difficult to hack, at least without an inside account. We only need two pieces of information from this table, the “*Selector*”, and the “*Token*”, the selector is already usable, but the token is in binary, so will need to be converted using the “*Bin2Hex*” page mentioned in Step Two.

Password Reset

Please check your email!

An email containing instructions on how to reset your password will be sent to your account.

Email...

Reset Password

Figure 6:

Password Reset Data:

Reset Id:	Email:	Selector:	Token:	Expiry:
21	rmcgill@gmail.com	6c4e00274fd0bf4c	\$2y\$10\$voWuwzEJz/6dmvLLXUx5e8oMH5koWt/ROISgtXefJEGPT5oolG2	1616439986

Figure 7:

7 Step Six

Open the “*Bin2Hex*” page and insert the string that we pulled from under the “*Token*” field (**Fig. 8**). After submitting the token the form will output the result in the “*Result*” field underneath the “*Password Reset Token*” field. Copy the contents of the “*Result*” field to be used later.

Bin To Hex

Password Reset Token

\$2y\$10\$voWuwzEJz/6dmvLLXiUx5e8oMH5koWt/ROIS.gtXefJEGPT5oolG2

Result:

24327924313024766f5775777a454a7a2f36646d764c4c58695578356538
6f4d48356b6f57742f524f49532e67745865664a45475054356f6f6c4732

Submit

Figure 8:

8 Step Seven

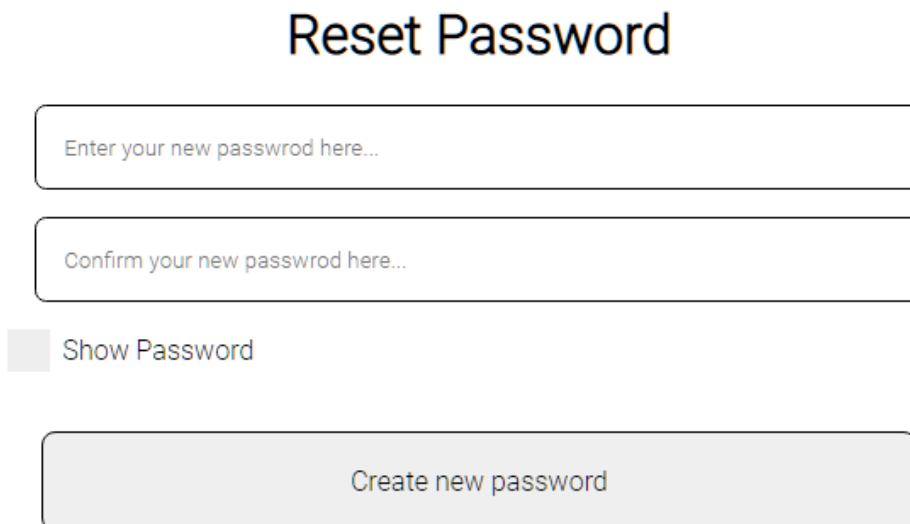
Now that we have the user's email address, the password reset selector and token we can change the user's password. We start by inputting the URL of the website, "*iFruit.com/pwdReset/newpwd.php?*", and adding "*selector=*" followed by the selector found in Step Four, which in this case is "*6c4e00274fd0bf4c*", followed by "*validator=*" and inserting the hexadecimal value we found in Step Six,

"24327924313024766f5775777a454a7a2f36646d764c4c586955783565386f4d48356b6f57742f524f49532e67745865664a45475054356f6f6c4732".

The final URL will look something like this,

"http:iFruit.com/pwdreset/newpwd.php?selector=6c4e00274fd0bf4cvalidator=24327924313024766f5775777a454a7a2f36646d764c4c586955783565386f4d48356b6f57742f524f49532e67745865664a45475054356f6f6c4732".

The page will load and look something like this (**Fig. 9**).



Reset Password

Enter your new password here...

Confirm your new password here...

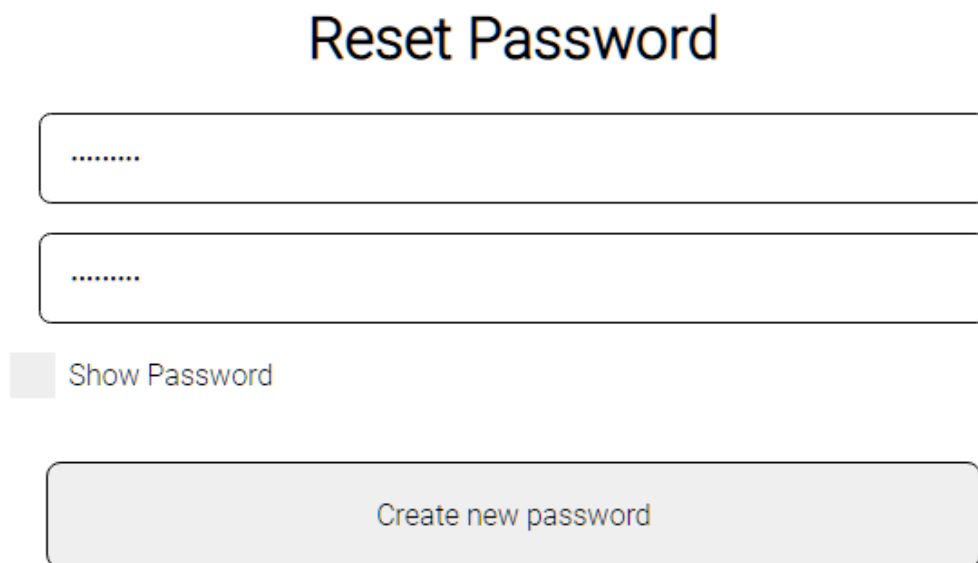
☐ Show Password

Create new password

Figure 9:

9 Step Eight

Enter a string of characters into Form and press the “*Create new password*” button (**Fig. 10**). The website should then redirect you the “*Login*” page and the URL should read, “*iFruit.com?newpwd=pwdupdated*”, this means that the password was successfully reset and you can log into the user’s account using the new password.. If the URL reads, “*iFruit.com?newpwd=empty*” the reset attempt failed and you will need to retry, making sure that you copy the email address, selector and token correctly.



Reset Password

.....

.....

☐ Show Password

Create new password

Figure 10: