

[<-- home](#)


Paypal 2FA Bypass

October 22, 2016

Recently I was in a hotel needing to make a payment, there was no phone signal so I could not receive my Two Factor Auth token. Luckily for me Paypal's 2FA took less than five minutes to bypass.

Proof of Concept

Step 1: Login with a valid username and password, click on the "Try another way" link.



Receive a Text

We'll send you a text with a special code. Just tell us which number to send the text to.

XXXXXXXXXX

Don't have your phone handy? [Try another way](#)

Send Me the Text

Step 2: Enter any answer for security questions.

Verify your account

We don't recognise the device you're using.

Answer security questions

What's the name of your first pet?

test

What's the name of the hospital in which you were born?

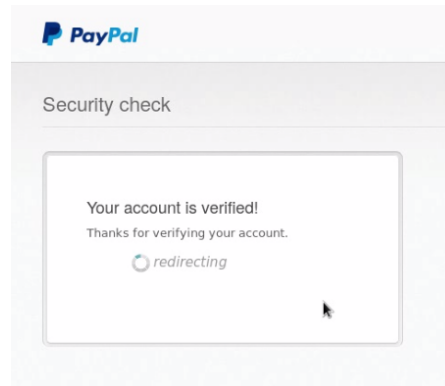
tel

Continue

Step 3: Using a proxy, remove "securityQuestion0" and "securityQuestion1" from the post data.

```
selectOption=SECURITY_QUESTION&securityQuestion0=test&securityQuestion1=test&jsEnabled=1&execution=e2s16_sms_ivr_continue_btn_label=Continue&default_continu
```

Step 4: Profit

**Advisory Timeline**

- 03/10/16 - Reported issue to Paypal
- 04/10/16 - Paypal begin investigation of issue
- 21/10/16 - Paypal report issue as fixed
- 21/10/16 - Paypal award bounty