

# SpookTastic

It is an xss challenge

```
try:
    browser.get(f"{HOST}/bot?token={BOT_TOKEN}")

    WebDriverWait(browser, 3).until(EC.alert_is_present())

    alert = browser.switch_to.alert
    alert.accept()
    send_flag(user_ip)
except Exception as e:
    pass
finally:
    registered_emails.clear()
    browser.quit()
```

The bot visits a page and check it if alerts, if it does, it gives flag

```
@app.route("/bot")
def bot():
    if request.args.get("token", "") != BOT_TOKEN:
        return abort(404)
    return render_template("bot.html", emails=registered_emails)
```

```

@app.route("/api/register", methods=["POST"])
def register():
    if not request.is_json or not request.json["email"]:
        return abort(400)

    if not blacklist_pass(request.json["email"]):
        return abort(401)

    registered_emails.append(request.json["email"])
    Thread(target=start_bot, args=(request.remote_addr,)).start()
    return {"success": True}

```

Sent the payload

# Our Newsletter

Promotion new products and sales. Directly to  
your inbox



Book Now

Got flag

94.237.63.93:30454 says

HTB{al3rt5\_c4n\_4nd\_w1l1\_c4us3\_jumpsc4r35!!}

OK