Northeastern University

UNIVERSITÀ DI TRENTO

FIU
FLORIDA INTERNATIONAL UNIVERSITY

You've Got (a Reset) Mail: A Security Analysis of Email-Based Password Reset Procedures

Tommaso Innocenti, Seyed Ali Mirheidari, Amin Kharraz, Bruno Crispo, and Engin Kirda

innocenti.t@northeastern.edu

18th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2021

Outline:

- Introduction
- Research questions
- Recent news
- State of the art
- Methodology
- Results
- Takeaways

- ⇨ User’s authentication is a primary functionality for websites
  - Websites provide sensitive information and functionality to users
  - User’s account are the first target for malicious actors
- ⇨ Authentication flaws pose a major threat
  - Leakage of credentials expose user’s information
- ⇨ No Standard is available for these procedures
  - Heterogenous implementations are more prone to vulnerability

Research questions that drove our work:

1. How do websites implement the account recovery process?
2. How prevalent are account recovery problems?
3. What are the immediate threats of the misconfigured recovery process?

Recent news

Hacking GitHub with Unicode's dotless 'i'.

security · Nov 28, 2019

Company: GitHub

Vulnerability: Password reset emails delivered to the wrong address.

Cause: Forgot password emails validated against lowercase value on file, but sent the provided email.

https://eng.getwisdom.io/hacking-github-with-unicode-dotless-i/

How I Could Have Hacked Multiple Facebook Accounts

Gurkirat Follow

Aug 25, 2016 · 5 min read ★

https://medium.com/hackernoon/how-i-could-have-hacked-multiple-facebook-accounts-d9d335188d9b

Tech

Grindr accounts could be easily hacked with email address

5 October 2020

A hack on Grindr allowed anyone with the email address linked to a valid account to reset the user's password and take over their profile.

https://www.bbc.com/news/technology-54418933

allTop9 Blog Advertise About Us Contact Us

Hack Facebook with Password Reset Bug – Here's How to Secure it

APPS, SOCIAL MEDIA, TECH
TIPS

January 9, 2021

https://www.alltop9.com/hack-facebook-password-reset-bug

Why do attackers target account recovery procedures?

- Weakest link of the authentication process

- Phishing remains the top threat vector for today's cyber-criminals[1].
  Of the 62.6 billion cyber-threats detected by Trend Micro last year,
  over 91% were sent via email.

- A complex procedure that is every day more used (~80 user's account[2])

[1] Trend Micro 2020 Annual Cybersecurity Report, https://www.trendmicro.com/vinfo/ph/security/research-and-analysis/threat-reports/roundup/a-constant-state-of-flux-trend-micro-2020-annual-cybersecurity-report

[2] Hanamsagar, A., Woo, S.S., Kanich, C., Mirkovic, J.: Leveraging semantic transformation to investigate password habits and their causes. (2018)

⇨ SMS reset with OTP

- Implementation mistakes are widespread among sites (98.5% sites[3])
- The used channel is not always secure[4]
- Even large banks and popular sites(e.g Google)[5] suffer from SMS-authentication elusion

⇨ Password reset via email verification

- Email traffic isn't always encrypted, no protection against service-provider attacks[6]
- Multiple studies[7-9] focus on reset email effectiveness

[3] Ma, S., Feng, R., Li, J., Liu, Y., Nepal, S., Bertino, E., Deng, R.H., Ma, Z., Jha,S.: An empirical study of sms one-time password authentication in android apps. (2019)
[4] Mulliner, C., Borgaonkar, R., Stewin, P., Seifert, J.P.: Sms-based one-time passwords: attacks and defense. (2013)
[5] Dmitrienko, A., Liebchen, C., Rossow, C., Sadeghi, A.R.: Security analysis of mobile two-factor authentication schemes. Intel Technology Journal 18(4) (2014)
[6] Raponi, S., Di Pietro, R.: A longitudinal study on web-sites password management (in) security: Evidence and remedies. IEEE Access 8, 52075–52090 (2020)
[7] Al Maqbali, F., Mitchell, C.J.: Email-based password recovery-risking or rescuing users? In: 2018 International Carnahan Conference on Security Technology (ICCST). pp. 1–5. IEEE (2018)
[8] Al Maqbali, F., Mitchell, C.J.: Web password recovery: A necessary evil? In: Proceedings of the Future Technologies Conference. pp. 324–341. Springer (2018)
[9] Li, Y.,Wang, H., Sun, K.: Email as a master key: Analyzing account recovery in the wild. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications. pp. 1646–1654. IEEE (2018)

⇨ Propose a methodology to identify weaknesses in email-based password recovery process

- We based our test on OWASP guidelines[10]

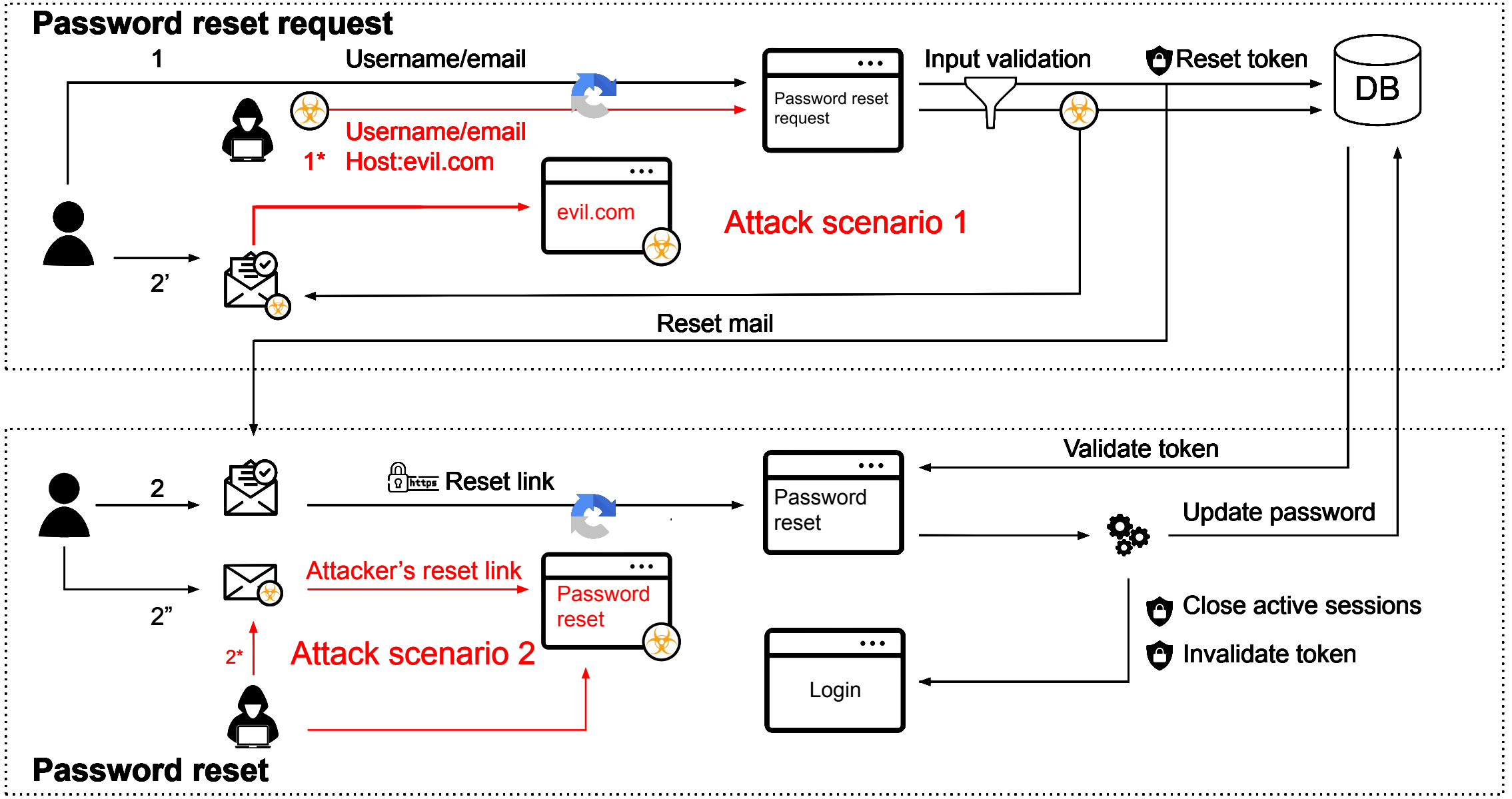
⇨ Present a measurement of common weaknesses among Alexa top 5K

- Build a semi-automated crawler on top of Selenium
- Studied 3 different site groups to identify behavioral differences

⇨ Measured the prevalence of web-based attacks against email-based password recovery

- Identified a variation of the well-known Login CSRF (i.e., Auth-CSRF)
- Expanded header injection attack with 23 Non-Standard HTTP headers

[10] OWASP: Forgot password cheat sheet, https://cheatsheetseries.owasp.org/cheatsheets/ForgotPasswordCheatSheet.html

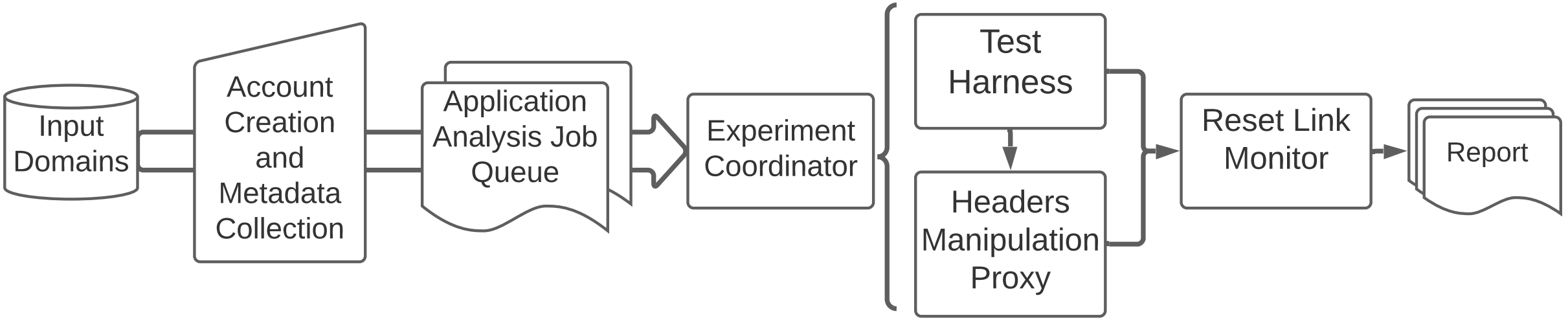

Password reset request
1
Username/email
Password reset request
Input validation
Reset token
DB
Username/email
1* Host:evil.com
evil.com
Attack scenario 1
2'
Reset mail
2
Reset link
Validate token
Password reset
Update password
Attacker's reset link
Password reset
2"
2*
Attack scenario 2
Close active sessions
Invalidate token
Login
Password reset

Measured 6 Weaknesses

- Insecure Reset Link (IRL)
- No Session Termination (NST)
- No Expiration (NE)
- Multi Use Token (MUT)
- No Change Notification (NCN)
- Multiple Valid Tokens (MVT)

Tested 2 attack scenarios

- Login CSRF (LC)
- Headers Manipulation (HM)



- Selected 900 sites and created 3 groups based on site's popularity
- Excluded sites without free users account and with captcha
- Measured 366 sites' recovery procedure

Table 1: Recovery types summary

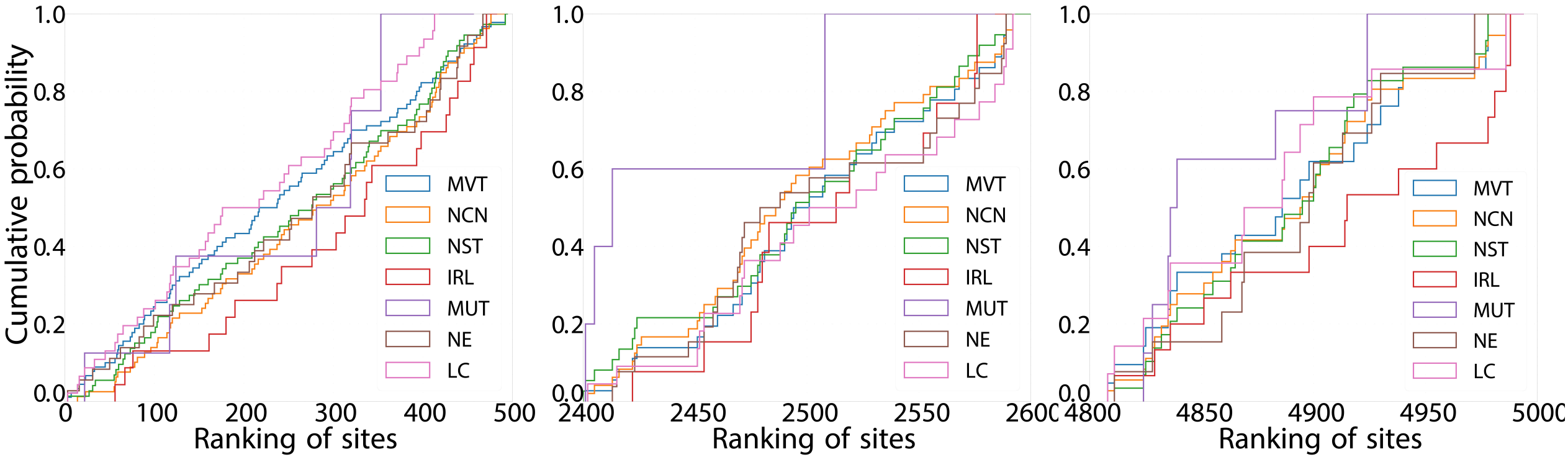
Recovery Type	Channel	# Sites
Text-Msg	SMS	5 (1.4%)
Original Password	E-mail	7 (1.9%)
One-time Security Code	E-mail	27 (7.4%)
Temporary Password	E-mail	25 (6.8%)
Password Reset Link	E-mail	302 (82.5%)
Total		366 (100%)

- Email-based recovery procedures are the first method to perform an account recovery

Table 2: Common Weaknesses Statistics

Weakness	All Sites
No Change Notification (NCN)	163 (44.5%)
Multiple Valid Tokens (MVT)	147 (40.2%)
No Session Termination (NST)	139 (38.0%)
Login CSRF (LC)	82 (22.4%)
No Expiration (NE)	75 (20.5%)
Insecure Reset Link (IRL)	52 (14.2%)
Multi Use Token (MUT)	21 (5.7%)
Headers Manipulation (HM)	6 (2.0%)
Total	262 (71.6%)

- 57.7% of websites misimplemented a security check on reset token.
- 54.0% of websites wrongly managed the active sessions after a password reset, or missed a confirmation email after a successful password reset.



⇨ Surprisingly site's popularity does not affect weakness distribution

⇨ 6 out of 366 sites (2%) suffer from headers injection vulnerability

- No interaction needed to redirect the user to a malicious domain and to takeover the user's account.
- Reset links are usually hidden behind HTML button in reset mail blocking any visual check

⇨ 82 out of 366 sites (22.4%) suffer from Login CSRF

- The reset link possession is the only account ownership validation requested to enable automatic login after a password reset.

Responsible disclosure

- We used the disclose.io dB[11](62 sites) and the Whois dB to obtain the site's contact.
- We followed all previous work recommendations[12-14]
- We received 38 acknowledgments (14.5%)
- All sites contacted thought broker replied but, provided limited response actions
- Only 19 out of 243 sites contacted through email replied

[11] **disclose.io** is a cross-industry, vendor-agnostic standardization project for safe harbor best practices to enable good-faith security research https://disclose.io

[12] Mirheidari, S.A., Arshad, S., Onarlioglu, K., Crispo, B., Kirda, E., Robertson, W.: Cached and confused: Web cache deception in the wild. (USENIX Security 20)

[13] Stock, B., Pellegrino, G., Li, F., Backes, M., Rossow, C.: Didn't You Hear Me? -Towards More Successful Web Vulnerability Notifications. (NDSS) Symposium (2018)

[14] Stock, B., Pellegrino, G., Rossow, C., Johns, M., Backes, M.: Hey, you have a problem: On the feasibility of large-scale web vulnerability notification. (USENIX Security 16)

Takeaways

- The missing of a standard is reducing the security of password reset procedures
- Password reset procedure needs to be resilient even in the presence of an attack
- Only 13% of sites correctly implemented the OWASP guidelines
- Still need a more effective way to report vulnerability

Northeastern University

Thank you.

Are there any questions?

My academic page: innotommy.com

innocenti.t@northeastern.edu