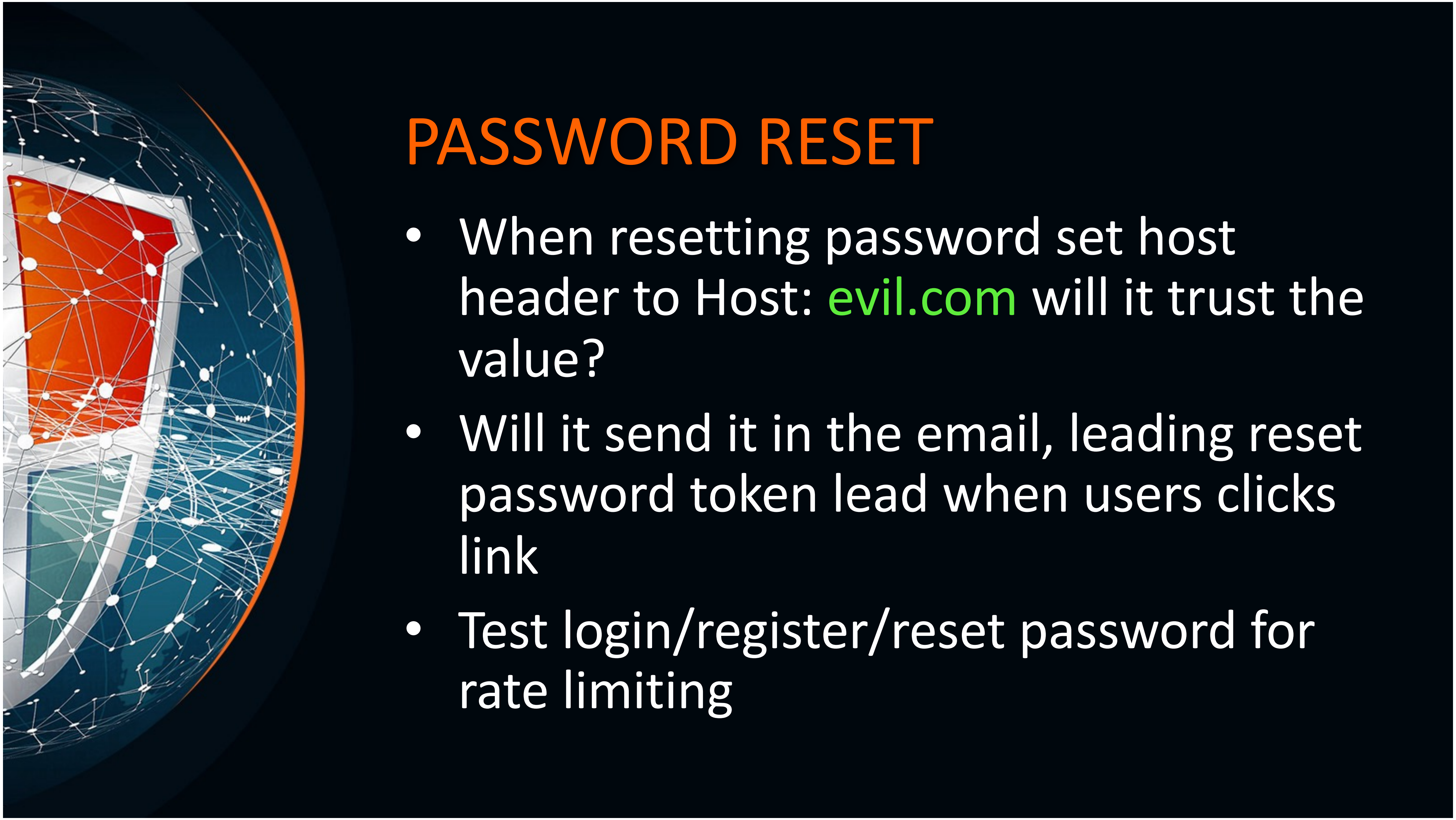
Password Reset Bug Hunting Methodology

Become a Successful Bug Bounty Hunter

PASSWORD RESET

- When resetting password, what parameters are used?
- IDOR? inject an ID parameter and test of HPP (HTTP Parameter Pollution)
- Is the host header trusted?
- Can the reset token be used on another account? Can it be re-used?



PASSWORD RESET

- When resetting password set host header to Host: evil.com will it trust the value?
- Will it send it in the email, leading reset password token lead when users clicks link
- Test login/register/reset password for rate limiting

Thank You!

Become a Successful
Bug Bounty Hunter