PAPRYQARZ
WE TEST WITH TASTE

Przeprowadzanie testów penetracyjnych

11.05.2016

Poznajmy się!

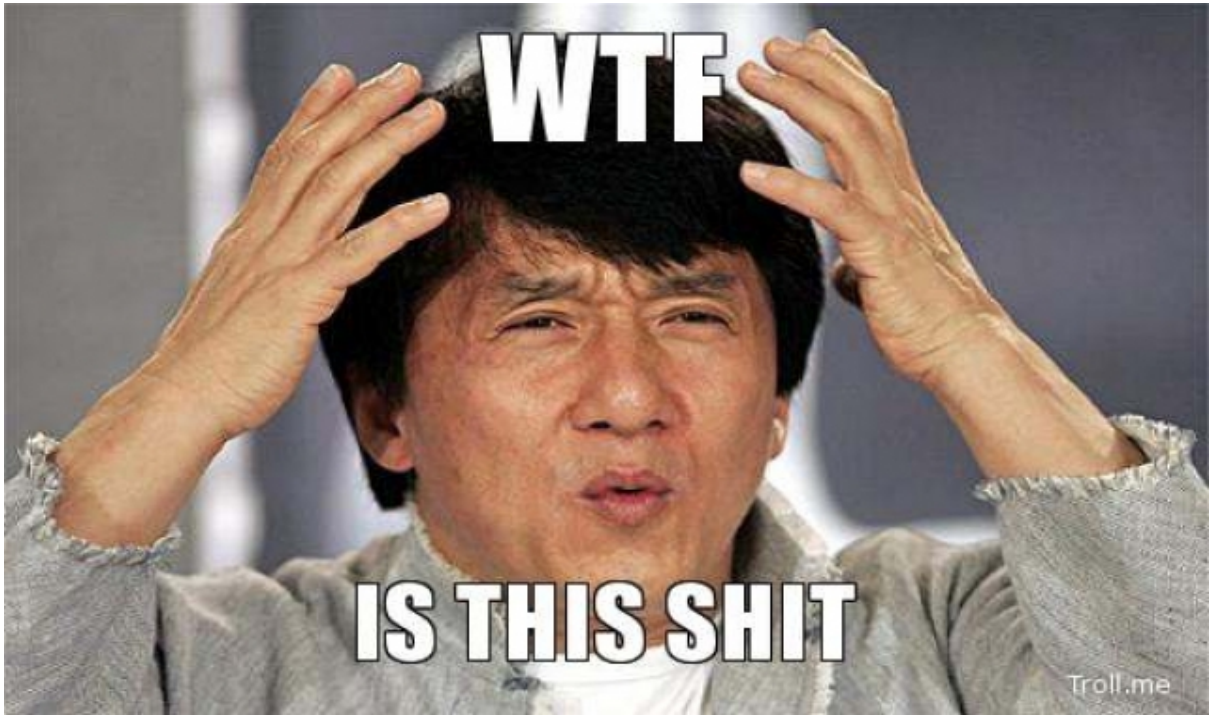
Piotr Gębala (piotr.gebala@blstream.com)

Prowadzenie działalności gospodarczej

Inżynier Zapewniania Jakości (Home.pl)

Inżynier ds. Jakości Oprogramowania (BLStream)

O co chodzi z `Testami Penetracyjnymi`



Psuć, ale gdzie? Co? Komu? No i po co?

Facebook, Google, Yahoo, Mozilla, Wordpress, Chromium, Samsung, Avast, Microsoft, Github, Apple, Adobe, AT&T, eBay

https://bugcrowd.com
https://hackerone.com
http://www.vulnerability-lab.com/list-of-bug-bounty-programs.php

Faza I - Przygotowanie

Zbieranie Informacji o Celu

Pasywne

Aktywne

Pasywne 1/3

Wyszukiwarki internetowe (Google / Bing / Yahoo / Baidu / Shodan)

Whois / Dane z RIR (AFRINIC / ARIN / APNIC / LACNIC / RIPE NCC)

Informacje o pracownikach (facebook.com / indeed.com / linked.in / goldenline.com / twitter.com / namechk.com / pgp.mit.edu)

Kod źródłowy pracowników / firmy (github / bitbucket / sourceforge / codeplex / gitorious)

Pasywne 2/3

Serwisy zbierające metadane (connect.data.com / fullcontact.com / builtwith.com / netcraft.com / censys.io)

Informacje zawarte w systemach zabezpieczających (ssltools.com / vpnhunter.com)

Informacje o wcześniejszych wyciekach (haveibeenpwned.com, GHDB, punkspider.org, xssed.com, openbugbounty.org)

Lokalizacja / zdjęcia (freegeoip.net / ipinfodb.com / flickr.com / maps.googleapis.com / instagram.com / picasa.com / twitter.com / youtube.com)

Pasywne 3/3

Panie... Jak to zautomatyzować?

- TheHarvester (github.com/laramies/theHarvester)
- Recon-ng (bitbucket.org/LaNMaSteR53/recon-ng)

Aktywne 1/3

Skanowanie portów / Banner Grabbing / OS Fingerprint

Szukanie domen (DNS Discovery / RevDNS / DNS Bruteforce)

Wyszukiwanie katalogów / Web Spiders / Crawlers

Wykrywanie systemów IDS / WAF

Aktywne 2/3

A tego też nie można zautomatyzować?

Skanery automatyczne (Acunetix WVS / AppScan / App Scanner / AVDS / BugBlast / Burp Suite / Contrast / Canvas / GamaScan / Grabber / Grendel-Scan / GoLismero / IKare / IndusGuard Web / N-Stealth / Netsparker / Nessus / Nexpose / Nikto / AppSpider / ParosPro / Proxy.app / QualysGuard / Retina / Securus / Sentinel / Sqlmap / Sqlninja / Vega / Wapiti / WebApp360 / WebInspect / SOATest / Trustkeeper Scanner / WebReaver / WebScanService / Websecurify Suite / Wikto / w3af / Xenotix XSS Exploit Framework / Zed Attack Proxy)

Aktywne 3/3

Testy manualne (w końcu !!!)

Poznanie działania aplikacji (testy eksploracyjne)

Zbudowanie modelu aplikacji

Określenie wektorów ataku

Faza 2 – Właściwe Testy

Weryfikacja znalezionych automatycznie luk

Analiza kodu źródłowego

Szukanie nowych podatności

Aktualizacja zakresu testów

Błędy Autoryzacji / Autentykacji 1/2

Autoryzacja != Autentykacja

HTTP Jest protokołem bezstanowym

Session Prediction / Collision

Session Fixation / Hijack

Błędy Autoryzacji / Autentykacji 2/2

Słabości implementacji OAuth / OpenID

Polityka haseł / przypomnienie hasła / zmiana hasła

Słabości kontroli dostępu

Wstrzykiwanie Kodu

SQL Injection / Blind SQL Injection

OS Command Injection

Local / Remote File inclusion

SOAP / SMTP / LDAP / XML / Xpath (…) Injection

Atakowanie innych użytkowników

Cross Site Scripting (XSS)

Cross Site Request Forgery (CSRF)

HTTP Headers Injection / Response Splitting

Frame Injection / Clickjacking

Atakowanie Logiki Aplikacji

Dodanie Produktu do koszyka

Autentykacja / rejestracja użytkownika

Użycie kodu rabatowego

Finalizacja zamówienia

Faza 3 – Zgłaszanie nieprawidłowości

Przygotowanie POC dot. luki

Opisanie wpływu na działanie aplikacji / użytkowników

Czekanie na przyjęcie, potwierdzenie i poprawę zgłoszenia

Weryfikacja poprawki

Co jeszcze? / Skąd czerpać informację?

https://www.owasp.org
http://www.isecom.org

http://www.pentest-standard.org
https://www.sans.org

https://bitquark.co.uk/blog/
https://nealpoole.com/blog/
https://whitton.io/
http://blog.bentkowski.info/
https://miki.it/blog/
https://prakharprasad.com/
https://blog.detectify.com/

http://www.breaksec.com/
http://stephensclafani.com/
http://nahamsec.com/
http://www.rafayhackingarticles.net/
http://sakurity.com/blog
http://josipfranjkovic.blogspot.com/
http://www.paulosyibelo.com/

Thats All Folks...

Jakieś Pytania?

Koniec

THE END