Polowanie na błędy

Krótki przewodnik dla myśliwego

SecuRing

Mateusz Olejarka

SECONference
9-10 maja, Kraków

c:\>whoami

- (Były) programista
- SecuRing – konsultant
- Testerzy.pl - trener
- OWASP Poland – w zarządzie

Agenda

- Definicje
- Wybór programu
- Polowanie
- Pytania
- Konkurs!

Definicje

Responsible disclosure - odpowiedzialne ujawnianie błędu.

Badacz:

- **Daje firmie odpowiednią ilość czasu na poprawę błędu**
- **Ujawnia informacje publicznie po opublikowaniu poprawki**

Definicje

Bug bounty to nagroda dla badacza za odpowiedzialne zgłoszenie błędu.

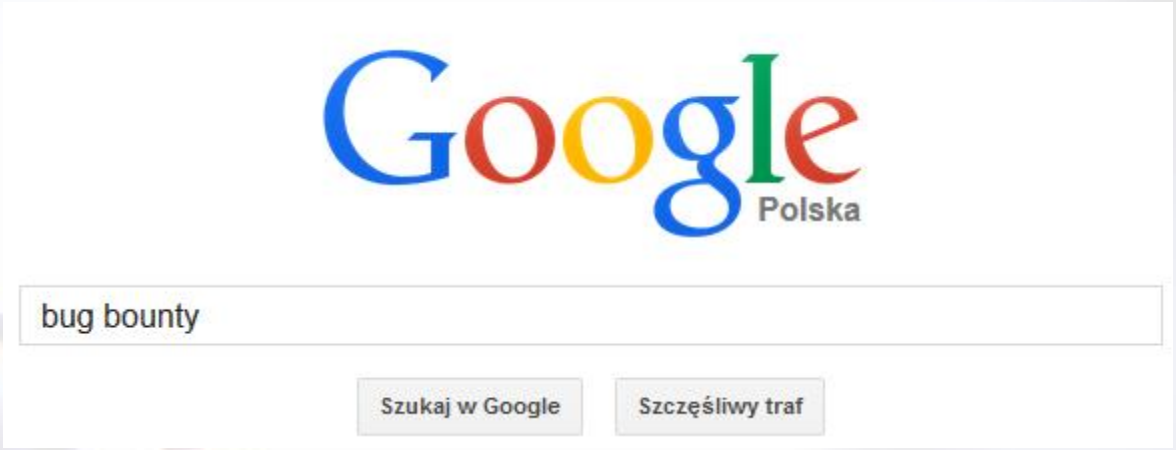
Typy:

- **Hall of Fame**
- **Gadżety**
- **$$$**

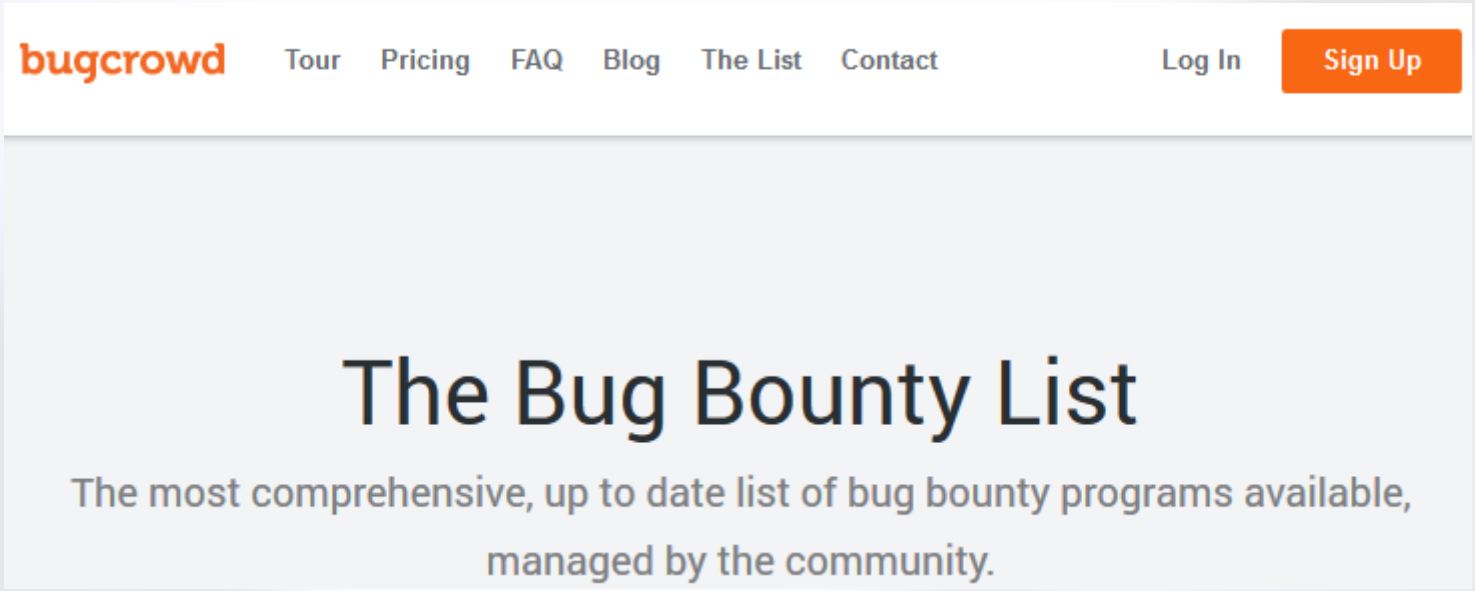
Wybór programu

- Gdzie szukać?
- Jak wybrać?

Gdzie szukać?



Gdzie szukać?



Jak wybrać?

- **Zasady gry**
- **Aplikacja**
  - Technologia
  - Biznes
  - Złożoność

Polowanie

- Co wiedzieć?
- Czego szukamy?
- Co robić?
- Czego unikać?
- Na co się przygotować?
- Co zyskamy?

Co wiedzieć?

- **HTTP, HTML, JS**
- **Technologia serwerowa**
- **Narzędzia:**
  - HTTP proxy (np. Burp, Fiddler)
  - Ulubiona przeglądarka

Czego szukamy?

- **XSS, CSRF**
- **Podatności w:**
  - Uwierzytelnieniu
  - Autoryzacji
  - Kontroli dostępu
- **OWASP TOP 10**
- **OWASP ASVS**

Co robić?

- Wygospodarować czas
- Podchodzić systematycznie
- Być absolutnie pewnym trafień
- Nie poddawać się!
- Dokumentować pracę

Czego unikać?

- Teoretyzowania i hipotez
- Marnej angielszczyzny
- Roszczeń

Na co się przygotować?

- Na odpowiedź można długo poczekać, np. miesiąc
- Ktoś to trafił przed Nami
- Nasz błąd nie jest godzien
- W między czasie przypadkiem poprawili

Motywacja

- Czemu w ogóle to robię?!
- Przecież inni lepsi testowali to przede mną!

1928

Co zyskamy?

- Doświadczenie
- If (sukces) dobry wpis w CV
- Wiedza (security, technologia, narzędzia)
- Dużo dobrej zabawy!

Pytania

???

Konkurs!

http://szyfr.ga.securing.pl

Dziękuję za uwagę

http://www.securing.pl
e-mail: info@securing.pl
tel. (12) 4252575
fax. (12) 4252593

Mateusz Olejarka
mateusz.olejarka@securing.pl

Materiały

https://bugcrowd.com/list-of-bug-bounty-programs

http://en.wikipedia.org/wiki/Full_disclosure_(computer_security)

https://www.owasp.org/index.php/Top_10_2013-Top_10

Materiały

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

https://www.google.com/about/appsecurity/hall-of-fame/

https://www.facebook.com/whitehat