A10 - Insufficient Logging & Monitoring

globo.com

GTS 33 | PA 05/2019

Agenda - A10 - Insufficient Logging & Monitoring

globo.com

1. Do que se trata?
2. Classe de registros (*What to log*)
3. Criando bons registros em aplicações
4. Exemplo de registro completo
5. Como se proteger?
6. Games Irados

Do que se trata?

Ocorre quando há falta de registros de logs ou monitoração, permitindo que um atacante possa realizar ações sem ser percebido.

Classes de registros (*What to log*)

- Eventos de acesso, autenticação e autorização:
  - Tentativas de autenticação: falhas ou não.
  - Acesso a sistema e recursos (Ex: acesso a uma rota da aplicação).

Classes de registros (*What to log*)

- Mudanças na aplicação e no sistema, mudança de privilégios.
- Inclusão/remoção/alteração de dados.

Classes de registros (*What to log*)

- Disponibilidade:
  - Erros que afetem a disponibilidade da aplicação.
  - Inicialização, *shutdown* e reinicialização de sistema.

Classes de registros (*What to log*)

- Problemas com recursos:
  - Falhas de conexão.
  - Esgotamento de recursos (Ex: máquina sem memória).

Classes de registros (*What to log*)

- Ameaças e "maldades":
  - Abusos na aplicação (Ex.: *Inputs* inválidos).
  - Problemas de segurança que afetem o funcionamento da aplicação (Ex.: rajadas de requisições).

Five Ws

From Wikipedia, the free encyclopedia

For other uses, see W5 (disambiguation).

The **Five Ws** (sometimes referred to as **Five Ws and How** considered basic in information gathering or problem solvi research and police investigations.[2] They constitute a for the principle of the Five Ws, a report can only be consider interrogative word:[1]

- *Who* was involved?
- *What* happened?
- *Where* did it take place?
- *When* did it take place?
- *Why* did that happen?

Some authors add a sixth question, *how*, to the list:[1]

- *How* did it happen?

globo.com

Criando bons registros em aplicações

Criando bons registros em aplicações

O quê? Ação, resposta a esta ação

Quem? IP de origem, Identificador do usuário

Onde? Rota da aplicação, função, módulo

Quando? Data/hora

Como? Método, como a requisição foi feita

Por quê? Efeito da ação (Ex.: Causa do erro)

Criando bons registros em aplicações

globo.com

- Classificar registros por níveis de severidade ajuda na hora de auditar
  - INFO, ERROR, WARNING …
  - 1, 2, 3 …
- Padronização de nomes nos campos do log

Atenção!!!

Dados sensíveis nunca devem ser registrados nos logs!

Registro completo


```
{
   "_id" :"5bd1e38ba9be09328062a974",
   "owner" : {
      "name" : "user",
      "ip" : "[::1]:52355"
   },
   "action" : "Insert Vulnerability",
   "response_status" : 400,
   "request" : {
      "route" : "/vuln",
      "method" : "POST"
   },
   "errors" : [  "Parâmetros inválidos" ],
   "start_time" : "2018-10-25T15:38:51.870Z",
   "end_time" : 2018-10-25T15:38:51.870Z",
   "level": "ERROR"
}
```

Quem?

O quê?

Como?

Onde?

Por quê?

Quando?

Como se proteger?

- Links Interessantes:
  - Classes de eventos e estrutura de registro: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.173.2198&rep=rep1&type=pdf
  - Padronização de campos: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf

    http://docs.graylog.org/en/2.4/pages/gelf.html

Novos games IRADOS!

The Elder Scrolls V - SKYRIM

The Elder Scrolls V: Skyrim, the 2011 Game of the Year, is the next chapter in the highly anticipated Elder Scrolls saga. Developed by Bethesda Game Studios, the 2011 Studio of the Year, that brought

FIFA 2019

Become a Champion through the stories of Alex Hunter, Danny Williams, and Kim Hunter. Each hero will face career-defining

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a10/games-irados
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:3001
```

globo.com

A10 - Insufficient Logging & Monitoring