Curso de Férias - Dia 2

Estevam Arantes

Programação (manhã)

- OWASP - O que é e importância para a segurança
- Projetos da OWASP
- Cheat sheet series
- Top 10
- SQL e SQL/NoSQL Injection
- XSS
  - Reflected/Self, DOM e Stored
- CSRF

Programação (tarde)

- WebGoat
  - Login individual
  - Guias simplificados da maioria das vulnerabilidades comentadas
  - Exercícios após as explicações
- Juiceshop
  - Aplicação “real” para testes
- Revisar exercícios de web de ontem

OWASP

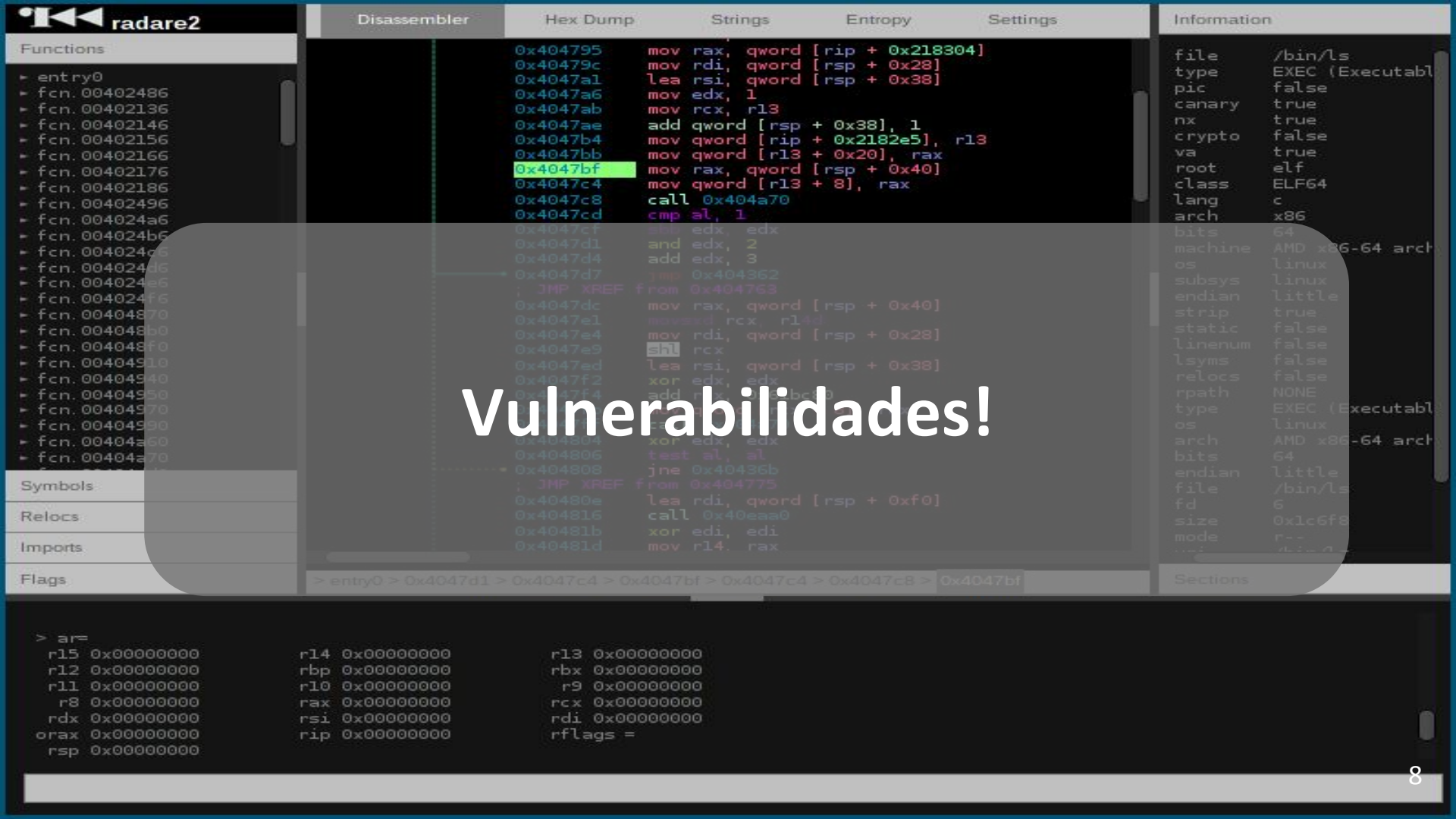
Projetos da OWASP

- Guias
  - OWASP Application Security Verification Standard (ASVS)
  - OWASP Testing Guide
- Ferramentas
  - AMASS
  - Zed Attack Proxy (ZAP)
- Aplicações para estudos
  - Juice Shop
  - Webgoat/nodegoat

T10 OWASP Top 10 Application Security Risks – 2017

A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

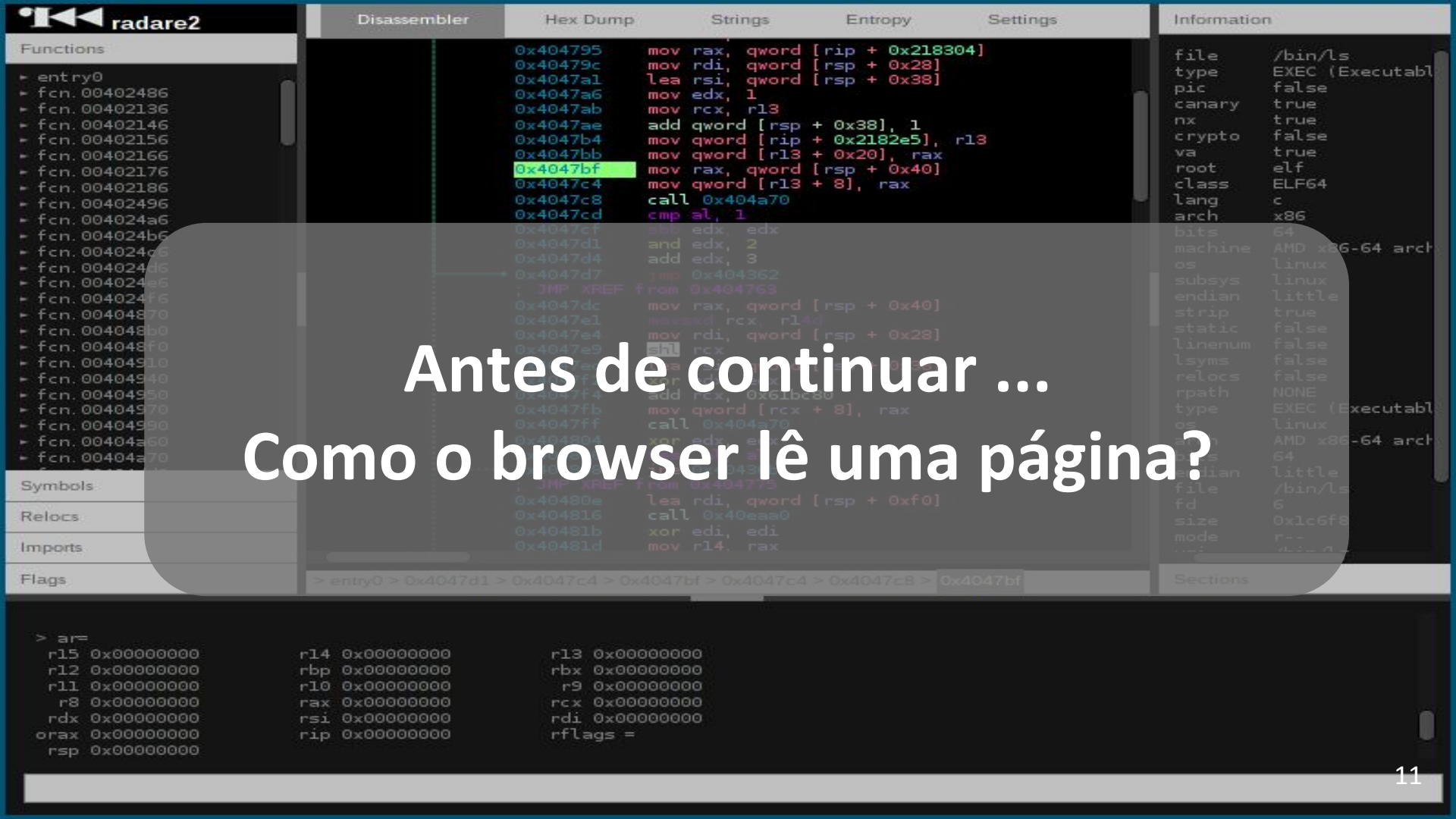

radare2
Disassembler
Hex Dump
Strings
Entropy
Settings
Information
Functions
Symbols
Relocs
Imports
Flags
Sections
0x404795 mov rax, qword [rip + 0x218304]
0x40479c mov rdi, qword [rsp + 0x28]
0x4047a1 lea rsi, qword [rsp + 0x38]
0x4047a6 mov edx, 1
0x4047ab mov rcx, r13
0x4047ae add qword [rsp + 0x38], 1
0x4047b4 mov qword [rip + 0x2182e5], r13
0x4047bb mov qword [r13 + 0x20], rax
0x4047bf mov rax, qword [rsp + 0x40]
0x4047c4 mov qword [r13 + 8], rax
0x4047c8 call 0x404a70
0x4047cd cmp al, 1
Vulnerabilidades!

Injection

- Dados não confiáveis entrando para um interpretador como se fossem.
- Dados de um atacante podem ser feitos para atacar a maneira como o interpretador entende o código e assim conseguir execução de comandos ou acesso a dados indevidos.

SQL Injection

- Falhas na aplicação, não no banco de dados em si (normalmente)
- Ocorre quando o programador faz *queries* dinâmicas
- Relativamente comum e poderoso
  - ‘or ‘1’=’1 ?



Antes de continuar ...
Como o browser lê uma página?

CSRF - Cross Site Request Forgery

- One click attack
- CSRF ou XSRF

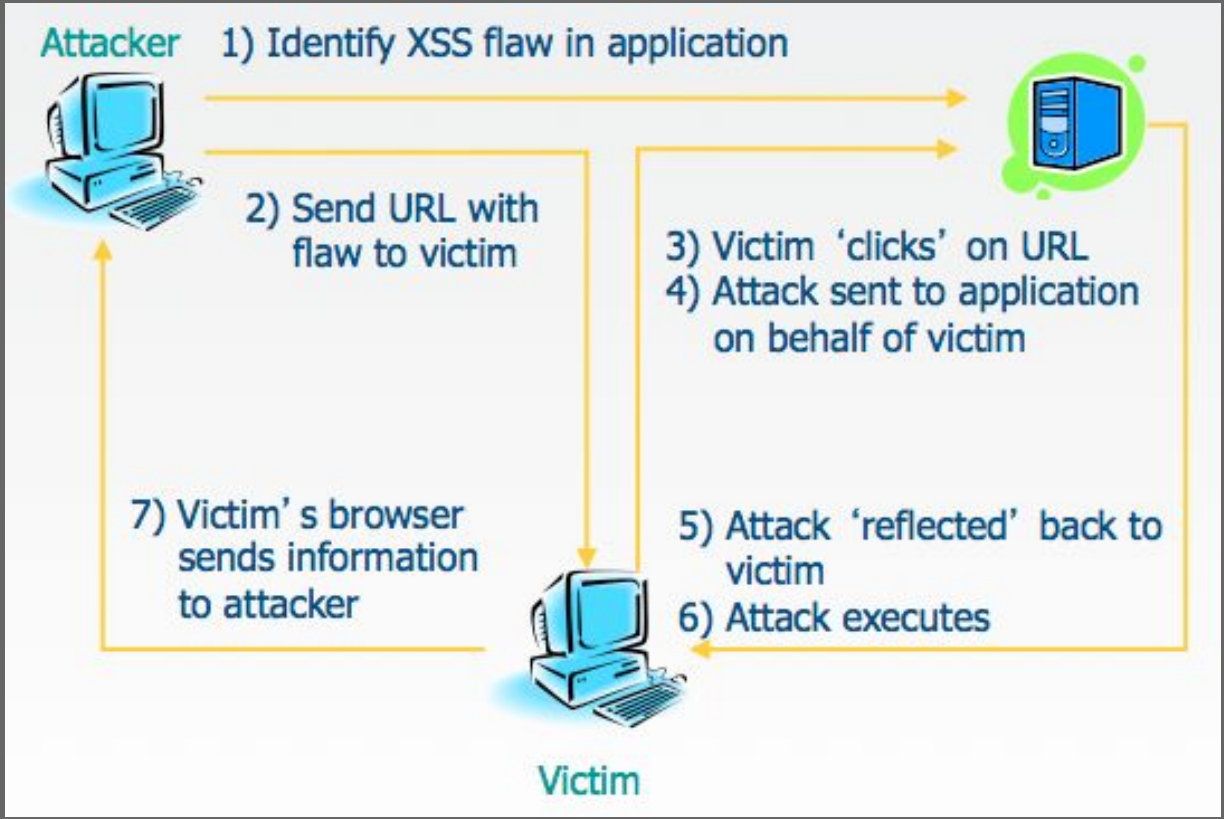
- Comandos não autorizados são transmitidos para uma aplicação que o usuário confia
- MUITO COMUM!

XSS - Cross Site Scripting

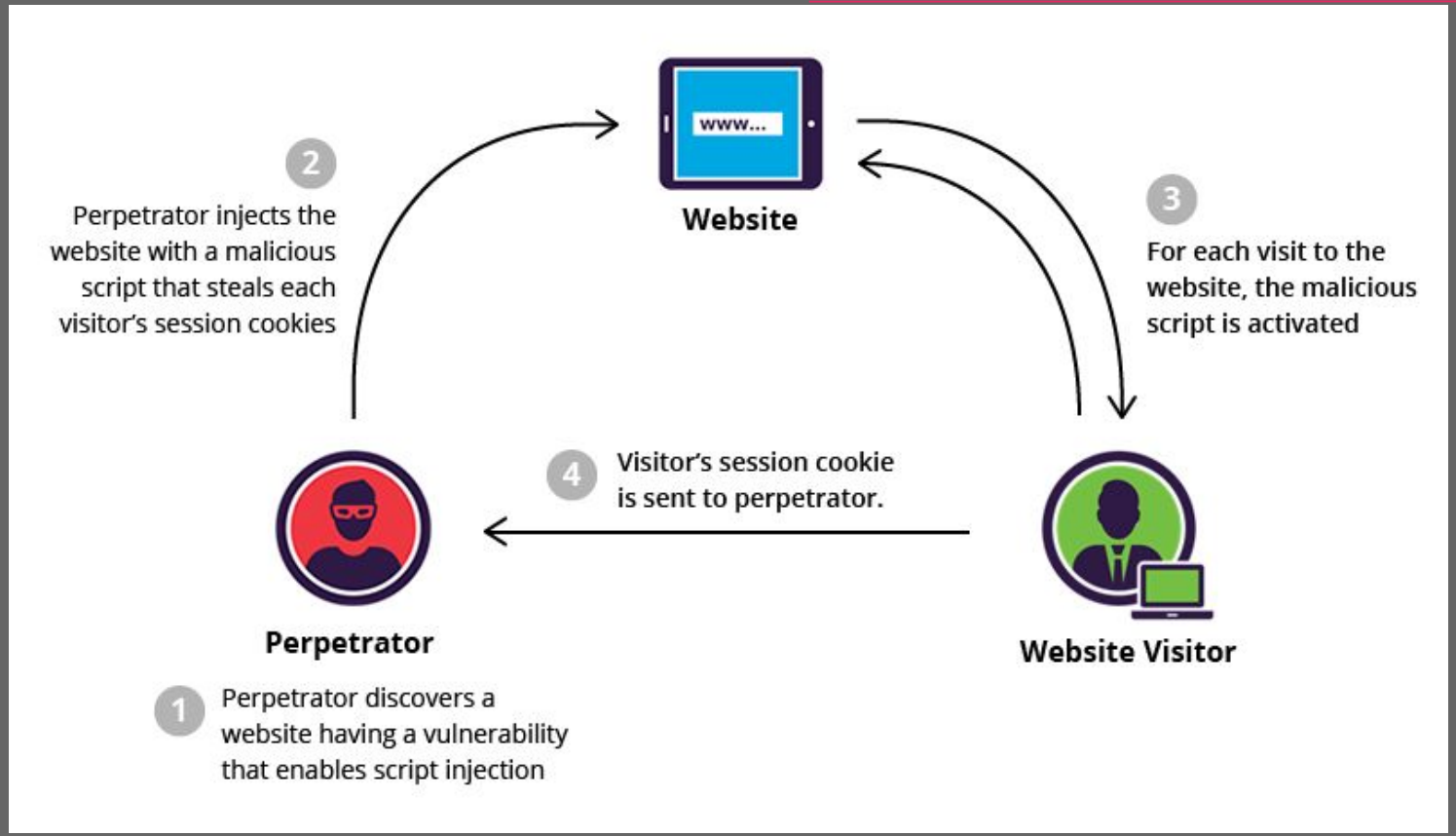
- É um tipo de injection
- O dado recebido é enviado para o browser sem validar/escapar.
- Permite executar scripts no browser da vítima

- Roubos de cookies, sessões, preencher formulários, redirecionar usuário

XSS - Tipos - Reflected e DOM



XSS - Tipos - Stored XSS



GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br