Seguridad en Arquitecturas Web

Ezequiel Gutesman

Agenda

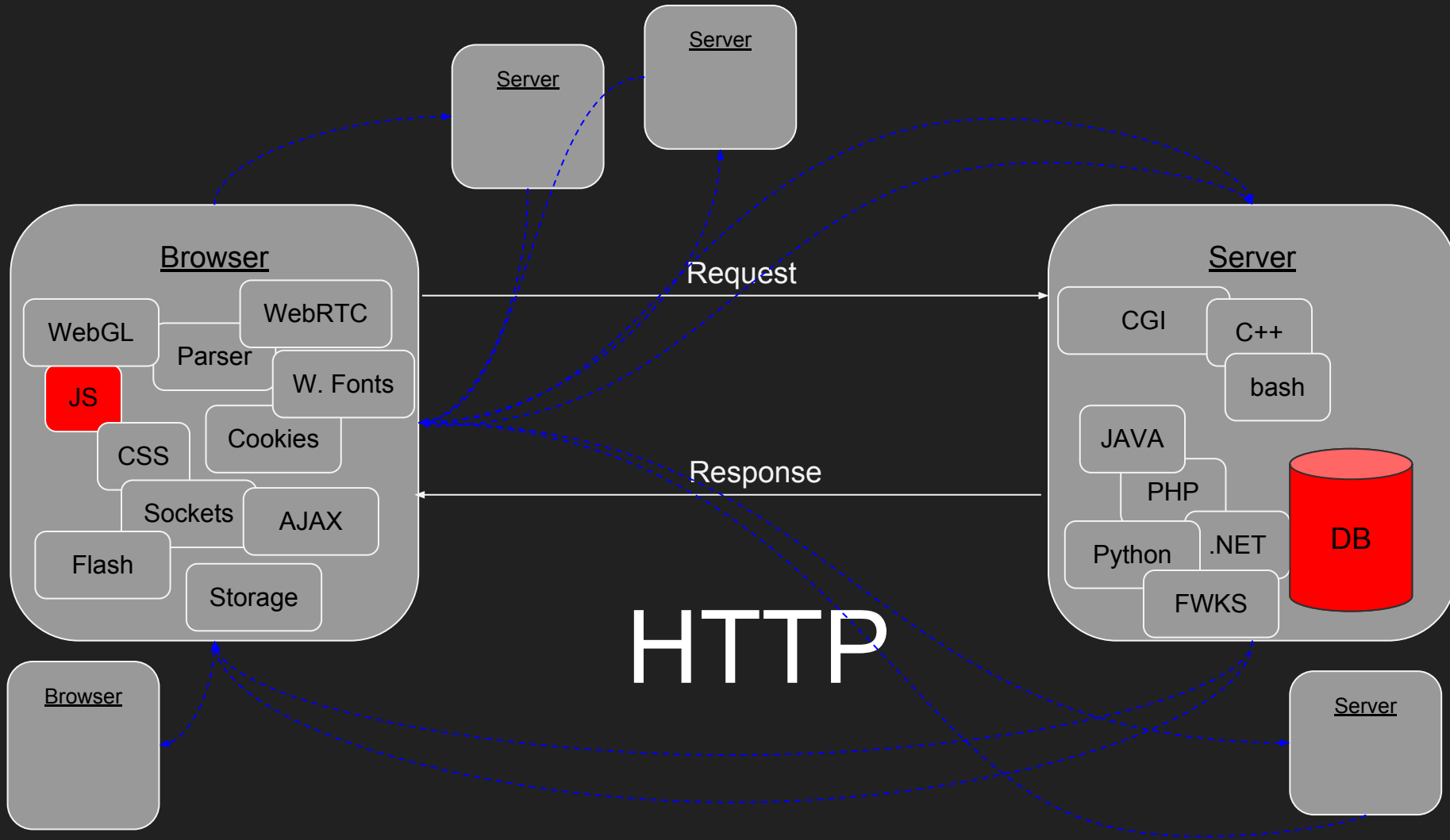
1. Evolución de las aplicaciones web
2. Qué es una vulnerabilidad? Por qué existen?
3. Familias de vulnerabilidades. El camino recorrido. OWASP Top 10.
4. Conclusiones
5. Referencias útiles

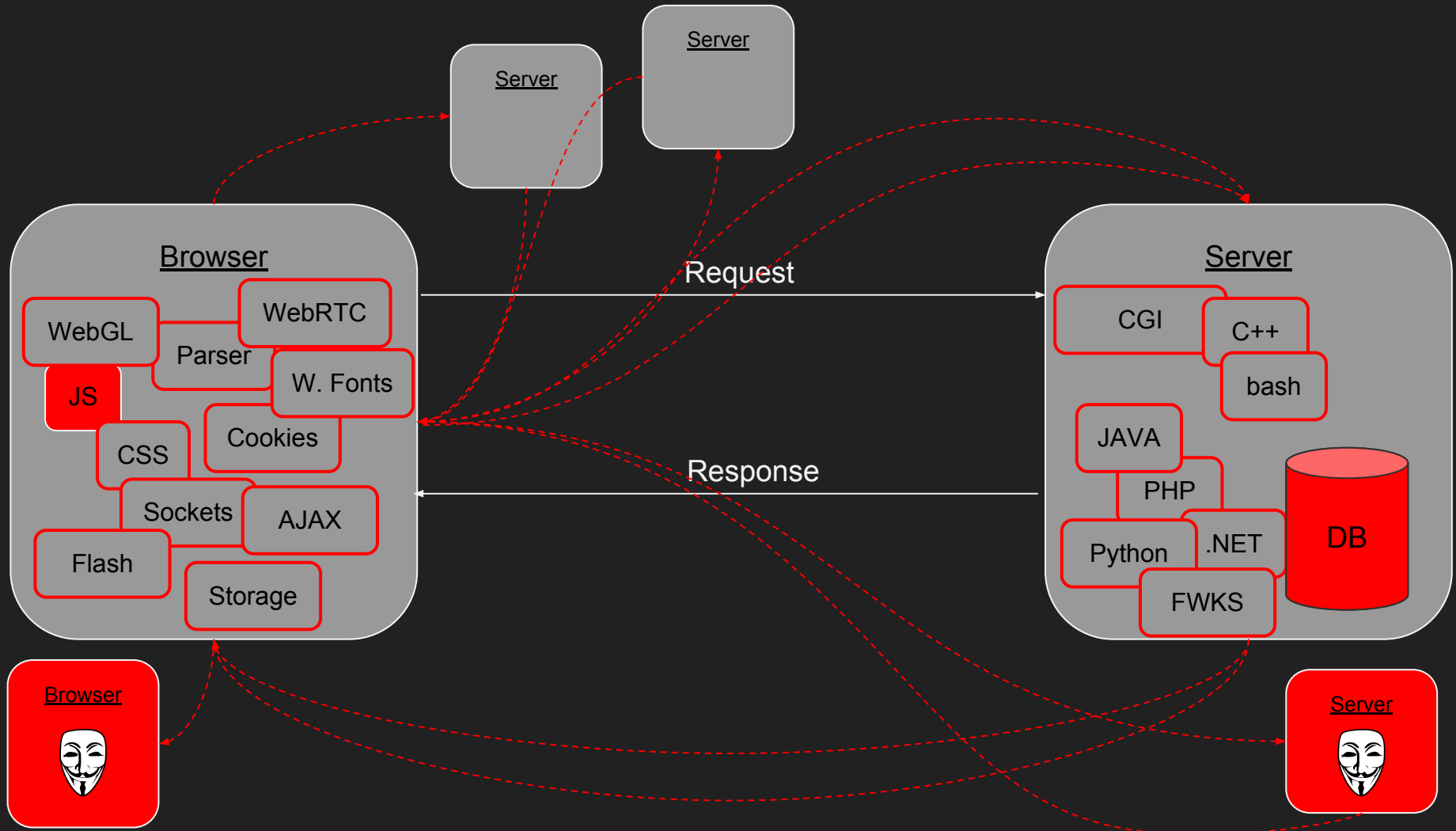
Evolución de las Aplicaciones Web

http://www.evolutionoftheweb.com/#/evolution/night

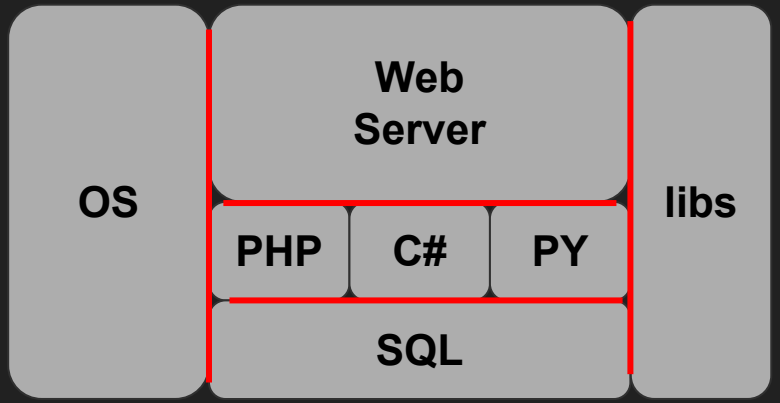
Qué es una Vulnerabilidad? Por qué Existen?(*)


Browser
Parser
doc
Business / Investment Opportunity
TRADERS INN CHILIWACK!
Past, present and future,
the facts and figures,
occupancy, size and profit margins
Motel
Details
Location
Motel for sale in beautiful
British Columbia, Canada
Server
doc
FS

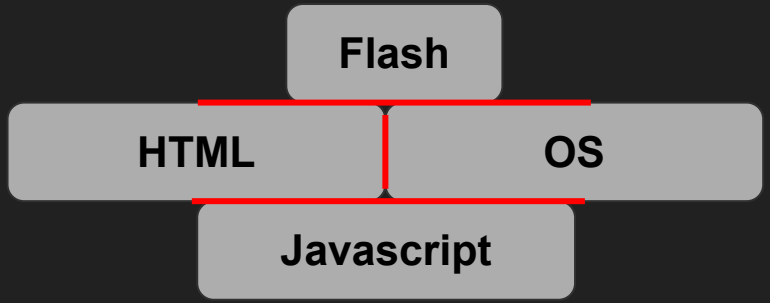

Server
Server
Server
Browser
WebGL
WebRTC
Parser
JS
W. Fonts
CSS
Cookies
Sockets
AJAX
Flash
Storage
Request
Response
Server
CGI
C++
bash
JAVA
PHP
Python
.NET
FWKS
DB
HTTP
Browser
Server


Server
Server
Server
Browser
WebGL
WebRTC
Parser
W. Fonts
JS
Cookies
CSS
Sockets
AJAX
Flash
Storage
Request
Response
Server
CGI
C++
bash
JAVA
PHP
Python
.NET
FWKS
DB
Browser
Server

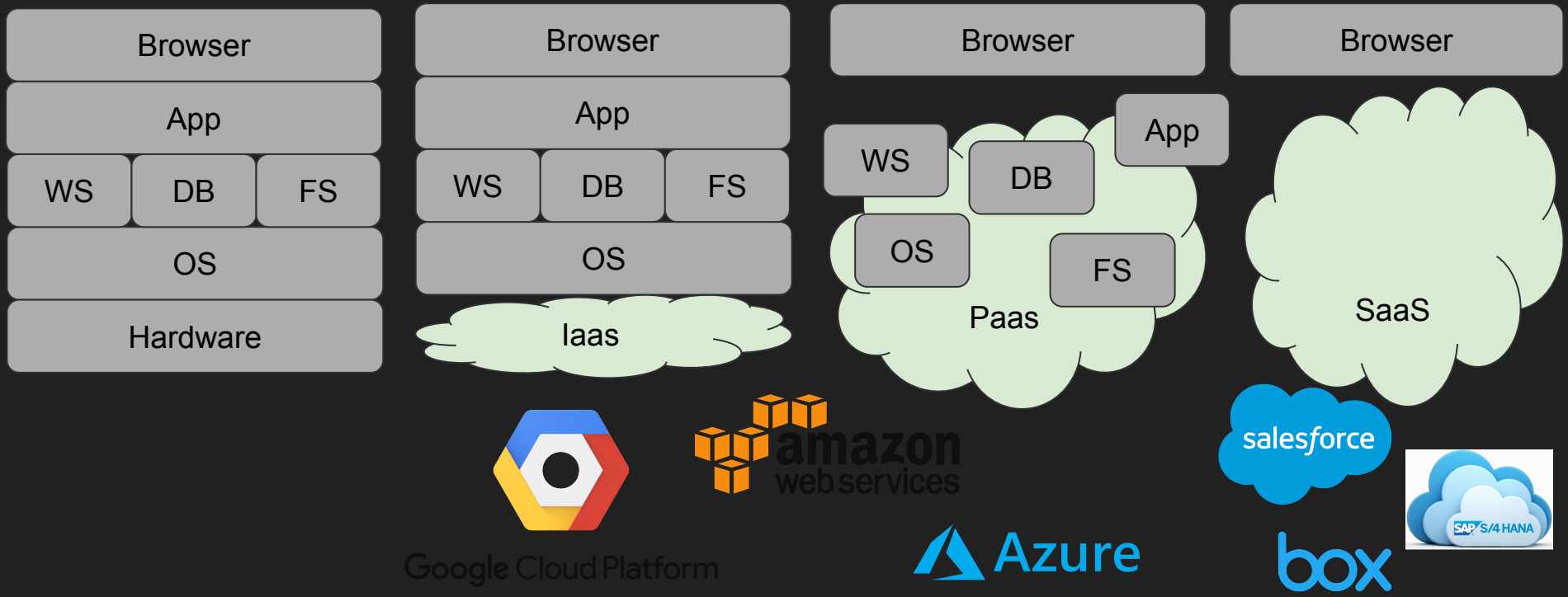
Fronteras



HTTP

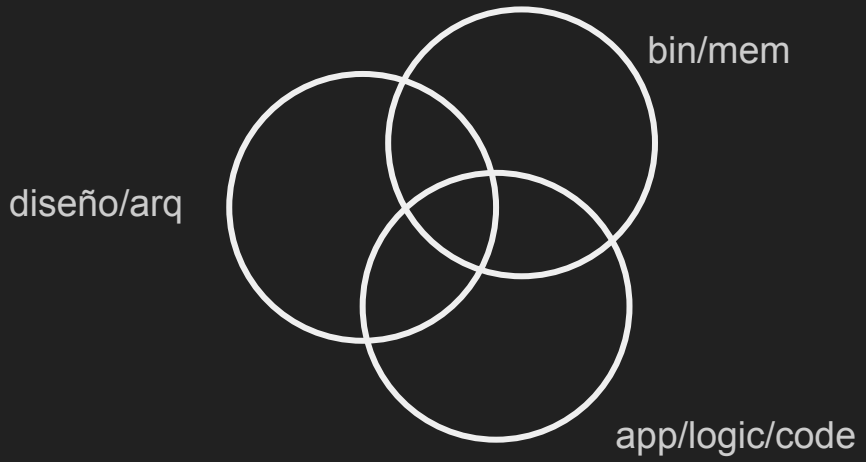


Arquitecturas web...



Vulnerabilidades

“In computer security, a vulnerability is a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorised actions within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.” https://en.wikipedia.org/wiki/Vulnerability_(computing)



Familias de Vulnerabilidades (OWASP)

1. Injection (SQL, NoSQL, LDAP, OS, etc)
2. Broken Authentication (auth, session mgmt, etc)
3. Sensitive Data Exposure (financiera, credit cards, passwords, etc)
4. XML External Entities (XXE - Parsers viejos!)
5. Broken Access Control
6. Security Misconfiguration
7. Cross Site Scripting (XSS - JS, browser API/HTML, etc)
8. Insecure Deserialization
9. Using Components With Known Vulnerabilities (:P)
10. Insufficient Logging & Monitoring

VER: https://cwe.mitre.org/data/index.html | https://www.owasp.org/index.php/Top_10-2017_Top_10

Conclusiones

- Seguridad como atributo de calidad != feature
- Quién la gestiona en ambientes cloud?
- Acoplamiento entre componentes / dependencias
- Seguridad de la app/infra
- Penetration Testing
- Secure Coding
- Conocimiento *profundo* de las tecnologías y protocolos
- Como atributo de calidad → RNF

Referencias

- https://tools.ietf.org/html/rfc7230 - RFC vigente para HTTP
- http://www.evolutionoftheweb.com/#/evolution/night - The Evolution of Web
- https://www.usenix.org/legacy/events/hotbots07/tech/full_papers/provos/provos.pdf - The Ghost In The Browser (Niels Provos - 2007)
- https://code.google.com/archive/p/browsersec/wikis/Main.wiki - Browser Security Handbook (Michal Zalewski)
- https://www.owasp.org/index.php/Main_Page - The Open Web Application Security Project OWASP
- http://langsec.org/papers/Sassaman.pdf - The Halting Problems of Network Insecurity (L. Sassaman, M. Patterson, S. Bratus, A. Shubina)
- https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470 - The Web Application hacker's Handbook. D. Stuttard, A. Pinto.
- https://www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998/ref=sr_1_2?ie=UTF8&qid=1526991664&sr=8-2&keywords=threat+modeling - Threat Modeling, Designing for Security. A. Shoestack
- https://www.usenix.org/
- https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference
- https://developers.google.com/web/fundamentals/performance/http2/ - HTTP/2 fundamentals. SPDY origins

Contacto

Ezequiel Gutesman

egutesman@onapsis.com

PGP fingerprint: 2A8E A3DB 562A F5BE DEC0 4346 987B 703F 6947 5746