Secure Coding for Startups

Anderson Dadario

CISSP, CSSLP

Topics for today

- Why Information Security
- OWASP Top 10
- SPA and API Security
- Cloud Security
- Next Steps
- References
- Recommended Articles / Sites

Why Information Security

- Information worth money
- Provide Security Visibility / Risk Awareness
- Competitive Advantage
- Keep/Enhance Brand Integrity / PR
- Etc ..

OWASP Top 10 (2013)

A1 - Injection

A2 - Broken Authentication and Session Management

A3 - Cross-Site Scripting (XSS)

A4 - Insecure Object References

A5 - Security Misconfiguration

A6 - Sensitive Data Exposure

A7 - Missing Function Level Access Control

A8 - Cross-Site Request Forgery

A9 - Using Components with Known Vulnerabilities

A10 - Unvalidated Redirects and Forwards

SQL Injection

User.where("age = #{params[:age]}")

Age = "18"

SELECT * FROM users WHERE age = 18;

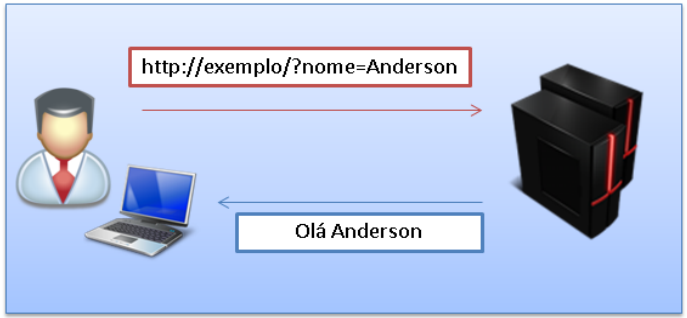
User.where("age = #{params[:age]}")

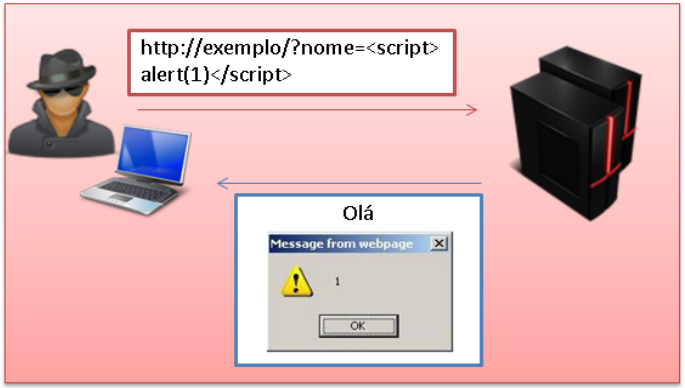
Age = "18 AND admin=true"

SELECT * FROM users WHERE age = 18 AND admin=true;

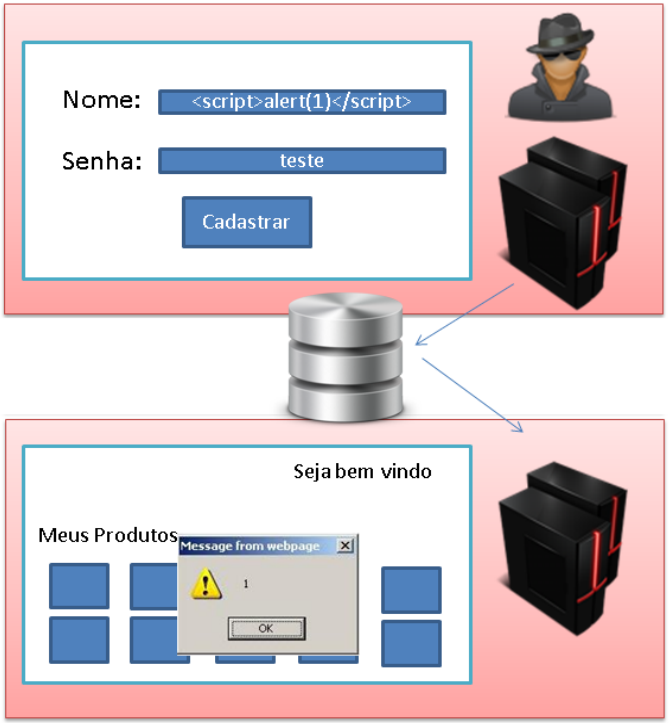
Cross-Site Scripting (XSS)

Reflected





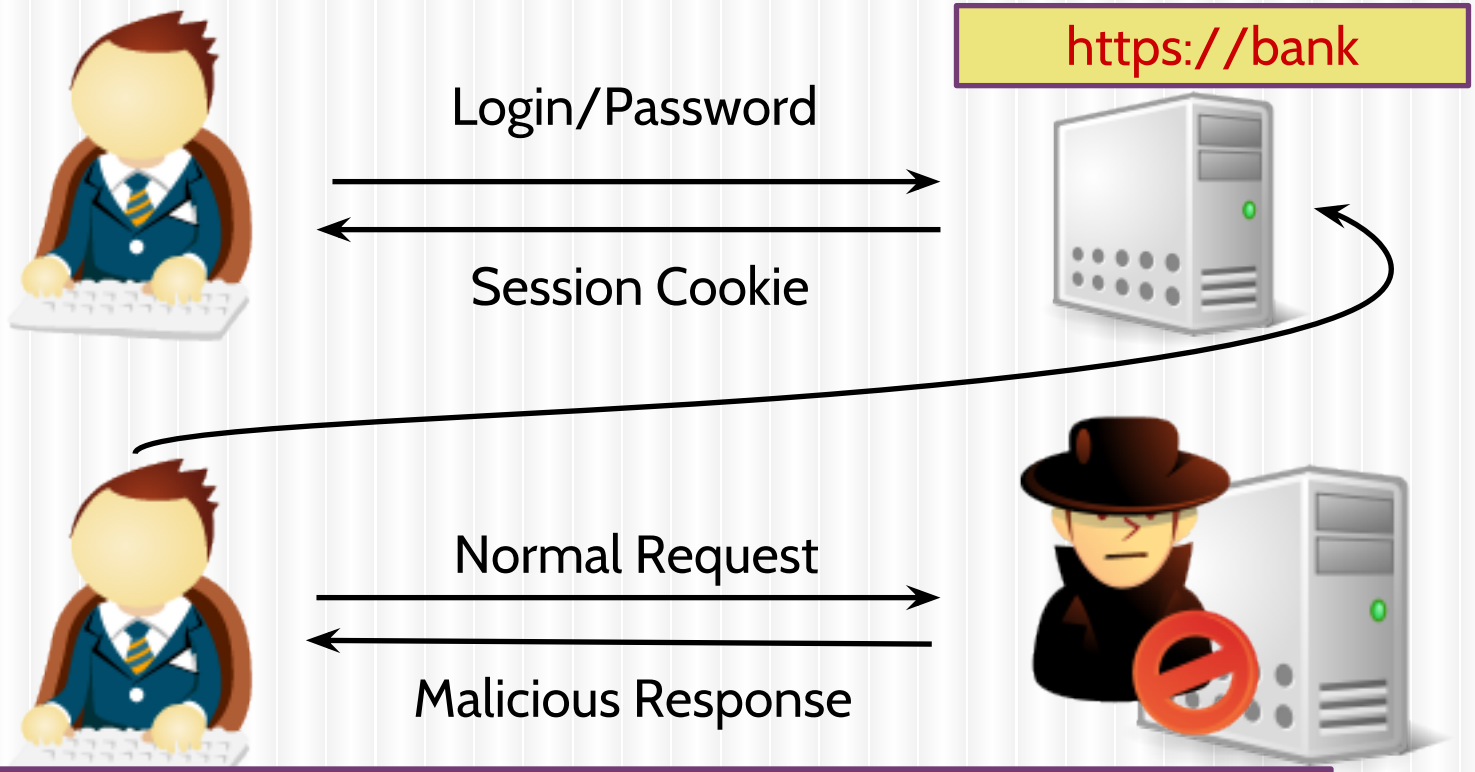
Stored



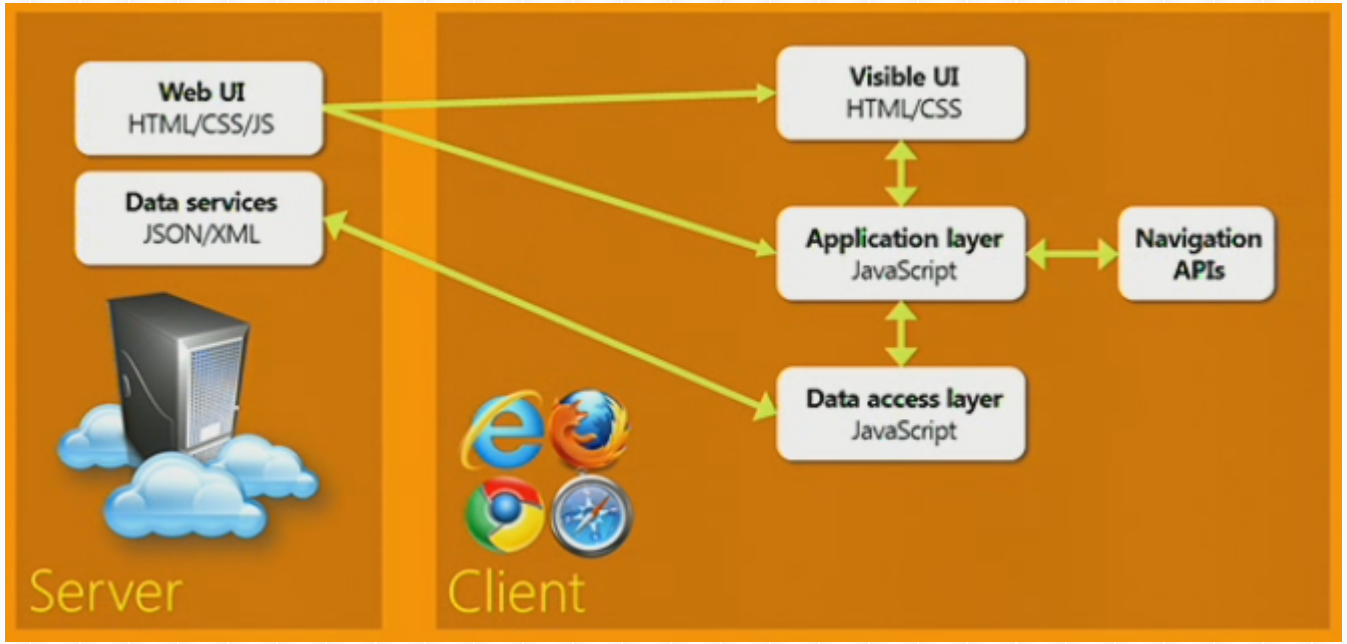
Universal

DOM Based

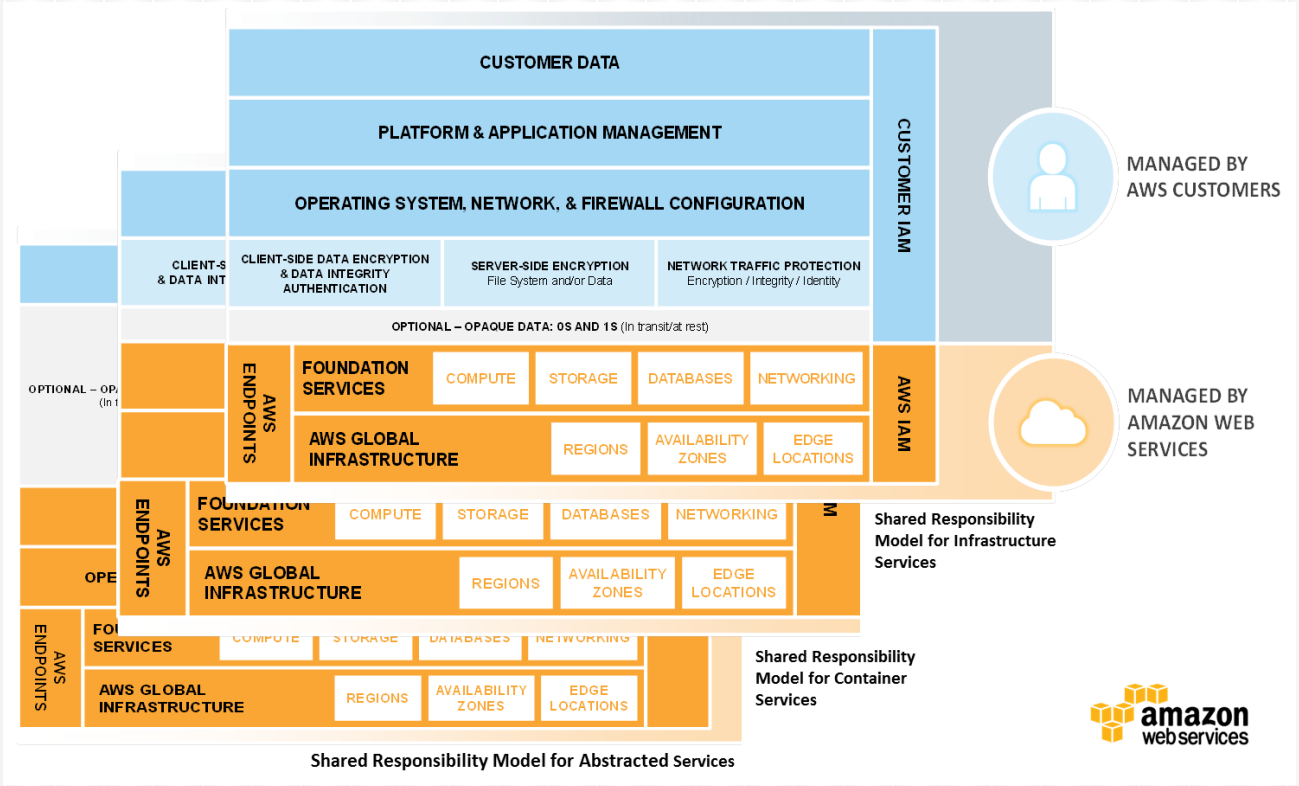
Cross-Site Request Forgery (CSRF)



SPA and API Security



Cloud Security



Next Steps

- Risk Management
- Threat Modeling
- Integrate Security into your Software Development Life Cycle (SDLC)
- Server Hardening
- Vulnerability Management
- Incident Response
- Security Awareness
- Access Control Review

References

- OWASP Top 10 (2013) https://www.owasp.org/index.php/Top_10_2013-Top_10
- AWS Cloud Security Best Practices http://blogs.aws.amazon.com/security/post/TxDA6TS0KJK82R/New-Whitepaper-AWS-Cloud-Security-Best-Practices

Recommended Articles / Sites

- Dev hacked after submitting AWS credentials to GitHub http://vertis.io/2013/12/16/unauthorised-litecoin-mining.html
- AWS Security Center http://aws.amazon.com/en/security/
- OWASP https://www.owasp.org
- NIST 800 series guides
- Reddit /r/netsec
- Microsoft Security Development Lifecyle http://www.microsoft.com/security/sdl/default.aspx