

globo
.com



GTS 33 | PA 05/2019

secDevLabs:

Tutorial de Desenvolvimento Seguro

Daniel Carlier

daniel.carlier@corp.globo.com

Silvia Pimpão

silvia.vasquez@corp.globo.com



1. Motivações
2. Planejamento do treinamento
3. Como funciona a dinâmica?
4. Resultados dentro da Globo.com
5. Abordagem GTS 33

1. Motivações

2013

globo
.com



XSS

- ▶ Qualquer dado refletido pela aplicação é um possível local vulnerável a XSS
- ▶ `<input type="text" name="address" value="myxsstest">`
 - ▶ `"><script>alert(1)</script>`
- ▶ `<script>var a='myxsstest';var b=123;</script>`
 - ▶ `';alert(1); var=foo'`

- Focado em treinar desenvolvedores a encontrar falhas de segurança.
- Focado na parte teórica das vulnerabilidades.
- Realizado fisicamente ao longo de uma semana com 20~30 desenvolvedores por vez.

2. Planejamento do treinamento



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.

O curso apresenta aplicações intencionalmente vulneráveis criadas pelo Time de Segurança da Globo.com baseadas no OWASP Top 10 2017.

2. Planejamento do treinamento



OWASP Top 10 (2017) apps:

Disclaimer: You are about to install vulnerable apps in your machine! 🔥

| Vulnerability | Language | Application |
|--|----------|--|
| A1 - Injection | Golang | CopyNPaste API |
| A2 - Broken Authentication | Python | Saidajaula Monster Fit |
| A2 - Broken Authentication | Golang | Insecure go project |
| A3 - Sensitive Data Exposure | Golang | SnakePro |
| A4 - XML External Entities (XXE) | PHP | ViniJr Blog |
| A5 - Broken Access Control | Golang | Vulnerable Ecommerce API |
| A6 - Security Misconfiguration | PHP | Vulnerable Wordpress Misconfig |
| A6 - Security Misconfiguration | NodeJS | Stegonography |
| A7 - Cross-Site Scripting (XSS) | Python | Gossip World |
| A8 - Insecure Deserialization | Python | Amarelo Designs |
| A9 - Using Components With Known Vulnerabilities | PHP | Cimentech |
| A10 - Insufficient Logging & Monitoring | Python | Gameslrados.com |

<https://github.com/globocom/secDevLabs>

2. Planejamento do treinamento



SAIDAJAULA MONSTRO FIT

SIGN UP · LOG IN

Saidajaula Monstro Fit

Você vai ser um verdadeiro
MONSTRO!

SnakePro

A screenshot of the SnakePro game interface. It shows a large white rectangular area representing the game board, with a blue horizontal bar at the top right. The interface is clean and minimalist.

I'M VINICIUS JUNIOR.

Flamengo, Brazil, Real Madrid

f t i s+ t

A photograph of Vinicius Junior, a Brazilian footballer, pointing upwards with his right hand. He is wearing a white jersey with a gold trim.

Gossip World

Home · New gossip · Login

Last gossips

Chico Buarque buy baguettes for snack

The singer and composer was dressed in shorts, T-shirts and slippers along the streets of Leblon, South Zone of Rio

[Read more →](#)

Posted on 2018-01-21 by viloris

[← Older](#) [Newer →](#)

Search

Copyright © Gossip World 2018

3. Como funciona a dinâmica?



Apresentação do tópico

Agenda - A6 - Security Misconfiguration

1. Do que se trata?
2. Exemplos
3. Como se proteger?
4. Stegonography



3. Como funciona a dinâmica?



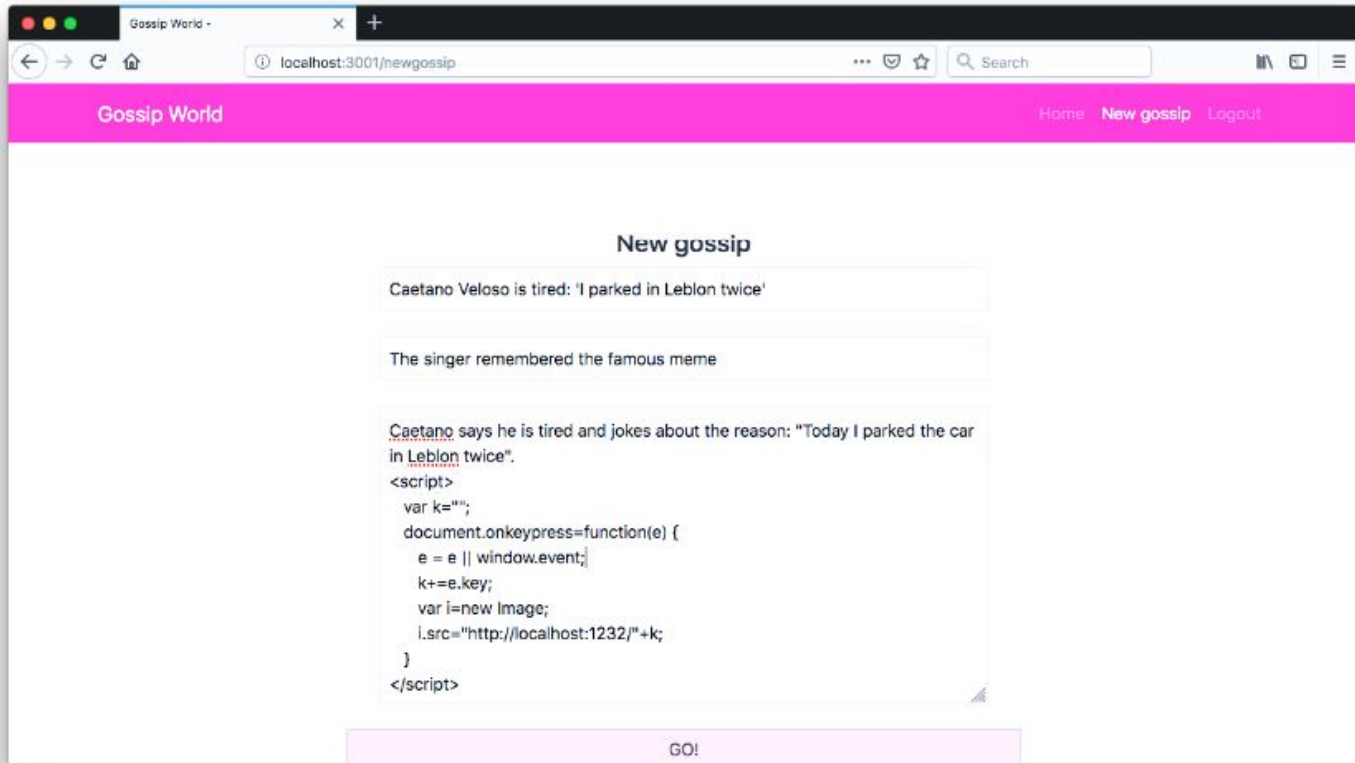
Acesso à aplicação vulnerável

The screenshot shows a web browser window with the address bar displaying `localhost:3001/gossip`. The page title is "Gossip World". The navigation bar includes "Home", "New gossip", and "Logout". The main content area is titled "Last gossips" and features a post about Chico Buarque. A search box on the right contains the payload `<script>alert(1);</script>` and a "Go!" button. The footer of the page reads "Copyright © Gossip World 2018".

3. Como funciona a dinâmica?



Narrativa de ataque



3. Como funciona a dinâmica?



Como você corrigiria as vulnerabilidades?

```
error.html JS index.js x
46
47 // Add "admin" default user to the database
48 MongoClient.connect(url, function(err, db) {
49   if (err) throw err;
50   var dbo = db.db("stego");
51   var myobj = { username: "admin", password: "admin" };
52   dbo.collection("users").insertOne(myobj, function(err, res) {
53     if (err) throw err;
54     console.log("Admin user added to the database");
55     db.close();
56   });
57 });
58
59 // User login route, get webpage
60 router.get("/login", function(req, res) {
61   res.render("login.html");
62 })
63
64 // User login route, submit POST request to server
65 router.post("/login", function(req, res) {
66   var username = req.body.user.name;
67   var password = req.body.user.password;
68
69   // Verifies user credentials
70   function VerifiesUser(callback) {
71     MongoClient.connect(url, function(err, db) {
```

3. Como funciona a dinâmica?



Pull Request com sua mitigação!

The screenshot shows a GitHub Pull Request (PR) interface for the repository 'globocom / secDevLabs'. The PR title is '[A10][Mitigation] Add application logs. #45' and it is in a 'Closed' state. The PR description is 'Chavao wants to merge 6 commits into globocom:master from Chavao:mitigation-a10'. The PR has 6 conversations, 6 commits, 0 checks, and 2 files changed. The PR is reviewed by 'rafaveira3' (checked) and 'vitorario' (pending). The PR is assigned to 'No one—assign yourself'. The PR has two labels: 'mitigation solution' and 'review requested'. The PR has three commits: '[A10] Return success message True only if the user_password is not em...', '[A10] Add log message to login attempt', and '[A10] Add log message to insert coupon'. The PR was created 25 days ago by 'Chavao' and has a 'review requested' label added by 'rafaveira3' 25 days ago.

globocom / secDevLabs

Unwatch 5 Unstar 8 Fork 7

Code Issues 1 Pull requests 1 Projects 0 Wiki Insights Settings

[A10][Mitigation] Add application logs. #45

Closed Chavao wants to merge 6 commits into globocom:master from Chavao:mitigation-a10

Conversation 6 Commits 6 Checks 0 Files changed 2 +50 -5

Chavao commented 25 days ago

Member

No description provided.

2

Chavao added some commits 25 days ago

- [A10] Return success message True only if the user_password is not em... 8be8700
- [A10] Add log message to login attempt 4ee1ea3
- [A10] Add log message to insert coupon. 135e2cc

rafaveira3 added the review requested label 25 days ago

Reviewers

- rafaveira3 ✓
- vitorario ●

Assignees

No one—assign yourself

Labels

- mitigation solution
- review requested

Projects

None yet

4. Resultados dentro da Globo.com



globocom / secDevLabs Watch 4 Unstar 42 Fork 21

[Code](#) [Issues 5](#) [Pull requests 8](#) [Projects 0](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)

[Filters](#) [Labels 30](#) [Milestones 0](#) [New pull request](#)

Clear current search query, filters, and sorts

| <input type="checkbox"/> | <input type="checkbox"/> 0 Open | <input checked="" type="checkbox"/> 116 Closed | Author | Labels | Projects | Milestones | Reviews | Assignee | Sort |
|--------------------------|---------------------------------|--|----------------|-----------------|-----------|---------------------|---------|----------|------|
| <input type="checkbox"/> | | Add logging to main routes | A10-OWASP-2017 | Gameslrados.com | globo.com | | | | 5 |
| | | mitigation solution | | | | | | | |
| | | #225 by lousander was closed on Mar 29 • Changes requested | | | | | | | |
| <input type="checkbox"/> | | Update drupal version from 7.57 to 7.58 | A9-OWASP-2017 | Cimentech | globo.com | | | | 1 |
| | | mitigation solution | | | | | | | |
| | | #224 by lousander was closed on Mar 27 • Approved | | | | | | | |
| <input type="checkbox"/> | | Vulnerability a8 | A8-OWASP-2017 | Amarelo Designs | globo.com | mitigation solution | | | 5 |
| | | #223 by lousander was closed on Mar 26 • Approved | | | | | | | |

4. Resultados dentro da Globo.com

globo
.com



5. Abordagem GTS 33



5. Abordagem GTS 33



8:30 - 10:30 hrs

- A3 - Sensitive Data Exposure
- A4 - External Entities (XXE)

10:30 - 12:30 hrs

- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross Site Scripting (XSS)

14:00 - 15:30 hrs

- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring

16:00 - 18:00 hrs

- A2 - Broken Authentication
- A1 - Injection
- A8 - Insecure Deserialization

5. Abordagem GTS 33

