ORNA™

Secure Coding Workshop

One of the weakest links in cybersecurity are the attack vectors created within applications.

Learn how to evaluate and integrate security and software development in this one-day workshop.

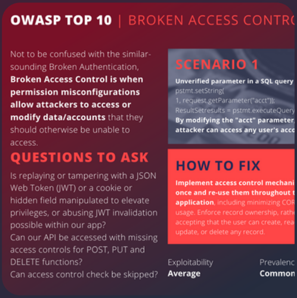
UP TO 50 PARTICIPANTS
9 AM TO 5 PM
ONLINE OR IN-PERSON

Register now! Go to www.orna.app or chat with our Special Advisory Services (SAS) team to book this workshop. Limited slots available.

© 2021-2022 ORNA Inc. All rights reserved.

SECURITY BY DESIGN

In 2022, secure software is a must - and it starts with your dev team. Learn how to build security into your SDLC to reduce development and testing effort, automate workflows and improve on your reputation.



OWASP TOP 10 | BROKEN ACCESS CONTR

Not to be confused with the similar-sounding Broken Authentication, **Broken Access Control is when permission misconfigurations allow attackers to access or modify data/accounts** that they should otherwise be unable to access.

QUESTIONS TO ASK

Is replaying or tampering with a JSON Web Token (JWT) or a cookie or hidden field manipulated to elevate privileges, or abusing JWT invalidation possible within our app?
Can our API be accessed with missing access controls for POST, PUT and DELETE functions?
Can access control check be skipped?

SCENARIO 1

Unverified parameter in a SQL query

```
pstmt.setString(
1, request.getParameter("acct"));
ResultSetresults = pstmt.executeQuery
```

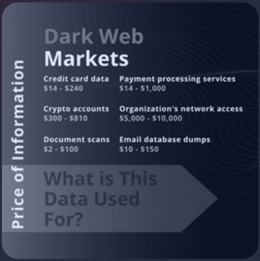
By modifying the "acct" parameter, attacker can access any user's acc

HOW TO FIX

Implement access control mechani once and re-use them throughout t application, including minimizing COR usage. Enforce record ownership, rath accepting that the user can create, rea update, or delete any record.

Exploitability
Average

Prevalenc
Common



Price of Information

Dark Web **Markets**

Credit card data
$14 - $240

Payment processing services
$14 - $1,000

Crypto accounts
$300 - $810

Organization's network access
$5,000 - $10,000

Document scans
$2 - $100

Email database dumps
$10 - $150

What is This Data Used For?

AGENDA

9 AM - Registration an Short Introductions

9:30 AM to 10:30 AM - Software Development Models & Lifecycle
- Agile, Waterfall, SDLC & DevSecOps

10:30 AM to 12 PM - Software Vulnerabilities Types & Origins
- encryption & hashing-based attacks
- data & command injections
- request forgery and more

12 PM to 1 PM - Lunch

1 PM to 2 PM - Secure Coding Techniques & Best Practices
- input validation
- secure authentication
- session management
- database security and more

2 PM to 3 PM - Manual & Automatic Code Security Reviews

3 PM to 4:30 PM - Security Testing Tools & Frameworks

4:30 PM to 5 PM - Future of Code, Where are we now?, Wrap Up

Each chapter includes interactive exercises and discussions.

© 2021-2022 ORNA Inc. All rights reserved.