OWASP® and beyond
-
much more than just OWASP Top 10

OWASP®

OWASP FOUNDATION

MISSION

The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Our programming includes:

- Community-led open source software projects
- Over 250+ local chapters worldwide
- Tens of thousands of members
- Industry-leading educational and training conferences

The OWASP Community

- OWASP is a worldwide **free** and **open community** focused on improving the security of application software.
- Our mission is to make application security **visible** so that people and organisations can make **informed decisions** about application security **risks**.

Session at Global AppSec Amsterdam

Its all for free

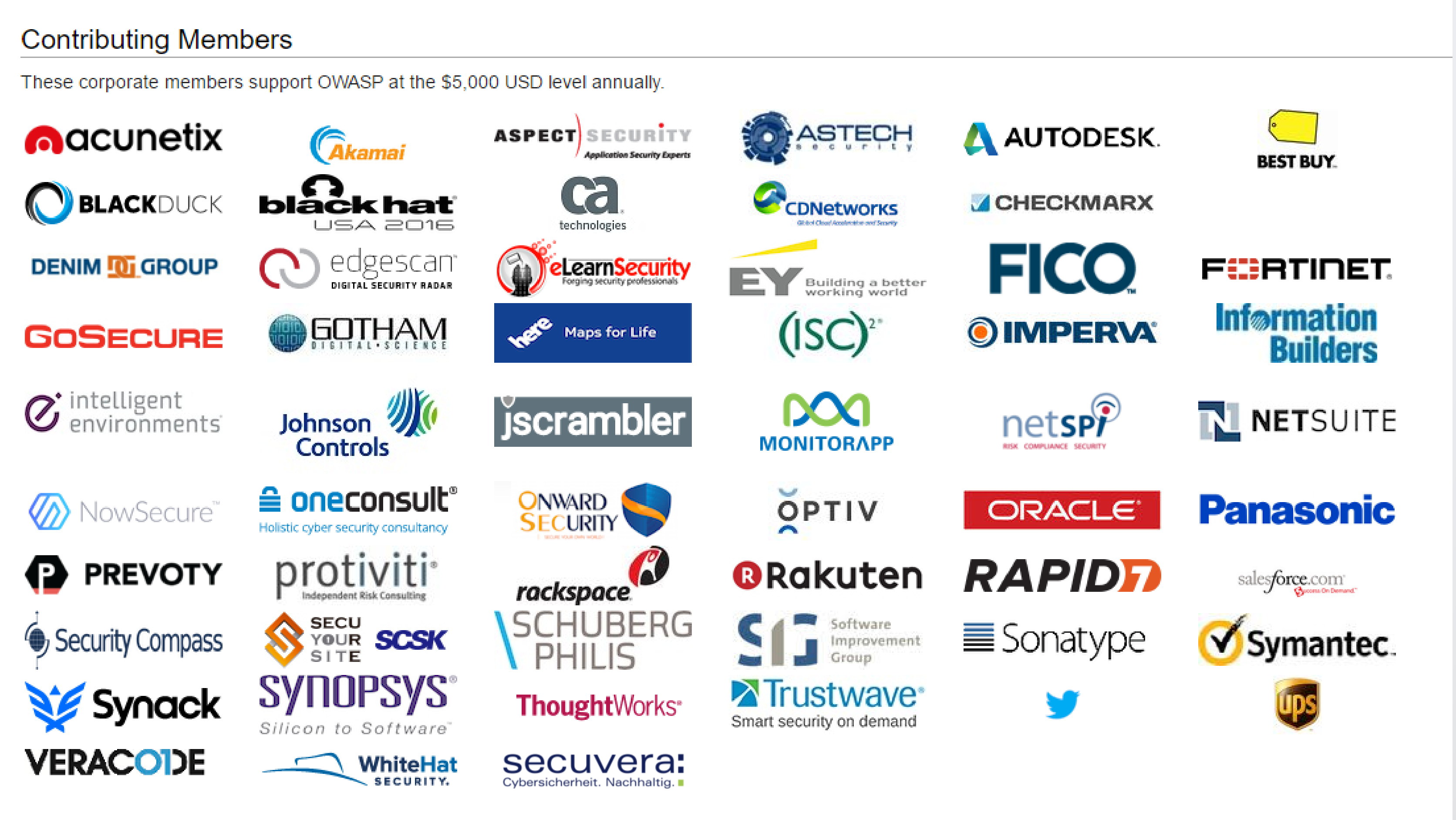
- Everyone is **free** to participate in OWASP and **all** of our materials are available under a **free** and **open** software license.

- All OWASP events *(except conferences)* are free to attend by both members and non-members of OWASP - and can be attended by anyone who is interested in Application Security and Cyber Security in general.

Member Lounge at OWASP Conference

The OWASP Foundation

- We are a **Global not-for-profit charitable** organisation
- Vendor-Neutral Community
- **Collective Wisdom** of the **Best Minds in Application Security Worldwide**
- Provide **free** tools, guidance, documentation
- Meetings are **free to attend** *(free drinks & food included)*
- Meetings are usually **2-hour seminars**
  (usually 2 main talks, with optional lightning talks)



Contributing Members

These corporate members support OWASP at the $5,000 USD level annually.

acunetix
Akamai
ASPECT SECURITY Application Security Experts
ASTECH security
AUTODESK.
BEST BUY.
BLACKDUCK
black hat USA 2016
ca technologies
CDNetworks Global Cloud Acceleration and Security
CHECKMARX
DENIM GROUP
edgescan DIGITAL SECURITY RADAR
eLearnSecurity Forging security professionals
EY Building a better working world
FICO
FORTINET.
GoSecure
GOTHAM DIGITAL SCIENCE
here Maps for Life
(ISC)²
IMPERVA
Information Builders
intelligent environments
Johnson Controls
jscrambler
MONITORAPP
netSPI RISK COMPLIANCE SECURITY
NETSUITE
NowSecure
oneconsult Holistic cyber security consultancy
ONWARD SECURITY
OPTIV
ORACLE
Panasonic
PREVOTY
protiviti Independent Risk Consulting
rackspace
Rakuten
RAPID7
salesforce.com Success On Demand
Security Compass
SECU YOUR SITE
SCSK
SCHUBERG PHILIS
Software Improvement Group
Sonatype
Symantec.
Synack
SYNOPSYS Silicon to Software
ThoughtWorks
Trustwave Smart security on demand
ups
VERACODE
WhiteHat SECURITY.
secuvera: Cybersicherheit. Nachhaltig.

Diamond members

apiiro

CEQUENCE™ SECURITY

Platinum members

Adobe

ATLASSIAN

BIONIC

Bloomberg®

BLACK BELT SECURITY

COALFIRE®

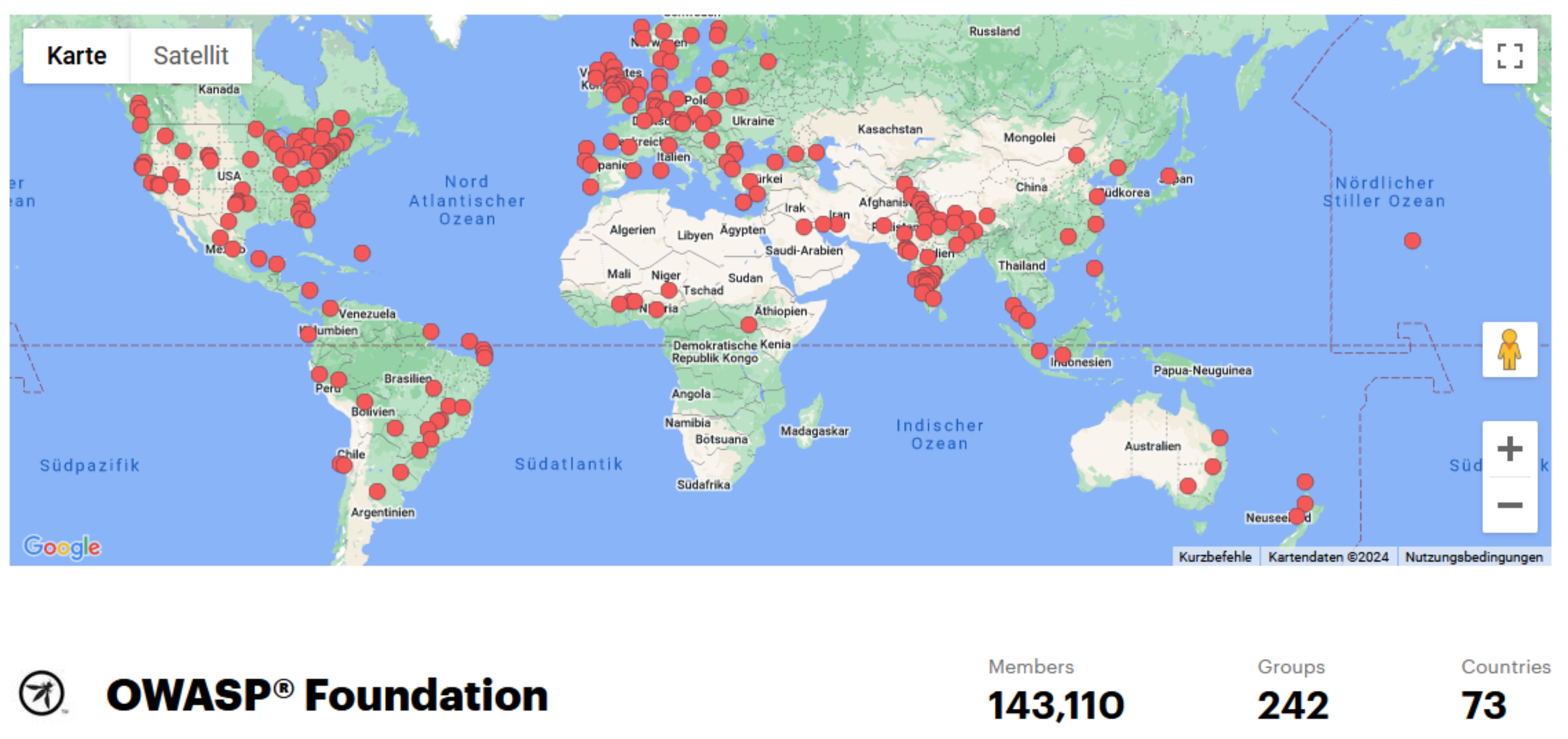
Contrast SECURITY

Fortify

Qualys®

salesforce

World Wide



OWASP® Foundation

Members	Groups	Countries
143,110	242	73

OWASP German Chapter

www.owasp.de

OWASP German Chapter

- City Chapter Meetings
- Regional Chapter Meetings
- German OWASP Day (2024)

We are volunteers

45,000+ OWASP volunteers worldwide

- Located Stuttgart/Gäufelden
- Foundation: July 1, 1982
- Owner-managed
- Vendor-independent
- IT-Security since 1988
- Pure service provider

Great Place To Work®
Certified
DEZ 2023-DEZ 2024
DE

Beste Arbeitgeber™
Consulting
Great Place To Work®
Deutschland
2024

Beste Arbeitgeber™
Baden-Württemberg
Great Place To Work®
Deutschland
2024

Beste Arbeitgeber™
kleiner Mittelstand
Great Place To Work®
Deutschland
2024

- Three consulting areas
  - Security Consulting („BSI-Grundschutz“/ISO 27001)
  - Penetration testing
  - BSI-Evaluation Facility 62443 / Industrial Security

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierter
IT-Sicherheitsdienstleister

A P
C D

Zertifikat Nummer:
BSI-APS-9002
gültig bis 31.03.2025

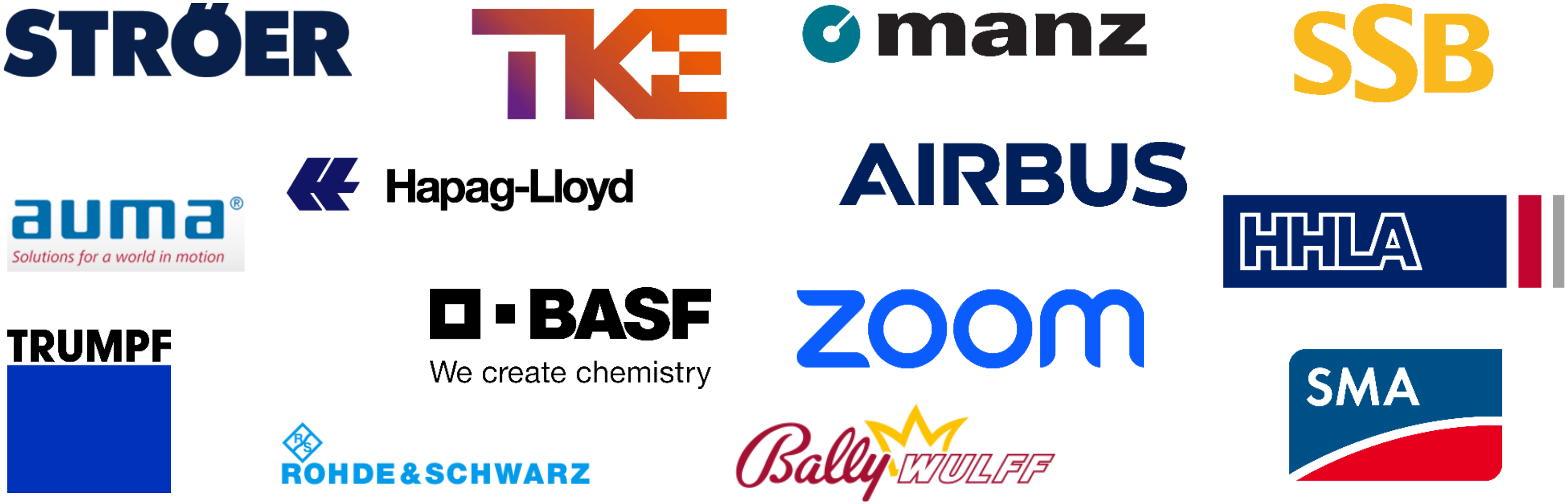
Bundesamt
für Sicherheit in der
Informationstechnik

Anerkannte Prüfstelle
für IT-Sicherheit

A P
C D

BSI-Registriernummer:
BSI-APS-9002
gültig bis 31.03.2025

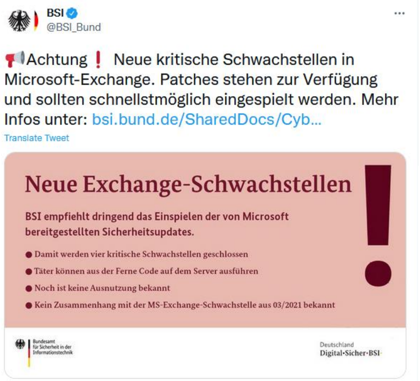
- Some of our valued customers



- whoami
  - Tobias Glemser, CEO of secuvera
  - +20 Cybersecurity Footprint
  - BSI certified Penetration Tester

secuvera

- Real World Examples



BSI
@BSI_Bund

📢Achtung ❗ Neue kritische Schwachstellen in Microsoft-Exchange. Patches stehen zur Verfügung und sollten schnellstmöglich eingespielt werden. Mehr Infos unter: bsi.bund.de/SharedDocs/Cyb...

Translate Tweet

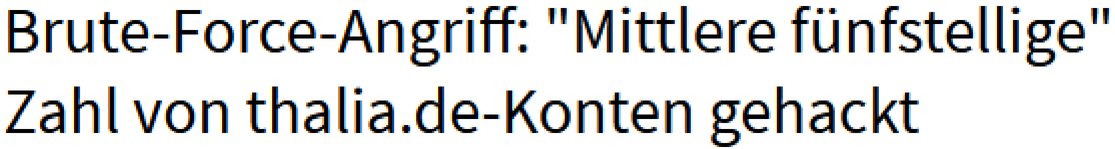
Neue Exchange-Schwachstellen

BSI empfiehlt dringend das Einspielen der von Microsoft bereitgestellten Sicherheitsupdates.

- Damit werden vier kritische Schwachstellen geschlossen
- Täter können aus der Ferne Code auf dem Server ausführen
- Noch ist keine Ausnutzung bekannt
- Kein Zusammenhang mit der MS-Exchange-Schwachstelle aus 03/2021 bekannt

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI

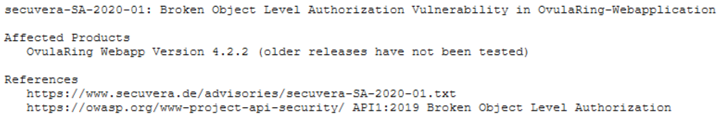


Brute-Force-Angriff: "Mittlere fünfstellige" Zahl von thalia.de-Konten gehackt

🔥 Alert!

Kritische Zero-Day-Lücke in Log4j gefährdet zahlreiche Server und Apps

Apple, Twitter, Amazon und tausende andere Dienste sind anfällig; erste Angriffe laufen bereits. Admins sollten unbedingt jetzt handeln.



```
secuvera-SA-2020-01: Broken Object Level Authorization Vulnerability in OvulaRing-Webapplication

Affected Products
   OvulaRing Webapp Version 4.2.2 (older releases have not been tested)

References
   https://www.secuvera.de/advisories/secuvera-SA-2020-01.txt
   https://owasp.org/www-project-api-security/ API1:2019 Broken Object Level Authorization
```

What is OWASP penetration testing?

We use OWASP. We‘re good.

We cover all risiks of OWASP Top 10.

- OWASP
  - Open Worldwide Application Security Project
  - Non-profit
  - Open-Source
  - Projects (+300): Documents and programs
  - Known for OWASP Top 10
  - Active in Chapters worldwide
  - In Germany
    - Regional Chapter
    - City-Chapters / „Stammtische“ (regular‘s table)

- OWASP Top 10 Risks
  - Methodology: Vocabulary
    - Common Weakness Enumeration (CWE): Types of vulnerabilities
    - Common Vulnerability Scoring System (CVSS): Metric for measuring the severity of a particular vulnerability
    - Common Vulnerabilities and Exposures (CVE): Vulnerability database for products (e.g., not cloud services)

- OWASP Top 10 Risks
  - Methodology
    - Data
      - Basis: (mostly) static code analysis of 12 manufacturers/service providers
      - Categorization according to CWE
      - If a CWE in a test: one point for this CWE
      - Multiple identical CWEs: one additional point for this CWE
    - Open survey of „experts“

- OWASP Top 10 Risks
  - Methodology
    - CWEs for A1

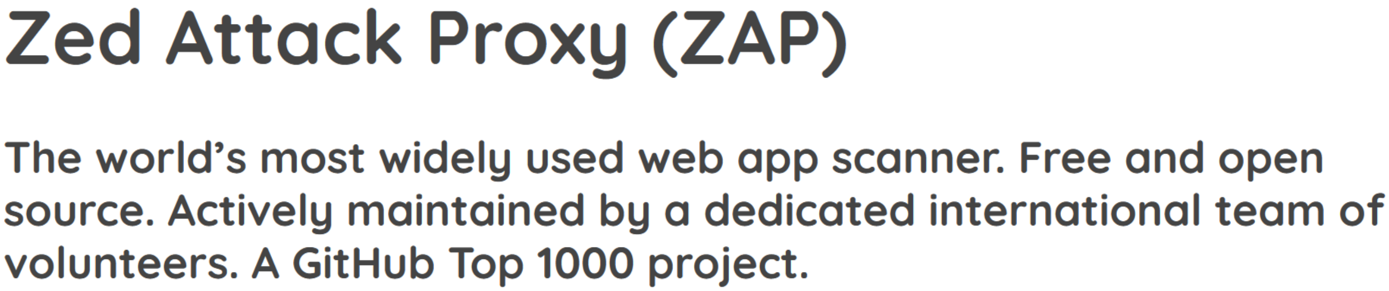
CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23 Relative Path Traversal
CWE-35 Path Traversal: '.../...//'
CWE-59 Improper Link Resolution Before File Access ('Link Following')
CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
CWE-201 Exposure of Sensitive Information Through Sent Data
CWE-219 Storage of File with Sensitive Data Under Web Root
CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)
CWE-275 Permission Issues
CWE-276 Incorrect Default Permissions
CWE-284 Improper Access Control
CWE-285 Improper Authorization
CWE-352 Cross-Site Request Forgery (CSRF)
CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
CWE-377 Insecure Temporary File
CWE-402 Transmission of Private Resources into a New Sphere ('Resource Leak')
CWE-425 Direct Request ('Forced Browsing')
CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')
CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory
CWE-540 Inclusion of Sensitive Information in Source Code
CWE-548 Exposure of Information Through Directory Listing
CWE-552 Files or Directories Accessible to External Parties
CWE-566 Authorization Bypass Through User-Controlled SQL Primary Key
CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
CWE-639 Authorization Bypass Through User-Controlled Key
CWE-651 Exposure of WSDL File Containing Sensitive Information
CWE-668 Exposure of Resource to Wrong Sphere
CWE-706 Use of Incorrectly-Resolved Name or Reference
CWE-862 Missing Authorization
CWE-863 Incorrect Authorization
CWE-913 Improper Control of Dynamically-Managed Code Resources
CWE-922 Insecure Storage of Sensitive Information
CWE-1275 Sensitive Cookie with Improper SameSite Attribute

- OWASP Top 10 2021
  - A01 Broken Access Control
  - A02 Cryptographic Failures
  - A03 Injection
  - A04 Insecure Design
  - A05 Security Misconfiguration
  - A06 Vulnerable and Outdated Components
  - A07 Identification and Authentication Failures
  - A08 Software and Data Integrity Failures
  - A09 Security Logging and Monitoring Failures
  - A10 Server Side Request Forgery (SSRF)

- OWASP Top 10
  - Use it for awareness
  - Use it for training
  - Use it for „push left“
  - Don‘t use it for anything else

Other ressources for other purposes

- (former OWASP) ZAP

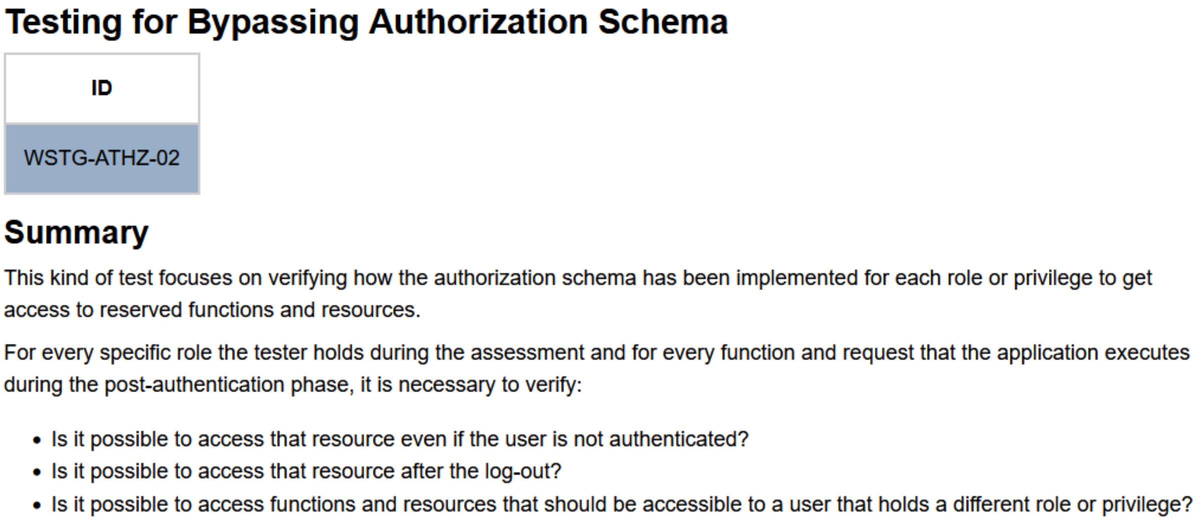


Zed Attack Proxy (ZAP)

The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers. A GitHub Top 1000 project.

  - Dynamic Application Security Testing (DAST)
  - CI/CD Integration
  - 140+ volunteers

- OWASP Web Security Testing Guide (WSTG)
  - Test yourself
  - Use as testing plan in a pentest



Testing for Bypassing Authorization Schema

ID
WSTG-ATHZ-02

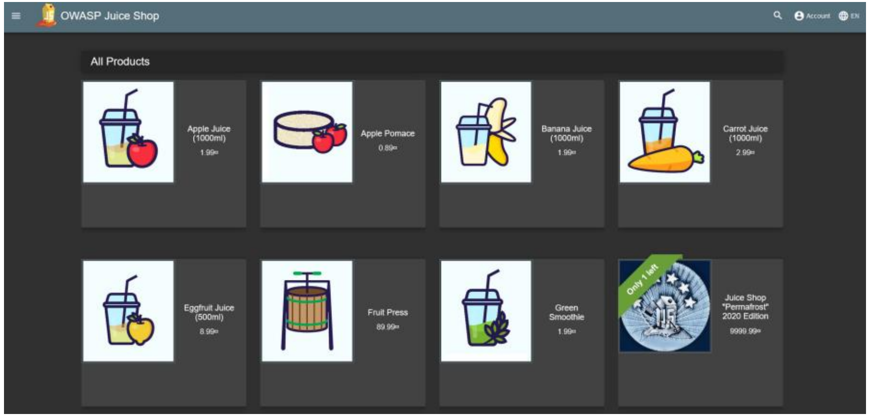
Summary

This kind of test focuses on verifying how the authorization schema has been implemented for each role or privilege to get access to reserved functions and resources.

For every specific role the tester holds during the assessment and for every function and request that the application executes during the post-authentication phase, it is necessary to verify:

- Is it possible to access that resource even if the user is not authenticated?
- Is it possible to access that resource after the log-out?
- Is it possible to access functions and resources that should be accessible to a user that holds a different role or privilege?

- OWASP Juice Shop
  - Educate yourself (or book a training ☺)
  - Flagship Project
  - node.js, Angular, Express, NoSQL, Websockets,…



All Products

Apple Juice (1000ml) 1.99¤

Apple Pomace 0.89¤

Banana Juice (1000ml) 1.99¤

Carrot Juice (1000ml) 2.99¤

Eggfruit Juice (500ml) 8.99¤

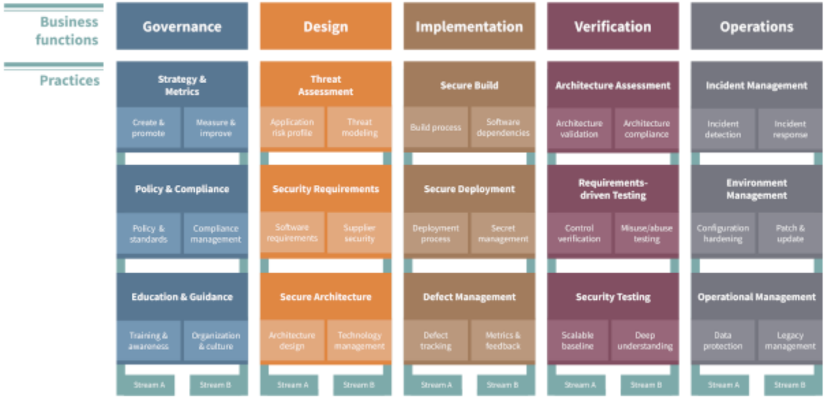
Fruit Press 89.99¤

Green Smoothie 1.99¤

Juice Shop "Permafrost" 2020 Edition 9999.99¤

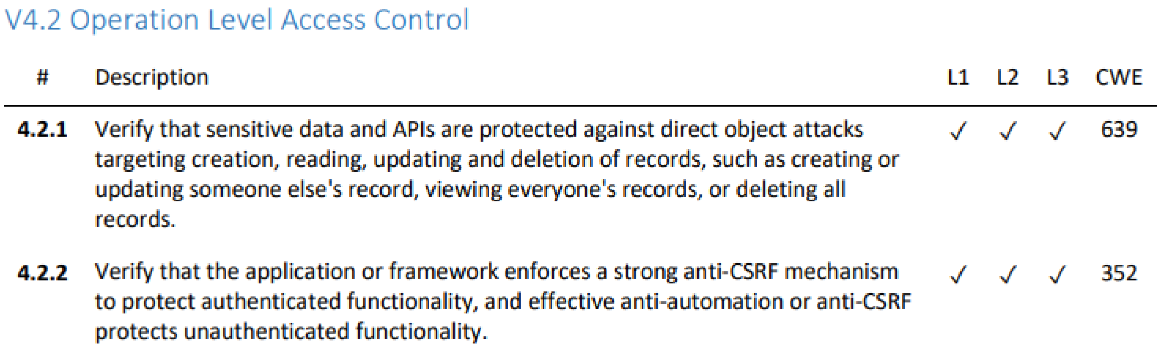
secuvera

- OWASP SAMM
  - Push Left
  - Secure Development Lifecycle
  - Very mature
  - Usable outside web (e. g. IEC 62443-4-1)



Business functions	Governance	Design	Implementation	Verification	Operations
Practices	Strategy & Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
	Create & promote Measure & improve	Application risk profile Threat modeling	Build process Software dependencies	Architecture validation Architecture compliance	Incident detection Incident response
	Policy & Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
	Policy & standards Compliance management	Software requirements Supplier security	Deployment process Secret management	Control verification Misuse/abuse testing	Configuration hardening Patch & update
	Education & Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management
	Training & awareness Organization & culture	Architecture design Technology management	Defect tracking Metrics & feedback	Scalable baseline Deep understanding	Data protection Legacy management
	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B

- OWASP Application Security Verification Standard (ASVS)
  - Governance
  - Checkliste
  - Heatmap



V4.2 Operation Level Access Control

#	Description	L1	L2	L3	CWE
4.2.1	Verify that sensitive data and APIs are protected against direct object attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	✓	✓	✓	639
4.2.2	Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	✓	✓	✓	352

Demo

ziener

Q&A

Thanks