
OWASP DAY
Viedma 2017

OWASP
The Open Web Application Security Project

BIENVENIDOS

OWASP DAY – Viedma 2017

OWASP
The Open Web Application Security Project

Antes de comenzar...

Gracias a:

- Ustedes por levantarse temprano y venir :)
- Giselle Roumec, Leandro Boisselier, Facundo Alcalde
- A los expositores por la buena onda

OWASP
The Open Web Application Security Project

Gracias a los patrocinadores de este evento!!!

ALTEC
Telecomunicaciones y Sistemas S.E.

UNIVERSIDAD NACIONAL DEL COMAHUE
1972

LEGISLATURA
del pueblo de la
Provincia de Río Negro

OWASP
The Open Web Application Security Project

¿Qué es OWASP?

OWASP es una organización sin fines de lucro que busca crear conciencia sobre la importancia de la seguridad en la información.

https://www.owasp.org/

OWASP
The Open Web Application Security Project

¿Qué es OWASP Day – Viedma 2017?

Es un día de conferencias dedicadas a la seguridad de la información. Con el objetivo de aprender, conocerse, intercambiar conocimientos y … tomar café gratis ;)

https://www.owasp.org/index.php/Patagonia#tab=OWASP_Day

200

Proyectos Activos

250+

Capítulos Activos


100+
Academic Supporters

OWASP

FLAGSHIP - TOOLS

mature projects

OWASP Zed Attack Proxy

OWASP Web Testing Environment Project

OWASP OWTF

OWASP Dependency Check

OWASP FLAGSHIP - CODE

mature projects

OWASP ModSecurity Core Rule Set Project

OWASP CSRFGuard Project

OWASP AppSensor Project

OWASP

FLAGSHIP - DOCs

mature projects

OWASP ASVS

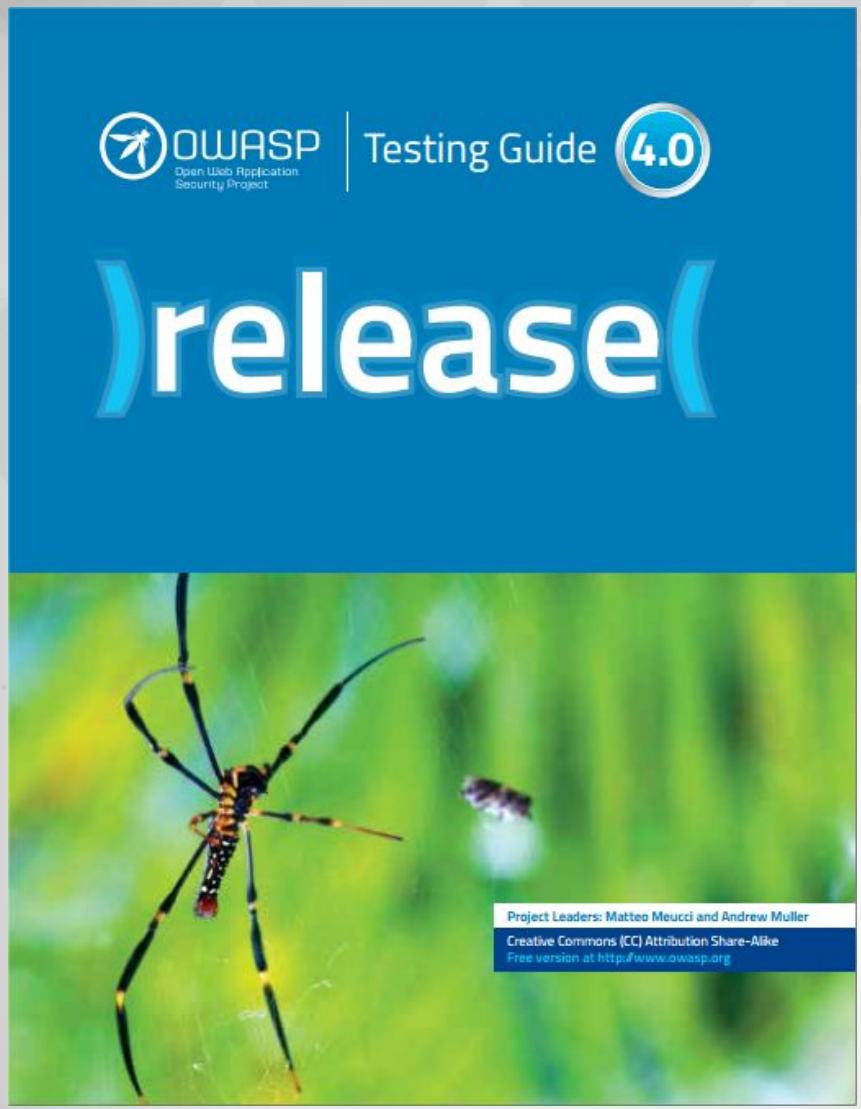
OWASP Software Assurance Maturity Model

OWASP AppSensor Project

OWASP Top Ten Project

OWASP Testing Guide Project

https://www.owasp.org/index.php/OWASP_SAMM_Project



How to test

Testing for access to administrative functions

For example, suppose that the 'AddUser.jsp' function is part of the administrative menu of the application, and it is possible to access it by requesting the following URL:

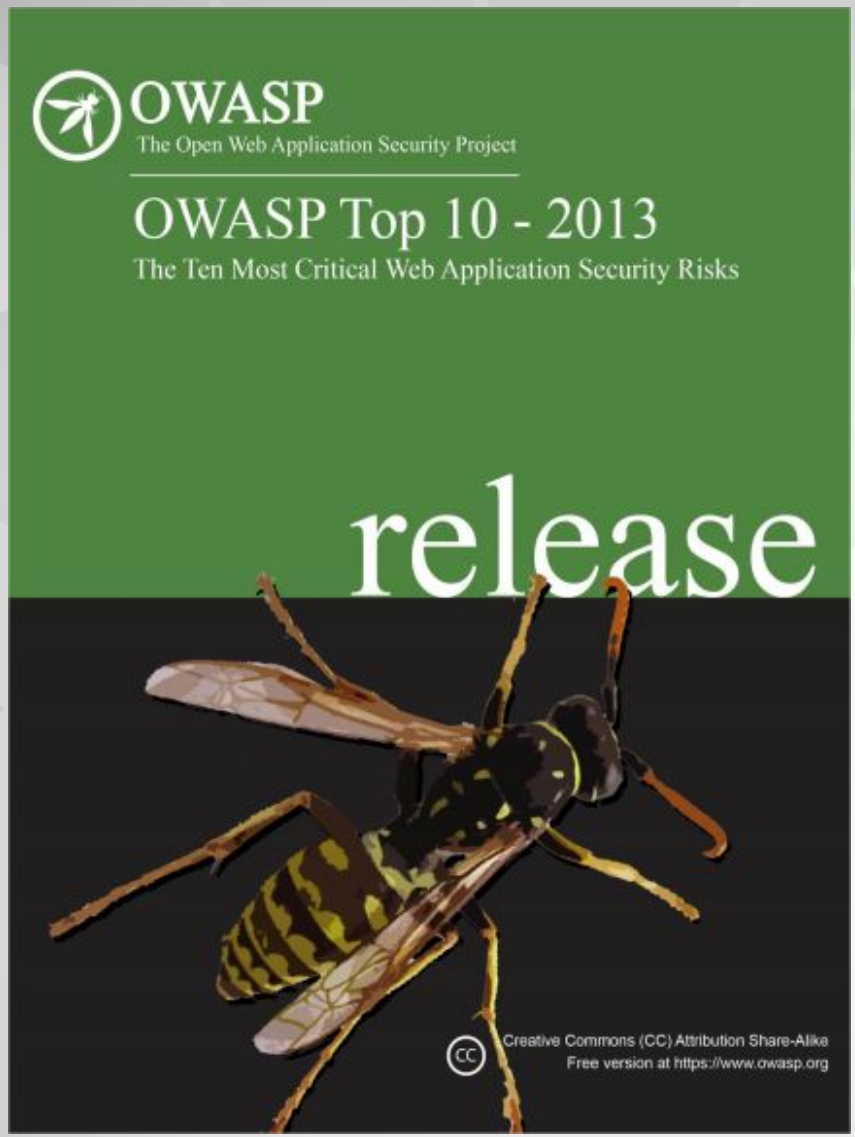
```
https://www.example.com/admin/addUser.jsp
```

Then, the following HTTP request is generated when calling the AddUser function:

```
POST /admin/addUser.jsp HTTP/1.1
Host: www.example.com
[other HTTP headers]

userID=fakeuser&role=3&group=grp001
```

What happens if a non-administrative user tries to execute that request? Will the user be created? If so, can the new user use their privileges?



T10 OWASP Top 10 Application Security Risks – 2013

A1 – Injection	Injection flaws, such as SQL, 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 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. 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.
A4 – Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 – Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6 – Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7 – Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8 - Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10 – Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

OWASP
The Open Web Application Security Project

Latam Tour de OWASP

- Conferencias Gratuitas de Seguridad
- 16 países recorridos durante el mes de abril
- Realizado en la Patagonia desde el 2015 en Neuquén
- https://www.owasp.org/index.php/LatamTour2017

OWASP

The Open Web Application Security Project

Hora	Conferencia	Expositor
09:30 - 10:00	Acreditación	
10:00 - 10:10	Presentación	Gastón Toth
10:10 - 10:50	La importancia de la Alerta Temprana - La Ciberseguridad en la República Argentina	Eduardo Martino
10:50 - 11:20	Pausa para café	
11:20 - 12:00	Experiencias en seguridad y gobierno	Arturo 'Buanzo' Busleiman
12:00 - 12:40	Ciberseguridad, panorama y retos a encarar	Pedro Janices
12:40 - 14:30	Pausa para almuerzo	
14:30 - 15:10	Seguridad en aplicaciones web	Gaston Toth
15:10 - 15:50	Hacking NFC/RFID	Nahuel Grisolia
15:50 - 16:20	Pausa para cafe	
16:20 - 17:00	Testing Android Apps	Gustavo Sorondo
17:00 - 17:10	Cierre	

OWASP
The Open Web Application Security Project

Certificado de Asistencia

Nombre Apellido

ha participado del OWASP Day – Viedma 2017, realizado el día 17 de Noviembre de 2017 en la ciudad de Viedma, Argentina.

Gastón Toth
Líder de Capítulo, Patagonia
OWASP Foundation

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

Contacto

- diego.dinardo@owasp.org
- gaston.toth@owasp.org

Twitter

- @OWASP_Patagonia
- Compartan fotos y comentarios!