Aplicaciones Web I

CC5325 - Taller de Hacking Competitivo
Diego Vargas

Contenidos

- Introducción a Web
- OWASP
- Técnicas básicas
- Demo

Introducción a Web

Análisis Estático

Se revisa los elementos estáticos del sitio web:

- Archivos HTML y JavaScript
- Código fuente
- Deobfuscación de código
- Cookies y almacenamiento local

Análisis Dinámico

Se revisa la interacción con el servidor web y sus recursos:

- Reenviar y modificar requests HTTP
- Se busca otros endpoints
- Se identifica tecnologías utilizadas
- Se intenta romper cosas

Notación

- **Vulnerabilidad**: debilidad teórica en el sistema que puede ser aprovechada por un adversario.
- **Exploit**: implementación de un ataque a una vulnerabilidad.
- **Payload**: request que gatilla la vulnerabilidad.
- **Parche**: Contramedida que elimina la vulnerabilidad.

Tipos de vulnerabilidades:

- Por implementación: Bugs -> Comportamiento inesperado
- Por lógica: Diseño vulnerable -> Exploit
- Por dependencias: Librería vulnerable -> CVE

En la realidad se encuentran combinaciones de estas

Pasos a seguir:

1. Reconocimiento: Identificar recursos protegidos y estructura del sitio web.
2. Pre-explotación: Preparar ambiente, encontrar posibles vulnerabilidades.
3. Explotación: Explotar vulnerabilidades y obtener acceso a recursos protegidos.
4. Post-explotación: Extraer información, utilizar recursos, escalar privilegios.

OWASP

“The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.”

https://owasp.org/

Top 10 Web Application Security Risks

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entity
5. Broken Access Control
6. Security Misconfiguration
7. Cross Site Scripting
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

https://owasp.org/www-project-top-ten/

Web Security Testing Guide

Guía que intenta estandarizar las pruebas de seguridad en aplicaciones web. Tiene explicaciones sobre por qué aparecen diferentes tipos de vulnerabilidades, cómo explotarlas y mitigarlas.

https://owasp.org/www-project-web-security-testing-guide/

Otros Proyectos de OWASP

- Dependency Track
- Software Assurance Maturity Model
- Mobile Security Testing Guide
- Zed Attack Proxy
- ModSecurity Core Rule Set

Técnicas Básicas

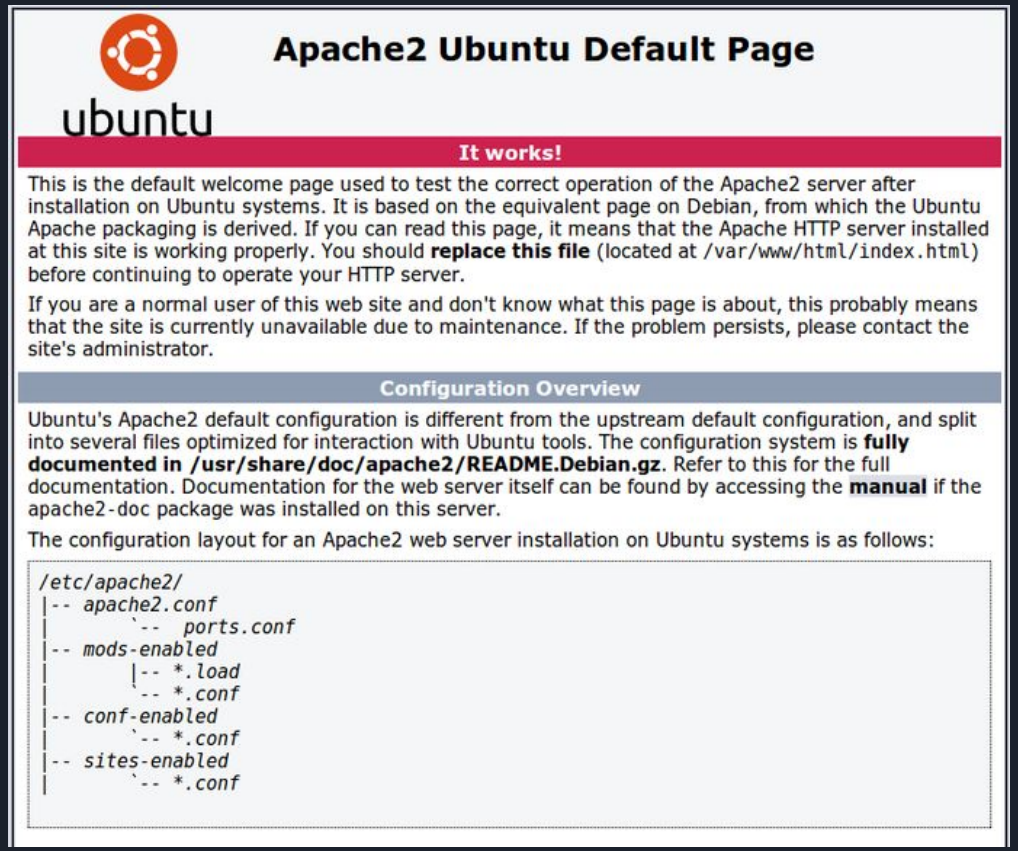
Enumeración

Objetivo:

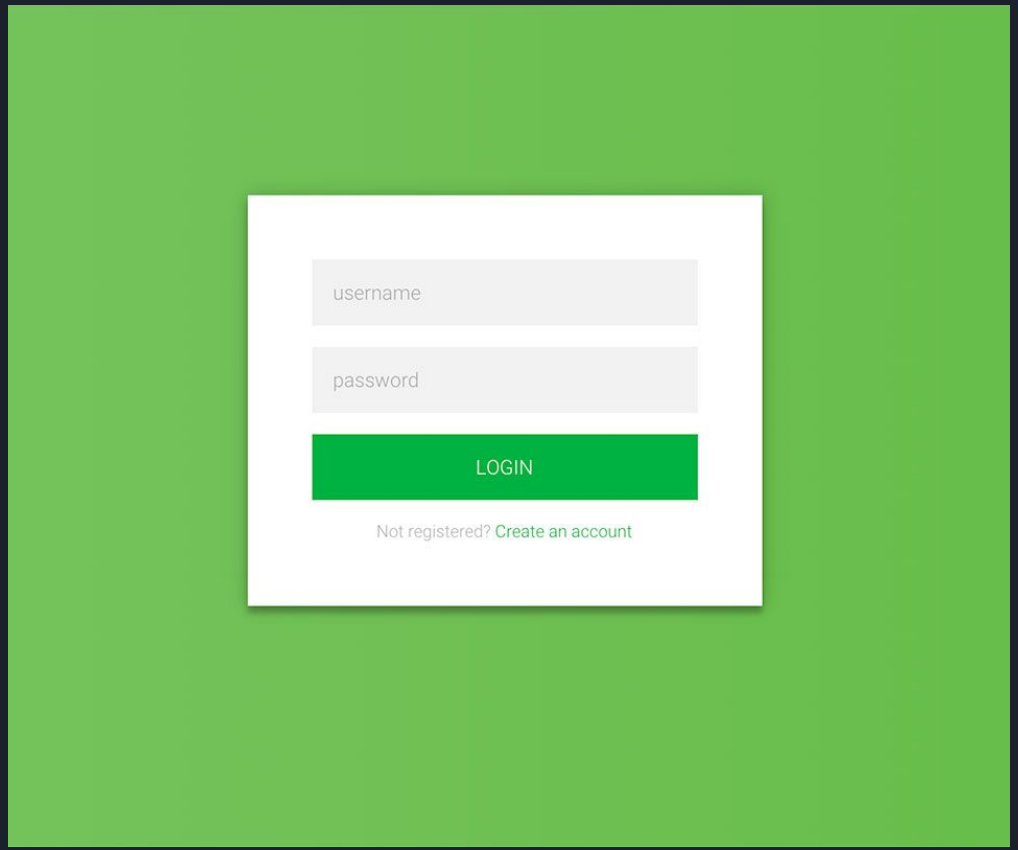
Encontrar recursos o información escondida mediante el uso de diccionarios o fuzzers.

Esto comprende enumeración de subdirectorios, subdominios, nombres de usuario, parámetros GET y POST, etc.

/index.html


Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

/secret-login.html

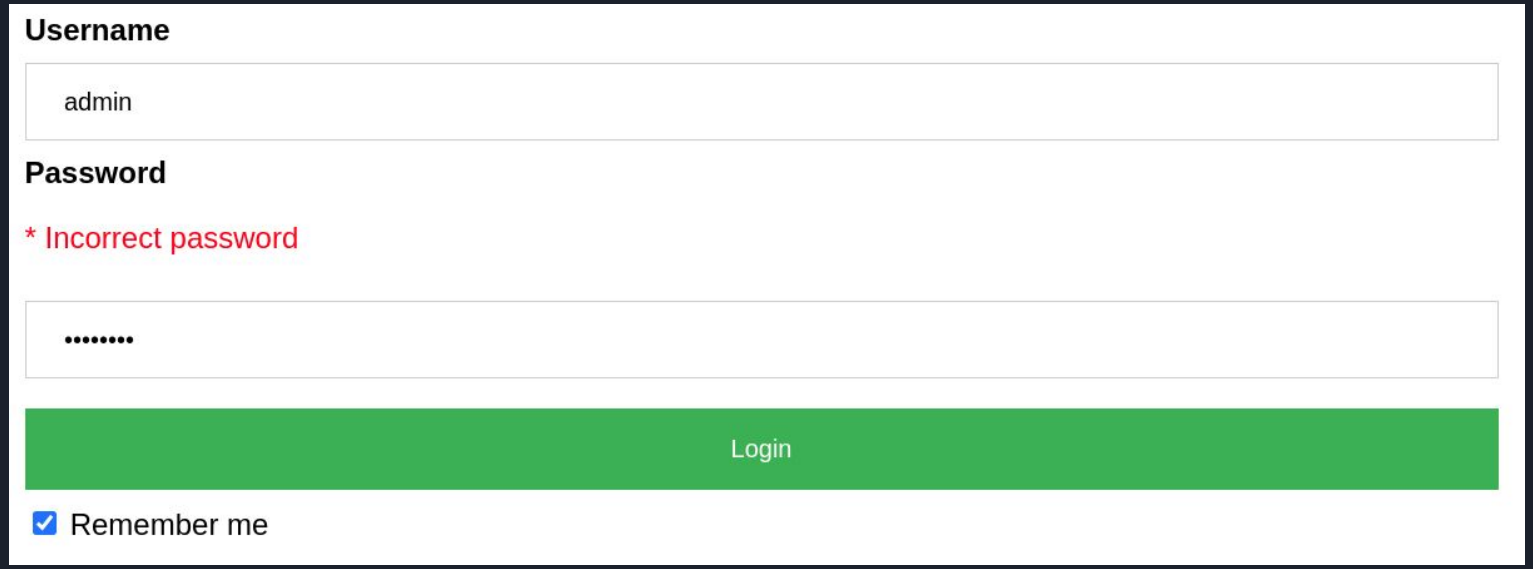


Fuerza Bruta

Objetivo:

Iterar por todos los valores de un parámetro (o al menos los más probables) hasta encontrar el correcto.

Se utiliza para encontrar la contraseña de un usuario, el valor de un “parámetro mágico”, secuencias específicas, etc.


Username
admin
Password
* Incorrect password
••••••••
Login
Remember me

Demo

Herramientas

- Firefox
- FoxyProxy (plugin)
- Burp Suite https://portswigger.net/burp/communitydownload
- Dirsearch https://github.com/maurosoria/dirsearch
- Wfuzz https://github.com/xmendez/wfuzz
- Hydra https://github.com/vanhauser-thc/thc-hydra