

Universidad Paraguay Aleman



**UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN**



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico.....	3
Recopilación de Información sobre un Sitio Web Usando Google Dorks.....	4
Objetivo:.....	4
Materiales Necesarios:	4
Instrucciones:	4
Paso 1: Identificar el Sitio Web de Interés.....	4
Paso 2: Realizar Búsquedas Básicas	4
Paso 3: Búsquedas de Seguridad.....	5
Paso 4: Identificar Vulnerabilidades	5
Paso 5: Documentación de Resultados	6
Ejemplo de Informe:	6
1. Resumen.....	6
2. Información Básica	6
3. Archivos Públicos	6
4. Búsquedas de Seguridad	7
5. Identificación de Vulnerabilidades	7
6. Recomendaciones de Seguridad	7
Conclusión	7
Consideraciones Éticas.....	8

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Recopilación de Información sobre un Sitio Web Usando Google Dorks

Objetivo:

El objetivo de esta tarea es utilizar técnicas avanzadas de búsqueda en Google, conocidas como Google Dorks, para recopilar información detallada sobre un sitio web específico. Los estudiantes aprenderán a identificar información sensible, archivos expuestos, y posibles vulnerabilidades en el sitio web seleccionado.

Materiales Necesarios:

- Una computadora con acceso a internet.
- Un navegador web.
- Una cuenta de Google (opcional para guardar búsquedas y resultados).

Instrucciones:

Paso 1: Identificar el Sitio Web de Interés

1. Selecciona un sitio web objetivo para la recopilación de información. Asegúrate de tener permiso para realizar estas búsquedas o usa un sitio web de práctica que permita la investigación de seguridad.

Paso 2: Realizar Búsquedas Básicas

1. **Información Básica del Sitio:**
 - Usa el siguiente dork para encontrar páginas indexadas en el sitio web.

```
site:example.com
```

2. **Archivos Públicos:**

- Busca documentos PDF en el sitio web.

```
site:example.com filetype:pdf
```

- Busca documentos de Word en el sitio web.

```
site:example.com filetype:doc OR filetype:docx
```

- Busca hojas de cálculo en el sitio web.

```
site:example.com filetype:xls OR filetype:xlsx
```

Paso 3: Búsquedas de Seguridad

1. Páginas de Inicio de Sesión:

- Encuentra páginas de inicio de sesión en el sitio web.

```
site:example.com inurl:login
```

2. Paneles de Administración:

- Busca paneles de administración expuestos.

```
site:example.com inurl:admin
```

3. Archivos de Configuración:

- Busca archivos de configuración que puedan estar expuestos.

```
site:example.com filetype:conf OR filetype:ini OR  
filetype:log
```

4. Códigos Fuente:

- Encuentra archivos que puedan contener código fuente.

```
site:example.com filetype:php OR filetype:asp OR  
filetype:jsp
```

Paso 4: Identificar Vulnerabilidades

1. Inyecciones SQL:

- Busca páginas que puedan ser vulnerables a inyecciones SQL.

```
site:example.com inurl:index.php?id=
```

2. Directorios Indexados:

- Encuentra directorios que están indexados públicamente.

```
site:example.com intitle:"index of /"
```

3. Cámaras Web Expuestas:

- Busca cámaras web que puedan estar expuestas.

```
site:example.com intitle:"Live View / - AXIS"
```

Paso 5: Documentación de Resultados

1. Crear un Informe Detallado:

- Documenta cada dork utilizado y los resultados obtenidos.
- Incluye capturas de pantalla de las páginas más relevantes.
- Anota cualquier información sensible o potencialmente vulnerable encontrada.

2. Recomendaciones de Seguridad:

- Basado en los resultados, proporciona recomendaciones para mejorar la seguridad del sitio web.
- Sugiere medidas para proteger la información sensible y evitar la exposición accidental.

Ejemplo de Informe:

Informe de Google Dorks para [Nombre del Sitio Web]

1. Resumen

Este informe detalla la información recopilada sobre el sitio web [Nombre del Sitio Web] utilizando técnicas de Google Dorks. Se identificaron varios archivos expuestos y posibles vulnerabilidades.

2. Información Básica

- **Páginas Indexadas:**

```
site:example.com
```

- Resultados: [Número de páginas]

3. Archivos Públicos

- **Documentos PDF:**

```
site:example.com filetype:pdf
```

- Resultados: [Número de documentos]

- **Documentos de Word:**

```
site:example.com filetype:doc OR filetype:docx
```

- Resultados: [Número de documentos]

4. Búsquedas de Seguridad

- **Páginas de Inicio de Sesión:**

```
site:example.com inurl:login
```

- Resultados: [Número de páginas]

- **Paneles de Administración:**

```
site:example.com inurl:admin
```

- Resultados: [Número de páginas]

5. Identificación de Vulnerabilidades

- **Inyecciones SQL:**

```
site:example.com inurl:index.php?id=
```

- Resultados: [Número de páginas]

- **Directorios Indexados:**

```
site:example.com intitle:"index of /"
```

- Resultados: [Número de directorios]

6. Recomendaciones de Seguridad

- **Protección de Documentos:**
 - Implementar medidas para proteger documentos confidenciales y evitar su indexación.
- **Seguridad de Inicio de Sesión:**
 - Asegurar que todas las páginas de inicio de sesión y paneles de administración estén protegidos con autenticación fuerte.
- **Validación de Entradas:**
 - Implementar validación y sanitización de entradas para prevenir inyecciones SQL.

Conclusión

El uso de Google Dorks permite identificar información sensible y posibles vulnerabilidades en un sitio web. Es crucial utilizar estas técnicas de manera ética y proporcionar recomendaciones para mejorar la seguridad del sitio.

Consideraciones Éticas

- **Legalidad:** Realiza estas búsquedas únicamente en sitios web donde tienes permiso explícito para hacerlo.
- **Privacidad:** Respeta la privacidad de la información encontrada y no la utilices para fines maliciosos.
- **Responsabilidad:** Informa a los propietarios del sitio web sobre cualquier vulnerabilidad descubierta para que puedan corregirla.

Esta tarea proporciona una comprensión práctica del uso de Google Dorks para la recopilación de información y la identificación de posibles vulnerabilidades en sitios web.