



# OWASP

Open Web Application  
Security Project

## CiberSOC: Aliado proactivo contra el Cibercrimen

### Enfoque forense



# Presentándome

- Estudiante de Maestría en Ciberseguridad
- Investigador Criminal-Informático
- Tutor de Informática Forense
- Lic. Informática

LinkedIn <https://cr.linkedin.com/in/kenneth-irvin-monge-quiros-4b30bb129>



**OWASP**  
Open Web Application  
Security Project

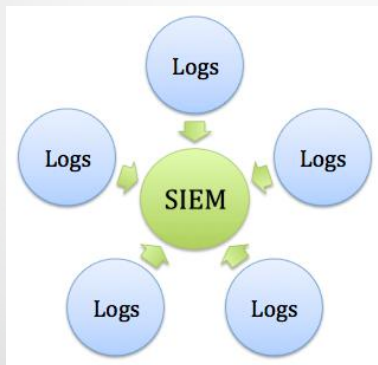
# Agenda

- Que es un SOC?
- Que necesitamos para la toma de decisiones?
- Investigación (Forense)
- Cross-site Scripting (XSS)-SQL Injection-Shellshock
- Tips de consulta
- Repositorios de malware
- Análisis de malware



# Que es un SOC?

- Un Ciber SOC (Security Operations Center)
- 24 horas 7 días a la semana 365 días del año
- SIEM (Security Information and Event Management)



# Que necesitamos para la toma de decisiones?

1. Logs
2. Revisión
3. Investigación

## Resultado

- Manejo de incidentes y eventos
- Ingeniería inversa
- Contramedidas



# Investigación (Forense)

## Cross-site Scripting (XSS)

Los ataques de secuencias de comandos entre sitios (XSS) son un tipo de inyección, en la cual los scripts maliciosos se inyectan en sitios web benignos y confiables. Los ataques XSS ocurren cuando un atacante usa una aplicación web para enviar código malicioso, generalmente en la forma de un script del lado del navegador, a un usuario final. [https://www.owasp.org/index.php/Cross-site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

## SQL Injection

Consiste en la inserción o "inyección" de una consulta SQL a través de los datos de entrada del cliente a la aplicación. Un exploit de inyección SQL exitoso puede leer datos sensibles de la base de datos, modificar datos de base de datos (Insertar / Actualizar / Eliminar), ejecutar operaciones de administración en la base de datos (como apagar el DBMS), recuperar el contenido de un archivo dado presente en el archivo DBMS sistema y, en algunos casos, emitir comandos al sistema operativo. [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)





# Cross-site Scripting (XSS)

XX.XX.XX.XX - - [01/Ene/2017:05:38:38 +0100]

"GET /target/index.php?file=<script>alert

(\"Very Long Qualys XSS Test String\")

</script> HTTP/1.1" 404 985 "-" "-"

Very Long Qualys XSS Test String



## How ZeroCMS Could Have Avoided Cross-Site Scripting Vulnerability CVE-2014-4710

Posted by [mayuresh](#) in [Security Labs](#) on July 24, 2014 2:20 PM

Vulnerability Details : [CVE-2014-4710](#) (1 public exploit)

Cross-site scripting (XSS) vulnerability in zero\_user\_account.php in ZeroCMS 1.0 allows remote attackers to inject arbitrary web script or HTML

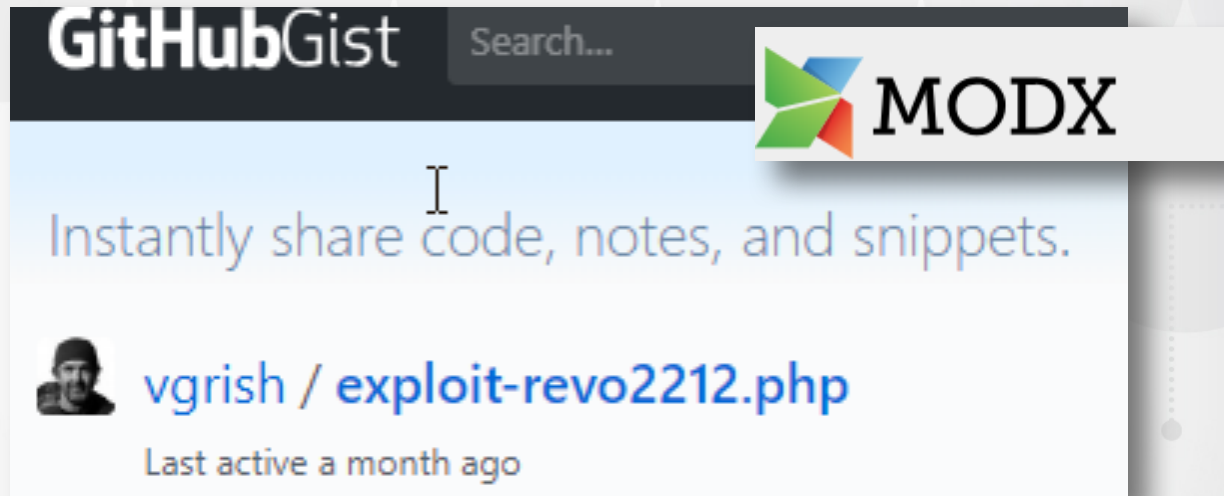
<https://www.cvedetails.com/cve/CVE-2014-4710/>



**OWASP**  
Open Web Application  
Security Project

# SQL Injection

/target/files/target.php?ctx[rank` IN (666) UNION SELECT  
id,username,password FROM modx\_users WHERE id IN(1);/\*]  
=fuckyoumodxrevolutionagain2



<https://gist.github.com/vgrish/f7f3fb94e39f48f08121>

```
100 }
101
102 SqlInjection::showLog('/*****
103 SqlInjection::showLog('/* Exploit for MODX Revolution 2.2.12 */');
104 SqlInjection::showLog('/* Author: Age1_Nash */');
105 SqlInjection::showLog('/* Date: 05.03.2014 */');
106 SqlInjection::showLog('/*****, true);
```



avos Términos de servicio y Política de privacidad, en vigencia a partir del 25 de mayo de 2018. [Más información](#)

re nosotros



Seguir



Funny moment with #skids and their #exploit  
#infosec "fuckyoumodxrevolutionagain2" -  
#pwned Poland Linksys?  
[shodan.io/host/80.82.28....](https://shodan.io/host/80.82.28.103)

```
2017-05-10T00:07:06+02:00 394803a4a6e7 00:07:06 +0200] "GET /connectors/resource/index.php?
ctx[rank%60+IN+
(666)+UNION+SELECT+id,username,password+FROM+modx_users+WHERE+id+IN(1);/*]=fuckyoumodxrev
olutionagain2 HTTP/1.1" 404 15713 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:51.0)
Gecko/20100101 Firefox/51.0" "3.29" - remote_addr 80.82.28.103 - realip 80.82.28.103 - x_forwarded_for
80.82.28.103 realip_header - request_body -
```

2:03 - 10 may. 2017 desde Milán, Lombardía



OWASP  
Open Web Application  
Security Project

# CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Switch to https://](#)

[Home](#)

## Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

## Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

## Search :

## Modx » Modx Revolution » 2.2.12 : Security Vulnerabilities

Cpe Name: `cpe:/a:modx:modx_revolution:2.2.12`

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](#)

[Copy Results](#) [Download Results](#)


#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	<a href="#">CVE-2014-8775</a>	<a href="#">200</a>	+Info		2014-12-03	2014-12-05	5.0

MODX Revolution 2.x before 2.2.15 does not include the HTTPOnly flag in a Set-Cookie header for the session cookie, which allows remote attackers to access this cookie.

[https://www.abuseipdb.com/check/\[REDACTED\]?page=1#report](https://www.abuseipdb.com/check/[REDACTED]?page=1#report)

[dannyb](#)

09 Oct 2017

 Anonymous


06 Oct 2017

`/connectors/resource/index.php?ctx[rank%60+IN+(666)+UNION+SELECT+id,username,password+FROM+modx_users+WHERE+id+IN(1);/*]=fuckyoumodxrevolutionagain2` [show less](#)

 Anonymous

06 Oct 2017

SQL Inject


 Anonymous

05 Oct 2017

multiple sql injection attempts GET `/connectors/resource/index.php?ctx[rank%60+IN+(666)+UNION+SELECT+id,username,password+FROM+modx_users+WHERE+id+IN(1);/*]=fuckyoumodxrevolutionagain2` [show less](#)

[dannyb](#)

05 Oct 2017

 Anonymous

01 Oct 2017

REQUEST\_URI ... `/connectors/resource/index.php?ctx[rank%60+IN+(666)+UNION+SELECT+id,username,password+FROM+modx_users+WHERE+id+IN(1);/*]=fuckyoumodxrevolutionagain2` [show less](#)

Brute-Force

Web App Attack

Web App Attack

Brute-Force

Exploited Host

Exploited Host

Port Scan

Brute-Force

Web App Attack

Web App Attack

# ShellShock

```
XX.XX.XX.XX - - [01/Ene/2017:23:07:17 0000] "GET /target.cgi HTTP/1.1  
" 302 292 "()" { _; } >_[$($())] { echo Nikto-Added-CVE-2014-6278:  
true; echo;echo; }" "()" { :: }; echo Nikto-Added-CVE-2014-6271:  
true;echo;echo;"
```

## Descripción

GNU Bash a 4.3 bash43-026 no analiza correctamente las definiciones de función en los valores de las variables de entorno, lo que permite a los atacantes remotos ejecutar comandos arbitrarios a través de un entorno diseñado, como lo demuestran los vectores que utilizan la función ForceCommand en OpenSSH sshd, mod\_cgi y mod\_cgid modules en el Servidor Apache HTTP, scripts ejecutados por clientes DHCP no especificados, y otras situaciones en las que se establece el entorno a través de un límite de privilegio desde la ejecución de Bash. NOTA: esta vulnerabilidad existe debido a una solución incompleta para [CVE-2014-6271](#), [CVE-2014-7169](#) y [CVE-2014-6277](#).

**Fuente:** MITRE

# 'ShellShock' Bash Vulnerability CVE-2014-6271 Test Tool

← → ↻ 🏠 ⓘ shellshock.brandonpotter.com

## 'ShellShock' Bash Vulnerability CVE-2014-6271 Test Tool

**Counter:** As of right now, 197426 tests have been run with 18489 vulnerabilities found.

### Test Web Site Root and Known URL Attack Points

Web Site Host Name (i.e. **myserver.com**):

### Test Specific Script URL

Specific CGI Script URL:

**WARNING:** This is an experimental tool. It attempts to exploit various HTTP headers to execute wget and curl requests back to this server. If this server receives the requests, then the vulnerability is confirmed.

Use at your own risk and on your own servers only.

This tool uses HTTP exploits only. Also check [www.shellshocktest.com](http://www.shellshocktest.com) for a test tool that uses Ping exploits, by @lukashed

And another test tool: [BashSmash.ccsir.org](http://BashSmash.ccsir.org)

How this tool works: [View Code](#) | [Some mildly interesting analysis of data this tool logs](#)

<http://shellshock.brandonpotter.com/>



**OWASP**  
Open Web Application  
Security Project

# Tips de consulta

- Talos Cisco (Black list-Who is)
- What Is My IP Address (Black list-IP)
- Abuse ip db (Reputación-Reportar-Lista negra)
- Netcraft (Who is)
- Surbl (Lookup)
- OWASP (TOP 10, etc)
- CVE Details (BD información de vulnerabilidades)
- Github (Proyectos ,código de herramientas, etc )

# Repositorios de malware

WEB	OBSERVACIONES
<b>Contagio Malware Dump</b>	Gratis, requiere registro
<b>Das Malwerk</b>	Gratuito
<b>FreeTrojanBotnet</b>	Gratis, requiere registro
<b>KernelMode.info</b>	Gratis, requiere registro
<b>MalShare</b>	Gratis, requiere registro
<b>Malware.lu's AVCaesar</b>	Gratis, requiere registro
<b>MalwareBlacklist</b>	Gratis, requiere registro
<b>Malware DB</b>	Gratuito
<b>Malwr</b>	Gratis, requiere registro
<b>Open Malware</b>	Gratuito
<b>Virussign</b>	Gratis, requiere registro
<b>VirusShare</b>	Gratuito

<https://protegermipc.net/2017/06/22/donde-descargar-virus-malware/>

<https://github.com/ytisf/theZoo>



**OWASP**  
Open Web Application  
Security Project



# Análisis Estático y Dinámico

- Estático
  - IDA
  - Note++
- Dinámico
  - Cuckoo Sandbox



# Referencias

- <https://www.cvedetails.com/cve/CVE-2014-4710/>
- [https://www.talosintelligence.com/reputation\\_center/lookup?search=66.249.64.1&action:Search=Search](https://www.talosintelligence.com/reputation_center/lookup?search=66.249.64.1&action:Search=Search)
- <https://whatismyipaddress.com/blacklist-check>
- <https://www.abuseipdb.com/>
- <https://www.netcraft.com/>
- <http://www.surbl.org/surbl-analysis>
- <https://www.owasp.org>
- <https://protegermipc.net/2017/06/22/donde-descargar-virus-malware>
- <https://github.com/>

