WordPress Yoast SEO Cross Site Scripting

Authored by Hammad Shamsi | Posted Aug 4, 2016

WordPress Yoast SEO plugin versions prior to 3.4.1 suffer from a stored cross site scripting vulnerability.

tags | exploit, xss
SHA-256 | b80f18dd61454008092f18d2cf58a5d038b3d8cc61191ec776c2072d67e86c08 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
#Vulnerability: Stored XSS Vulnerability in Yoast SEO Plugin
#Impact: High
#Authors: Hammad Shamsi
#Company: RHAinfoSEC
#Website: http://rafayhackingarticles.net & http://blog.sh3ifu.com/

*Introduction*

Yoast SEO (formerly known as WordPress SEO by Yoast) is the most complete WordPress SEO plugin that exists
today for WordPress.org users. It incorporates everything from a snippet editor and real time page analysis
functionality that helps you optimize your pages content, images titles, meta descriptions and more to XML
sitemaps, and loads of optimization options in between.


*Proof Of Concept*

A stored XSS scripting vulnerability was discovered in Yoast SEO plugin for wordpress. The plugin had built-in
blacklist filters which were blacklisting Parathesis as well as several functions such as alert. The following
POC bypassed:

<img src="z" onerror="prompt&#40document.cookie&#41">

*Impact*

The impact of this vulnerability is moderate as in order to trigger this vulnerability, the attacker must have
guest author priviledges. This is dangerous especially in case of news related blogs where anyone is allowed to
create a guest account and post articles for review.


*Remediation*

All user supplied input must be sanitized before it is reflected inside the application response.

Blacklist must be avoided, instead focus should be made on secure coding.

This issue is fixed on 3.4.1 Version on Yoast SEO Plugin
https://wordpress.org/plugins/wordpress-seo/changelog/
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 201 files
- Ubuntu 78 files
- Debian 24 files
- LiquidWorm 23 files
- malvuln 12 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 8 files
- T. Weber 4 files
- Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed