

Hidden casino links on 1 in 223 old Drupal sites

A survey of 37,881 public Drupal 7, 8 and 9 websites, October 2026. No site is named.

📅 21 October 2026

🕒 6 min read

🔒 Drupal Security

One old Drupal site in 223 carries spam that its owner did not write, and on most of them the owner cannot see it. This is the full write-up: the method, the counts, how the spam is hidden, a blurred example, a free five-minute check for your own site, and what fixing it involves. No site is named.

37,881

sites still on Drupal 7, 8
or 9

170

carrying planted spam

1 in 223

overall rate

1 in 167

on Drupal 8, the worst
affected

118

of the 170 advertise
gambling

68 of 79

still carried the spam
when re-checked

Summary

Between 26 September and 18 October 2026 I fetched the public pages of about 41,000 websites that public lists recorded as running Drupal 7, 8 or 9. 37,881 of them still ran one of those versions. 170 of those, one site in 223, carry spam for online casinos, prescription medicines, payday loans or essay mills that the owner did not write. On most of the affected sites the spam is hidden from visitors and readable only by search engines, and on 19 it is

served only when the visitor claims to be Googlebot. The site's standing in Google is being borrowed to rank someone else's pages, and the owners mostly do not know: of 79 sites re-checked a few days later, 68 still carried the spam.

Method

- **Sample.** 41,286 sites from public lists of websites running Drupal 7, 8 or 9 in 2025. Each site's home page, and where present its about, contact and news pages, were fetched once with an ordinary GET request, respecting robots.txt, at most six requests per site. 37,881 still ran Drupal 7, 8 or 9 when fetched (Drupal 7: 24,035; Drupal 8: 7,345; Drupal 9: 6,501). Sites that had moved to Drupal 10 or 11, or whose version could not be read, are left out of every ratio.
- **Detection.** Three signs were looked for in the saved HTML: a block hidden by an inline style (`display:none` , a 1px height, a position thousands of pixels off screen, zero opacity) whose text contains spam vocabulary and links to another site; a page meta description containing spam vocabulary; and external links whose anchor text is spam vocabulary. The vocabulary covers gambling, loans, medicines and essay services in eleven European languages. One stray link was not enough to flag a site.
- **Classification.** Every flagged site was read by hand. Gambling and pharmacy businesses, and sites that had moved off Drupal, were removed.
- **Cloaking.** A second pass fetched every home page twice, once as a browser and once with the Googlebot user agent. A page counted as cloaked when the Googlebot copy contained spam words the browser copy lacked. 19 sites met that test and are in the totals. A further 25 pages gave Googlebot extra links but no spam words; they are not counted.
- **Re-check.** 79 of the affected sites were fetched again live a few days later, with a browser, to confirm the spam was still there and to capture evidence screenshots.

Everything was read from the outside. Nothing was done to any site beyond fetching its public pages, and nothing here says how any site was broken into.

Results

By Drupal version

Version	Sites surveyed	With planted spam	Rate	Security support ended
Drupal 8	7,345	44	1 in 167	2 November 2021
Drupal 7	24,035	105	1 in 229	5 January 2025
Drupal 9	6,501	21	1 in 310	1 November 2023
All	37,881	170	1 in 223	

Drupal 8 stands out. It has been without security fixes for longest: every core and module advisory since November 2021 applies to it unpatched. Drupal 7 received fixes until January 2025, so a Drupal 7 site kept up to date until then has fewer open holes than a Drupal 8 site abandoned in 2021.

By what the spam advertises

Advertises	Sites	Share of 170
Online casinos, slots, sports betting	118	69%
Prescription medicines	36	21%
Payday and quick loans	11	6%
Essay-writing services	3	2%

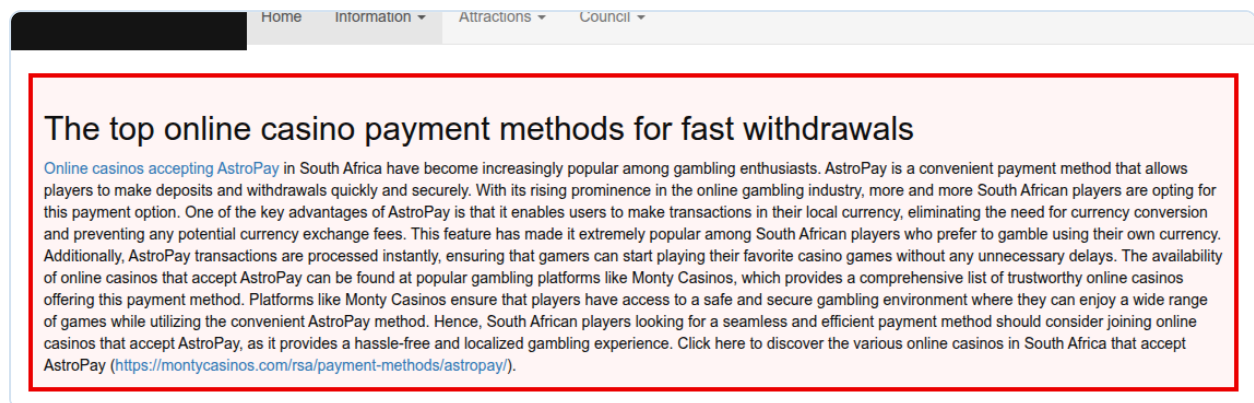
A site can advertise more than one thing. The spam is written in the language of the site it lands on.

By how it is hidden

Method	Sites
A block hidden from visitors by an inline style. People never see it; search engines read it and count the links.	81
Spam written into the page meta description. The page looks normal; the snippet Google shows under the site's name reads "Buy cialis online".	49
Spam links in the visible content only, often as an extra paragraph in the about page that a reader skims past.	25
Cloaking. A browser gets the normal page; a request that says it is Googlebot gets the spam. The owner cannot see it even in View Source.	19

A site can use more than one method, so the column adds to more than 170.

Example



A community website from the re-check. The hidden block under the menu was made visible and outlined in red: a heading and 160 words about casino payment methods, with two links to a casino affiliate. The site name and logo are blacked out.

Check your own site in five minutes, for free

Only check sites you own or look after.

1. **Search Google for your site plus a spam word.** Type `site:yourdomain.com casino`, then the same with `viagra`, `loan` and `slot`. Any result is a page Google has indexed with that word on it. The snippet under your home page in a plain `site:yourdomain.com` search is your meta description.
2. **Read the page source.** Open your home page, press Ctrl+U (Cmd+Option+U on a Mac) and search for `casino`, `display:none` and `-9999`. Repeat on the about and contact pages. Genuine uses of `display:none` exist, so look at the text inside the hidden element.
3. **Fetch the page as Googlebot.** In Google Search Console, inspect your home page and open "View crawled page". A difference between what Google received and what you see is cloaking.
4. **Check the content and user lists.** Look at `/sitemap.xml` and the Drupal content list for pages you did not create, and the people list for accounts you did not add.

5. **Run the free checker.** [Is my Drupal site hacked?](#) runs the checks used for this report against one address you own. It reads public pages only and keeps nothing but a log of the address, date and result.

What fixes it

Removing the planted text takes minutes and on its own it does not last. The intruder got in through a known hole in an unpatched Drupal core or module, or a reused password, and left a way back in: a PHP file in the files folder, an extra administrator account, or a cron hook. A clean-up that holds does four things.

1. **Find and close the way in.** Compare the code on the server with a clean copy of the same Drupal version, list every administrative user, look at files modified since the spam appeared, and read the logs.
2. **Remove the spam** from nodes, blocks, theme templates and meta description settings, then rebuild the caches and clear any CDN.
3. **Change every password and key:** Drupal accounts, the database, FTP or SSH, and the hosting control panel.
4. **Get back on a supported version.** Drupal 7, 8 and 9 receive no security fixes. A site on Drupal 11 with its modules kept current closes the holes this spam arrives through. For most small sites the upgrade is a bounded, fixed-price job; the [Drupal 7](#) and [Drupal 8](#) pages set out what it involves and costs.

Afterwards, ask Google to recrawl the affected pages from Search Console and watch the `site:` searches until the spam results drop out.

Clean-up and upgrade

I clean up compromised Drupal 7, 8 and 9 sites and move them to Drupal 11 as a fixed-price job, with the clean-up and the upgrade quoted together so the fix holds. Start with the [free checker](#), or read the [Drupal support](#) page. Also in [French](#), [Dutch](#), [German](#), [Swedish](#), [Finnish](#) and [Portuguese](#).

Limits of this survey

- The sample is sites that public lists recorded as Drupal in 2025, so it leans towards English-language sites that were already old. It says nothing about Drupal 10 and 11.
- Only the home page and up to three inner pages were read, and the cloaking pass read the home page only. The true rate is higher than 1 in 223, not lower.
- The vocabulary was built from the spam seen on the first sites found, so spam in other languages or about other products was missed.
- No site was examined from the inside, so nothing here says how any one site was compromised.

Download

[Download this report as a PDF](#) (no site names, free to share).

[Graith Internet](#) is a UK web development company specialising in PHP, Drupal, and AI-assisted development.