How To (Not) Get Hacked

A Security Checklist for Drupal Server Administrators

Hi! 👋

Mike Richardson

Hi! 👋

Mike Richardson

ironstar.io

Hi! 👋

Mike Richardson

ironstar.io tokaido.io

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.4.0

1. Select your target

URL [ ] Lock on

IP [ ] Lock on

2. Ready?

CHARGING MY LASER

Selected target

NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: This is LOIC

Port: 80

Method:

Threads: 10

Wait for reply

<= faster Speed slower =>

Attack status

Idle | Connecting | Requesting | Downloading | Downloaded | Requested | Failed

Common Types of Attacks

- Remote Code Execution (RCE)
- Cross-site scripting (XSS)
- SQL Injection
- Phishing
- Session Hijacking (Man-in-the-middle)
- Distributed Denial of Service (DDoS)

Audience

- You administer one or more Drupal sites
- You pay someone else to host, and want to double-check
- Beginner to intermediate

Obligatory Disclaimer

- I’m not a security expert
- Your requirements are unique
- You’re only as secure as your least secure component
- We are deliberately skipping some basics

Drupal is secure

IRONSTAR

Defence in Depth

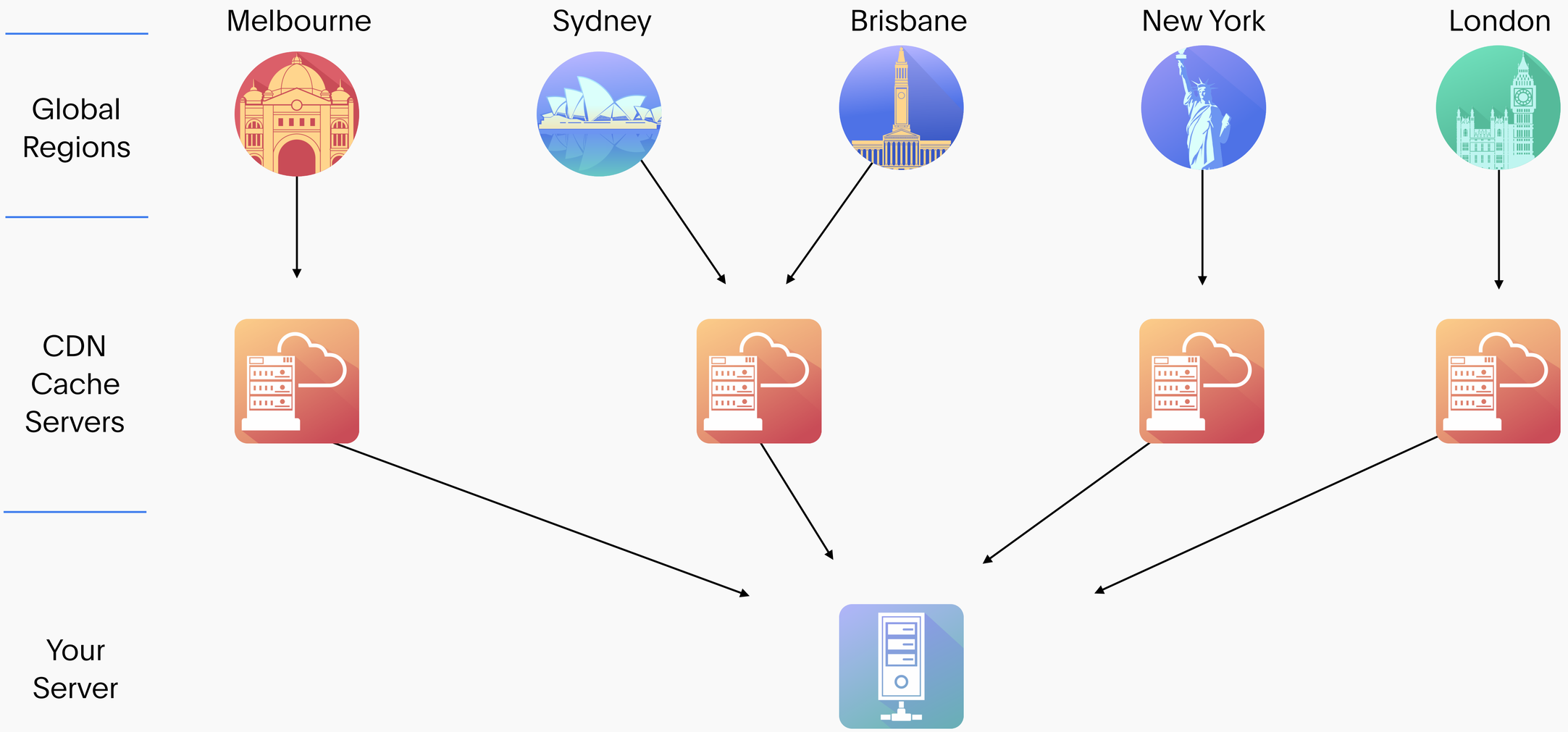
- Web Application Firewalls
- Content Delivery Networks
- Separate Web and PHP Users
- Use named SSH logins
- Encrypt everything
- Centralise security controls
- Immutable environments
- Read-only environments

let's hack something

IRONSTAR

1. Deploy a Content Delivery Network

IRONSTAR


Melbourne
Sydney
Brisbane
New York
London
Global Regions
CDN Cache Servers
Your Server

CDN Benefits

- Improved page load times
- Caches anonymous traffic - ~80% offload
- Hides your web server - no direct attacks
- Automatically blocks network-based attacks
- Cheap (now)

CDN Providers

- AWS / GCP / Azure - all have their own offering
- Fastly - pay per GB, has an NZ caching node
- Akamai - best in class, enterprise, $$$
- Cloudflare - Free, full-featured

2. Deploy a Web Application Firewall

IRONSTAR

WAF Benefits

- Scans incoming traffic for known malicious signatures
- Can be programmed with custom rules
- Some providers rapidly deploy new rules
- Built-in protection for XSS, SQL injection, etc

WAF + CDN Providers

- AWS/GCP/Azure - Pay as you go - $20 and up/month
- Fastly - included in CDN service (?)
- Akamai - $$$$
- Cloudflare - US$200/month

3. Run PHP and Apache/Nginx as separate users

PHP and Web Server Users

- Don’t run as root
- Web server user has read-only access
- FPM server user has read-write access
- Don’t trust Apache or Nginx

4. Only give write access when it’s essential

Permissions

	Path	Admins/Devs	PHP FPM	Web Server
Site Root	`/app/site`	Read/Write	No Access	No Access
Private Files	`/app/site/private`	Read/Write	Read/Write	No Access
Drupal Root	`/app/site/web`	Read/Write	Read/Only	Read Only
Public Files	`/app/site/web/sites/default/files`	Read/Write	Read/Write	Read Only

5. Don’t use .htaccess files

Disable .htaccess

- .htaccess creates decentralised security rules
- Difficult to audit and control
- Negative performance impact
- Even Apache Foundation recommends avoiding it

6. Immutable Infrastructure

IRONSTAR

Create Ephemeral Environments

- Absence of evidence is not evidence of absence
- Replace entire systems with each deploy
- If a hack takes place, patch it and just re-deploy
- Also leads to more predictable test environments

7. Use Docker Containers

IRONSTAR

Use Docker Containers

- Containers are ephemeral by nature
- Easy to move around
- Easy to inspect
- Lots of really great examples to “borrow” from

8. Encrypt Everything

Encrypt Everything

- Disks should be encrypted, this is really easy on Cloud
- Database connections and other servers should use

  TLS
- Most hosted providers don't offer TLS for MySQL, but try

9. Noexec mounts, Remove PHP, Bash, etc

IRONSTAR

Further Info

- Uncovering Drupalgeddon 2 - ironstar.link/dg2
- These slides and exploit code - ironstar.link/ds2019
- https://www.pentesterlab.com/

IRONSTAR