Curated Scan Report

- Run: `poc3`
- Reports dir: `reports/`

Severity Legend

Score	Level	Description
1	Info	Informational, negligible risk
2	Low	Low risk, minor impact
3	Medium	Moderate risk, requires attention
4	High	Serious risk, exploitable
5	Critical	Critical risk, immediate remediation

Summary

- Consolidated findings: **33**
- PoCs discovered (compact): **14**

Severity Table

Type	Target	Severity	PoCs
sqli-error	http://testphp.vulnweb.com/search.php?test=query	5	1
sqli-error	http://testphp.vulnweb.com/secured/newuser.php	5	1
xss-reflected	http://testphp.vulnweb.com/guestbook.php	4	1
xss-reflected	http://testphp.vulnweb.com/search.php?test=query	4	1
xss-reflected	http://testphp.vulnweb.com/secured/newuser.php	4	1
xss-none	http://testphp.vulnweb.com/	3	0
sqli-none	http://testphp.vulnweb.com/	3	0
xss-none	http://testphp.vulnweb.com/artists.php?artist=1	3	3
sqli-none	http://testphp.vulnweb.com/artists.php?artist=1	3	3
xss-none	http://testphp.vulnweb.com/artists.php?artist=2	3	3
sqli-none	http://testphp.vulnweb.com/artists.php?artist=2	3	3
xss-none	http://testphp.vulnweb.com/artists.php?artist=3	3	3
sqli-none	http://testphp.vulnweb.com/artists.php?artist=3	3	3
xss-none	http://testphp.vulnweb.com/guestbook.php	3	1
sqli-none	http://testphp.vulnweb.com/guestbook.php	3	1
xss-none	http://testphp.vulnweb.com/hpp/?pp=12	3	2
sqli-none	http://testphp.vulnweb.com/hpp/?pp=12	3	2
xss-none	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	3	2
sqli-none	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	3	2
xss-none	http://testphp.vulnweb.com/listproducts.php?cat=1	3	1
sqli-none	http://testphp.vulnweb.com/listproducts.php?cat=1	3	1

Type	Target	Severity	PoCs
xss-none	http://testphp.vulnweb.com/listproducts.php?cat=2	1	2
sqli-none	http://testphp.vulnweb.com/listproducts.php?cat=2	1	2
xss-none	http://testphp.vulnweb.com/listproducts.php?cat=3	1	3
sqli-none	http://testphp.vulnweb.com/listproducts.php?cat=3	1	3
xss-none	http://testphp.vulnweb.com/listproducts.php?cat=4	1	4
sqli-none	http://testphp.vulnweb.com/listproducts.php?cat=4	1	4
xss-none	http://testphp.vulnweb.com/search.php?test=query	1	1
sqli-none	http://testphp.vulnweb.com/search.php?test=query	1	1
xss-none	http://testphp.vulnweb.com/secured/newuser.php	1	1
sqli-none	http://testphp.vulnweb.com/secured/newuser.php	1	1
xss-none	http://testphp.vulnweb.com/userinfo.php	1	1
sqli-none	http://testphp.vulnweb.com/userinfo.php	1	1

---

sqli-error — `http://testphp.vulnweb.com/search.php?test=query`

- **Severity:** 5
- **Occurrences merged:** 6
- **PoCs (1):**
  - http://testphp.vulnweb.com/search.php?test=query — status: `200`
- **Examples / notes:** evidence:

`SQL syntax`

- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

sqli-error — `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 5
- **Occurrences merged:** 2
- **PoCs (1):**
  - http://testphp.vulnweb.com/secured/newuser.php — status: `200`
- **Examples / notes:** evidence:

`SQL syntax`

- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-reflected — `http://testphp.vulnweb.com/guestbook.php`

- **Severity:** 4
- **Occurrences merged:** 6
- **PoCs (1):**
  - http://testphp.vulnweb.com/guestbook.php — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

xss-reflected — `http://testphp.vulnweb.com/search.php?test=query`

- **Severity:** 4
- **Occurrences merged:** 4
- **PoCs (1):**
  - http://testphp.vulnweb.com/search.php?test=query — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

xss-reflected — `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 4
- **Occurrences merged:** 2
- **PoCs (1):**
  - http://testphp.vulnweb.com/secured/newuser.php — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

xss-none — `http://testphp.vulnweb.com/`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**

  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/artists.php?artist=1`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - `http://testphp.vulnweb.com/artists.php?artist=1` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=2` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=3` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/artists.php?artist=1`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - `http://testphp.vulnweb.com/artists.php?artist=1` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=2` — status: 200

  - http://testphp.vulnweb.com/artists.php?artist=3 — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — http://testphp.vulnweb.com/artists.php?artist=2

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - http://testphp.vulnweb.com/artists.php?artist=1 — status: 200
  - http://testphp.vulnweb.com/artists.php?artist=2 — status: 200
  - http://testphp.vulnweb.com/artists.php?artist=3 — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — http://testphp.vulnweb.com/artists.php?artist=2

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - http://testphp.vulnweb.com/artists.php?artist=1 — status: 200
  - http://testphp.vulnweb.com/artists.php?artist=2 — status: 200
  - http://testphp.vulnweb.com/artists.php?artist=3 — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/artists.php?artist=3`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - `http://testphp.vulnweb.com/artists.php?artist=1` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=2` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=3` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/artists.php?artist=3`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (3):**
  - `http://testphp.vulnweb.com/artists.php?artist=1` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=2` — status: 200
  - `http://testphp.vulnweb.com/artists.php?artist=3` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/guestbook.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/guestbook.php — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**

  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/guestbook.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/guestbook.php — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/hpp/?pp=12`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (2):**
  - `http://testphp.vulnweb.com/hpp/?pp=12` — status: 200
  - `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/hpp/?pp=12`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (2):**
  - `http://testphp.vulnweb.com/hpp/?pp=12` — status: 200
  - `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (2):**
  - `http://testphp.vulnweb.com/hpp/?pp=12` — status: 200
  - `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (2):**
  - `http://testphp.vulnweb.com/hpp/?pp=12` — status: 200
  - `http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/listproducts.php?cat=1`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - `http://testphp.vulnweb.com/listproducts.php?cat=1` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=2` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**

  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/listproducts.php?cat=1`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - `http://testphp.vulnweb.com/listproducts.php?cat=1` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=2` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/listproducts.php?cat=2`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - `http://testphp.vulnweb.com/listproducts.php?cat=1` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=2` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/listproducts.php?cat=2`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - `http://testphp.vulnweb.com/listproducts.php?cat=1` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=2` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/listproducts.php?cat=3`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - `http://testphp.vulnweb.com/listproducts.php?cat=1` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=2` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/listproducts.php?cat=3`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**

  - http://testphp.vulnweb.com/listproducts.php?cat=1 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=2 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=3 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=4 — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — http://testphp.vulnweb.com/listproducts.php?cat=4

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - http://testphp.vulnweb.com/listproducts.php?cat=1 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=2 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=3 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=4 — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — http://testphp.vulnweb.com/listproducts.php?cat=4

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (4):**
  - http://testphp.vulnweb.com/listproducts.php?cat=1 — status: 200
  - http://testphp.vulnweb.com/listproducts.php?cat=2 — status: 200

  - `http://testphp.vulnweb.com/listproducts.php?cat=3` — status: 200
  - `http://testphp.vulnweb.com/listproducts.php?cat=4` — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/search.php?test=query`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/search.php?test=query — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/search.php?test=query`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/search.php?test=query — status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/secured/newuser.php — status: 200
- **Examples / notes:**
  - (no compact excerpt available)

- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/secured/newuser.php — status: `200`
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none — `http://testphp.vulnweb.com/userinfo.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - `http://testphp.vulnweb.com/userinfo.php` — status: `200`
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

sqli-none — `http://testphp.vulnweb.com/userinfo.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - `http://testphp.vulnweb.com/userinfo.php` — status: `200`
- **Examples / notes:**
  - (no compact excerpt available)
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
