

Curated Scan Report

- Run: poc_destruct
- Reports dir: reports/

Summary

- Consolidated findings: **33**
 - PoCs discovered (compact): **3**
-

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

- Severity: 5
 - Occurrences merged: 3
 - PoCs: *none attached*
 - 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: 1
 - PoCs: *none attached*
 - 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: 3
- 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.

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

- Severity: 4
 - Occurrences merged: 2
 - 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.
-

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

- Severity: 4
 - 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.
-

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

- Severity: 2
 - Occurrences merged: 3
 - 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.
-

sql-injection — <http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12>

- Severity: 2
- Occurrences merged: 3
- 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/>

- 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.
-

sql-injection — <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: *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.
-

sql-injection — <http://testphp.vulnweb.com/artists.php?artist=1>

- 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=2>

- **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.
-

sql-injection-none — <http://testphp.vulnweb.com/artists.php?artist=2>

- **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=3>

- **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/artists.php?artist=3>

- **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/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:** *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/hpp/?pp=12>

- **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/hpp/?pp=12>

- **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/listproducts.php?cat=1>

- **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/listproducts.php?cat=1>

- **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/listproducts.php?cat=2>

- **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/listproducts.php?cat=2>

- **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/listproducts.php?cat=3>

- **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/listproducts.php?cat=3>

- **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/listproducts.php?cat=4>

- **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.
-

sql-injection-none — <http://testphp.vulnweb.com/listproducts.php?cat=4>

- **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/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.
-

sql-injection-none — <http://testphp.vulnweb.com/search.php?test=query>

- **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/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.
-

sql-injection-none — <http://testphp.vulnweb.com/secured/newuser.php>

- 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/userinfo.php>

- 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.
-

sql-injection-none — <http://testphp.vulnweb.com/userinfo.php>

- 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.
-

Mapping diagnostics (auto-generated)

- mapping candidates processed: 3
 - unmapped PoCs: 0
-

Generated by pentest pipeline — curated output.