

# Curated Scan Report

- Run: smoke-test
- Reports dir: reports/

## Summary

- Consolidated findings: **42**
  - 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
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
-

## xss-reflected â€” <http://testphp.vulnweb.com/guestbook.php>

- **Severity:** 4
  - **Occurrences merged:** 3
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

## xss-reflected â€” <http://testphp.vulnweb.com/search.php?test=query>

- **Severity:** 4
  - **Occurrences merged:** 2
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

## xss-reflected â€” <http://testphp.vulnweb.com/secured/newuser.php>

- **Severity:** 4
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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:** 3
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
- 

**external-tool-sqlmap** " <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {**meta**: {**tool**: **sqlmap**,  
**status**: **ran**}, **result**: {**cmd**:  
[**usr/bin/sqlmap**, **-u**, **https://**  
**testphp.vulnweb.com**, **--batch**, **--risk=1**,  
**--level=1**, **--random-agent**,  
**--timeout=10**], **rc**: 0, **stdout**: **\_\_H\_\_ [I\_\_ \_\_ {1.8.12#stable}|-|.[]|.â™™|.||\_|[]|\_|\_|**  
**|||Vâ€|\_| https://sqlmap.orglegal disclaimer: Usage of sqlmap for**  
**attacking targets without prior mutual consent is illegal. It is the**  
**end userâ€™s responsibility to obey all applicable local, state and**  
**federal laws. Developers assume no liability and are not**

responsible for any misuse or damage caused by this programstarting @ 12:38:25 /2025-10-07/01b[?1049h01b[22;0;0t01b[1;24r01b(B01b[m01b[4l01b[?7h01b[24;1H01b[?1049l01b[23;0;0t01b[?1l01b>[12:38:25] [INFO] fetched random HTTP User-Agent header value â€˜Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10\_5\_6; fr-fr) AppleWebKit/525.27.1 (KHTML, like Gecko) Version/3.2.1 Safari/525.27.1â€™™ from file â€˜~/usr/share/sqlmap/data/txt/user-agents.txtâ€™™ URL:https://testphp.vulnweb.comyou want to test this URL? [Y/n/q]> Ytesting URL â€˜https://testphp.vulnweb.comâ€™™ using â€˜~/home/asd/.local/share/sqlmap/output/results-10072025\_1238pm.csvâ€™™ as the CSV results file in multiple targets modetesting connection to the target URLcanâ€™™t establish SSL connection, ski

- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: heuristic
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

## external-tool-wpscan\_adapter â€˜" <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œtoolâ€œ: â€œwpscanâ€œ, â€œstatusâ€œ: â€œranâ€œ, â€œcâ€œ: 1, â€œvulnerabilitiesâ€œ: [], â€œstdoutâ€œ: â€œâ€œ,â€œstderrâ€œ: â€œ~/usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:16:in <module:LoggerThreadSafeLevel>': uninitialized constant ActiveSupport::LoggerThreadSafeLevel::Logger (NameError)\n\n Logger::Severity.constants.each do |severity|\n^^^^^^\n\tfrom /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:9:inâ€˜~/usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:8:in <top (required)>'\n\tfrom <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:inrequireâ€™™ <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:in require'\n\tfrom /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_silence.rb:5:in<top (required)>â€™™ <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:in require'\n\tfrom <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:inrequireâ€™™ /usr/

```
share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/
active_support/logger.rb:3:in <top (required)>' \n\tfrom
<internal:/usr/lib/ruby/vendor_ruby/rubygems/core_ext/
kernel_require.rb>:85:inrequireâ€™ <internal:/usr/lib/ruby/
vendor_ruby/rubygems/core_ext/kernel_require
```

- **AI suggestion:**

- predicted type: unknown (confidence: 0.00)
- explanation: model-error

- **Recommended remediation (high level):**

- Review input validation, encoding, and access controls for this endpoint.

---

## external-tool-wpscan â€™ <no-target>

- **Severity:** 2

- **Occurrences merged:** 1

- **PoCs:** *none attached*

- **Examples / notes:**

- evidence: {â€™œtoolâ€™: â€™œwpscanâ€™, â€™œstatusâ€™: â€™œranâ€™, â€™œercâ€™: 1, â€™œvulnerabilitiesâ€™: [], â€™œstdoutâ€™: â€™œâ€™, â€™œstderrâ€™: â€™œ/usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:16:in <module:LoggerThreadSafeLevel>': uninitialized constant ActiveSupport::LoggerThreadSafeLevel::Logger (NameError) \n\n Logger::Severity.constants.each do |severity|\n^^^^^^\n\tfrom /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:9:inâ€™~ /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_thread\_safe\_level.rb:8:in <top (required)>' \n\tfrom <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:inrequireâ€™ <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:in require' \n\tfrom /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger\_silence.rb:5:in<top (required)>â€™~ <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:in require' \n\tfrom <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:inrequireâ€™ /usr/share/rubygems-integration/all/gems/activesupport-6.1.7.10/lib/active\_support/logger.rb:3:in <top (required)>' \n\tfrom <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require.rb>:85:inrequireâ€™ <internal:/usr/lib/ruby/vendor\_ruby/rubygems/core\_ext/kernel\_require

- **AI suggestion:**

- predicted type: unknown (confidence: 0.00)

- explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-nikto\_adapter " " <no-target>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - evidence: { "tool": "nikto", "status": "ran", "count": 0, "findings": ["+ 0 host(s) tested"], "stdout": "- Nikto v2.5.0", "stderr": "0 host(s) tested", "output\_file": "runs/smoke-test/generated/tools/nikto\_adapter.json" }
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-nikto " " <no-target>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - evidence: { "tool": "nikto", "status": "ran", "count": 0, "findings": ["+ 0 host(s) tested"], "stdout": "- Nikto v2.5.0", "stderr": "0 host(s) tested", "output\_file": "runs/smoke-test/generated/tools/nikto\_adapter.json" }
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-nuclei\_adapter " " <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*

- **Examples / notes:**
    - evidence: {`tool`: `nuclei`, `status`: `error`, `error`: `stderr`: `timeout`}
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-nuclei " " <no-target>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - evidence: {`tool`: `nuclei`, `status`: `error`, `error`: `stderr`: `timeout`, `output_file`: `runs/smoke-test/generated/tools/nuclei_adapter.json`}
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-wapiti " " <no-target>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - evidence: {`status`: `error`, `tool`: `wapiti`, `error`: `Errno 2` No such file or directory: `~wapiti` }
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

## external-tool-nmap " " <unknown>

- **Severity:** 2

- **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - evidence: null
  - **AI suggestion:**
    - predicted type: unknown (confidence: 0.00)
    - explanation: model-error
  - **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.
- 

**xss-none** â€” **http://testphp.vulnweb.com/**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

**sqli-none** â€” **http://testphp.vulnweb.com/**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
- 

**xss-none** â€” **http://testphp.vulnweb.com/artists.php?artist=1**

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)

- **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)

- **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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)

- **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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)
- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: heuristic

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

**xss-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=1**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

**sqli-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=1**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
- 

**xss-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=2**

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: xss (confidence: 0.50)
  - explanation: heuristic

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

**sqli-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=2**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
- 

**xss-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=3**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

**sqli-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=3**

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: heuristic

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

**xss-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=4**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

**sqli-none** â€” **http://testphp.vulnweb.com/listproducts.php?cat=4**

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.
- 

**xss-none** â€” **http://testphp.vulnweb.com/search.php?test=query**

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - <http://testphp.vulnweb.com/search.php?test=query> â€” status: 200
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: xss (confidence: 0.50)
  - explanation: heuristic

- **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:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **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:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: heuristic

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

**xss-none** â€” <http://testphp.vulnweb.com/userinfo.php>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: xss (confidence: 0.50)
    - explanation: heuristic
  - **Recommended remediation (high level):**
    - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.
- 

**sqli-none** â€” <http://testphp.vulnweb.com/userinfo.php>

- **Severity:** 2
  - **Occurrences merged:** 1
  - **PoCs:** *none attached*
  - **Examples / notes:**
    - (no compact excerpt available)
  - **AI suggestion:**
    - predicted type: sqli (confidence: 0.50)
    - explanation: heuristic
  - **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 â€” curated output.