Curated Scan Report

- Run: `ai-demo`
- Reports dir: `reports/`

Summary

- Consolidated findings: **83**
- PoCs discovered (compact): **3**

---

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

- **Severity:** 5
- **Occurrences merged:** 39
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: SQL syntax
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

sqli-error â€” `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 5
- **Occurrences merged:** 11
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: SQL syntax
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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:** 35
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `xss` (confidence: 1.00)
  - explanation: keyword-map
- **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:** 26
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `xss` (confidence: 1.00)
  - explanation: keyword-map
- **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:** 11
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `xss` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

xss-none â€” `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 â€” `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: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

external-tool-sqlmap â€” `<no-target>`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œsqlmapâ€}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œwpscanâ€}
- **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 â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œtoolâ€: â€œniktoâ€, â€œstatusâ€: â€œranâ€, â€œrcâ€: 0, â€œfindingsâ€: [â€œ+ 0 host(s) testedâ€], â€œstdoutâ€: â€œ- Nikto v2.5.0â€”â€”â€”

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

---

external-tool-nuclei_adapter â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
    - evidence: {â€œtoolâ€: â€œnucleiâ€, â€œstatusâ€: â€œranâ€, â€œrcâ€: null, â€œfindingsâ€: [], â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œtimeoutâ€}
- **AI suggestion:**
    - predicted type: `sqli` (confidence: 1.00)
    - explanation: keyword-map
- **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-nuclei â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
    - evidence: {â€œtoolâ€: â€œnucleiâ€, â€œstatusâ€: â€œranâ€, â€œrcâ€: null, â€œfindingsâ€: [], â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œtimeoutâ€, â€œoutput_fileâ€: â€œruns/testphp.vulnweb.com/ai-demo/generated/tools/nuclei_adapter.jsonâ€}
- **AI suggestion:**
    - predicted type: `sqli` (confidence: 0.50)
    - explanation: keyword-map
- **Recommended remediation (high level):**
    - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-wapiti â€” <no-target>

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

- **Examples / notes:**
  - evidence: {â€œstatusâ€�: â€œerrorâ€�, â€œtoolâ€�: â€œwapitiâ€�, â€œerrorâ€�: â€œ[Errno 2] No such file or directory: â€˜wapitiâ€™â€�}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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€�: â€œwpscanâ€�, â€œstatusâ€�: â€œranâ€�, â€œrcâ€�: 1, â€œvulnerabilitiesâ€�: [], â€œstdoutâ€�: â€œâ€œ,â€�stderrâ€�: 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: `sqli` (confidence: 1.00)
  - explanation: keyword-map

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

---

external-tool-amass â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œamassâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for amassâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-arachni â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œarachniâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for arachniâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-boofuzz â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œboofuzzâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€:

{â€œstdoutâ€�: â€œmock output for boofuzzâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-certspotter â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œcertspotterâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for certspotterâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-commix â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€�: â€œskipped_by_safetyâ€�, â€œtoolâ€�: â€œcommixâ€�}
- **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-create_proof â€” <no-target>

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

- **Examples / notes:**
  - evidence: {â€œstatusâ€�: â€œerrorâ€�, â€œtoolâ€�: â€œcreate_proofâ€�, â€œerrorâ€�: â€œmain() takes 0 positional arguments but 2 were givenâ€�}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-crtsh â€” `<no-target>`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œcrtshâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for crtshâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-dalfox â€” `<no-target>`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œdalfoxâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for dalfoxâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-dirb â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œdirbâ€, â€œstatusâ€: â€œtimeoutâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/dirbâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: null, â€œstderrâ€: â€œtimeoutâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-enum4linux â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œenum4linuxâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/enum4linuxâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œERROR: Target hostname "https://testphp.vulnweb.com" contains some illegal charactersâ€, â€œstderrâ€: â€œâ€œ},â€parsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-ffuf â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œffufâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/ffufâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œFuzz Faster U Fool - v2.1.0-

devOPTIONS:-H Header \"Name: Value\", separated by colon. Multiple -H flags are accepted.-X HTTP method to use-b Cookie data \"NAME1=VALUE1; NAME2=VALUE2\" for copy as curl functionality.-cc Client cert for authentication. Client key needs to be defined as well for this to work-ck Client key for authentication. Client certificate needs to be defined as well for this to work-d POST data-http2 Use HTTP2 protocol (default: false)-ignore-body Do not fetch the response content. (default: false)-r Follow redirects (default: false)-raw Do not encode URI (default: false)-recursion Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in it. (default: false)-recursion-depth Maximum recursion depth. (default: 0)-recursion-strategy Recursion strategy: "default" for a redirect based, and "greedy" to recurse on all matches (default: default)-replay-proxy Replay matched requests using this proxy.-sni Target TLS SNI, does not support FUZZ keyword-timeout HTTP request timeout in seconds. (default: 10)-u Target URL-x

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

---

external-tool-gitleaks â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œgitleaksâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for gitleaksâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-gitrob â€” <no-target>

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

- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œgitrobâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for gitrobâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-gobuster â€” `<no-target>`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œgobusterâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/gobusterâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œError: unknown command "https://testphp.vulnweb.com" for "gobuster"â€˜gobuster â€“helpâ€™ for usage.â€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.67)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-graphql-fuzzer â€” `<no-target>`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œgraphql-fuzzerâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for graphql-fuzzerâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-hashcat â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œhashcatâ€}
- **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-httprobe â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œhttprobeâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for httprobeâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-hydra â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œhydraâ€}
- **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-john â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œjohnâ€}
- **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-masscan â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œmasscanâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/masscanâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œFAIL: unknown command-line parameter "https://testphp.vulnweb.com"did you want "â€“https://testphp.vulnweb.com"?â€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: sqli (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-medusa â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œmedusaâ€}
- **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-msfconsole â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œstatusâ€: â€œskipped_by_safetyâ€, â€œtoolâ€: â€œmsfconsoleâ€}
- **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-newman â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œnewmanâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for newmanâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-radamsa â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œradamsaâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for radamsaâ€}, â€œparsed_findingsâ€: []}

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

---

external-tool-searchsploit â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œsearchsploitâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/searchsploitâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 0, â€œstdoutâ€: â€œExploits: No Results: No Resultsâ€, â€œstderrâ€: â€œâ€œ},â€parsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-smbclient â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œsmbclientâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/smbclientâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œ:\\testphp.vulnweb.com: Not enough â€˜\â€™ characters in serviceâ€, â€œstderrâ€: â€œUsage: smbclient [-?EgqBNPkV] [-?|â€“help] [â€“usage] [-M|â€“message=HOST]USERNAME[%PASSWORD]] [-N|â€“no-pass]service â€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-smtp-user-enum â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œsmtp-user-enumâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/smtp-user-enumâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 1, â€œstdoutâ€: â€œsmtp-user-enum v1.2 (http://pentestmonkey.net/tools/smtp-user-enum): smtp-user-enum [options] (-u username | -U file-of-usernames) (-t host | -T file-of-targets)are:-m n Maximum number of processes (default: 5)M mode Method to use for username guessing EXPN, VRFY or RCPT (default: VRFY)u user Check if user exists on remote systemf addr MAIL FROM email address. Used only in "RCPT TO" mode (default: user@example.com)-D dom Domain to append to supplied user list to make email addresses (Default: none)Use this option when you want to guess valid email addresses instead of just usernamese.g.Â "-D example.com" would guess foo@example.com, bar@example.com, etc. Instead of simply the usernames foo and bar.U file File of usernames to check via smtp servicet host Server host running smtp serviceT file File of hostnames running the smtp servicep port TCP port on which smtp service runs (default: 25)d Debugging outputw n Wait a maximum of n seconds for reply (default: 5)v Verboseh This help messagesee smtp-user-enum-user-docs.pdf from the smtp-user-enum tar ball.:$ smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.33)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-sslyze â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œsslyzeâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for sslyzeâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.33)
  - explanation: keyword-map

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

---

external-tool-subfinder â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œsubfinderâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for subfinderâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-trufflehog â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œtrufflehogâ€, â€œstatusâ€: â€œmocked_no_binaryâ€}, â€œresultâ€: {â€œstdoutâ€: â€œmock output for trufflehogâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-unicornscan â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œunicornscanâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/unicornscanâ€, â€œhttps://

testphp.vulnweb.comâ€�], â€œercâ€�: 0, â€œestdoutâ€�: â€œwhat host(s) should i scan?, ive got nothing to doâ€�, â€œestderrâ€�: â€œMain [Error cidr.c:263] dns lookup fails for `https': Unknown host\nMain [Error getconfig.c:434] cant add workunit for argumenthttps://testphp.vulnweb.comâ€™: dont understand address `//testphp.vulnweb.comâ€™â€�}, â€œparsed_findingsâ€�: []}

- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-w3af â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œw3afâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for w3afâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-wappalyzer â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œwappalyzerâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for wappalyzerâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-wfuzz â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œwfuzzâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/wfuzzâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 0, â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€ /usr/lib/python3/dist-packages/wfuzz/**init**.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzzâ€™s documentation for more information./usr/lib/python3/dist-packages/wfuzz/wfuzz.py:78: UserWarning:Fatal exception: Bad usage: You must specify a payload.â€œ},â€parsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-whatweb â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€: {â€œtoolâ€: â€œwhatwebâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/whatwebâ€, â€œhttps://testphp.vulnweb.comâ€], â€œrcâ€: 0, â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œ01b[1m01b[31mERROR Opening: https://testphp.vulnweb.com - execution expired01b[0mâ€}, â€œparsed_findingsâ€: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.67)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-xsstrike â€” <no-target>

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

- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œxsstrikeâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for xsstrikeâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Sanitize and encode untrusted input before rendering. Use context-specific encoding (HTML, JS, attribute). Implement CSP.

---

external-tool-zmap â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œmetaâ€�: {â€œtoolâ€�: â€œzmapâ€�, â€œstatusâ€�: â€œmocked_no_binaryâ€�}, â€œresultâ€�: {â€œstdoutâ€�: â€œmock output for zmapâ€�}, â€œparsed_findingsâ€�: []}
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.50)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-nmap â€” <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.

---

external-tool-init â€” <unknown>

- **Severity:** 2
- **Occurrences merged:** 1

- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: null
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-adapter_base â€” <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.

---

external-tool-manager â€” <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.

---

external-tool-parsers â€” <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: 1.00)
    - explanation: keyword-map
- **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 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: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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=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/artists.php?artist=2

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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=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/artists.php?artist=3

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

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

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/guestbook.php 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 â€” `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: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none â€” `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 â€” `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: 1.00)
  - explanation: keyword-map
- **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: 1.00)
  - explanation: keyword-map
- **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: 1.00)
  - explanation: keyword-map
- **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: 1.00)
  - explanation: keyword-map
- **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: 1.00)
  - explanation: keyword-map
- **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 â€” `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: 1.00)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Use parameterized queries / prepared statements. Validate and escape inputs. Review DB permissions.

---

xss-none â€” `http://testphp.vulnweb.com/secured/newuser.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs (1):**
  - http://testphp.vulnweb.com/secured/newuser.php 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 â€” `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: 1.00)
  - explanation: keyword-map
- **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: `sqli` (confidence: 1.00)
  - explanation: keyword-map
- **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: 1.00)
  - explanation: keyword-map
- **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.