Curated Scan Report

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

Summary

- Consolidated findings: **25**
- PoCs discovered (compact): **2**

---

sqli-error â€” `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: 0.92)
  - 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:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: SQL syntax
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.92)
  - 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/search.php?test=query`

- **Severity:** 4
- **Occurrences merged:** 2
- **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:** 1
- **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: 0.92)
  - 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/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: 0.94)
  - 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€œmetaâ€: {â€œtoolâ€: â€œsqlmapâ€, â€œstatusâ€: â€œranâ€}, â€œresultâ€: {â€œcmdâ€: [â€œ/usr/bin/sqlmapâ€, â€œ-uâ€, â€œhttp://testphp.vulnweb.comâ€, â€œâ€“batchâ€, â€œâ€“risk=1â€, â€œâ€“level=1â€, â€œâ€“random-agentâ€, â€œâ€“timeout=10â€], â€œrcâ€: 0, â€œstdoutâ€: â€” **_H___ *[â€™]*__ ___ ___** {1.8.12#stable}|_ -| . [â€™] | .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 @ 22:12:19 /2025-10-04/fetched random HTTP User-Agent header value â€˜Mozilla/5.0 (Windows; U; Windows NT 6.0; it; rv:1.9.1b2) Gecko/20081201 Firefox/3.1b2â€™ from file â€˜/usr/share/sqlmap/data/txt/user-agents.txtâ€™testing connection to the target URLchecking if the target is protected by some kind of WAF/IPStesting if the target URL content is stabletarget URL content is stableno parameter(s) found for testing in the provided data (e.g.Â GET parameter â€˜idâ€™ in â€˜www.site.com/index.php?id=1â€™). You are advised to rerun with â€˜â€“forms â€“crawl=2â€™your sqlmap version is outdatedending @ 22:12:26 /2025-10-04/â€œ,â€stderrâ€: â€œâ€œ},â€parsed_findingsâ€: [], â€œoutp
- **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€: 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: unknown (confidence: 0.97)
  - 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€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: unknown (confidence: 0.97)
  - explanation: keyword-map
- **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€: null, â€œfindingsâ€: [], â€œstdoutâ€: â€œâ€œ,â€stderrâ€: â€œtimeoutâ€}
- **AI suggestion:**
  - predicted type: unknown (confidence: 0.98)
  - explanation: keyword-map
- **Recommended remediation (high level):**
  - Review input validation, encoding, and access controls for this endpoint.

---

external-tool-nikto â€” <no-target>

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - evidence: {â€œtoolâ€: â€œniktoâ€, 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-http/generated/tools/nikto_adapter.jsonâ€}
- **AI suggestion:**
  - predicted type: unknown (confidence: 0.98)
  - 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: unknown (confidence: 0.98)
  - 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-http/generated/tools/nuclei_adapter.jsonâ€}
- **AI suggestion:**
  - predicted type: unknown (confidence: 0.98)
  - 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: unknown (confidence: 0.91)
  - 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: 1.00)
  - explanation: keyword-map
- **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: 0.92)
  - 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/`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.94)
  - 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: 0.92)
  - 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/hpp/?pp=12`

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

- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.94)
  - 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: 0.92)
  - 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/search.php?test=query`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.94)
  - 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: 0.92)
  - 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/secured/newuser.php`

- **Severity:** 2
- **Occurrences merged:** 1
- **PoCs:** *none attached*
- **Examples / notes:**
  - (no compact excerpt available)
- **AI suggestion:**
  - predicted type: `sqli` (confidence: 0.94)
  - 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: `xss` (confidence: 0.92)
  - 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: 0.94)
  - 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: 2
- unmapped PoCs: 0

Generated by pentest pipeline â€” curated output.