

Report Generated by EasySAST | Ashok Dhungana

Report for 1744345703_deserialization.php.txt:

No vulnerabilities detected.

Report for 1744345710_deserialization.php.txt:

No vulnerabilities detected.

Report for 1744345881_configuration.php.txt:

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: define("PASSWORD","pwd123**")

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: \$DB_PASS="password"

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: \$secret_flag="a2'&vkzg%"

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: \$token="1213144142353962062"

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: \$pwd="mysuper_cr3dz"

Name: Hardcoded Credential

File: uploads\1744345881_configuration.php

Line: 1

Code: \$Pass="case!nsenSitiveP@ss"

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code:

\$base64="TXITdXBldBhc3N3b3JkT3lganVzdCBhbm90aGVyIGJhY2tkb29yIGluIHlvdXlgY29kZSB5b3

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code:

\$hex="4d79537570657250617373776f72644f72206a75737420616e6f74686572206261636b646f6f72

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code: \$fakeAPI1="Alzad8e8fca2dc0f896fd7cb4cb0031ba249123"

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code: \$fakeAPI2="AKIAD8E8FCA2DC0F896F"

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code: \$hash2="\$1\$VnG/6ABB\$t6w9bQFxl9tf0sFJf2TR."

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code: \$hash3="d8e8fca2dc0f896fd7cb4cb0031ba249"

Name: High Entropy String

File: uploads\1744345881_configuration.php

Line: 4

Code:

if(\$pass=="\$6\$q8C1F6tv\$zTP/eEVixqyQBefsSbTidUJfnaE2ojNlpTwTHava/UhFORv3V4ehyTOGdQE

Report for 1744346440_assert.php.txt:

Name: Remote Command Execution

File: uploads\1744346440_assert.php

Line: 2

Code: "strpos('templates/' . \$page . '.php', '..')

Name: Remote Command Execution

File: uploads\1744346440_assert.php

Line: 2

Code: "file_exists('templates/'. \$page . '".php'

Report for 1744346472_backtick.php.txt:

No vulnerabilities detected.
