Cloud Configuration Scan Results

Check ID	File	Resource	Check Name	Line	Potential CVE/CWE	Guideline URL	Status
CKV_AZURE_160	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that HTTP (port 80) access is restricted from the internet	37-86	1. CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability 2. CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 3. CWE-20: Improper Input Validation	https://docs.bridgecrew.io/docs/ensure-azure-http-port-80-access-from-the-internet-is-restricted	FAILED
CKV_AZURE_10	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that SSH access is restricted from the internet	37-86	1. CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability 2. CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 3. CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	https://docs.bridgecrew.io/docs/bc_azr_networking_3	FAILED
CKV_AZURE_50	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure Virtual Machine Extensions are not Installed	127-184	1. CVE-2019-3396: Improper Access Control 2. CWE-284: Improper Access Control 3. CWE-732: Incorrect Permission Assignment for Critical Resource	https://docs.bridgecrew.io/docs/bc_azr_general_14	FAILED
CKV_AZURE_179	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure VM agent is installed	127-184			FAILED
CKV_AZURE_119	/main.tf	azurerm_network_interface.nic-automate-test	Ensure that Network Interfaces don't use public IPs	113-124	1. CVE-2019-19781: Improper Access Control 2. CWE-306: Missing Authentication for Critical Function 3. CWE-264: Permissions Privileges and Access Controls	https://docs.bridgecrew.io/docs/ensure-that-network-interfaces-dont-use-public-ips	FAILED
CKV_AZURE_183	/main.tf	azurerm_virtual_network.vn-automate-test	Ensure that VNET uses local DNS addresses	16-26			PASSED
CKV_AZURE_182	/main.tf	azurerm_virtual_network.vn-automate-test	Ensure that VNET has at least 2 connected DNS Endpoints	16-26			PASSED
CKV_AZURE_9	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that RDP access is restricted from the internet	37-86		https://docs.bridgecrew.io/docs/bc_azr_networking_2	PASSED
CKV_AZURE_77	/main.tf	azurerm_network_security_group.sg-automate-test	Ensure that UDP Services are restricted from the Internet	37-86		https://docs.bridgecrew.io/docs/ensure-that-udp-services-are-restricted-from-the-internet	PASSED
CKV_AZURE_118	/main.tf	azurerm_network_interface.nic-automate-test	Ensure that Network Interfaces disable IP forwarding	113-124		https://docs.bridgecrew.io/docs/ensure-that-network-interfaces-disable-ip-forwarding	PASSED
CKV_AZURE_1	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure Azure Instance does not use basic authentication(Use SSH Key Instead)	127-184		https://docs.bridgecrew.io/docs/bc_azr_networking_1	PASSED
CKV_AZURE_178	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure linux VM enables SSH with keys for secure communication	127-184			PASSED
CKV_AZURE_149	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure that Virtual machine does not enable password authentication	127-184		https://docs.bridgecrew.io/docs/ensure-azure-virtual-machine-does-not-enable-password-authentication	PASSED
CKV_AZURE_92	/main.tf	azurerm_linux_virtual_machine.vmachine-automate-test	Ensure that Virtual Machines use managed disks	127-184		https://docs.bridgecrew.io/docs/ensure-that-virtual-machines-use-managed-disks	PASSED

Configuration Scripts Scan Results

File: config_lemp.tpl

WARNING! apt update is not perform before installtions of package

```
|:|sudo apt update
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Before installing any packages using apt, it is advisable to run the above command.

File: config_php_xfer.tpl

No vulnerability found in: [config_php_xfer.tpl]

File: config_server.tpl

No vulnerability found in: [config_server.tpl]

File: config_web.tpl

No vulnerability found in: [config_web.tpl]

File: lempstack.tpl

No vulnerability found in: [lempstack.tpl]

File: very_vuln.tpl

WARNING! apt update is not perform before installtions of package

```
|:|sudo apt update
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Before installing any packages using apt, it is advisable to run the above command.

Potential vulnerability found in: [vlc 3.0.17]

```
|:|Multiple vulnerabilities in VideoLAN VLC [2022-11-29] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [libxml2 2.10.2]

```
|:|Multiple vulnerabilities in Libxml2 [2022-10-30] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [mumble 1.3.0]

```
|:|Remote code execution in Mumble [2021-02-22] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Usage of weak encryption in Mumble [2020-07-24] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [samba 3.6.3]

```
|:|Multiple vulnerabilities in Samba [2022-07-27] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Information disclosure in Samba [2022-01-31] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Remote code execution in Samba [2022-01-31] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in Samba [2021-11-10] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Out-of-bounds read in Samba [2021-04-29] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in Samba [2020-10-29] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in Samba [2018-08-14] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|OpenSUSE Linux update for samba [2017-11-30] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in Samba [2017-11-21] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in Samba [2017-09-20] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [vsftpd 2.3.4]

```
|:|Security restrictions bypass in vsftpd [2022-01-09] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|OS Command Injection in vsftpd [2019-11-27] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Security restrictions bypass in vsftpd [2015-01-28] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [polkit 0.113]

```
|:|Denial of service in polkit [2022-03-13] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Privilege escalation in polkit pkexec [2022-01-26] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
|:|Privilege escalation in Polkit [2021-06-07] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [nginx 1.17.0]

```
|:|Multiple vulnerabilities in nginx [2022-10-19] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Security restrictions bypass in nginx [2022-01-09] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Remote code execution in nginx [2021-05-25] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Information disclosure in nginx [2020-03-19] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|HTTP request smuggling in Nginx [2020-01-13] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Remote denial of service in nginx [2019-08-13] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [mariadb 10.3.34]

```
|:|Denial of service in MariaDB [2022-09-26] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Buffer overflow in MariaDB [2022-08-04] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Buffer overflow in MariaDB [2022-08-04] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Improper Resource Shutdown or Release in MariaDB [2022-05-31] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in MariaDB [2022-05-23] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in MariaDB [2022-05-23] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in MariaDB [2022-05-23] |:|Severity:Medium |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [php 7.1.12]

```
|:|Privilege escalation in PHP [2021-10-26] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Remote code execution in PHP [2019-10-27] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2019-01-10] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-12-07] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-11-22] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-11-09] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Denial of service vulnerabilities in PHP [2018-10-12] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-10-10] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-08-20] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Information disclosure in PHP [2018-08-09] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [php 7.1.0]

```
|:|Privilege escalation in PHP [2021-10-26] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Remote code execution in PHP [2019-10-27] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2019-01-10] |:|Severity:High |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-12-07] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-11-22] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-11-09] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Denial of service vulnerabilities in PHP [2018-10-12] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-10-10] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Multiple vulnerabilities in PHP [2018-08-20] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|Information disclosure in PHP [2018-08-09] |:|Severity:Low |:|Verified:Yes
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Mysql-secure-installation is not performed properly! The following command was not executed.

```
|:|sudo mysql -e "UPDATE mysql.user SET Password = PASSWORD('$database_pwd') WHERE User = 'root'"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|sudo mysql -e "DROP USER ''@'$(hostname)'"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|sudo mysql -e "DROP DATABASE test"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

File: very_vuln2.tpl

WARNING! apt update is not perform before installtions of package

```
    |:|sudo apt update
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Before installing any packages using apt, it is advisable to run the above command.

Potential vulnerability found in: [libxml2 2.10.2]

```
    |:|Multiple vulnerabilities in Libxml2 [2022-10-30] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [samba 3.6.3]

```
    |:|Multiple vulnerabilities in Samba [2022-07-27] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Information disclosure in Samba [2022-01-31] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Remote code execution in Samba [2022-01-31] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Samba [2021-11-10] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Out-of-bounds read in Samba [2021-04-29] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Samba [2020-10-29] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Samba [2018-08-14] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|OpenSUSE Linux update for samba [2017-11-30] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Samba [2017-11-21] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Samba [2017-09-20] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [vsftpd 2.3.4]

```
    |:|Security restrictions bypass in vsftpd [2022-01-09] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|OS Command Injection in vsftpd [2019-11-27] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Security restrictions bypass in vsftpd [2015-01-28] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [mysql 5.1.3]

```
    |:|Debian update for mysql-connector-java [2020-06-15] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in MySQL Connectors [2020-04-19] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Authentication bypass using an alternate path or channel in Oracle MySQL Connectors [2018-10-17] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Google, mysql [2014-01-15] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Google, mysql [2014-01-15] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Input validation error in Oracle MySQL Server [2013-10-16] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Input validation error in Oracle MySQL Server [2013-07-17] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Input validation error in Oracle MySQL Server [2013-07-17] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Input validation error in Google, mysql [2013-04-17] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Multiple vulnerabilities in Google, mysql [2013-04-17] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [polkit 0.113]

```
    |:|Denial of service in polkit [2022-03-13] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Privilege escalation in polkit pkexec [2022-01-26] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Privilege escalation in Polkit [2021-06-07] |:|Severity:Low |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [mumble 1.3.0]

```
    |:|Remote code execution in Mumble [2021-02-22] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|Usage of weak encryption in Mumble [2020-07-24] |:|Severity:Medium |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Potential vulnerability found in: [vlc 3.0.17]

```
    |:|Multiple vulnerabilities in VideoLAN VLC [2022-11-29] |:|Severity:High |:|Verified:Yes
    -------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

Mysql-secure-installation is not performed properly! The following command was not executed.

```
|:|sudo mysql -e "UPDATE mysql.user SET Password = PASSWORD('$database_pwd') WHERE User = 'root'"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|sudo mysql -e "DROP USER ''@'$(hostname)'"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|sudo mysql -e "DROP DATABASE test"
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

Click here for more detail!

PHP Files Scan Results

Potential vulnerability found in: [ssert-use.php]

```
|:|vulnID:[A03.4] | line:|6| assert($tainted);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A03.4] | line:|12| assert($tainted > 1);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A03.4] | line:|16| assert($name);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A03.4] | line:|22| assert($name > 1);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: **A03.4**
>>> Details: **Calling assert with user input is equivalent to eval'ing.**
>>> Severity: **Medium**
>>> OWASP: **A03:2021 - Injection**
>>> CWE: **CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')**
>>> Recommendation: **Avoid using user-controlled input for assert command.**
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [backticks-use.php]

```
|:|vulnID:[A03.8] | line:|4| echo `ping -n 3 {$user_input}`;
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: **A03.8**
>>> Details: **Backticks use may lead to command injection vulnerabilities.**
>>> Severity: **High**
>>> OWASP: **A03:2021 - Injection**
>>> CWE: **CWE-94: Improper Control of Generation of Code ('Code Injection')**
>>> Recommendation: **Avoid using backticks with user-controlled input. Consider using execution commands with proper input validation.**
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [curl-ssl-verifypeer-off.php]

```
|:|vulnID:[A02.3] | line:|9| curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: **A02.3**
>>> Details: **SSL verification is disabled but should not be (currently CURLOPT_SSL_VERIFYPEER=$IS_VERIFIED)**
>>> Severity: **Low**
>>> OWASP: **A02:2021 - Cryptographic Failures**
>>> CWE: **CWE-319: Cleartext Transmission of Sensitive Information**
>>> Recommendation: **SSL verification should be enabled**
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

```
|:|vulnID:[A10.1] | line:|3| $ch = curl_init();
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|5| curl_setopt($ch, CURLOPT_URL, "http://www.example.com/");
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|6| curl_setopt($ch, CURLOPT_HEADER, 0);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|9| curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|12| curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, true);
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: **A10.1**
>>> Details: **The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.**
>>> Severity: **High**
>>> OWASP: **A10:2021 - Server-Side Request Forgery (SSRF)**
>>> CWE: **CWE-918: Server-Side Request Forgery (SSRF)**
>>> Recommendation: **Avoid using dangerous functions with payload data. https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html**
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [deserialization.php]

```
|:|vulnID:[A08.1] | line:|12| extract($var_array, EXTR_PREFIX_SAME, "wddx");
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A08.1] | line:|16| extract($bad, EXTR_PREFIX_SAME, "wddx");
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A08.1] | line:|21| extract($bad2, EXTR_PREFIX_SAME, "wddx");
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A08.1] | line:|25| extract($ok, EXTR_SKIP, "wddx");
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: **A08.1**
>>> Details: **Do not call 'extract()' on user-controllable data.**
>>> Severity: **Medium**
>>> OWASP: **A08:2021 - Software and Data Integrity Failures**
>>> CWE: **CWE-502: Deserialization of Untrusted Data**
>>> Recommendation: **Provide the EXTR_SKIP flag extract($VAR, EXTR_SKIP,...) to prevent overwriting existing variables.**
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [val-use.php]

```
     |:|vulnID:[A03.5] | line:|4| eval($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A03.5
>>> Details: Evaluating non-constant commands. This can lead to command injection.
>>> Severity: High
>>> OWASP: A03:2021 - Injection
>>> CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
>>> Recommendation: Avoid using user-controlled input for eval command.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [xec-use.php]

```
     |:|vulnID:[A03.3] | line:|4| exec($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|10| passthru($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|13| $proc = proc_open($cmd, $descriptorspec, $pipes);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|16| $handle = popen($user_input, "r");
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|19| $output = shell_exec($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|22| $output = system($user_input, $retval);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.3] | line:|25| pcntl_exec($path);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A03.3
>>> Details: Executing non-constant commands. This can lead to command injection.
>>> Severity: High
>>> OWASP: A03:2021 - Injection
>>> CWE: CWE-94: Improper Control of Generation of Code ('Code Injection')
>>> Recommendation: Avoid using user-controlled input for execution commands.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [ile-inclusion.php]

```
     |:|vulnID:[A03.1] | line:|6| include($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.1] | line:|12| include_once($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.1] | line:|18| require($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.1] | line:|24| require_once($user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.1] | line:|30| include(__DIR__ . $user_input);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A03.1] | line:|46| require_once $pth;
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A03.1
>>> Details: Detected non-constant file inclusion. This can lead to local file inclusion (LFI) or remote file inclusion (RFI) if user input reaches this statement. LFI and RFI could lead to sensitive files being obtained by attackers. Instead, explicitly specify what to include. If that is not a viable solution, validate user input thoroughly.
>>> Severity: Medium
>>> OWASP: A03:2021 - Injection
>>> CWE: CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
>>> Recommendation: Valid user input thoroughly or explicitly specify what to include.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [p-use.php]

```
     |:|vulnID:[A02.4] | line:|4| $conn_id = ftp_connect($ftp_server);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
     |:|vulnID:[A02.4] | line:|7| $login_result = ftp_login($conn_id, $ftp_user_name, $ftp_user_pass);
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.4
>>> Details: FTP allows for unencrypted file transfers. Consider using an encrypted alternative.
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-319: Cleartext Transmission of Sensitive Information
>>> Recommendation: Consider using ssh2_scp_send()
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [info.php]

```
     |:|vulnID:[A01.1] | line:|2| phpinfo();
     ----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A01.1
>>> Details: The 'phpinfo' function may reveal sensitive information about your environment.
>>> Severity: Medium
>>> OWASP: A01:2021 - Broken Access Control
>>> CWE: CWE-200: Exposure of Sensitive Information
>>> Recommendation: Recommended to remove phpinfo page in production environment.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [dap-bind-without-password.php]

```
    |:|vulnID:[A07.1] | line:|12| ldap_bind($ldapconn, NULL, NULL);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|15| ldap_bind($ldapconn, "username", "");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|20| ldap_bind($ldapconn, $a, $b);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|25| ldap_bind($ldapconn, $c, $d);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|30| ldap_bind($ldapconn, $e, $f);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|33| ldap_bind($ldapconn, "username", "password");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A07.1] | line:|36| ldap_bind($ldapconn, $username, $password);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A07.1
>>> Details: Detected anonymous LDAP bind. This permits anonymous users to execute LDAP statements.
>>> Severity: Low
>>> OWASP: A07:2021 - Identification and Authentication Failures
>>> CWE: CWE-287: Improper Authentication
>>> Recommendation: Consider enforcing authentication for LDAP.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [b-ereg-replace-eval.php]

```
    |:|vulnID:[A03.6] | line:|4| mb_ereg_replace($pattern, $replacement, $string, $user_input_options);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A03.6
>>> Details: Calling mb_ereg_replace with user input in the options can lead to arbitrary code execution. The eval modifier (`e`) evaluates the replacement argument as code.
>>> Severity: Medium
>>> OWASP: A03:2021 - Injection
>>> CWE: CWE-94: Improper Control of Generation of Code ('Code Injection')
>>> Recommendation: Avoid using user-controlled input for mb_ereg_replace.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [crypt-use.php]

```
    |:|vulnID:[A02.5] | line:|16| openssl_encrypt($plaintext, $cipher, $key, $options=0, $iv, $tag);
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.5
>>> Details: Static IV used with AES in CBC mode. Static IVs enable chosen-plaintext attacks against encrypted data
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-329: Generation of Predictable IV with CBC Mode
>>> Recommendation: Avoid using static IV for AES-CBC mode.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [d5-loose-equality.php]

```
    |:|vulnID:[A02.1] | line:|4| md5("240610708") == "0";
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|7| 0 == md5("240610708");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|10| 0 == md5_file("file.txt");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|13| md5("240610708") == md5_file("file.txt");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|16| md5("240610708") === "0";
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.1
>>> Details: Detected usage of weak crypto function. Consider using stronger alternatives
>>> Severity: Low
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm
>>> Recommendation: Consider using stronger alternatives such as sodium
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    |:|vulnID:[A02.2] | line:|4| md5("240610708") == "0";
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|7| 0 == md5("240610708");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|10| 0 == md5_file("file.txt");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|13| md5("240610708") == md5_file("file.txt");
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|16| md5("240610708") === "0";
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.2
>>> Details: It looks like MD5 is used as a password hash. MD5 is not considered a secure password hash because it can be cracked by an attacker in a short amount of time. Use a suitable password hashing function such as scrypt that is RAM-limited. You can use `password_hash($PASSWORD, PASSWORD_BCRYPT, $OPTIONS);`
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-328: Use of Weak Hash
>>> Recommendation: Consider using password_hash() function for password
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
|:|vulnID:[OVN.1] | line:|4| md5("240610708") == "0";
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[OVN.1] | line:|7| 0 == md5("240610708");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[OVN.1] | line:|10| 0 == md5_file("file.txt");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[OVN.1] | line:|13| md5("240610708") == md5_file("file.txt");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
>>> Vulnerability ID: OVN.1
>>> Details: Make sure comparisons involving hash values are strict.
>>> Severity: Low
>>> OWASP:
>>> CWE: CWE-697: Incorrect Comparison
>>> Recommendation: (use `===` not `==`)
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [d5-used-as-password.php]

```
|:|vulnID:[A02.2] | line:|4| $pass = md5($value);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.2] | line:|10| $pass = hash('md5', $value);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
>>> Vulnerability ID: A02.2
>>> Details: It looks like MD5 is used as a password hash. MD5 is not considered a secure password hash because it can be cracked by an attacker in a short amount of time. Use a suitable password hashing function such as scrypt that is RAM-limited. You can use `password_hash($PASSWORD, PASSWORD_BCRYPT, $OPTIONS);`
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-328: Use of Weak Hash
>>> Recommendation: Consider using password_hash() function for password
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [non-literal-header.php]

```
|:|vulnID:[A03.7] | line:|5| header("Some-Header: $data");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A03.7] | line:|9| header("Some-Header: ".$data);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
>>> Vulnerability ID: A03.7
>>> Details: Using user input when setting headers with `header()` is potentially dangerous. This could allow an attacker to inject a new line and add a new header into the response.
>>> Severity: Low
>>> OWASP: A03:2021 - Injection
>>> CWE: CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
>>> Recommendation: Avoid using user-controlled input in HTTP header.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [penssl-cbc-static-iv.php]

```
|:|vulnID:[A02.2] | line:|41| $hash = substr($ivHashCiphertext, 16, 32);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.2] | line:|54| $hash = substr($ivHashCiphertext, 16, 32);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
>>> Vulnerability ID: A02.2
>>> Details: It looks like MD5 is used as a password hash. MD5 is not considered a secure password hash because it can be cracked by an attacker in a short amount of time. Use a suitable password hashing function such as scrypt that is RAM-limited. You can use `password_hash($PASSWORD, PASSWORD_BCRYPT, $OPTIONS);`
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-328: Use of Weak Hash
>>> Recommendation: Consider using password_hash() function for password
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
|:|vulnID:[A02.5] | line:|9| $ciphertext = openssl_encrypt($plaintext, $method, $key, OPENSSL_RAW_DATA, $iv);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.5] | line:|21| $ciphertext = openssl_encrypt($plaintext, $method, $key, OPENSSL_RAW_DATA, $iv);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.5] | line:|32| $ciphertext = openssl_encrypt($plaintext, "AES-256-CBC", $key, OPENSSL_RAW_DATA, $iv);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.5] | line:|48| return openssl_decrypt($ciphertext, $method, $key, OPENSSL_RAW_DATA, $iv);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A02.5] | line:|61| return openssl_decrypt($ciphertext, $method, $key, OPENSSL_RAW_DATA, $iv);
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
>>> Vulnerability ID: A02.5
>>> Details: Static IV used with AES in CBC mode. Static IVs enable chosen-plaintext attacks against encrypted data
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-329: Generation of Predictable IV with CBC Mode
>>> Recommendation: Avoid using static IV for AES-CBC mode.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [php-permissive-cors.php]

```
|:|vulnID:[A07.2] | line:|5| header("Access-Control-Allow-Origin: *");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A07.2] | line:|8| header("Access-Control-Allow-Origin:* ");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A07.2] | line:|11| Header("access-control-allow-origin: *");
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: A07.2
>>> Details: Access-Control-Allow-Origin response header is set to "*". This will disable CORS Same Origin Policy restrictions.
>>> Severity: Low
>>> OWASP: A07:2021 - Identification and Authentication Failures
>>> CWE: CWE-346: Origin Validation Error
>>> Recommendation:
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [php-ssrf.php]

```
|:|vulnID:[A10.1] | line:|5| $ch = curl_init($_GET['r']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|11| $ch = curl_init($url);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|15| $ch = curl_init();
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|17| curl_setopt($ch, CURLOPT_URL, $_POST['image_url']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|21| $ch = curl_init();
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|24| curl_setopt($ch, CURLOPT_URL, $url);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|30| $file = fopen($url, 'rb');
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|35| $file = fopen($_POST['r'], 'rb');
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|41| $file = file_get_contents($url);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|46| $file = file_get_contents($_POST['r']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|51| $file = file_get_contents("index.php");
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A10.1] | line:|57| $file = fopen("/tmp/test.txt", 'rb');
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: A10.1
>>> Details: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.
>>> Severity: High
>>> OWASP: A10:2021 - Server-Side Request Forgery (SSRF)
>>> CWE: CWE-918: Server-Side Request Forgery (SSRF)
>>> Recommendation: Avoid using dangerous functions with payload data. https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [direct-to-request-uri.php]

```
|:|vulnID:[A01.2] | line:|4| header('Location: '.$_SERVER['REQUEST_URI']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A01.2] | line:|7| header('location:'.$_SERVER['REQUEST_URI']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A01.2] | line:|10| header('Location: '.$_SERVER['REQUEST_URI'].'/');
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A01.2] | line:|13| header("Location: ".$_SERVER['REQUEST_URI']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A01.2] | line:|16| header('Location: '.$_SERVER["REQUEST_URI"]);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
|:|vulnID:[A01.2] | line:|25| header('Location: https://semgrep.dev'.$_SERVER['REQUEST_URI']);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: A01.2
>>> Details: Redirecting to the current request URL may redirect to another domain, if the current path starts with two slashes.
>>> Severity: Low
>>> OWASP: A01:2021 - Broken Access Control
>>> CWE: CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
>>> Recommendation: Avoid using user-controlled input for redirection.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [unlink-use.php]

```
|:|vulnID:[A01.3] | line:|5| unlink("/storage/" . $data . "/test");
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: A01.3
>>> Details: Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor could use this to modify or access files they have no right to.
>>> Severity: Medium
>>> OWASP: A01:2021 - Broken Access Control
>>> CWE: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
>>> Recommendation: Avoid using user-controlled input for unlinking files.
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

Potential vulnerability found in: [unserialize-use.php]

```
|:|vulnID:[A08.2] | line:|5| $object = unserialize($data);
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
```

>>> Vulnerability ID: A08.2
>>> Details: Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution
>>> Severity: Low
>>> OWASP: A08:2021 - Software and Data Integrity Failures

```
>>> CWE: CWE-502: Deserialization of Untrusted Data
>>> Recommendation: Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Potential vulnerability found in: [weak-crypto.php]

```
    |:|vulnID:[A02.1] | line:|4| $hashed_password = crypt('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|7| $hashed_password = md5('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|10| $hashed_password = md5_file('filename.txt');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|13| $hashed_password = sha1('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|16| $hashed_password = sha1_file('filename.txt');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.1] | line:|19| $hashed_password = str_rot13('totally secure');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.1
>>> Details: Detected usage of weak crypto function. Consider using stronger alternatives
>>> Severity: Low
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm
>>> Recommendation: Consider using stronger alternatives such as sodium
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    |:|vulnID:[A02.2] | line:|4| $hashed_password = crypt('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|7| $hashed_password = md5('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|10| $hashed_password = md5_file('filename.txt');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|13| $hashed_password = sha1('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|16| $hashed_password = sha1_file('filename.txt');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|19| $hashed_password = str_rot13('totally secure');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
    |:|vulnID:[A02.2] | line:|22| $hashed_password = sodium_crypto_generichash('mypassword');
    ------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


>>> Vulnerability ID: A02.2
>>> Details: It looks like MD5 is used as a password hash. MD5 is not considered a secure password hash because it can be cracked by an attacker in a short amount of time. Use a suitable password hashing function such as scrypt that is RAM-limited. You can use `password_hash($PASSWORD, PASSWORD_BCRYPT, $OPTIONS);`
>>> Severity: Medium
>>> OWASP: A02:2021 - Cryptographic Failures
>>> CWE: CWE-328: Use of Weak Hash
>>> Recommendation: Consider using password_hash() function for password
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```