**Cyber-Security Report Batch-4**

BY: Mayank Singh Tomar

Email: [tomarm698@gmail.com](mailto:tomarm698@gmail.com)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Project-1:  **OWASP ZAP Scan Reports**

**This is the Report of Website:**

**1.** [**http://testfire.net/**](http://testfire.net/)

**2.** [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ZAP Generated Report for “** [**http://testfire.net/**](http://testfire.net/) **”**

# ZAP Scanning Report

Generated with [[The ZAP logo](https://zaproxy.org/)ZAP](https://zaproxy.org) on Sun 29 May 2022, at 11:00:01

## Contents

* [About this report](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#about-this-report)
  + [Report parameters](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#report-parameters)
* [Summaries](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#summaries)
  + [Alert counts by risk and confidence](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#risk-confidence-counts)
  + [Alert counts by site and risk](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#site-risk-counts)
  + [Alert counts by alert type](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-counts)
* [Alerts](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts)
  + [Risk=High, Confidence=Medium (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-3-confidence-2)
  + [Risk=Medium, Confidence=High (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-3)
  + [Risk=Medium, Confidence=Medium (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-2)
  + [Risk=Medium, Confidence=Low (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-1)
  + [Risk=Low, Confidence=Medium (3)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-1-confidence-2)
  + [Risk=Low, Confidence=Low (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-1-confidence-1)
  + [Risk=Informational, Confidence=Medium (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-0-confidence-2)
* [Appendix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#appendix)
  + [Alert types](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-types)

## About this report

### Report parameters

#### Contexts

No contexts were selected, so all contexts were included by default.

#### Sites

The following sites were included:

* http://testfire.net

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

#### Risk levels

Included: High, Medium, Low, Informational

Excluded: None

#### Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

## Summaries

| This table shows the number of alerts for each level of risk and confidence included in the report.  (The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Confidence | | | | |
| **User Confirmed** | **High** | **Medium** | **Low** | **Total** |
| Risk | **High** | 0 (0.0%) | 0 (0.0%) | 1 (11.1%) | 0 (0.0%) | 1 (11.1%) |
| **Medium** | 0 (0.0%) | 1 (11.1%) | 1 (11.1%) | 1 (11.1%) | 3 (33.3%) |
| **Low** | 0 (0.0%) | 0 (0.0%) | 3 (33.3%) | 1 (11.1%) | 4 (44.4%) |
| **Informational** | 0 (0.0%) | 0 (0.0%) | 1 (11.1%) | 0 (0.0%) | 1 (11.1%) |
| **Total** | 0 (0.0%) | 1 (11.1%) | 6 (66.7%) | 2 (22.2%) | 9 (100%) |

### Alert counts by risk and confidence

### Alert counts by site and risk

| This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.  Alerts with a confidence level of "False Positive" have been excluded from these counts.  (The numbers in brackets are the number of alerts raised for the site at or above that risk level.) | | | | | |
| --- | --- | --- | --- | --- | --- |
|  | | Risk | | | |
| **High (= High)** | **Medium (>= Medium)** | **Low (>= Low)** | **Informational (>= Informational)** |
| Site | **http://testfire.net** | 1 (1) | 3 (4) | 4 (8) | 1 (9) |

| This table shows the number of alerts of each alert type, together with the alert type's risk level.  (The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.) | | |
| --- | --- | --- |
| Alert type | Risk | Count |
| [Cross Site Scripting (Reflected)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-0) | High | 2 (22.2%) |
| [Absence of Anti-CSRF Tokens](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-1) | Medium | 140 (1,555.6%) |
| [Content Security Policy (CSP) Header Not Set](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-2) | Medium | 140 (1,555.6%) |
| [Missing Anti-clickjacking Header](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-3) | Medium | 63 (700.0%) |
| [Cookie without SameSite Attribute](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-4) | Low | 3 (33.3%) |
| [Cross-Domain JavaScript Source File Inclusion](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-5) | Low | 1 (11.1%) |
| [Timestamp Disclosure - Unix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-6) | Low | 112 (1,244.4%) |
| [X-Content-Type-Options Header Missing](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-7) | Low | 101 (1,122.2%) |
| [Information Disclosure - Suspicious Comments](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-8) | Informational | 15 (166.7%) |
| Total |  | 9 |

### Alert counts by alert type

## Alerts

### Risk=High, Confidence=Medium (1)

#### http://testfire.net (1)

##### [Cross Site Scripting (Reflected)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-0) (1)

* + - 1. POST http://testfire.net/sendFeedback

### Risk=Medium, Confidence=High (1)

#### http://testfire.net (1)

##### [Content Security Policy (CSP) Header Not Set](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-2) (1)

* + - 1. GET http://testfire.net/

### Risk=Medium, Confidence=Medium (1)

#### http://testfire.net (1)

##### [Missing Anti-clickjacking Header](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-3) (1)

* + - 1. GET http://testfire.net/

### Risk=Medium, Confidence=Low (1)

#### http://testfire.net (1)

##### [Absence of Anti-CSRF Tokens](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-1) (1)

* + - 1. GET http://testfire.net/

### Risk=Low, Confidence=Medium (3)

#### http://testfire.net (3)

##### [Cookie without SameSite Attribute](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-4) (1)

* + - 1. GET http://testfire.net/

##### [Cross-Domain JavaScript Source File Inclusion](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-5) (1)

* + - 1. GET <http://testfire.net/index.jsp?content=personal_investments.html>.

##### [X-Content-Type-Options Header Missing](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-7) (1)

* + - 1. GET http://testfire.net/

### Risk=Low, Confidence=Low (1)

#### http://testfire.net (1)

##### [Timestamp Disclosure - Unix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-6) (1)

* + - 1. GET http://testfire.net/index.jsp?content=inside\_press.htm

### Risk=Informational, Confidence=Medium (1)

#### http://testfire.net (1)

##### [Information Disclosure - Suspicious Comments](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-8) (1)

* + - 1. GET http://testfire.net/login.jsp

## Appendix

### Alert types

This section contains additional information on the types of alerts in the report.

#### Cross Site Scripting (Reflected)

|  |  |
| --- | --- |
| **Source** | raised by an active scanner ([Cross Site Scripting (Reflected)](https://www.zaproxy.org/docs/alerts/40012/)) |
| **CWE ID** | [79](https://cwe.mitre.org/data/definitions/79.html) |
| **WASC ID** | 8 |
| **Reference** | * + <http://projects.webappsec.org/Cross-Site-Scripting>   + <http://cwe.mitre.org/data/definitions/79.html> |

#### Absence of Anti-CSRF Tokens

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Absence of Anti-CSRF Tokens](https://www.zaproxy.org/docs/alerts/10202/)) |
| **CWE ID** | [352](https://cwe.mitre.org/data/definitions/352.html) |
| **WASC ID** | 9 |
| **Reference** | * + <http://projects.webappsec.org/Cross-Site-Request-Forgery>   + <http://cwe.mitre.org/data/definitions/352.html> |

#### Content Security Policy (CSP) Header Not Set

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Content Security Policy (CSP) Header Not Set](https://www.zaproxy.org/docs/alerts/10038/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * + <https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy>   + <https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html>   + <http://www.w3.org/TR/CSP/>   + <http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html>   + <http://www.html5rocks.com/en/tutorials/security/content-security-policy/>   + <http://caniuse.com/#feat=contentsecuritypolicy>   + <http://content-security-policy.com/> |

#### Missing Anti-clickjacking Header

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Anti-clickjacking Header](https://www.zaproxy.org/docs/alerts/10020/)) |
| **CWE ID** | [1021](https://cwe.mitre.org/data/definitions/1021.html) |
| **WASC ID** | 15 |
| **Reference** | * + <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options> |

#### Cookie without SameSite Attribute

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cookie without SameSite Attribute](https://www.zaproxy.org/docs/alerts/10054/)) |
| **CWE ID** | [1275](https://cwe.mitre.org/data/definitions/1275.html) |
| **WASC ID** | 13 |
| **Reference** | * + <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site> |

#### Cross-Domain JavaScript Source File Inclusion

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cross-Domain JavaScript Source File Inclusion](https://www.zaproxy.org/docs/alerts/10017/)) |
| **CWE ID** | [829](https://cwe.mitre.org/data/definitions/829.html) |
| **WASC ID** | 15 |

#### Timestamp Disclosure - Unix

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Timestamp Disclosure](https://www.zaproxy.org/docs/alerts/10096/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |
| **Reference** | * + <http://projects.webappsec.org/w/page/13246936/Information%20Leakage> |

#### X-Content-Type-Options Header Missing

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([X-Content-Type-Options Header Missing](https://www.zaproxy.org/docs/alerts/10021/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * + <http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>   + <https://owasp.org/www-community/Security_Headers> |

#### Information Disclosure - Suspicious Comments

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Information Disclosure - Suspicious Comments](https://www.zaproxy.org/docs/alerts/10027/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

SQL-Injection for **“** [**http://testfire.net/**](http://testfire.net/) **”**

Mitigation using SQL through Login page is done as followed:

* 1. Let’s try to login using login portal at <http://testfire.net/login.jsp>
  2. Let’s try login using unexpected values like ‘ & . as username & password.
  3. Do some more uncertain trial and then try recording their error like:

**Syntax error: Encountered "\'" at line 1, column 63.**

* 1. Then try using **‘ or 1=1 – –** as username and fill password with any random values.
  2. Sometimes u might get user or even admin access.
  3. Or Simply try using sqlmap tool in kali to get better sql-injections.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ZAP Generated Report for “** [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/) **”**

# ZAP Scanning Report

Generated with [[The ZAP logo](https://zaproxy.org/)ZAP](https://zaproxy.org) on Sun 29 May 2022, at 11:26:45

## Contents

* [About this report](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#about-this-report)
  + [Report parameters](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#report-parameters)
* [Summaries](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#summaries)
  + [Alert counts by risk and confidence](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#risk-confidence-counts)
  + [Alert counts by site and risk](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#site-risk-counts)
  + [Alert counts by alert type](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-counts)
* [Alerts](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts)
  + [Risk=High, Confidence=Medium (2)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-3-confidence-2)
  + [Risk=Medium, Confidence=High (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-3)
  + [Risk=Medium, Confidence=Medium (2)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-2)
  + [Risk=Medium, Confidence=Low (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-2-confidence-1)
  + [Risk=Low, Confidence=Medium (4)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-1-confidence-2)
  + [Risk=Low, Confidence=Low (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-1-confidence-1)
  + [Risk=Informational, Confidence=Medium (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-0-confidence-2)
  + [Risk=Informational, Confidence=Low (1)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alerts--risk-0-confidence-1)
* [Appendix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#appendix)
  + [Alert types](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-types)

## About this report

### Report parameters

#### Contexts

No contexts were selected, so all contexts were included by default.

#### Sites

The following sites were included:

* http://testphp.vulnweb.com
* http://testfire.net

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

#### Risk levels

Included: High, Medium, Low, Informational

Excluded: None

#### Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

## Summaries

### Alert counts by risk and confidence

| This table shows the number of alerts for each level of risk and confidence included in the report.  (The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Confidence | | | | |
| **User Confirmed** | **High** | **Medium** | **Low** | **Total** |
| Risk | **High** | 0 (0.0%) | 0 (0.0%) | 2 (15.4%) | 0 (0.0%) | 2 (15.4%) |
| **Medium** | 0 (0.0%) | 1 (7.7%) | 2 (15.4%) | 1 (7.7%) | 4 (30.8%) |
| **Low** | 0 (0.0%) | 0 (0.0%) | 4 (30.8%) | 1 (7.7%) | 5 (38.5%) |
| **Informational** | 0 (0.0%) | 0 (0.0%) | 1 (7.7%) | 1 (7.7%) | 2 (15.4%) |
| **Total** | 0 (0.0%) | 1 (7.7%) | 9 (69.2%) | 3 (23.1%) | 13 (100%) |

### Alert counts by site and risk

| This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.  Alerts with a confidence level of "False Positive" have been excluded from these counts.  (The numbers in brackets are the number of alerts raised for the site at or above that risk level.) | | | | | |
| --- | --- | --- | --- | --- | --- |
|  | | Risk | | | |
| **High (= High)** | **Medium (>= Medium)** | **Low (>= Low)** | **Informational (>= Informational)** |
| Site | **http://testphp.vulnweb.com** | 1 (1) | 1 (2) | 1 (3) | 1 (4) |
| **http://testfire.net** | 1 (1) | 3 (4) | 4 (8) | 1 (9) |

### Alert counts by alert type

| This table shows the number of alerts of each alert type, together with the alert type's risk level.  (The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.) | | |
| --- | --- | --- |
| Alert type | Risk | Count |
| [Cross Site Scripting (Reflected)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-0) | High | 18 (138.5%) |
| [SQL Injection](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-1) | High | 7 (53.8%) |
| [.htaccess Information Leak](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-2) | Medium | 7 (53.8%) |
| [Absence of Anti-CSRF Tokens](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-3) | Medium | 181 (1,392.3%) |
| [Content Security Policy (CSP) Header Not Set](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-4) | Medium | 188 (1,446.2%) |
| [Missing Anti-clickjacking Header](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-5) | Medium | 108 (830.8%) |
| [Cookie without SameSite Attribute](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-6) | Low | 3 (23.1%) |
| [Cross-Domain JavaScript Source File Inclusion](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-7) | Low | 1 (7.7%) |
| [Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-8) | Low | 63 (484.6%) |
| [Timestamp Disclosure - Unix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-9) | Low | 112 (861.5%) |
| [X-Content-Type-Options Header Missing](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-10) | Low | 169 (1,300.0%) |
| [Charset Mismatch (Header Versus Meta Content-Type Charset)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-11) | Informational | 32 (246.2%) |
| [Information Disclosure - Suspicious Comments](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-12) | Informational | 16 (123.1%) |
| Total |  | 13 |

## Alerts

### Risk=High, Confidence=Medium (2)

#### http://testphp.vulnweb.com (1)

##### [SQL Injection](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-1) (1)

* + - 1. POST http://testphp.vulnweb.com/secured/newuser.php

#### http://testfire.net (1)

##### [Cross Site Scripting (Reflected)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-0) (1)

* + - 1. POST http://testfire.net/sendFeedback

### Risk=Medium, Confidence=High (1)

#### http://testfire.net (1)

##### [Content Security Policy (CSP) Header Not Set](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-4) (1)

* + - 1. GET http://testfire.net/

### Risk=Medium, Confidence=Medium (2)

#### http://testphp.vulnweb.com (1)

##### [.htaccess Information Leak](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-2) (1)

* + - 1. GET http://testphp.vulnweb.com/Mod\_Rewrite\_Shop/.htaccess

#### http://testfire.net (1)

##### [Missing Anti-clickjacking Header](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-5) (1)

* + - 1. GET http://testfire.net/

### Risk=Medium, Confidence=Low (1)

#### http://testfire.net (1)

##### [Absence of Anti-CSRF Tokens](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-3) (1)

* + - 1. GET http://testfire.net/

### Risk=Low, Confidence=Medium (4)

#### http://testphp.vulnweb.com (1)

##### [Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-8) (1)

* + - 1. GET http://testphp.vulnweb.com/

#### http://testfire.net (3)

##### [Cookie without SameSite Attribute](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-6) (1)

* + - 1. GET http://testfire.net/

##### [Cross-Domain JavaScript Source File Inclusion](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-7) (1)

* + - 1. GET http://testfire.net/index.jsp?content=personal\_investments.html.

##### [X-Content-Type-Options Header Missing](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-10) (1)

* + - 1. GET http://testfire.net/

### Risk=Low, Confidence=Low (1)

#### http://testfire.net (1)

##### [Timestamp Disclosure - Unix](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-9) (1)

* + - 1. GET http://testfire.net/index.jsp?content=inside\_press.htm

### Risk=Informational, Confidence=Medium (1)

#### http://testfire.net (1)

##### [Information Disclosure - Suspicious Comments](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-12) (1)

* + - 1. GET http://testfire.net/login.jsp

### Risk=Informational, Confidence=Low (1)

#### http://testphp.vulnweb.com (1)

##### [Charset Mismatch (Header Versus Meta Content-Type Charset)](file:///C:\Users\lenovo\ZAP-Reports\2022-05-29-ZAP-Report-.html#alert-type-11) (1)

* + - 1. GET http://testphp.vulnweb.com/

## Appendix

### Alert types

This section contains additional information on the types of alerts in the report.

#### Cross Site Scripting (Reflected)

|  |  |
| --- | --- |
| **Source** | raised by an active scanner ([Cross Site Scripting (Reflected)](https://www.zaproxy.org/docs/alerts/40012/)) |
| **CWE ID** | [79](https://cwe.mitre.org/data/definitions/79.html) |
| **WASC ID** | 8 |
| **Reference** | * + <http://projects.webappsec.org/Cross-Site-Scripting>   + <http://cwe.mitre.org/data/definitions/79.html> |

#### SQL Injection

|  |  |
| --- | --- |
| **Source** | raised by an active scanner ([SQL Injection](https://www.zaproxy.org/docs/alerts/40018/)) |
| **CWE ID** | [89](https://cwe.mitre.org/data/definitions/89.html) |
| **WASC ID** | 19 |
| **Reference** | * + <https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html> |

#### .htaccess Information Leak

|  |  |
| --- | --- |
| **Source** | raised by an active scanner ([.htaccess Information Leak](https://www.zaproxy.org/docs/alerts/40032/)) |
| **CWE ID** | [94](https://cwe.mitre.org/data/definitions/94.html) |
| **WASC ID** | 14 |
| **Reference** | * + <http://www.htaccess-guide.com/> |

#### Absence of Anti-CSRF Tokens

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Absence of Anti-CSRF Tokens](https://www.zaproxy.org/docs/alerts/10202/)) |
| **CWE ID** | [352](https://cwe.mitre.org/data/definitions/352.html) |
| **WASC ID** | 9 |
| **Reference** | * + <http://projects.webappsec.org/Cross-Site-Request-Forgery>   + <http://cwe.mitre.org/data/definitions/352.html> |

#### Content Security Policy (CSP) Header Not Set

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Content Security Policy (CSP) Header Not Set](https://www.zaproxy.org/docs/alerts/10038/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * + <https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy>   + <https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html>   + <http://www.w3.org/TR/CSP/>   + <http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html>   + <http://www.html5rocks.com/en/tutorials/security/content-security-policy/>   + <http://caniuse.com/#feat=contentsecuritypolicy>   + <http://content-security-policy.com/> |

#### Missing Anti-clickjacking Header

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Anti-clickjacking Header](https://www.zaproxy.org/docs/alerts/10020/)) |
| **CWE ID** | [1021](https://cwe.mitre.org/data/definitions/1021.html) |
| **WASC ID** | 15 |
| **Reference** | * + <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options> |

#### Cookie without SameSite Attribute

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cookie without SameSite Attribute](https://www.zaproxy.org/docs/alerts/10054/)) |
| **CWE ID** | [1275](https://cwe.mitre.org/data/definitions/1275.html) |
| **WASC ID** | 13 |
| **Reference** | * + <https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site> |

#### Cross-Domain JavaScript Source File Inclusion

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Cross-Domain JavaScript Source File Inclusion](https://www.zaproxy.org/docs/alerts/10017/)) |
| **CWE ID** | [829](https://cwe.mitre.org/data/definitions/829.html) |
| **WASC ID** | 15 |

#### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)](https://www.zaproxy.org/docs/alerts/10037/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |
| **Reference** | * + <http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>   + <http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html> |

#### Timestamp Disclosure - Unix

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Timestamp Disclosure](https://www.zaproxy.org/docs/alerts/10096/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |
| **Reference** | * + <http://projects.webappsec.org/w/page/13246936/Information%20Leakage> |

#### X-Content-Type-Options Header Missing

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([X-Content-Type-Options Header Missing](https://www.zaproxy.org/docs/alerts/10021/)) |
| **CWE ID** | [693](https://cwe.mitre.org/data/definitions/693.html) |
| **WASC ID** | 15 |
| **Reference** | * + <http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>   + <https://owasp.org/www-community/Security_Headers> |

#### Charset Mismatch (Header Versus Meta Content-Type Charset)

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Charset Mismatch](https://www.zaproxy.org/docs/alerts/90011/)) |
| **CWE ID** | [436](https://cwe.mitre.org/data/definitions/436.html) |
| **WASC ID** | 15 |
| **Reference** | * + <http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection> |

#### Information Disclosure - Suspicious Comments

|  |  |
| --- | --- |
| **Source** | raised by a passive scanner ([Information Disclosure - Suspicious Comments](https://www.zaproxy.org/docs/alerts/10027/)) |
| **CWE ID** | [200](https://cwe.mitre.org/data/definitions/200.html) |
| **WASC ID** | 13 |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**