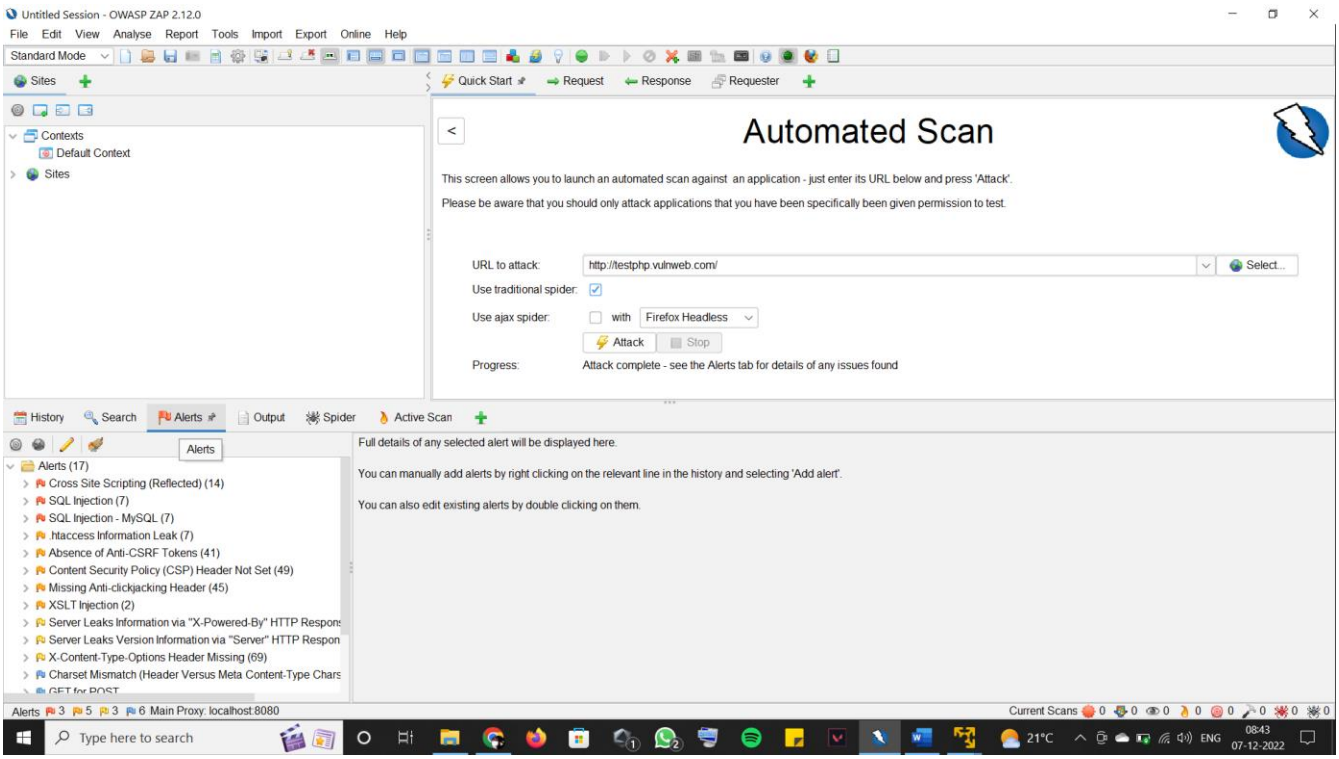
Cyber Security by Threat Prism

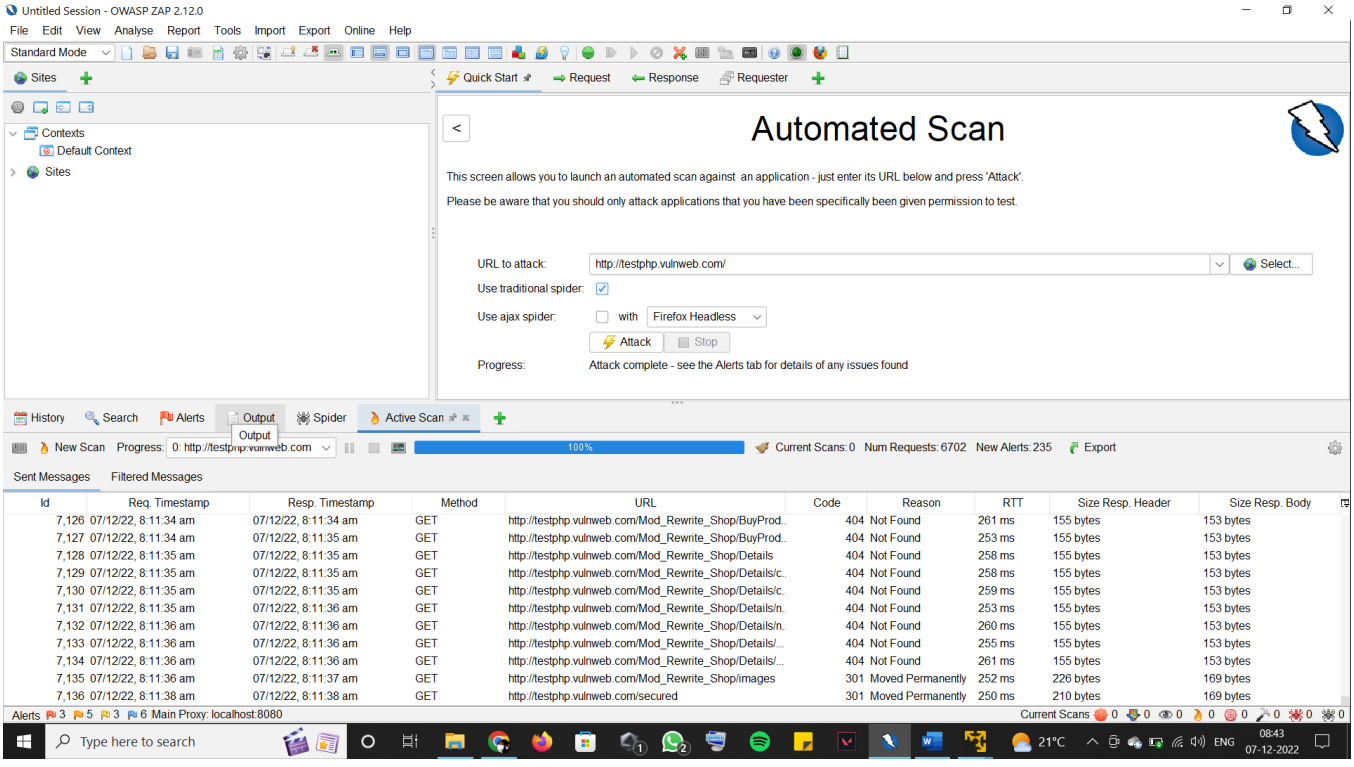
BATCH 7

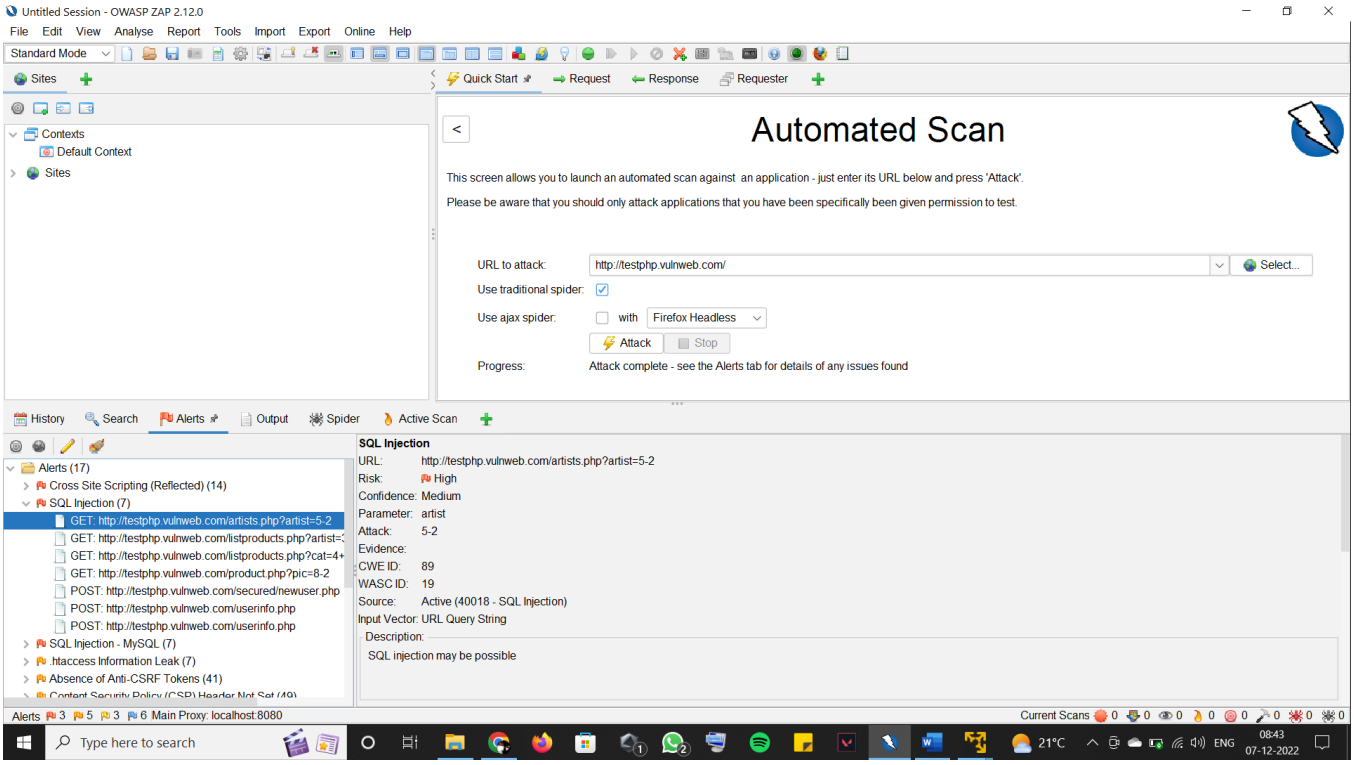
Sai Goutham Reddy Alavala

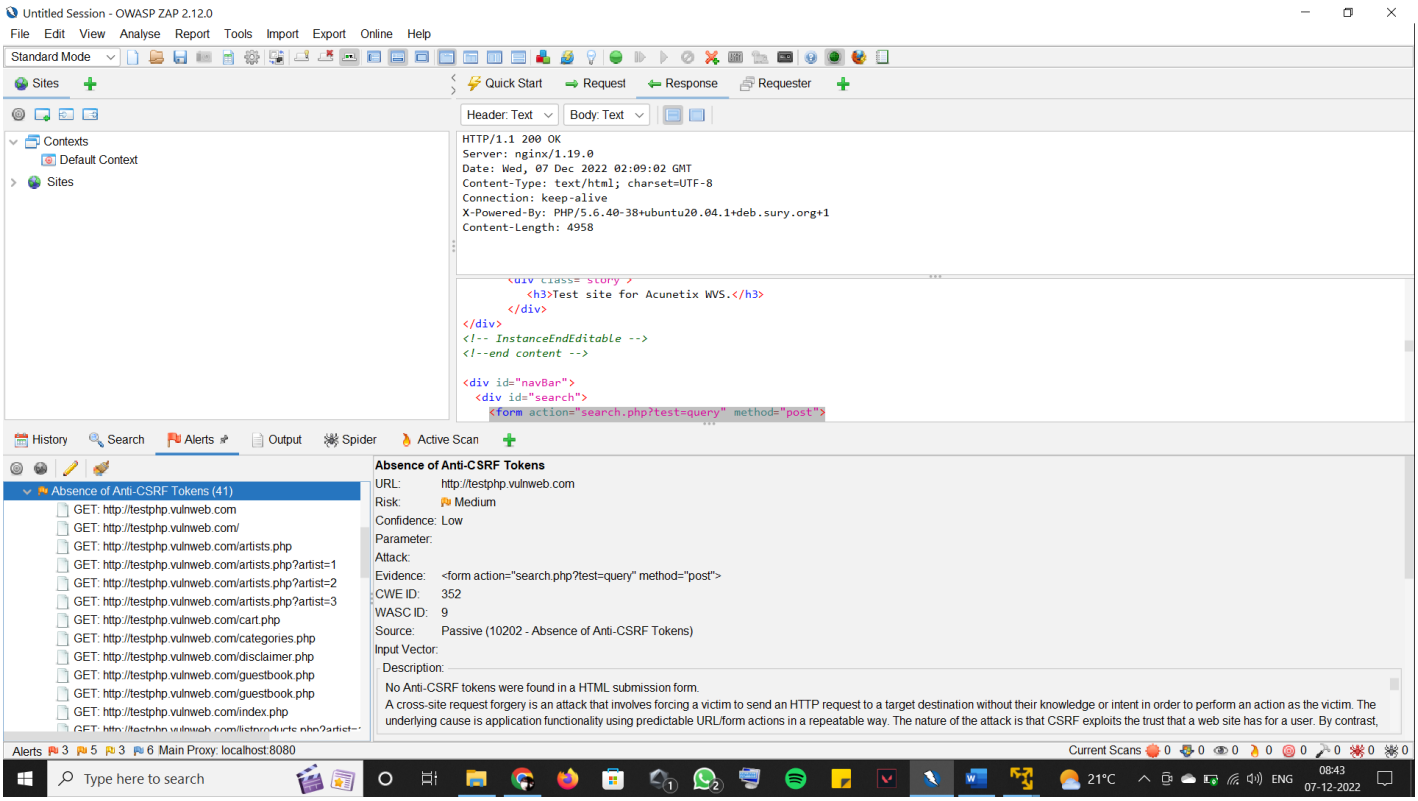
Cyber Security/Ethical Hacking - Scanning using OWASP ZAP.
Threat Prism Project – 1

The vulnerable website we used to scan using OWASP ZAP tool is http://testphp.vulnweb.com/ where we have done automatic scan and the results are as followed:


Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://testphp.vulnweb.com/
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
Alerts
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts (17)
Cross Site Scripting (Reflected) (14)
SQL Injection (7)
SQL Injection - MySQL (7)
.htaccess Information Leak (7)
Absence of Anti-CSRF Tokens (41)
Content Security Policy (CSP) Header Not Set (49)
Missing Anti-clickjacking Header (45)
XSLT Injection (2)
Server Leaks Information via "X-Powered-By" HTTP Respons
Server Leaks Version Information via "Server" HTTP Respon
X-Content-Type-Options Header Missing (69)
Charset Mismatch (Header Versus Meta Content-Type Chars
GET for POST
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0
Type here to search
21°C
ENG
08:43
07-12-2022

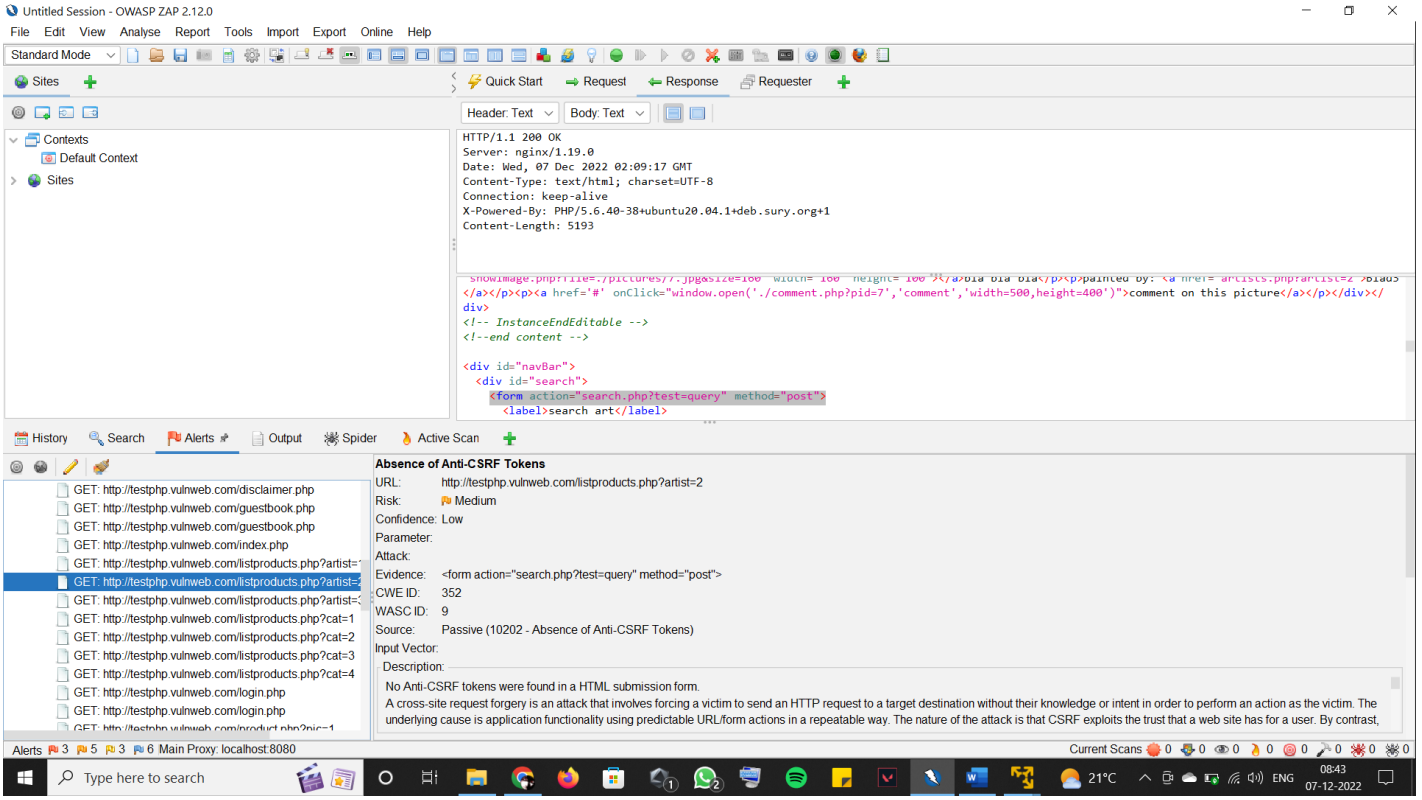

Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://testphp.vulnweb.com/
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
Output
New Scan
Progress:
0: http://testphp.vulnweb.com
100%
Current Scans: 0
Num Requests: 6702
New Alerts: 235
Export
Sent Messages
Filtered Messages
Id
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
7,126 07/12/22, 8:11:34 am 07/12/22, 8:11:34 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProd.. 404 Not Found 261 ms 155 bytes 153 bytes
7,127 07/12/22, 8:11:34 am 07/12/22, 8:11:35 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProd.. 404 Not Found 253 ms 155 bytes 153 bytes
7,128 07/12/22, 8:11:35 am 07/12/22, 8:11:35 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details 404 Not Found 258 ms 155 bytes 153 bytes
7,129 07/12/22, 8:11:35 am 07/12/22, 8:11:35 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/c.. 404 Not Found 258 ms 155 bytes 153 bytes
7,130 07/12/22, 8:11:35 am 07/12/22, 8:11:35 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/c.. 404 Not Found 259 ms 155 bytes 153 bytes
7,131 07/12/22, 8:11:35 am 07/12/22, 8:11:36 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/n.. 404 Not Found 253 ms 155 bytes 153 bytes
7,132 07/12/22, 8:11:36 am 07/12/22, 8:11:36 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/n.. 404 Not Found 260 ms 155 bytes 153 bytes
7,133 07/12/22, 8:11:36 am 07/12/22, 8:11:36 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/... 404 Not Found 255 ms 155 bytes 153 bytes
7,134 07/12/22, 8:11:36 am 07/12/22, 8:11:36 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/... 404 Not Found 261 ms 155 bytes 153 bytes
7,135 07/12/22, 8:11:36 am 07/12/22, 8:11:37 am GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/images 301 Moved Permanently 252 ms 226 bytes 169 bytes
7,136 07/12/22, 8:11:38 am 07/12/22, 8:11:38 am GET http://testphp.vulnweb.com/secured 301 Moved Permanently 250 ms 210 bytes 169 bytes
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0
Type here to search
21°C
ENG
08:43
07-12-2022


Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://testphp.vulnweb.com/
Select...
Use traditional spider:
Use ajax spider: with Firefox Headless
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
Active Scan
Alerts (17)
Cross Site Scripting (Reflected) (14)
SQL Injection (7)
GET: http://testphp.vulnweb.com/artists.php?artist=5-2
GET: http://testphp.vulnweb.com/listproducts.php?artist=
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php
SQL Injection - MySQL (7)
.htaccess Information Leak (7)
Absence of Anti-CSRF Tokens (41)
SQL Injection
URL: http://testphp.vulnweb.com/artists.php?artist=5-2
Risk: High
Confidence: Medium
Parameter: artist
Attack: 5-2
Evidence:
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Input Vector: URL Query String
Description:
SQL injection may be possible
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans
Type here to search
21°C
ENG
08:43
07-12-2022

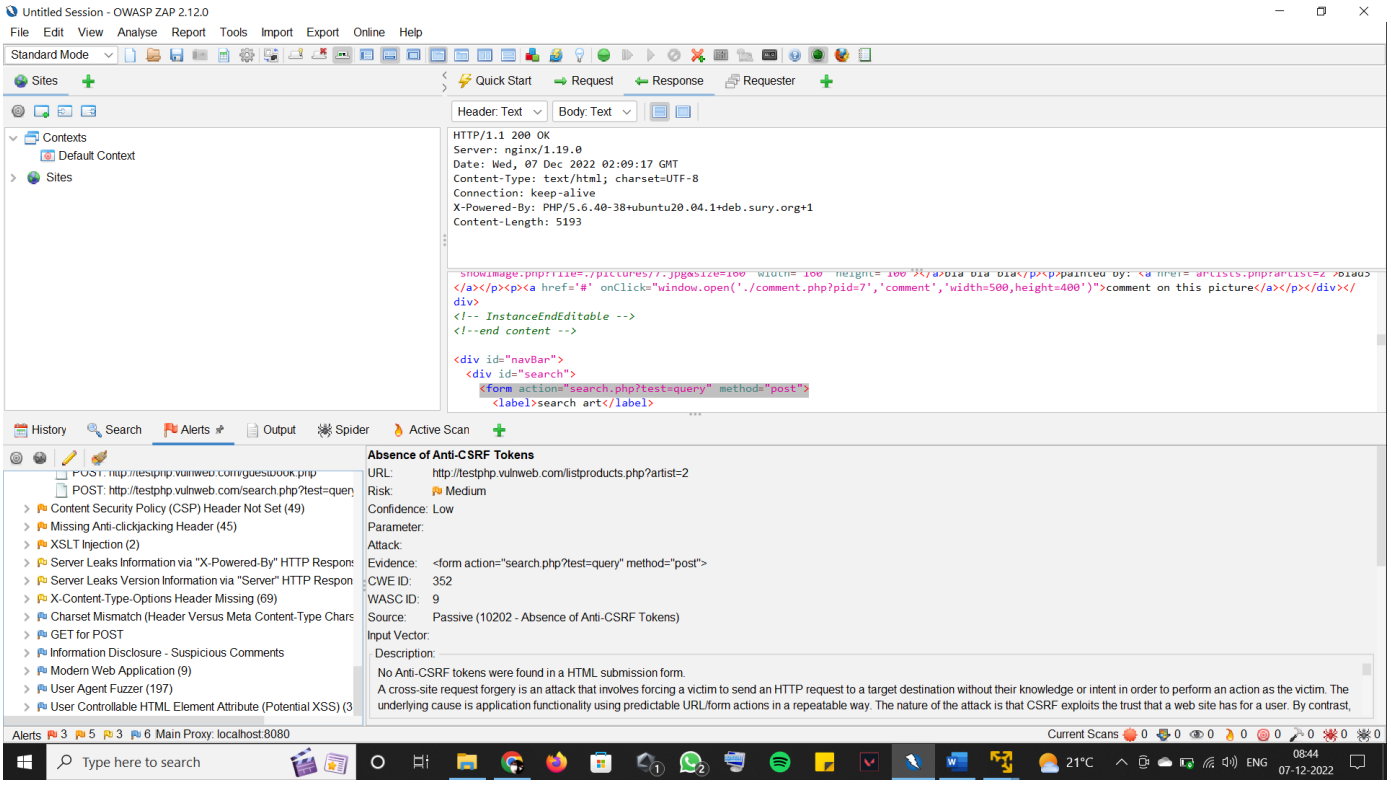

Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 07 Dec 2022 02:09:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 4958
<h3>Test site for Acunetix WVS.</h3>

<!-- InstanceEndEditable -->
<!--end content -->

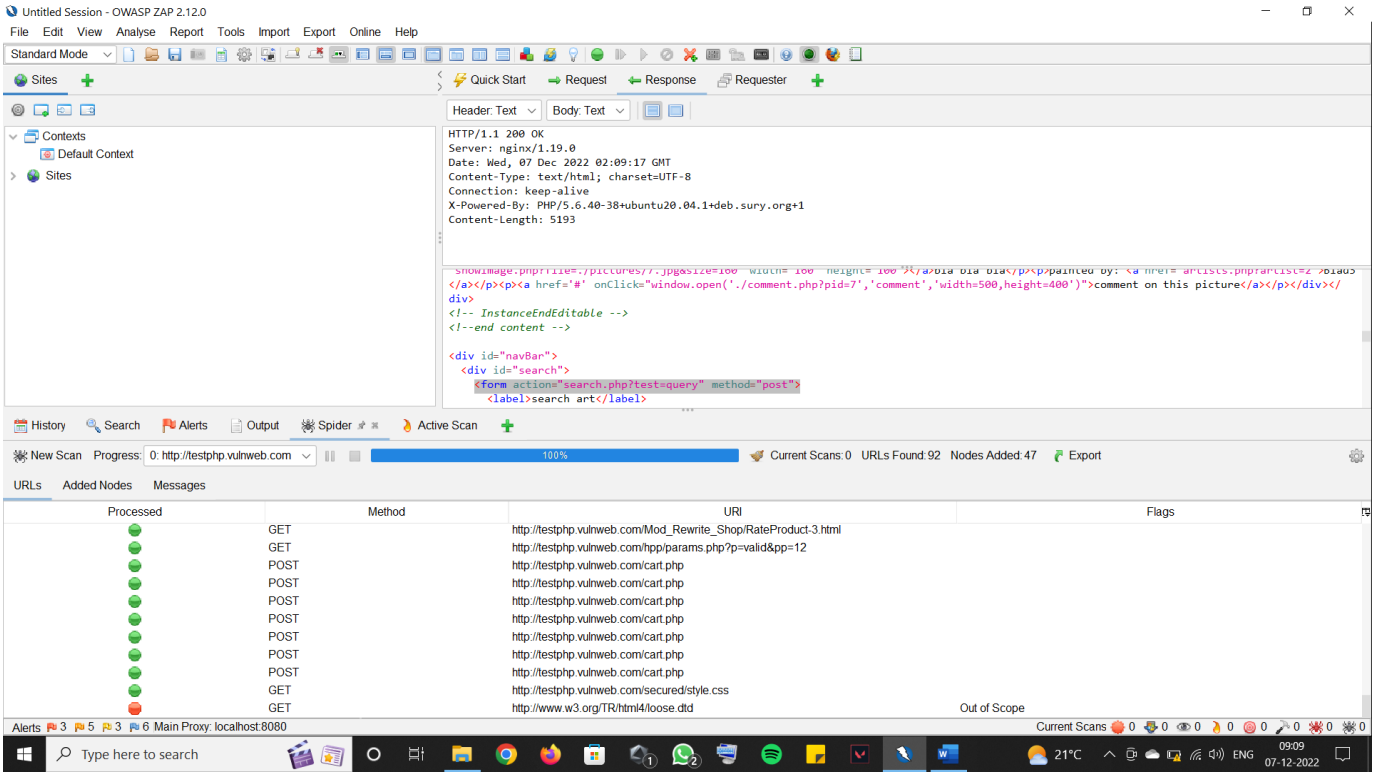
<form action="search.php?test=query" method="post">
History
Search
Alerts
Output
Spider
Active Scan
Absence of Anti-CSRF Tokens (41)
GET: http://testphp.vulnweb.com
GET: http://testphp.vulnweb.com/
GET: http://testphp.vulnweb.com/artists.php
GET: http://testphp.vulnweb.com/artists.php?artist=1
GET: http://testphp.vulnweb.com/artists.php?artist=2
GET: http://testphp.vulnweb.com/artists.php?artist=3
GET: http://testphp.vulnweb.com/cart.php
GET: http://testphp.vulnweb.com/categories.php
GET: http://testphp.vulnweb.com/disclaimer.php
GET: http://testphp.vulnweb.com/guestbook.php
GET: http://testphp.vulnweb.com/guestbook.php
GET: http://testphp.vulnweb.com/index.php
Absence of Anti-CSRF Tokens
URL: http://testphp.vulnweb.com
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="search.php?test=query" method="post">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans
Type here to search
21°C
ENG
08:43
07-12-2022


Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 07 Dec 2022 02:09:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 5193
<!-- InstanceEndEditable -->
<!--end content -->

<form action="search.php?test=query" method="post">
<label>search art</label>
History
Search
Alerts
Output
Spider
Active Scan
GET: http://testphp.vulnweb.com/disclaimer.php
GET: http://testphp.vulnweb.com/guestbook.php
GET: http://testphp.vulnweb.com/guestbook.php
GET: http://testphp.vulnweb.com/index.php
GET: http://testphp.vulnweb.com/listproducts.php?artist=1
GET: http://testphp.vulnweb.com/listproducts.php?artist=2
GET: http://testphp.vulnweb.com/listproducts.php?artist=3
GET: http://testphp.vulnweb.com/listproducts.php?cat=1
GET: http://testphp.vulnweb.com/listproducts.php?cat=2
GET: http://testphp.vulnweb.com/listproducts.php?cat=3
GET: http://testphp.vulnweb.com/listproducts.php?cat=4
GET: http://testphp.vulnweb.com/login.php
GET: http://testphp.vulnweb.com/login.php
Absence of Anti-CSRF Tokens
URL: http://testphp.vulnweb.com/listproducts.php?artist=2
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="search.php?test=query" method="post">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans
Type here to search
21°C
ENG
08:43
07-12-2022


Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 07 Dec 2022 02:09:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 5193
<!-- InstanceEndEditable -->
<!--end content -->

<form action="search.php?test=query" method="post">
<label>search art</label>
History
Search
Alerts
Output
Spider
Active Scan
POST: http://testphp.vulnweb.com/search.php?test=query
Content Security Policy (CSP) Header Not Set (49)
Missing Anti-clickjacking Header (45)
XSLT Injection (2)
Server Leaks Information via "X-Powered-By" HTTP Respons
Server Leaks Version Information via "Server" HTTP Respon
X-Content-Type-Options Header Missing (69)
Charset Mismatch (Header Versus Meta Content-Type Chars
GET for POST
Information Disclosure - Suspicious Comments
Modern Web Application (9)
User Agent Fuzzer (197)
User Controllable HTML Element Attribute (Potential XSS) (3
Absence of Anti-CSRF Tokens
URL: http://testphp.vulnweb.com/listproducts.php?artist=2
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="search.php?test=query" method="post">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
Alerts 3 5 3 6 Main Proxy: localhost:8080
Current Scans
Type here to search
21°C
ENG
08:44
07-12-2022



The report generated is as below:

ZAP Scanning Report

Generated with ZAP on Mon 21 Nov 2022, at 11:03:07

Contents

1. About this report
    1. Report parameters
2. Summaries
    1. Alert counts by risk and confidence
    2. Alert counts by site and risk
    3. Alert counts by alert type
3. Alerts
    1. Risk=High, Confidence=Medium (3)
    2. Risk=Medium, Confidence=High (1)
    3. Risk=Medium, Confidence=Medium (3)
    4. Risk=Medium, Confidence=Low (1)
    5. Risk=Low, Confidence=Medium (2)
    6. Risk=Low, Confidence=Medium (2)
    7. Risk=Informational, Confidence=High (1)
    8. Risk=Informational, Confidence=Medium (2)
    9. Risk=Informational, Confidence=Low (3)
4. Appendix
    1. 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

(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%)	3 (17.6%)	0 (0.0%)	3 (17.6%)
	Medium	0 (0.0%)	1 (5.9%)	3 (17.6%)	1 (5.9%)	5 (29.4%)
	Low	0 (0.0%)	1 (5.9%)	2 (11.8%)	0 (0.0%)	3 (17.6%)
	Informational	0 (0.0%)	1 (5.9%)	2 (11.8%)	3 (17.6%)	6 (35.3%)
	Total	0 (0.0%)	3 (17.6%)	10 (58.8%)	4 (23.5%)	17 (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	3 (3)	5 (8)	3 (11)	6 (17)

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)	High	14 (82.4%)
SQL Injection	High	8 (47.1%)
SQL Injection - MySQL	High	4 (23.5%)
.htaccess Information Leak	Medium	7 (41.2%)
Absence of Anti-CSRF Tokens	Medium	41 (241.2%)
Content Security Policy (CSP) Header Not Set	Medium	49 (288.2%)
Missing Anti-clickjacking Header	Medium	45 (264.7%)
XSLT Injection	Medium	2 (11.8%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	63 (370.6%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	75 (441.2%)
X-Content-Type-Options Header Missing	Low	69 (405.9%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	52 (306.2%)
GET for POST	Informational	1 (5.9%)
Information Disclosure - Suspicious Comments	Informational	1 (5.9%)
Modern Web Application	Informational	9 (52.9%)
User Agent Fuzzer	Informational	197 (1,158.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (17.6%)
Total		17

Alerts

1. **Risk=High, Confidence=Medium (3)**
    1. **http://testphp.vulnweb.com (3)**
        1. **Cross Site Scripting (Reflected)** (9)
            1. ► POST http://testphp.vulnweb.com/guestbook.php
        2. **SQL Injection** (0)
            1. ► POST http://testphp.vulnweb.com/secured/newuser.php
        3. **SQL Injection - MySQL** (0)
            1. ► POST http://testphp.vulnweb.com/userinfo.php
2. **Risk=Medium, Confidence=High (1)**
    1. **http://testphp.vulnweb.com (1)**
        1. **Content Security Policy (CSP) Header Not Set** (0)
            1. ► GET http://testphp.vulnweb.com/robots.txt
3. **Risk=Medium, Confidence=Medium (3)**
    1. **http://testphp.vulnweb.com (3)**
        1. **.htaccess Information Leak** (0)
            1. ► GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
        2. **Missing Anti-clickjacking Header** (1)
            1. ► GET http://testphp.vulnweb.com/
        3. **XSLT Injection** (1)
            1. ► GET http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Finvpbp.vulnweb.com%3A22%27%29%22%2F%3E
4. **Risk=Medium, Confidence=Low (1)**
    1. **http://testphp.vulnweb.com (1)**
        1. **Absence of Anti-CSRF Tokens** (0)
            1. ► GET http://testphp.vulnweb.com/
5. **Risk=Low, Confidence=High (1)**
    1. **http://testphp.vulnweb.com (1)**
        1. **Server Leaks Version Information via "Server" HTTP Response Header Field** (1)
            1. ► GET http://testphp.vulnweb.com/robots.txt
6. **Risk=Low, Confidence=Medium (2)**
    1. **http://testphp.vulnweb.com (2)**
        1. **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)** (0)
            1. ► GET http://testphp.vulnweb.com/
        2. **X-Content-Type-Options Header Missing** (0)
            1. ► GET http://testphp.vulnweb.com/
7. **Risk=Informational, Confidence=High (1)**
    1. **http://testphp.vulnweb.com (1)**
        1. **GET for POST** (0)
            1. ► GET http://testphp.vulnweb.com/cart.php
8. **Risk=Informational, Confidence=Medium (2)**
    1. **http://testphp.vulnweb.com (2)**
        1. **Modern Web Application** (1)
            1. ► GET http://testphp.vulnweb.com/artists.php
        2. **User Agent Fuzzer** (1)
            1. ► POST http://testphp.vulnweb.com/guestbook.php
9. **Risk=Informational, Confidence=Low (3)**
    1. **http://testphp.vulnweb.com (3)**
        1. **Charset Mismatch (Header Versus Meta Content-Type Charset)** (1)
            1. ► GET http://testphp.vulnweb.com/
        2. **Information Disclosure - Suspicious Comments** (0)
            1. ► GET http://testphp.vulnweb.com/AJAX/index.php
        3. **User Controllable HTML Element Attribute (Potential XSS)** (1)
            1. ► POST http://testphp.vulnweb.com/search.php?test=query

Appendix

Alert types

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

1. **Cross Site Scripting (Reflected)**

    Source raised by an active scanner (Cross Site Scripting (Reflected))
    CWE ID 79
    WASC ID 8
    Reference
    1. http://projects.webappsec.org/Cross-Site-Scripting
    2. http://cwe.mitre.org/data/definitions/79.html

2. **SQL Injection**

    Source raised by an active scanner (SQL Injection)
    CWE ID 89
    WASC ID 19
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

3. **SQL Injection - MySQL**

    Source raised by an active scanner (SQL Injection - MySQL)
    CWE ID 89
    WASC ID 19
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

4. **.htaccess Information Leak**

    Source raised by an active scanner (.htaccess Information Leak)
    CWE ID 94
    WASC ID 14
    Reference
    1. http://www.htaccess-guide.com/

5. **Absence of Anti-CSRF Tokens**

    Source raised by a passive scanner (Absence of Anti-CSRF Tokens)
    CWE ID 352
    WASC ID 9
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
    2. http://projects.webappsec.org/Cross-Site-Request-Forgery
    3. http://cwe.mitre.org/data/definitions/352.html

6. **Content Security Policy (CSP) Header Not Set**

    Source raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
    CWE ID 693
    WASC ID 15
    Reference
    1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
    2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
    3. http://www.w3.org/TR/CSP/
    4. http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
    5. http://www.html5rocks.com/en/tutorials/security/content-security-policy/
    6. http://caniuse.com/#feat=contentsecuritypolicy
    7. http://content-security-policy.com/

7. **Missing Anti-clickjacking Header**

    Source raised by a passive scanner (Anti-clickjacking Header)
    CWE ID 1021
    WASC ID 15
    Reference
    1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

8. **XSLT Injection**

    Source raised by an active scanner (XSLT Injection)
    CWE ID 91
    WASC ID 23
    Reference
    1. https://www.contextis.com/blog/xslt-server-side-injection-attacks

9. **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))
    CWE ID 200
    WASC ID 13
    Reference
    1. https://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
    2. http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

10. **Server Leaks Version Information via "Server" HTTP Response Header Field**

    Source raised by a passive scanner (HTTP Server Response Header)
    CWE ID 200
    WASC ID 13
    Reference
    1. https://httpd.apache.org/docs/current/mod/core.html#servertokens
    2. http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
    3. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
    4. http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

11. **X-Content-Type-Options Header Missing**

    Source raised by a passive scanner (X-Content-Type-Options Header Missing)
    CWE ID 693
    WASC ID 15
    Reference
    1. https://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
    2. https://owasp.org/www-community/Security_Headers

12. **Charset Mismatch (Header Versus Meta Content-Type Charset)**

    Source raised by a passive scanner (Charset Mismatch)
    CWE ID 436
    WASC ID 15
    Reference
    1. http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

13. **GET for POST**

    Source raised by an active scanner (GET for POST)
    CWE ID 16
    WASC ID 20

14. **Information Disclosure - Suspicious Comments**

    Source raised by a passive scanner (Information Disclosure - Suspicious Comments)
    CWE ID 200
    WASC ID 13

15. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)

16. **User Agent Fuzzer**

    Source raised by an active scanner (User Agent Fuzzer)
    Reference
    1. https://owasp.org/wstg

17. **User Controllable HTML Element Attribute (Potential XSS)**

    Source raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
    CWE ID 20
    WASC ID 20
    Reference
    1. http://websecurityinfo.codeplex.com/wikipage?title=Checkpoint-controlled-html-attribute