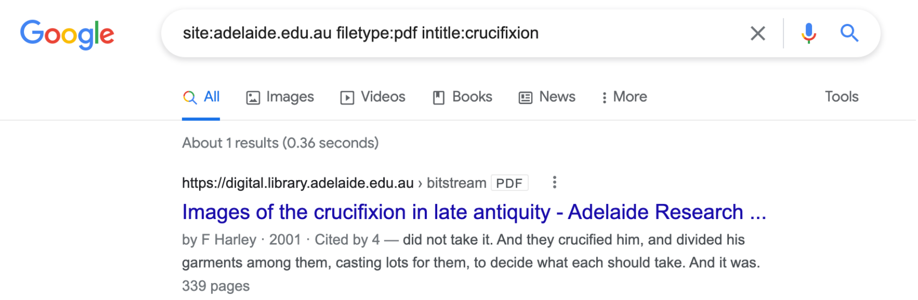
Assignment 0x02

Question 1

(a) Google Search syntax: **site:adelaide.edu.au filetype:pdf intitle:crucifixion**



site:adelaide.edu.au filetype:pdf intitle:crucifixion

About 1 results (0.36 seconds)

https://digital.library.adelaide.edu.au › bitstream PDF

Images of the crucifixion in late antiquity - Adelaide Research ...

by F Harley · 2001 · Cited by 4 — did not take it. And they crucified him, and divided his garments among them, casting lots for them, to decide what each should take. And it was.

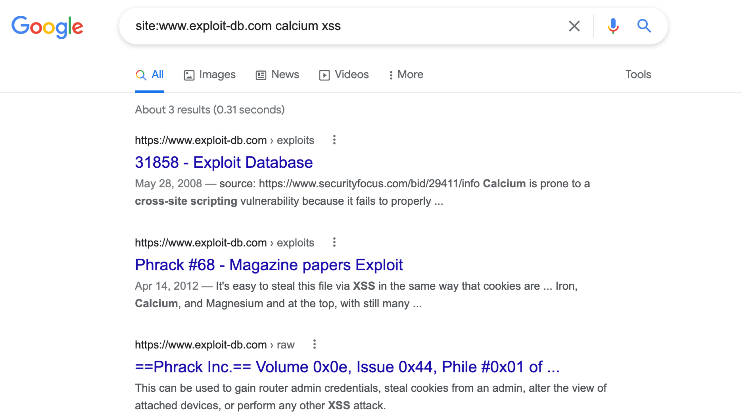
339 pages

(b) The author is **F Harley**

Question 2

Exploit-db is a good hack database (https://www.exploit-db.com/)

Search using: site:www.exploit-db.com calcium xss



site:www.exploit-db.com calcium xss

About 3 results (0.31 seconds)

https://www.exploit-db.com › exploits

31858 - Exploit Database

May 28, 2008 — source: https://www.securityfocus.com/bid/29411/info **Calcium** is prone to a **cross-site scripting** vulnerability because it fails to properly ...

https://www.exploit-db.com › exploits

Phrack #68 - Magazine papers Exploit

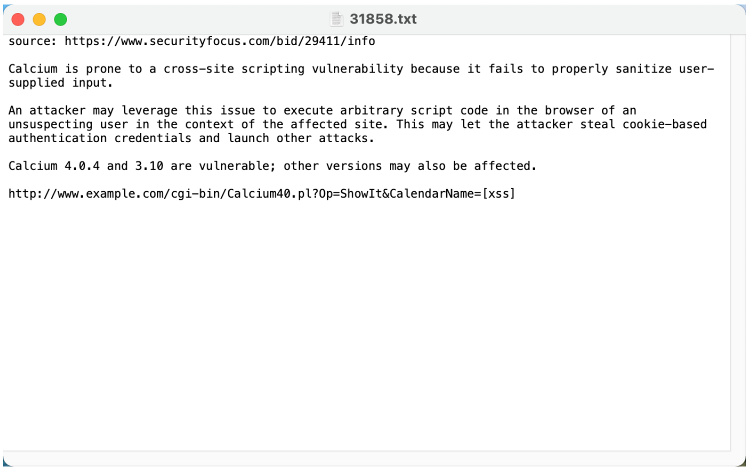
Apr 14, 2012 — It's easy to steal this file via **XSS** in the same way that cookies are ... Iron, **Calcium**, and Magnesium and at the top, with still many ...

https://www.exploit-db.com › raw

==Phrack Inc.== Volume 0x0e, Issue 0x44, Phile #0x01 of ...

This can be used to gain router admin credentials, steal cookies from an admin, alter the view of attached devices, or perform any other **XSS** attack.

And the content:

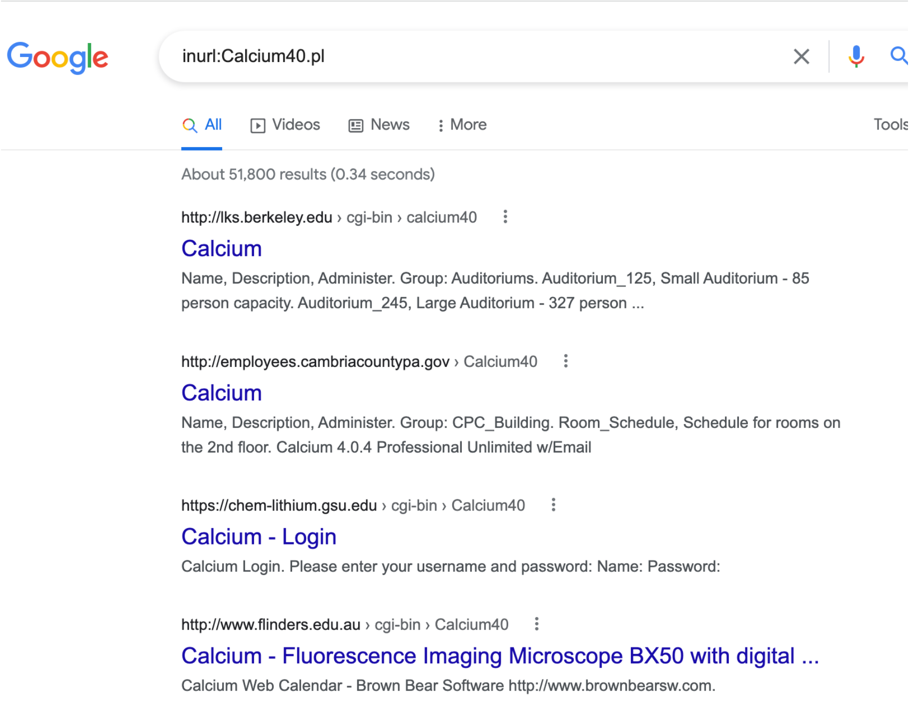


```
source: https://www.securityfocus.com/bid/29411/info

Calcium is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-
supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an
unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based
authentication credentials and launch other attacks.

Calcium 4.0.4 and 3.10 are vulnerable; other versions may also be affected.

http://www.example.com/cgi-bin/Calcium40.pl?Op=ShowIt&CalendarName=[xss]
```

Pay attention to:

http://www.example.com/cgi-bin/Calcium40.pl?Op=ShowIt&CalendarName=[xss]

Search the URL which contains key word:



inurl:Calcium40.pl

About 51,800 results (0.34 seconds)

http://lks.berkeley.edu › cgi-bin › calcium40

Calcium

Name, Description, Administer. Group: Auditoriums. Auditorium_125, Small Auditorium - 85 person capacity. Auditorium_245, Large Auditorium - 327 person ...

http://employees.cambriacountypa.gov › Calcium40

Calcium

Name, Description, Administer. Group: CPC_Building. Room_Schedule, Schedule for rooms on the 2nd floor. Calcium 4.0.4 Professional Unlimited w/Email

https://chem-lithium.gsu.edu › cgi-bin › Calcium40

Calcium - Login

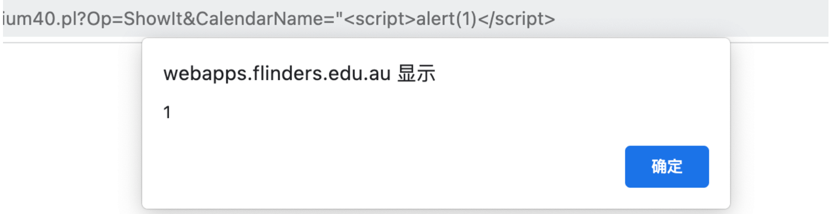
Calcium Login. Please enter your username and password: Name: Password:

http://www.flinders.edu.au › cgi-bin › Calcium40

Calcium - Fluorescence Imaging Microscope BX50 with digital ...

Calcium Web Calendar - Brown Bear Software http://www.brownbearsw.com.

Test one of them: We could configurate specific js script to make it able to run, such as https://webapps.flinders.edu.au/cgi-bin/Calcium40.pl?Op=ShowIt&CalendarName="<script>alert(1)</script>



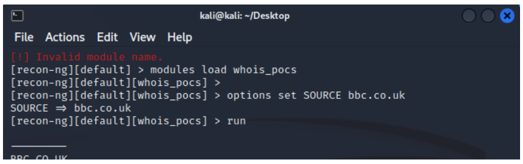
ium40.pl?Op=ShowIt&CalendarName="<script>alert(1)</script>

webapps.flinders.edu.au 显示

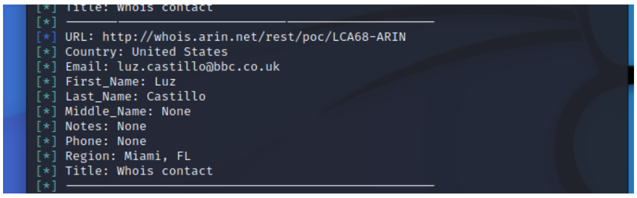
1

Question 3

Install tools: **marketplace install whois_pocs**



```
[!] Invalid module name.
[recon-ng][default] > modules load whois_pocs
[recon-ng][default][whois_pocs] >
[recon-ng][default][whois_pocs] > options set SOURCE bbc.co.uk
SOURCE ⇒ bbc.co.uk
[recon-ng][default][whois_pocs] > run

---------
BBC.CO.UK
```

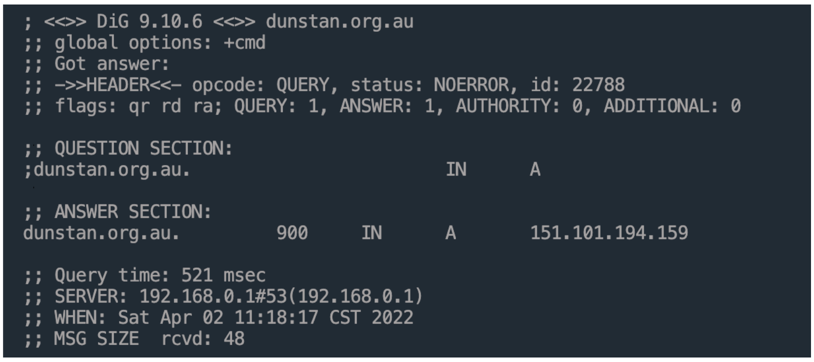


```
[*] Title: Whois contact
[*] ------------------------------------------------------------
[*] URL: http://whois.arin.net/rest/poc/LCA68-ARIN
[*] Country: United States
[*] Email: luz.castillo@bbc.co.uk
[*] First_Name: Luz
[*] Last_Name: Castillo
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Miami, FL
[*] Title: Whois contact
[*] ------------------------------------------------------------
```

The name is **Luz Castillo**

Question 4

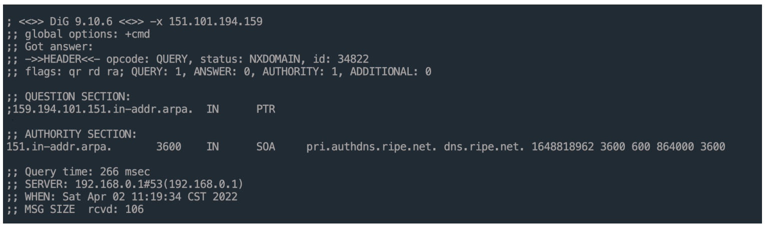
(1) Using **dig dunstan.org.au**



```
; <<>> DiG 9.10.6 <<>> dunstan.org.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22788
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dunstan.org.au.                        IN      A

;; ANSWER SECTION:
dunstan.org.au.         900     IN      A       151.101.194.159

;; Query time: 521 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Apr 02 11:18:17 CST 2022
;; MSG SIZE  rcvd: 48
```

The IP address is 151.101.194.159

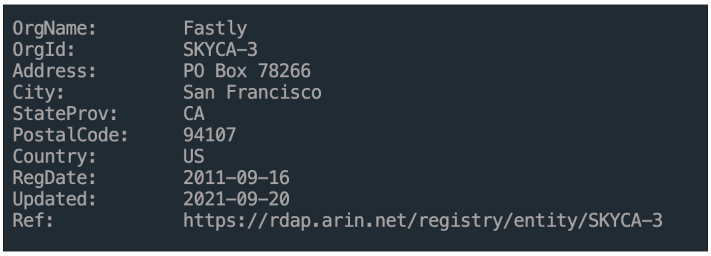
(2) Using **dig -x 151.101.194.159**



```
; <<>> DiG 9.10.6 <<>> -x 151.101.194.159
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 34822
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;159.194.101.151.in-addr.arpa.  IN      PTR

;; AUTHORITY SECTION:
151.in-addr.arpa.       3600    IN      SOA     pri.authdns.ripe.net. dns.ripe.net. 1648818962 3600 600 864000 3600

;; Query time: 266 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Apr 02 11:19:34 CST 2022
;; MSG SIZE  rcvd: 106
```

Domain names: pri.authdns.ripe.net. dns.ripe.net.

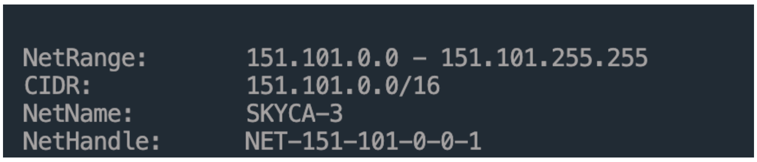
(3) Using **whois 151.101.194.159**



```
OrgName:        Fastly
OrgId:          SKYCA-3
Address:        PO Box 78266
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2011-09-16
Updated:        2021-09-20
Ref:            https://rdap.arin.net/registry/entity/SKYCA-3
```

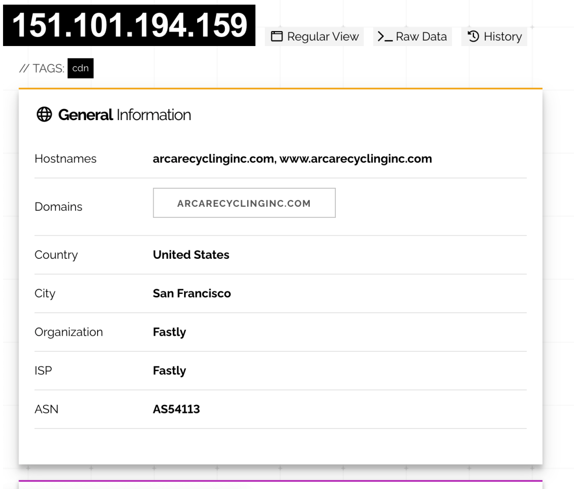
The owner is **Fastly**

(4) The IP range is **151.101.0.0 - 151.101.255.255**



```
NetRange:       151.101.0.0 - 151.101.255.255
CIDR:           151.101.0.0/16
NetName:        SKYCA-3
NetHandle:      NET-151-101-0-0-1
```

(5) The ASN number is **54113**



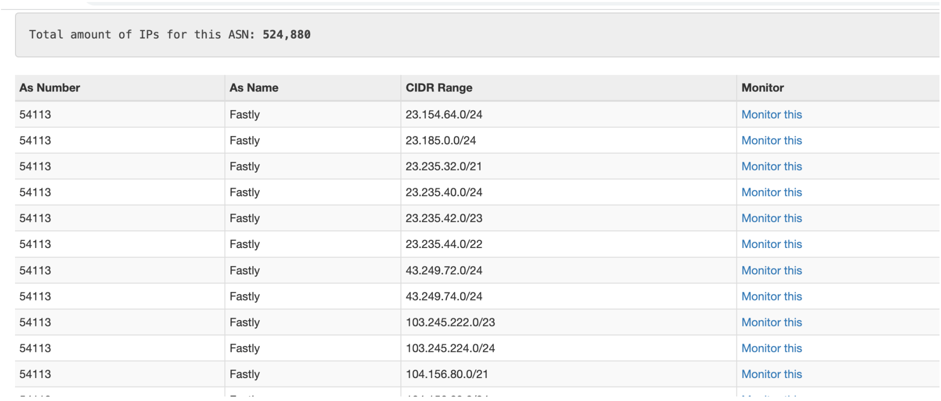
151.101.194.159

// TAGS: cdn

General Information

Hostnames	arcarecyclinginc.com, www.arcarecyclinginc.com
Domains	ARCARECYCLINGINC.COM
Country	United States
City	San Francisco
Organization	Fastly
ISP	Fastly
ASN	AS54113

(6) Using online tools: https://mxtoolbox.com/SuperTool.aspx

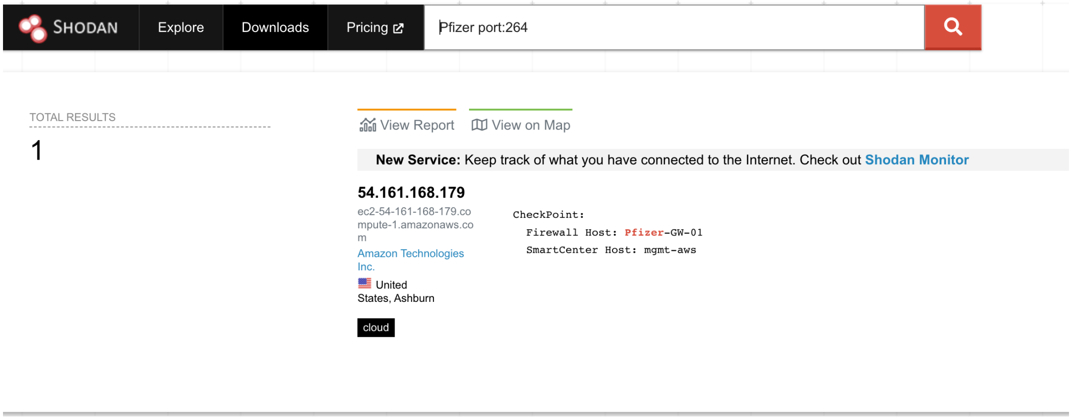


```
Total amount of IPs for this ASN: 524,880
```

As Number	As Name	CIDR Range	Monitor
54113	Fastly	23.154.64.0/24	Monitor this
54113	Fastly	23.185.0.0/24	Monitor this
54113	Fastly	23.235.32.0/21	Monitor this
54113	Fastly	23.235.40.0/24	Monitor this
54113	Fastly	23.235.42.0/23	Monitor this
54113	Fastly	23.235.44.0/22	Monitor this
54113	Fastly	43.249.72.0/24	Monitor this
54113	Fastly	43.249.74.0/24	Monitor this
54113	Fastly	103.245.222.0/23	Monitor this
54113	Fastly	103.245.224.0/24	Monitor this
54113	Fastly	104.156.80.0/21	Monitor this

Question 5

(1)



Pfizer port:264

TOTAL RESULTS

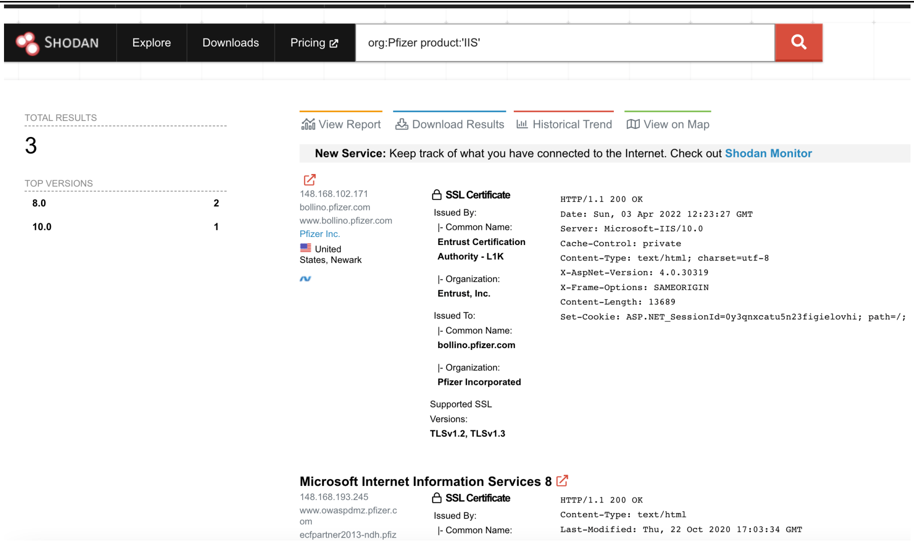
1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

54.161.168.179
ec2-54-161-168-179.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn

```
CheckPoint:
  Firewall Host: Pfizer-GW-01
  SmartCenter Host: mgmt-aws
```

(2) org:Pfizer product:'IIS'



org:Pfizer product:'IIS'

TOTAL RESULTS

3

TOP VERSIONS

8.0	2
10.0	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

148.168.102.171
bollino.pfizer.com
www.bollino.pfizer.com
Pfizer Inc.
United States, Newark

SSL Certificate
Issued By:
|- Common Name:
Entrust Certification Authority - L1K
|- Organization:
Entrust, Inc.
Issued To:
|- Common Name:
bollino.pfizer.com
|- Organization:
Pfizer Incorporated
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Sun, 03 Apr 2022 12:23:27 GMT
Server: Microsoft-IIS/10.0
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-AspNet-Version: 4.0.30319
X-Frame-Options: SAMEORIGIN
Content-Length: 13689
Set-Cookie: ASP.NET_SessionId=0y3qnxcatu5n23figielovhi; path=/;
```

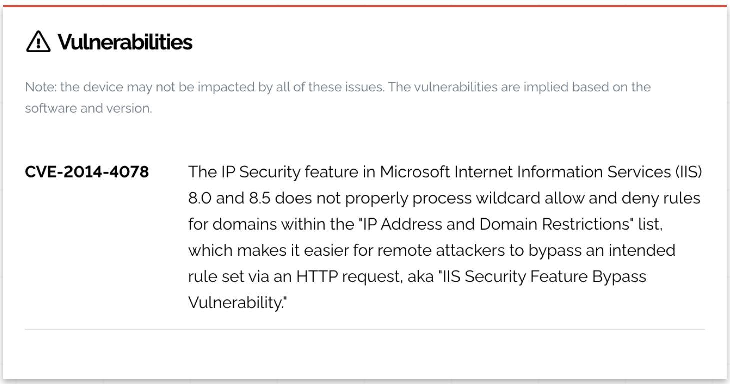
Microsoft Internet Information Services 8
148.168.193.245
www.owaspdmz.pfizer.com
ecfpartner2013-ndh.pfiz

SSL Certificate
Issued By:
|- Common Name:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 22 Oct 2020 17:03:34 GMT
```

We see 8.0 and 10.0

(3) CVE-2014-4078

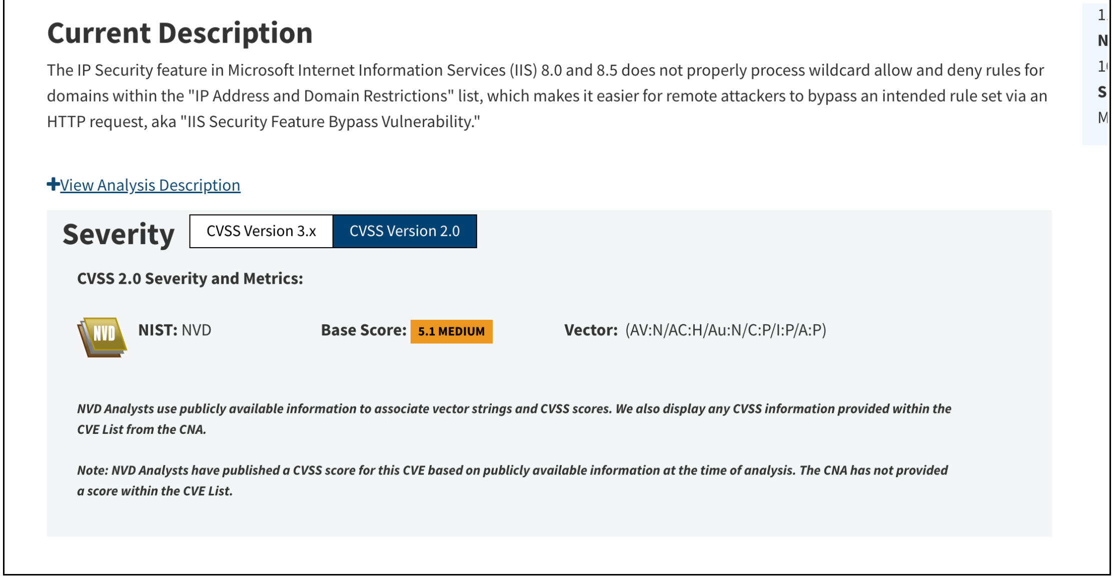


Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-4078 The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

(4) (AV:N/AC:H/Au:N/C:P/I:P/A:P)



Current Description

The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

+View Analysis Description

Severity

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 5.1 MEDIUM **Vector:** (AV:N/AC:H/Au:N/C:P/I:P/A:P)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

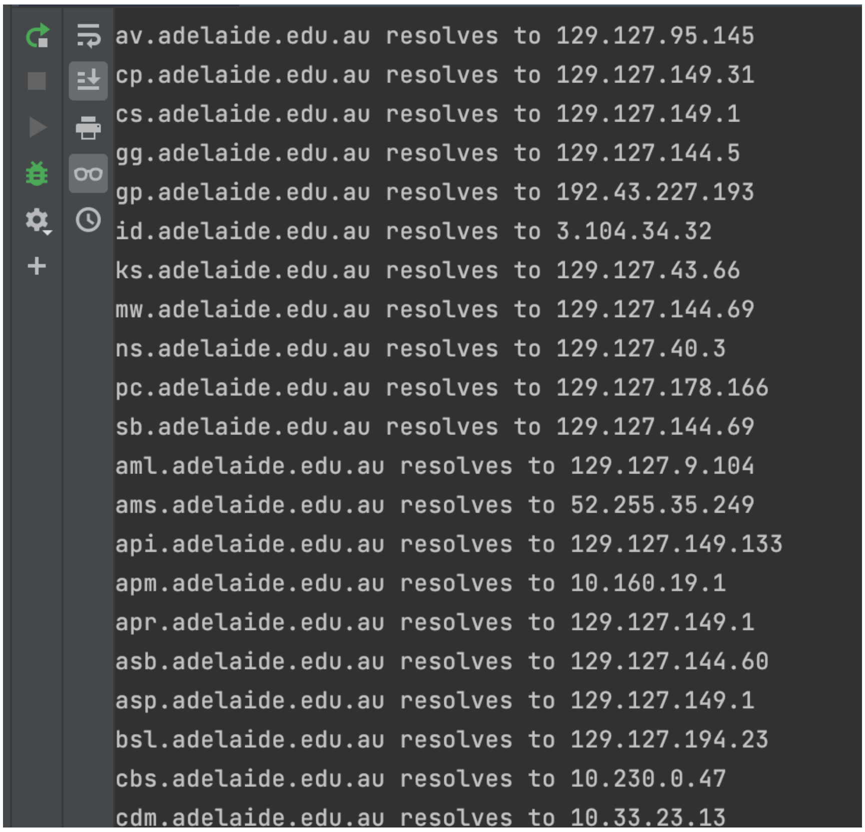
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Question 6

The python code for this question:

```
import sys, socket
socket.setdefaulttimeout(0.1)
base = "adelaide.edu.au"
with open("dnsmap.txt") as f:
    for line in f:
        try:
            host = line.strip()+"."+base
            ip = socket.gethostbyname(host)
            print(f"{host} resolves to {ip}")
        except:
            pass
```

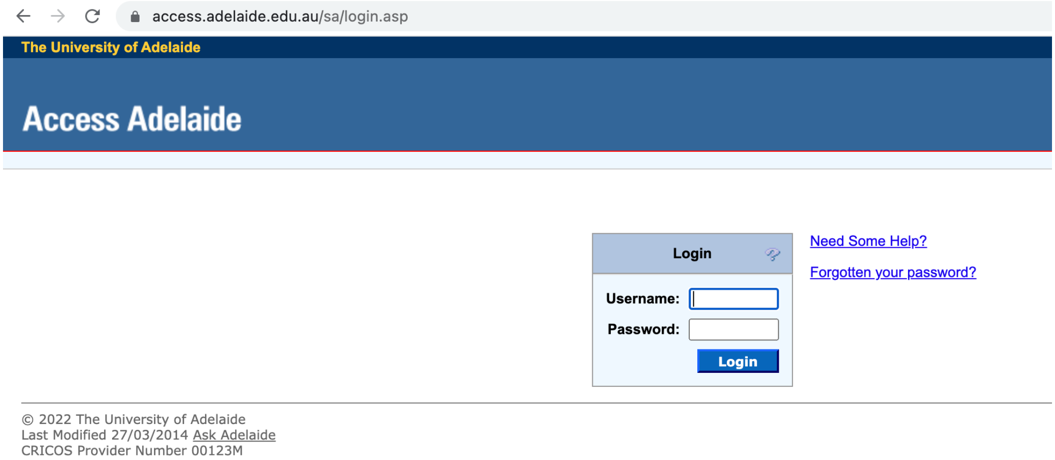
The result:



```
av.adelaide.edu.au resolves to 129.127.95.145
cp.adelaide.edu.au resolves to 129.127.149.31
cs.adelaide.edu.au resolves to 129.127.149.1
gg.adelaide.edu.au resolves to 129.127.144.5
gp.adelaide.edu.au resolves to 192.43.227.193
id.adelaide.edu.au resolves to 3.104.34.32
ks.adelaide.edu.au resolves to 129.127.43.66
mw.adelaide.edu.au resolves to 129.127.144.69
ns.adelaide.edu.au resolves to 129.127.40.3
pc.adelaide.edu.au resolves to 129.127.178.166
sb.adelaide.edu.au resolves to 129.127.144.69
aml.adelaide.edu.au resolves to 129.127.9.104
ams.adelaide.edu.au resolves to 52.255.35.249
api.adelaide.edu.au resolves to 129.127.149.133
apm.adelaide.edu.au resolves to 10.160.19.1
apr.adelaide.edu.au resolves to 129.127.149.1
asb.adelaide.edu.au resolves to 129.127.144.60
asp.adelaide.edu.au resolves to 129.127.149.1
bsl.adelaide.edu.au resolves to 129.127.194.23
cbs.adelaide.edu.au resolves to 10.230.0.47
cdm.adelaide.edu.au resolves to 10.33.23.13
```

Question 7

Now:



access.adelaide.edu.au/sa/login.asp

The University of Adelaide

Access Adelaide

Login

Username:

Password:

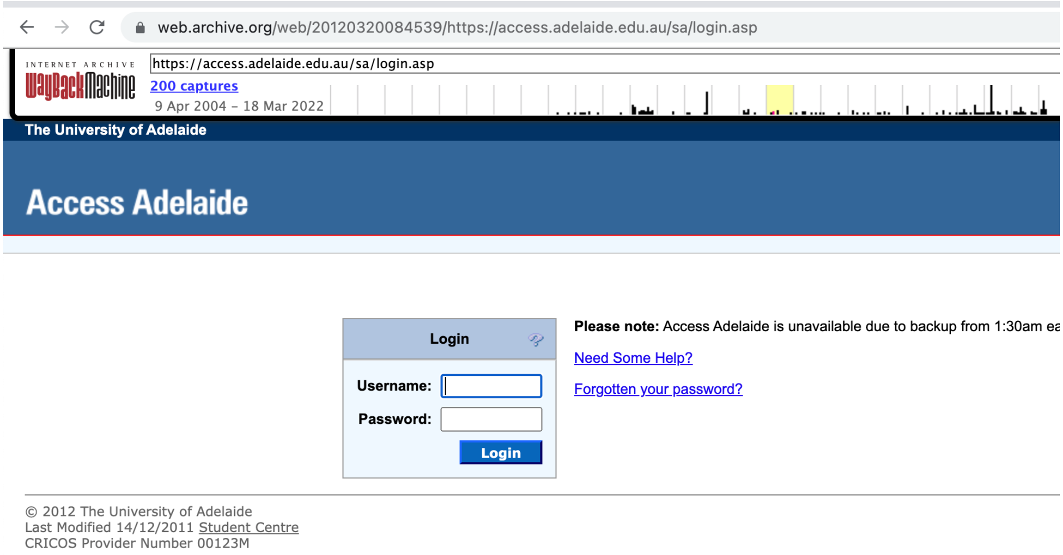
Login

Need Some Help?

Forgotten your password?

© 2022 The University of Adelaide
Last Modified 27/03/2014 Ask Adelaide
CRICOS Provider Number 00123M

10 years ago:



web.archive.org/web/20120320084539/https://access.adelaide.edu.au/sa/login.asp

INTERNET ARCHIVE WaybackMachine

https://access.adelaide.edu.au/sa/login.asp

200 captures

9 Apr 2004 – 18 Mar 2022

The University of Adelaide

Access Adelaide

Login

Username:

Password:

Login

Please note: Access Adelaide is unavailable due to backup from 1:30am ea

Need Some Help?

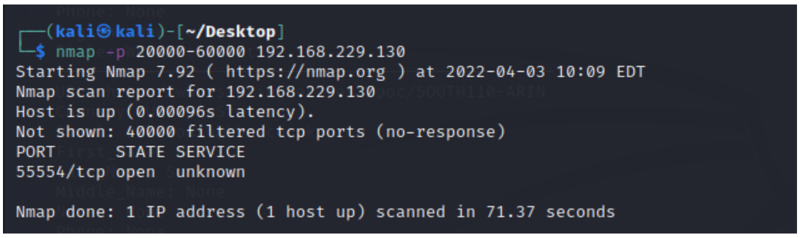
Forgotten your password?

© 2012 The University of Adelaide
Last Modified 14/12/2011 Student Centre
CRICOS Provider Number 00123M

We can find that Access Adelaide has really not changed much in the last 10 years.

Question 8

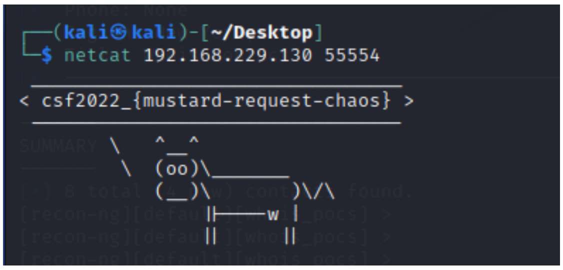
Using nmap scan the port of HackLab-VM: nmap -p 20000-60000 192.168.229.130



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 20000-60000 192.168.229.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-03 10:09 EDT
Nmap scan report for 192.168.229.130
Host is up (0.00096s latency).
Not shown: 40000 filtered tcp ports (no-response)
PORT      STATE SERVICE
55554/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 71.37 seconds
```

We could find that the port 55554 is opened.

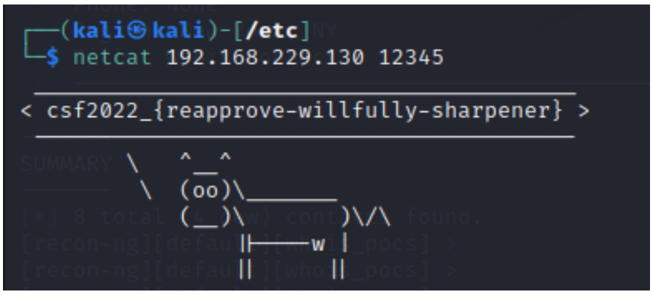
Then using netcat to find information: netcat 192.168.229.130 55554



```
┌──(kali㉿kali)-[~/Desktop]
└─$ netcat 192.168.229.130 55554
 ________________________________
< csf2022_{mustard-request-chaos} >
 --------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Question 9

netcat 192.168.229.130 12345



```
┌──(kali㉿kali)-[/etc]
└─$ netcat 192.168.229.130 12345
 _________________________________________
< csf2022_{reapprove-willfully-sharpener} >
 -----------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```