

Sri Lanka Institute of Information Technology



Assignment report 09

IT22357762

Web Security -IE2062

Web Security – IE2062

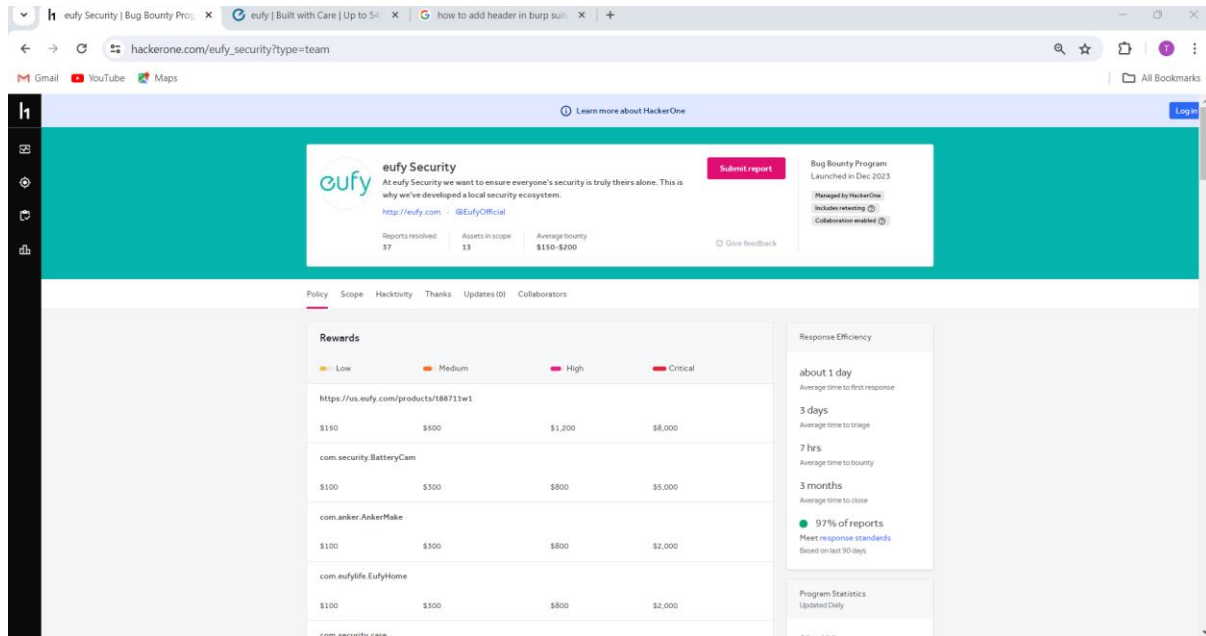
B.Sc. (Hons) in Information

Contents

| | | |
|-------|----------------------------|----|
| 1 | Eufy Security | 3 |
| 1.1 | Sub- domain list | 3 |
| 1.2 | Firewall detection | 5 |
| 1.3 | IP scanning | 5 |
| 1.4 | Port scanning | 6 |
| 1.5 | Nikto scanning | 7 |
| 1.6 | Burpsuite scanning | 9 |
| 1.7 | Netspaker scan | 10 |
| 1.8 | Vulnerabilities..... | 10 |
| 1.8.1 | Other vulnerabilities..... | 11 |

1 Eufy Security

A website where can be bought CCTV and security stuffs increasing security by providing local security system.



1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d eufy.com

```
a (tharu@kali)-[~]
└─$ amass enum -passive -d eufy.com
order.us.eufy.com
passport.eufy.com
beta.multipass.eufy.com
beta.community.security.eufy.com
beta.passport.eufy.com
beta.eufy.com
order.eu.eufy.com
au.eufy.com
cn.eufy.com
security.eufy.com
de.eufy.com
order.es.eufy.com
uk.eufy.com
multipass.eufy.com
order.uk.eufy.com
beta.community.eufy.com
shop.eufy.com
eufy.com
order.nl.eufy.com
us.eufy.com
ca.eufy.com
nl.eufy.com
www.eufy.com
support.eufy.com
preview.eufy.com
sgtm.eufy.com
community.security.eufy.com
preview.passport.eufy.com
order.fr.eufy.com
order.it.eufy.com
blog.eufy.com
community.eufy.com
es.eufy.com
order.de.eufy.com
fr.eufy.com
eu.eufy.com
it.eufy.com
order.ca.eufy.com

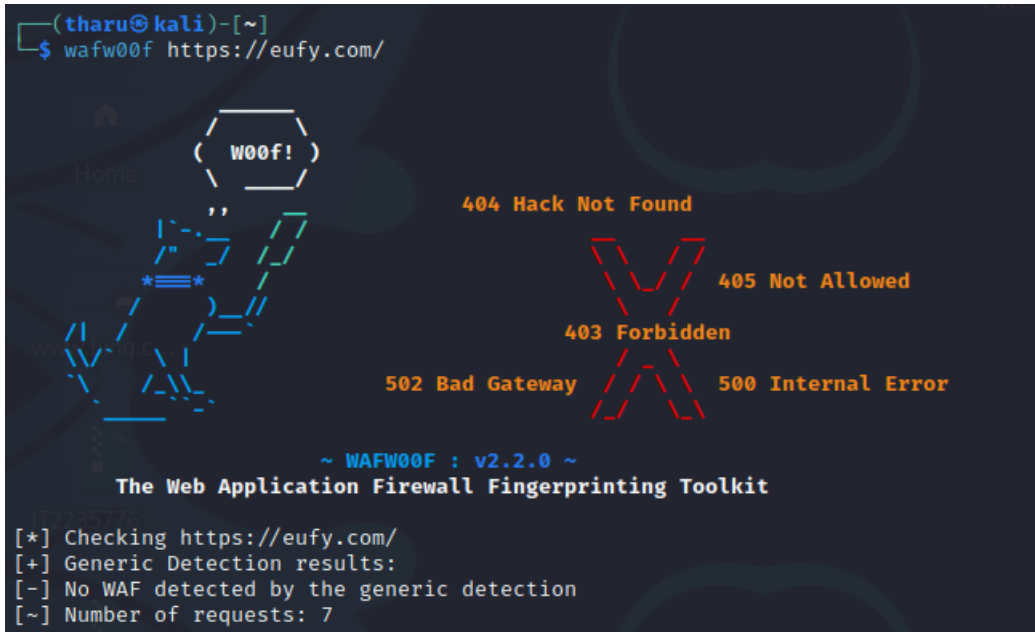
The enumeration has finished
Discoveries are being migrated into the local database
```

Sub domain list –

- order.us.eufy.com
- passport.eufy.com
- beta.multipass.eufy.com
- beta.community.security.eufy.com
- beta.passport.eufy.com
- beta.eufy.com
- order.eu.eufy.com
- au.eufy.com
- cn.eufy.com
- security.eufy.com
- de.eufy.com
- order.es.eufy.com
- uk.eufy.com
- multipass.eufy.com
- order.uk.eufy.com
- beta.community.eufy.com
- shop.eufy.com
- eufy.com
- order.nl.eufy.com
- us.eufy.com
- ca.eufy.com
- nl.eufy.com
- www.eufy.com
- support.eufy.com
- preview.eufy.com
- sgtm.eufy.com
- community.security.eufy.com
- preview.passport.eufy.com
- order.fr.eufy.com
- order.it.eufy.com
- blog.eufy.com
- community.eufy.com
- es.eufy.com
- order.de.eufy.com
- fr.eufy.com
- eu.eufy.com
- it.eufy.com
- order.ca.eufy.com

1.2 Firewall detection

Command – wafw00f https://eufy.com /



```
(tharu@kali)-[~]
$ wafw00f https://eufy.com/

Home (W00f!)

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

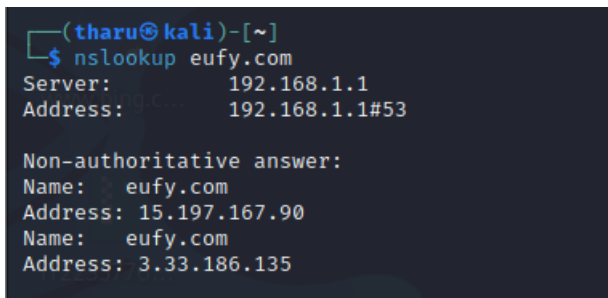
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://eufy.com/
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

1.3 IP scanning

Tool – nslookup

Command – nslookup eufy.com



```
(tharu@kali)-[~]
$ nslookup eufy.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   eufy.com
Address: 15.197.167.90
Name:   eufy.com
Address: 3.33.186.135
```

1.4 Port scanning

Tool - nmap

Command – nmap -sV -sC -Pn 15.197.167.90 -A

```
(tharu@kali)-[~]
└─$ nmap -sV -sC -Pn 15.197.167.90 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-17 00:57 +0530
Nmap scan report for afa7f374f51cc8991.awsglobalaccelerator.com (15.197.167.90)
Host is up (0.044s latency).
Not shown: 907 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http         Netlify
|_fingerprint-strings:
|_  DNSVersionBindReqTCP, GenericLines, Help, RPCCheck, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_  HTTP/1.1 400 Bad Request
|_  Content-Type: text/plain; charset=utf-8
|_  Connection: close
|_  Request
|_  FourOhFourRequest:
|_  HTTP/1.0 400 Bad Request
|_  Date: Tue, 16 Apr 2024 19:28:14 GMT
|_  Server: Netlify
|_  X-Nf-Request-Id: 01HVM6365K5PN915QAS99H8THQ
|_  Content-Length: 0
|_  GetRequest:
|_  HTTP/1.0 400 Bad Request
|_  Date: Tue, 16 Apr 2024 19:28:07 GMT
|_  Server: Netlify
|_  X-Nf-Request-Id: 01HVM6302C0QHVVX8WS5X42HQ6
|_  Content-Length: 0
|_  HTTPOptions:
|_  HTTP/1.0 400 Bad Request
|_  Date: Tue, 16 Apr 2024 19:28:08 GMT
|_  Server: Netlify
|_  X-Nf-Request-Id: 01HVM6302C0QHVVX8WS5X42HQ6
|_  Content-Length: 0
|_  _http-server-header: Netlify
|_  _http-title: Site doesn't have a title (text/plain; charset=utf-8).
443/tcp    open  ssl/https    Netlify
|_fingerprint-strings:
|_  FourOhFourRequest:
|_  HTTP/1.0 400 Bad Request
|_  Date: Tue, 16 Apr 2024 19:28:15 GMT
|_  Server: Netlify
|_  X-Nf-Request-Id: 01HVM637SSH8S0ZDMNABKE674F
|_  Content-Length: 0
|_  GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_  HTTP/1.1 400 Bad Request
|_  Content-Type: text/plain; charset=utf-8
|_  Connection: close
Request
Connection: close
GetRequest:
HTTP/1.0 400 Bad Request
Date: Tue, 16 Apr 2024 19:28:14 GMT
Server: Netlify
X-Nf-Request-Id: 01HVM6365NJT7DPMSMJVWF5E
Content-Length: 0
HTTPOptions:
HTTP/1.0 400 Bad Request
Date: Tue, 16 Apr 2024 19:28:14 GMT
Server: Netlify
X-Nf-Request-Id: 01HVM6370HYTFREYDY3RZRN9V
Content-Length: 0
ssl-cert: Subject: commonName=*.netlify.app/organizationName=Netlify, Inc/stateOrProvinceName=California/countryName=US
Subject Alternative Name: DNS:*.netlify.app, DNS:netlify.app
Not valid before: 2024-01-15T00:00:00
Not valid after: 2025-02-14T23:59:59
_http-title: Site doesn't have a title (text/plain; charset=utf-8).
_http-server-header: Netlify
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
--NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)--
SF:Port80-TCP:V=7.93xT=780-4/17xTime=66IED145XP-x86_64-pc-linux-gnuXr(GetR
SF:quest,92,"HTTP/1.0x20400x20Badx20Request\r\nDate:x20Tue,x2016x2
SF:0Aprx202024x2019:28:07x20GMT\r\nServer:x20Netlify\r\nX-Nf-Request-I
SF:d:x2001HVM6302C0QHVVX8WS5X42HQ6\r\nContent-Length:x200\r\n\r\n")Xr(HT
SF:TPOptions,92,"HTTP/1.0x20400x20Badx20Request\r\nDate:x20Tue,x2016
SF:20Aprx202024x2019:28:08x20GMT\r\nServer:x20Netlify\r\nX-Nf-Request-Id:x2001HVM6302C0QHVVX8WS5X42HQ6\r\nContent-Length:x200\r\n\r\n")Xr
SF:(RTSPRequest,67,"HTTP/1.1x20400x20Badx20Request\r\nContent-Type:x2
SF:0text/plain;x20charset=utf-8\r\nConnection:x20close\r\n\r\n400x20Bad
SF:x20Request")Xr(X11Probe,67,"HTTP/1.1x20400x20Badx20Request\r\nCont
SF:ent-Type:x20text/plain;x20charset=utf-8\r\nConnection:x20close\r\n\r
SF:n400x20Badx20Request")Xr(FourOhFourRequest,92,"HTTP/1.0x20400x20B
SF:adx20Request\r\nDate:x20Tue,x2016x20Aprx202024x2019:28:14x20GMT\r
SF:nServer:x20Netlify\r\nX-Nf-Request-Id:x2001HVM6365K5PN915QAS99H8THQ
SF:\r\nContent-Length:x200\r\n\r\n")Xr(GenericLines,67,"HTTP/1.1x20400
SF:x20Badx20Request\r\nContent-Type:x20text/plain;x20charset=utf-8\r\nC
SF:onnection:x20close\r\n\r\n400x20Badx20Request")Xr(RPCCheck,67,"HTTP
SF:/SF:1.1x20400x20Badx20Request\r\nContent-Type:x20text/plain;x20charse
SF:t=utf-8\r\nConnection:x20close\r\n\r\n400x20Badx20Request")Xr(DNSVer
SF:sionBindReqTCP,67,"HTTP/1.1x20400x20Badx20Request\r\nContent-Type:x
SF:20text/plain;x20charset=utf-8\r\nConnection:x20close\r\n\r\n400x20B
SF:adx20Request")Xr(Help,67,"HTTP/1.1x20400x20Badx20Request\r\nConten
SF:t-Type:x20text/plain;x20charset=utf-8\r\nConnection:x20close\r\n\r\n
SF:400x20Badx20Request")Xr(SSLSessionReq,67,"HTTP/1.1x20400x20Badx20
SF:Request\r\nContent-Type:x20text/plain;x20charset=utf-8\r\nConnection:
SF:x20close\r\n\r\n400x20Badx20Request")Xr(TerminalServerCookie,67,"HTT
SF:P/1.1x20400x20Badx20Request\r\nContent-Type:x20text/plain;x20char
SF:set=utf-8\r\nConnection:x20close\r\n\r\n400x20Badx20Request")Xr(TLS
SF:SessionReq,67,"HTTP/1.1x20400x20Badx20Request\r\nContent-Type:x20te
SF:xt/plain;x20charset=utf-8\r\nConnection:x20close\r\n\r\n400x20Badx2
```

```

SF:0Request");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.93%T=SSL%I=7%D=4/17%Time=661ED14C%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,92,"HTTP/1.0\x20400\x20Bad\x20Request\r\nDate:\x20Tue,\x
SF:2016\x20Apr\x202024\x2019:28:14\x20GMT\r\nServer:\x20Netlify\r\nX-Nf-Re
SF:quest-Id:\x2001HVM6365NJXT7DPSMJVWF5E\r\nContent-Length:\x200\r\n\r\n
SF:")%r(HTTPOptions,92,"HTTP/1.0\x20400\x20Bad\x20Request\r\nDate:\x20Tue
SF:,\x2016\x20Apr\x202024\x2019:28:14\x20GMT\r\nServer:\x20Netlify\r\nX-Nf
SF:-Request-Id:\x2001HVM6370HYTYFREYDY3RZRN9\r\nContent-Length:\x200\r\n\r\n
SF:")%r(FourOhFourRequest,92,"HTTP/1.0\x20400\x20Bad\x20Request\r\nDate:
SF:e:\x20Tue,\x2016\x20Apr\x202024\x2019:28:15\x20GMT\r\nServer:\x20Netlif
SF:y\r\nX-Nf-Request-Id:\x2001HVM637SSH8S0ZDMNABKE674F\r\nContent-Length:\x
SF:x200\r\n\r\n")%r(GenericLines,67,"HTTP/1.1\x20400\x20Bad\x20Request\r\
SF:nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\
SF:r\n\r\n400\x20Bad\x20Request")%r(RTSPRequest,67,"HTTP/1.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnec
SF:tion:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Help,67,"HTTP/1.1\x204
SF:00\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r
SF:nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(SSLSessionReq,6
SF:7,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x
SF:20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%
SF:r(TerminalServerCookie,67,"HTTP/1.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n
SF:400\x20Bad\x20Request")%r(TLSSessionReq,67,"HTTP/1.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n400\x20Bad\x20Request")%r(Kerberos,67,"HTTP/1.1\x2040
SF:0\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\
SF:nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(LPDString,67,"HT
SF:TP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(LDA
SF:SPSearchReq,67,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 246.01 seconds

```

1.5 Nikto scanning

Tool – Nikto

Command - sudo nikto -h eufy.com

```

root@kali:~# sudo nikto -h https://eufy.com/
[sudo] password for tharu:
- Nikto v2.5.0

+ Multiple IPs found: 3.33.186.135, 15.197.167.90
+ Target IP: 3.33.186.135
+ Target Hostname: eufy.com
+ Target Port: 443

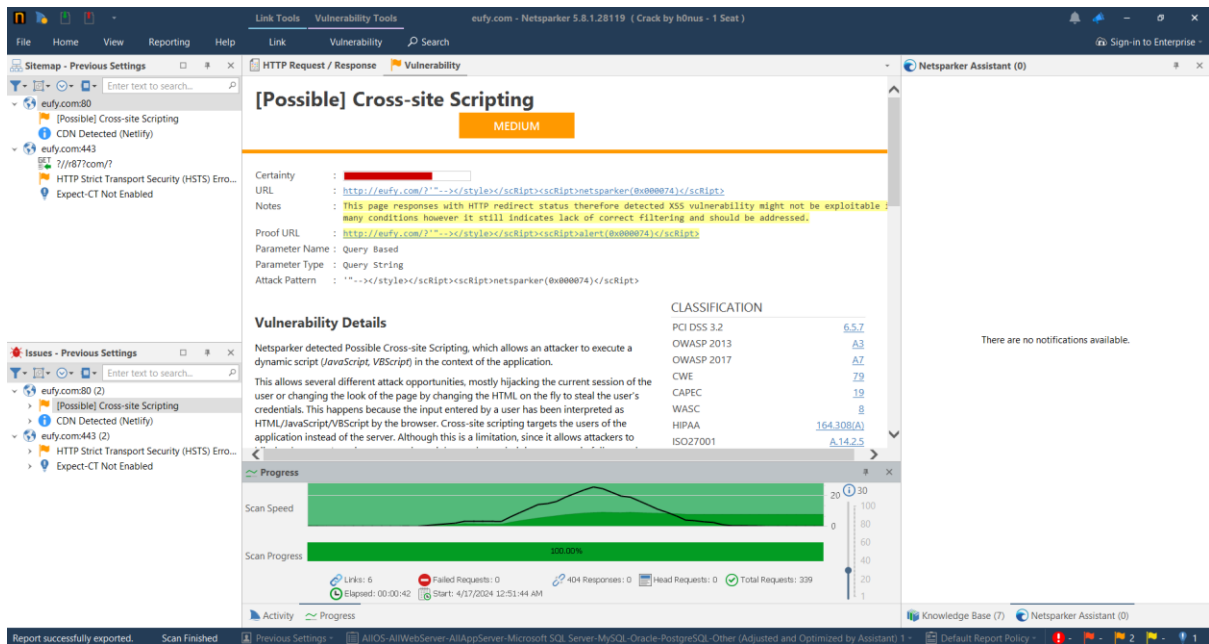
+ SSL Info: Subject: /CN=eufy.com
  Ciphers: TLS_AES_128_GCM_SHA256
  Issuers: C=US,O=Let's Encrypt,CN=R3
  Start Time: 2024-04-17 01:02:01 (GMT+5)

+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ Root page / redirects to: https://www.eufy.com/
+ No CGI Directories found (use -C all to force check all possible dirs)
+ /themes/mambosimple.php?detection-detected&siteName=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-120
4
+ /index.php?option=search&searchword=</script>alert(document.cookie)</script>: Mambo Site Server 4.0 build 10 is vulnerable to Cross Site Scripting (XSS).
+ /emailfriend/emailnews.php?id=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /emailfriend/emailfaq.php?id=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /emailfriend/emailarticle.php?id=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/upload.php?newBanner=1&choice=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).
+ /administrator/guest/functions/index.php?type=web&link=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/gallery/view.php?path=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/gallery/uploadimage.php?directory=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/gallery/navigation.php?directory=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/gallery/gallery.php?directory=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /index.php?dir=</script>alert('Vulnerable')</script>: Auto Directory Index 1.2.3 and prior are vulnerable to XSS attacks. See: https://vulners.com/osvdb/OSVDB-2820
+ https://adminer/01/index/</script>alert(document.cookie)</script>: Sun ONE Web Server 6.3 administration control is vulnerable to XSS attacks.
+ /clusterframe.jsp?cluster=</script>alert(document.cookie)</script>: Macromedia 300n 4.x JMC Interface, clusterframe.jsp file is vulnerable to a XSS attack. See: OSVDB-2876
+ /upload.php?Type=</script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS).
+ /userinfo.php?</script>alert('Vulnerable')</script>: The PHP script soinfo.php is vulnerable to Cross Site Scripting. Set expose_php - Off in php.ini. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1954
+ /servlets/MspPageAction-testMsg-</script>alert('Vulnerable')</script>: The NetDetector 3.0 and below are vulnerable to Cross Site Scripting (XSS).
+ /servlets/MspPageAction-balloingmsg-</script>alert('Vulnerable')</script>: The NetDetector install is vulnerable to Cross Site Scripting (XSS) in its invalid login message.
+ /admin/chk.asp?frames.aspx?file=Conf%20for%20386%20486%20register%20Web%20Mail%20MasterSettings%20Web_LogSettings.aspx?tab=TabWebServer&tab2=TabWebLogSettings&tab3=TabPageKey=5742D5874845936A13CD05F39C632408&returnURL=</script>alert(doc
ument.cookie)</script>: IIS 6 on Windows 2000 is vulnerable to Cross Site Scripting (XSS) in certain error messages.
+ /SiteServer/KnowledgeDefault.aspx?</script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17665
+ /_ms_bin/formlogin.aspx?</script>alert('Vulnerable')</script>: Site Server is vulnerable to Cross Site Scripting. See: OSVDB-17666
+ /WebCalendar/week.php?eventinfo=</script>alert(document.cookie)</script>: WebCalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). See: OSVDB-3624
+ /user.php?topuserinfoName=</script>alert('hi')</script>: The PHP-Nuke installation is vulnerable to Cross Site Scripting (XSS). Update to versions above 5.3.1.

```


[illegible]

1.7 Netsparker scan



1.8 Vulnerabilities

Vulnerability Title: Potential Cross-Site Scripting (XSS) Vulnerability

Vulnerability Description: XSS flaws let hackers run any script inside the application, which can lead to a number of problems, including session hijacking, page manipulation, phishing attacks, and data theft.

Affected Components: The vulnerability is present in the application's handling of input parameters, specifically within the method parameter value.

Impact Assessment: Impact of vulnerability includes,

- Session hijacking
- Page manipulating
- Phishing attack
- Intercept sensitive data

Steps to Reproduce:

1. Access the URL: `http://eufy.com/?'"--></style></scRipt><scRipt>alert(0x000074)</scRipt>`
2. Observe the behavior of the application in response to the provided input.
3. Verify if the input is interpreted as active HTML, JavaScript, or VBScript by the browser

Proof of concept:

Request

```
GET /?"--></style></script><script>netsparker(0x000074)</script> HTTP/1.1
Host: eufy.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 52.5767 Total Bytes Received : 375 Body Length : 92 Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
Server: Netlify
X-Nf-Request-Id: 01HVM5R7QGSS0GSNVT4DVVC9A7
Content-Length: 92
Content-Type: text/plain; charset=utf-8
Location: https://eufy.com/"--></style></script><script>netsparker(0x000074)</script>
Date: Tue, 16 Apr 2024 19:22:15 GMT

Redirecting to https://eufy.com/"--></style></script><script>netsparker(0x000074)</script>
```

Proposed Mitigation or Fix:

- Implement proper input validation and output encoding to prevent interpretation of input as active HTML, JavaScript, or VBScript.
- Consider using well-structured whitelist libraries such as OWASP Reform or Microsoft Anti-Cross-site Scripting.
- Implement a robust Content Security Policy (CSP) to mitigate the impact of XSS vulnerabilities and prevent successful exploitation by attackers.
- Regularly review and update security measures to address emerging threats and vulnerabilities.

1.8.1 Other vulnerabilities

1. Expect-CT Not Enabled
2. CDN Detected (Netlify)
3. HSTS not properly implemented

