Security Assessment Report

Website to be assessed: https://buymenow.org.uk

Step 1: Literature search

The assessment team carried out a literature search on national vulnerabilities database, reputable software sites and research portals and identified the 10 most important potential vulnerabilities with e-commerce websites:

1. Broken authentication & session
2. SQL Injection
3. Cross-Site Scripting (XSS)
4. Cross-site Request Forgery (CSRF)
5. Bad bots and Distributed Denial of Service (DDoS)
6. Insecure direct object references
7. Sensitive data exposure
8. Insufficient transport layer protection
9. Unvalidated redirects and forwards
10. Online payment fraud

Website in question will be assessed against these vulnerabilities in the next steps.

Step 2: Scanning

a. Tools:

The following tools were used during the scanning process:

Tool	**Remarks**
Ping	To verify the connectivity to the remote host
Traceroute	To get detailed information about the route from the local machine to the remote host
MTR	To identify a possible package loss throughout the route
Dig	To get detailed information about various DNS records of the website, which includes IP address the domain name points to and MX record

Whois	To find out more about domain name registration
Whatweb	To find out more about the technologies used by the website

b. Scan Results

i. Ping:

```
iMac:~ [redacted]$ ping -c 4 buymenow.org.uk
PING buymenow.org.uk (68.66.247.187): 56 data bytes
64 bytes from 68.66.247.187: icmp_seq=0 ttl=45 time=49.303 ms
64 bytes from 68.66.247.187: icmp_seq=1 ttl=45 time=48.945 ms
64 bytes from 68.66.247.187: icmp_seq=2 ttl=45 time=48.974 ms
64 bytes from 68.66.247.187: icmp_seq=3 ttl=45 time=49.048 ms

--- buymenow.org.uk ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 48.945/49.067/49.303/0.141 ms
```

Interpretation: The remote host is available. No problems detected concerning connectivity to the remote host.

ii. **Traceroute:**

First scan:

```
iMac:~ [redacted]$ traceroute buymenow.org.uk
traceroute to buymenow.org.uk (68.66.247.187), 64 hops max, 52 byte packets
 1  modem (192.168.1.1)  1.060 ms  0.591 ms  0.362 ms
 2  10.57.0.1 (10.57.0.1)  10.728 ms  13.894 ms  11.768 ms
 3  10.36.7.110 (10.36.7.110)  5.002 ms  4.717 ms  4.725 ms
 4  172.16.194.32 (172.16.194.32)  4.605 ms *  5.027 ms
 5  172.16.209.82 (172.16.209.82)  4.409 ms  4.365 ms  3.988 ms
 6  172.16.209.33 (172.16.209.33)  4.583 ms  4.434 ms  4.455 ms
 7  172.16.194.133 (172.16.194.133)  6.840 ms  4.810 ms  4.902 ms
 8  * * *
 9  10.40.169.127 (10.40.169.127)  7.774 ms  12.953 ms
    10.40.168.61 (10.40.168.61)  7.509 ms
10  * * *
11  ae2.3203.edge1.budapest1.level3.net (4.69.143.122)  52.446 ms  40.109 ms  40.050 ms
12  arelion-level3-budapest1.level3.net (4.68.62.150)  41.750 ms  42.069 ms  41.377 ms
13  win-bb3-link.ip.twelve99.net (62.115.124.112)  48.835 ms
    win-bb4-link.ip.twelve99.net (62.115.124.110)  48.091 ms  48.533 ms
14  ffm-bb2-link.ip.twelve99.net (62.115.138.22)  42.105 ms  42.366 ms  41.973 ms
15  adm-bb4-link.ip.twelve99.net (62.115.122.200)  48.725 ms  48.150 ms  48.477 ms
16  adm-b10-link.ip.twelve99.net (62.115.120.227)  49.380 ms  48.673 ms  49.119 ms
17  a2hosting-svc080530-ic370345.ip.twelve99-cust.net (62.115.145.217)  47.675 ms  47.275 ms  47.050 ms
18  v401.nl1-c2-040101_0209-38.a2webhosting.com (209.124.94.237)  49.743 ms  49.671 ms  49.633 ms
19  68.66.247.187.static.a2webhosting.com (68.66.247.187)  48.887 ms  48.772 ms  48.873 ms
```

When traceroute scan was run with default parameters, there was no response from the hops #8 and #10. It is likely that these hops are behind a firewall that prevents

the hops from responding to the request. Therefore, a second scan was run with -e flag to evade the firewalls.

Second scan:

```
iMac:~ [redacted]$ traceroute -e buymenow.org.uk
traceroute to buymenow.org.uk (68.66.247.187), 64 hops max, 52 byte packets
 1  modem (192.168.1.1)  1.369 ms  0.617 ms  0.424 ms
 2  10.57.0.1 (10.57.0.1)  11.534 ms  10.812 ms  8.171 ms
 3  10.36.7.110 (10.36.7.110)  4.886 ms  4.947 ms  4.877 ms
 4  172.16.194.32 (172.16.194.32)  4.636 ms  4.507 ms *
 5  172.16.209.82 (172.16.209.82)  4.804 ms  4.352 ms  4.243 ms
 6  172.16.209.33 (172.16.209.33)  4.846 ms  4.693 ms *
 7  172.16.194.133 (172.16.194.133)  5.617 ms  5.370 ms  5.318 ms
 8  10.40.169.122 (10.40.169.122)  6.996 ms * *
 9  10.40.168.61 (10.40.168.61)  9.208 ms
    10.40.169.127 (10.40.169.127)  5.481 ms
    10.40.168.61 (10.40.168.61)  6.303 ms
10  * * *
11  ae2.3203.edge1.budapest1.level3.net (4.69.143.122)  40.569 ms  39.703 ms  39.696 ms
12  arelion-level3-budapest1.level3.net (4.68.62.150)  41.957 ms  41.291 ms  41.571 ms
13  win-bb4-link.ip.twelve99.net (62.115.124.110)  48.114 ms
    win-bb3-link.ip.twelve99.net (62.115.124.112)  49.001 ms
    win-bb4-link.ip.twelve99.net (62.115.124.110)  57.486 ms
14  ffm-bb1-link.ip.twelve99.net (62.115.137.202)  41.054 ms  41.290 ms
    ffm-bb2-link.ip.twelve99.net (62.115.138.22)  41.840 ms
15  adm-bb4-link.ip.twelve99.net (62.115.122.200)  48.726 ms
    adm-bb1-link.ip.twelve99.net (62.115.120.240)  49.263 ms  48.547 ms
16  adm-b10-link.ip.twelve99.net (62.115.120.227)  49.193 ms  49.544 ms  48.849 ms
17  a2hosting-svc080530-ic370345.ip.twelve99-cust.net (62.115.145.217)  47.236 ms  46.471 ms  46.704 ms
18  v401.nl1-c2-040101_0209-38.a2webhosting.com (209.124.94.237)  50.070 ms  49.532 ms  49.655 ms
19  68.66.247.187.static.a2webhosting.com (68.66.247.187)  49.922 ms  49.379 ms  48.984 ms
```

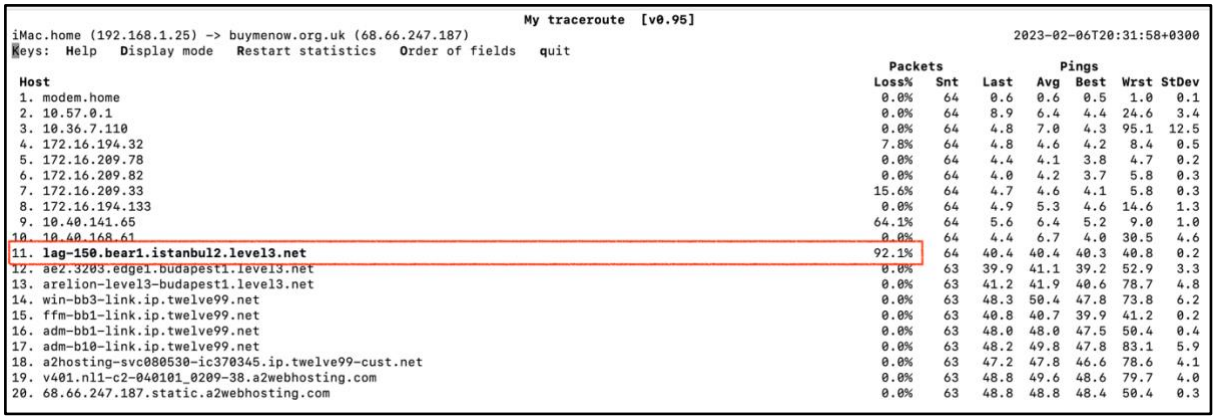
This time, hop #8 responds to the request, but hop #10 still doesn't. It is likely that there is another problem/configuration that prevents the hop from responding to the request. It might be due to a firewall that traceroute could not evade despite the -e flag or that the return signal somehow fails to reach the local machine.

Interpretation:

- It takes 19 hops from the local machine to the remote host.
- RTT increases dramatically after hop #10 which doesn't respond to the request, so it causes a delay.
- Hop #13 seems to have the highest RTT with approx. 57 ms but it has redundant switches which might return a RTT of 48-49 ms.

iii. **MTR:**

Since hop #10 cannot be identified, a MTR scan was conducted to identify the package loss throughout the route.



```
                                   My traceroute  [v0.95]
iMac.home (192.168.1.25) -> buymenow.org.uk (68.66.247.187)                2023-02-06T20:31:58+0300
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                Packets               Pings
 Host                                        Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. modem.home                               0.0%    64    0.6    0.6   0.5   1.0   0.1
 2. 10.57.0.1                                0.0%    64    8.9    6.4   4.4  24.6   3.4
 3. 10.36.7.110                              0.0%    64    4.8    7.0   4.3  95.1  12.5
 4. 172.16.194.32                            7.8%    64    4.8    4.6   4.2   8.4   0.5
 5. 172.16.209.78                            0.0%    64    4.4    4.1   3.8   4.7   0.2
 6. 172.16.209.82                            0.0%    64    4.0    4.2   3.7   5.8   0.3
 7. 172.16.209.33                            15.6%   64    4.7    4.6   4.1   5.8   0.3
 8. 172.16.194.133                           0.0%    64    4.9    5.3   4.6  14.6   1.3
 9. 10.40.141.65                             64.1%   64    5.6    6.4   5.2   9.0   1.0
10. 10.40.168.61                             0.0%    64    4.4    6.7   4.0  30.5   4.6
11. lag-150.bear1.istanbul2.level3.net       92.1%   64   40.4   40.4  40.3  40.8   0.2
12. ae2.3203.edge1.budapest1.level3.net      0.0%    63   39.9   41.1  39.2  52.9   3.3
13. arelion-level3-budapest1.level3.net      0.0%    63   41.2   41.9  40.6  78.7   4.8
14. win-bb3-link.ip.twelve99.net             0.0%    63   48.3   50.4  47.8  73.8   6.2
15. ffm-bb1-link.ip.twelve99.net             0.0%    63   40.8   40.7  39.9  41.2   0.2
16. adm-bb1-link.ip.twelve99.net             0.0%    63   48.0   48.0  47.5  50.4   0.4
17. adm-b10-link.ip.twelve99.net             0.0%    63   48.2   49.8  47.8  83.1   5.9
18. a2hosting-svc080530-ic370345.ip.twelve99-cust.net  0.0%  63  47.2  47.8  46.6  78.6  4.1
19. v401.nl1-c2-040101_0209-38.a2webhosting.com  0.0%  63   48.8   49.6  48.6  79.7   4.0
20. 68.66.247.187.static.a2webhosting.com    0.0%    63   48.8   48.8  48.4  50.4   0.3
```

Interpretation:

- Hop#10 in the traceroute scan results (#11 on the screenshot above) is identified successfully. Package loss is approx. 92%.
- However, since the packages go beyond this hop and the total package loss between the origin and the destination is 0%, this is not a problem.

iv. **Dig:**

When run with default parameters, dig scan produces this output:

```
bash-3.2# dig buymenow.org.uk

; <<>> DiG 9.18.11 <<>> buymenow.org.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38821
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;buymenow.org.uk.               IN      A

;; ANSWER SECTION:
buymenow.org.uk.        10738   IN      A       68.66.247.187

;; Query time: 3 msec
;; SERVER: fe80::1%6#53(fe80::1%6%6) (UDP)
;; WHEN: Mon Feb 06 20:54:19 +03 2023
;; MSG SIZE  rcvd: 60
```

So, **buymenow.org.uk domain name points to the IP address: 68.66.247.187**

In order to find out the MX record of the website, the dig scan was run with MX flag:

```
bash-3.2# dig buymenow.org.uk MX

; <<>> DiG 9.18.11 <<>> buymenow.org.uk MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25273
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;buymenow.org.uk.               IN      MX

;; ANSWER SECTION:
buymenow.org.uk.        14400   IN      MX      0 mail.buymenow.org.uk.

;; Query time: 86 msec
;; SERVER: fe80::1%6#53(fe80::1%6%6) (UDP)
;; WHEN: Mon Feb 06 20:58:30 +03 2023
;; MSG SIZE  rcvd: 65
```

It can be seen that **the MX record of the website is mail.buymenow.org.uk**

This time, another scan was carried out with ns flag to find out the nameservers of the website:

```
bash-3.2# dig ns buymenow.org.uk

; <<>> DiG 9.18.11 <<>> ns buymenow.org.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51611
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;buymenow.org.uk.               IN      NS

;; ANSWER SECTION:
buymenow.org.uk.        86307   IN      NS      ns4.a2hosting.com.
buymenow.org.uk.        86307   IN      NS      ns1.a2hosting.com.
buymenow.org.uk.        86307   IN      NS      ns2.a2hosting.com.
buymenow.org.uk.        86307   IN      NS      ns3.a2hosting.com.

;; Query time: 8 msec
;; SERVER: fe80::1%6#53(fe80::1%6%6) (UDP)
;; WHEN: Mon Feb 06 21:07:11 +03 2023
;; MSG SIZE  rcvd: 129
```

The nameservers of the website are:

- ns1.a2hosting.com
- ns2.a2hosting.com
- ns3.a2hosting.com
- ns4.a2hosting.com

v. **Whois:**

A whois check was carried out in order to find more about the domain name:

```
bash-3.2# whois buymenow.org.uk
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.nic.uk

domain:       UK

organisation: Nominet UK
address:      Minerva House
address:      Edmund Halley Road
address:      Oxford Science Park
address:      Oxford OX4 4DQ
address:      United Kingdom of Great Britain and Northern Ireland (the)

contact:      administrative
name:         TLD Registry Services Management
organisation: Nominet UK
address:      Minerva House
address:      Edmund Halley Road
address:      Oxford Science Park
address:      Oxford OX4 4DQ
address:      United Kingdom of Great Britain and Northern Ireland (the)
phone:        +44 1865 332211
e-mail:       registrymanagement@nominet.uk

contact:      technical
name:         TLD Registry Services Technical
organisation: Nominet UK
address:      Minerva House
address:      Edmund Halley Road
address:      Oxford Science Park
address:      Oxford OX4 4DQ
address:      United Kingdom of Great Britain and Northern Ireland (the)
phone:        +44 1865 332211
e-mail:       registrytechnical@nominet.uk

nserver:      DNS1.NIC.UK 213.248.216.1 2a01:618:400:0:0:0:0:1
nserver:      DNS2.NIC.UK 103.49.80.1 2401:fd80:400:0:0:0:0:1
nserver:      DNS3.NIC.UK 213.248.220.1 2a01:618:404:0:0:0:0:1
nserver:      DNS4.NIC.UK 2401:fd80:404:0:0:0:0:1 43.230.48.1
nserver:      NSA.NIC.UK 156.154.100.3 2001:502:ad09:0:0:0:0:3
nserver:      NSB.NIC.UK 156.154.101.3 2001:502:2eda:0:0:0:0:3
nserver:      NSC.NIC.UK 156.154.102.3 2610:a1:1009:0:0:0:0:3
nserver:      NSD.NIC.UK 156.154.103.3 2610:a1:1010:0:0:0:0:3
ds-rdata:     43876 8 2 a107ed2ac1bd14d924173bc7e827a1153582072394f9272ba37e2353bc659603

whois:        whois.nic.uk

status:       ACTIVE
remarks:      Registration information: http://www.nic.uk/

created:      1985-07-24
changed:      2022-08-31
source:       IANA

# whois.nic.uk


    Domain name:
        buymenow.org.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data source on 25-Apr-2022

    Registrar:
        eNom LLC [Tag = ENOM]
        URL: http://www.enom.com

    Relevant dates:
        Registered on: 25-Apr-2022
        Expiry date:  25-Apr-2023
        Last updated:  25-Apr-2022

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.a2hosting.com
        ns2.a2hosting.com
```

It can be seen that the domain is registered in the UK, but the registrant information is hidden.

vi. **Whatweb:**

Based on the output, we can see that the website is hosted in the United States. We also learn that the website is based on Bootstrap and HTML5.